Quantum codes: from Shor to topological quantum codes

Clarice D. de Albuquerque, Leandro B. de Lima and Giuliano G. La Guardia [*]

August 11, 2022

1 The Shor code

In this subsection we will describe the construction of the Shor code. In order to proceed further, we must construct first the *three qubit bit flip code* and after, the *three qubit phase flip code.* For more details about the encoding-decoding process we refer the reader to [15].

1.1 Three qubit bit flip code

The *bit flip channel* is defined below. Roughly speaking, this channel represents the action of the Pauli operator X

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let us define formally such a quantum noise.

Definition **1.1** *Let $|v\rangle = a|0\rangle + b|1\rangle$ be a qubit state (qubit for short). The bit flip channel acts on $|v\rangle$ as follows:*

- $|v\rangle \xrightarrow{\text{channel}} X|v\rangle = a|1\rangle + b|0\rangle$ *with probability p;*

[*] Clarice D. de Albuquerque is with Science and Technology Center, Federal University of Cariri (UFCA), Juazeiro do Norte, Cear, Brazil. Leandro B. de Lima is with Institute of Mathematics, Federal University of Mato Grosso do Sul (UFMS), Campus Aquidauana, MS, Brazil PR, Brazil. Giuliano G. La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), Ponta Grossa, PR, Brazil.

- $|v\rangle \xrightarrow{\text{channel}} |v\rangle$ *with probability* $1-p$.

In order to protect qubits against the effects of the bit flip channel, one utilizes the three qubit bit flip code. We begin by recalling that we write $|v_1v_2v_3\rangle$ to denote $|v_1\rangle \otimes |v_2\rangle \otimes |v_3\rangle$, as previously specified.

Let us consider a single qubit given by $|v\rangle = a|0\rangle + b|1\rangle$. Assume that $|v\rangle$ was encoded as $|v\rangle_{enc} = a|000\rangle + b|111\rangle$, where as it is usual, we define $|000\rangle$ as being the *logical zero* $|0_L\rangle$ and $|111\rangle$ as the *logical one* $|1_L\rangle$, i.e., $|0_L\rangle := |000\rangle$ and $|1_L\rangle := |111\rangle$. To this end, we have encoded $|0\rangle \xrightarrow{encode} |000\rangle$ and $|1\rangle \xrightarrow{encode} |111\rangle$.

The channel is assumed to be independent, that is, each qubit passes through an independent copy of it. Assume that one error (or none) has occurred to the encoded state $|v\rangle_{enc}$. For this channel one has four error syndromes corresponding to the four projection operators

First Procedure of measurement

To detect the error (if there exists), we perform a measurement in order to know which qubit was corrupted. The result of the measurement is said to be *error syndrome.* There exist four error syndromes corresponding to the following four projection operators:

- $P_0 := |000\rangle\langle 000| + |111\rangle\langle 111|$ (associated with no occurrence of error);
- $P_1 := |100\rangle\langle 100| + |011\rangle\langle 011|$ (error in the first qubit);
- $P_2 := |010\rangle\langle 010| + |101\rangle\langle 101|$ (error in the second qubit);
- $P_3 := |001\rangle\langle 001| + |110\rangle\langle 110|$ (error in the third qubit);

Let us see how the detection process works. Assume without loss of generality (w.l.o.g.) that an error corrupted the second qubit; then the state

$$|v\rangle_{enc} = a|000\rangle + b|111\rangle$$

becomes

$$|w\rangle = a|010\rangle + b|101\rangle.$$

Applying P_2 to $|w\rangle$ we have

$$\begin{aligned} p(2) = \langle w|P_2|w\rangle \\ &= (a^*\langle 010| + b^*\langle 101|)|010\rangle\langle 010|(a|010\rangle + b|101\rangle) \\ &+ (a^*\langle 010| + b^*\langle 101|)|101\rangle\langle 101|(a|010\rangle + b|101\rangle) \\ &= |a|^2 + |b|^2 = 1. \end{aligned}$$

Therefore, we know that the error occurred in the second qubit.

Remark **1.1** *In this detection process, it is interesting to observe that the corrupted state $a|010\rangle + b|101\rangle$ is not affected by the syndrome measurement. In fact, the syndrome contains only information about the corrupted qubit, but no information about the state being measured (a and b are not known). This is excellent, since none of the measurements applied for the decoding operation destroys the superpositions of quantum states that must be preserved by applying the encoding process.*

To recover the original encoded state $|v\rangle_{enc}$, note that since the error has occurred in the second qubit and since the channel flips the qubit, then it suffices to flip to second qubit again. Thus, the encoded state $|v\rangle_{enc}$ is recovered. It is clear that this procedure holds in general, independently in which qubit the error has occurred. If no error occurs in this process, by applying the operator P_0 we have $p(0) = \langle w|P_0|w\rangle = 1$, that is, we know that (probability one) that no error has occurred. Proceeding similarly, we can recover the original encoded state in all cases.

Second Procedure of measurement

We next present an alternative way to proceed the measurement process. Assume that we replace the four measurements operators P_0, P_1, P_2, P_3 by the observables $Z_1Z_2 := Z \otimes Z \otimes I$ and $Z_2Z_3 := I \otimes Z \otimes Z$, both with eigenvalues -1 and $+1$. To perform the measurement, we first apply Z_1Z_2 and, in the sequence, the observable Z_2Z_3.

The first operator has the following spectral decomposition

$$Z_1Z_2 = [(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I] - [(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I]$$

There are two possibilities for the result of the measurement of Z_1Z_2 : the eigenvalue is $+1$ or -1. Let us analyze all the situations.

Recall that the original encoded vector is $|v\rangle_{enc} = a|000\rangle + b|111\rangle$. If the channel corrupted the first qubit, then the corresponding qubit state is $|w\rangle = a|100\rangle + b|011\rangle$, so the result of the measurement of Z_1Z_2 is -1 because

$$\begin{aligned} &p(-1) \\ &\quad = \langle w|Z_1Z_2|w\rangle \\ &\quad = (a^*\langle 100| + b^*\langle 011|) - [(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I](a|100\rangle + b|011\rangle) \\ &\quad = (-[b^*\langle 1| + a^*\langle 0|], -[a|0\rangle + b|1\rangle]) \\ &\quad = |a|^2 + |b|^2 = 1. \end{aligned}$$

Analogously, if the channel corrupted the second qubit, the result of the measurement of Z_1Z_2 is also -1. Thus, if the eigenvalue equals -1, the first and the second qubit are distinct. If the eigenvalue is $+1$ then such qubits are equal. Analogously, when performing the measurement of the observable Z_2Z_3, if the eigenvalue is $+1$, then the second and the third qubit are equal; if it is -1, they are distinct.

We are now deduce in which (if any) qubit the error has occurred. Assume that the result of the measurements of Z_1Z_2 and Z_2Z_3 are both $+1$. Then all the three qubits are equal and no error has occurred. If the eigenvalues are $+1$ and -1, respectively, then the error corrupted with high probability the third qubit; if the eigenvalues are -1 and $+1$, respectively, the error occurred with high probability in the first qubit. Finally, if the results are -1 and -1 then (with high probability) the second qubit was corrupted. Note that none of the measurements give information about the states being measured like the first procedure. To recover the quantum state it suffices to proceed as in the first case, i.e., the corrupted qubit can be flipped again.

It is interesting to note that, in the latter procedure, we only need to use two observables to detect the error, whereas in the first case we need to have four operators of measurement. This is an advantage offered the the second procedure.

1.2 Three qubit phase flip code

The *phase flip channel* represents the action of the Pauli operator Z

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

This quantum noise shown is defined in the sequence.

Definition **1.2** *Let $|v\rangle = a|0\rangle + b|1\rangle$ be a qubit. The phase flip channel acts on $|v\rangle$ as follows:*

- $|v\rangle \xrightarrow{\text{channel}} Z|v\rangle = a|0\rangle - b|1\rangle$ *with probability p;*

- $|v\rangle \xrightarrow{\text{channel}} |v\rangle$ *with probability* $1 - p$.

The procedure to recover the encoded state is to turn the phase flip channel into a bit flip channel. In order to do this, let us consider the qubit basis $|+\rangle = (|0\rangle + |1\rangle)/2$ and $|-\rangle = (|0\rangle - |1\rangle)/2$. Since $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$, Z acts as a bit flip in such vectors. We then perform the encoding:

$$|0\rangle \xrightarrow{encode} |0_L\rangle := |+++\rangle$$

and

$$|1\rangle \xrightarrow{encode} |1_L\rangle := |-{-}{-}\rangle$$

to perform the encoding state. In this manner we can protect at least one qubit against phase flip errors. From this moment, the encoding, detection and the recovery process is the same as the bit flip channel with respect to the basis $|+\rangle$ and $|-\rangle$.

1.3 The Shor code

Here we present the Shor code, the first quantum error-correcting code to protect an arbitrary single qubit against an arbitrary quantum error. The code is constructed by means of concatenation of qubits as we can see in the following.

The construction of this code is based on the three qubit bit flip and the three qubit phase flip codes presented in Subsections 1.1 and 1.2, respectively.

The stages of construction of the Shor code is given in the sequence.

(1) The first stage is to utilize the three qubit phase flip code to encode the qubit, that is, $|0\rangle \xrightarrow{encode} |+{+}{+}\rangle$ and $|1\rangle \xrightarrow{encode} |-{-}{-}\rangle$.

(2) Each of these qubits (namely, $|+\rangle$ and $|-\rangle$) are encoded by applying the three qubit phase flip code, i.e., $|+\rangle \xrightarrow{encode} (|000\rangle + |111\rangle)/\sqrt{2}$ and $|-\rangle \xrightarrow{encode} (|000\rangle - |111\rangle)/\sqrt{2}$.

Thus, the resulting code is the Shor code given by

$$|0\rangle \xrightarrow{encode} |0_L\rangle := \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

and

$$|1\rangle \xrightarrow{encode} |1_L\rangle := \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

We will explain now how the Shor code can correct phase flip and bit flip errors on any single qubit. In fact, the analyze we will perform here is in the same spirit with as the Second Procedure of measurement shown in Subsection 1.

We present a scheme in order to clarify the understanding of how the code can recover the initial state.

First Case - Correcting bit flip errors Assume w.l.o.g. that an error has occurred in the seventh qubit. We then perform the measurement of the observable Z_7Z_8, finding the eigenvalue -1. After this, we follow by measuring Z_8Z_9 obtaining therefore the eigenvalue $+1$; so the seventh qubit is the corrupted one. Applying bit flip again in the seventh qubit one has the initial state. Proceeding similarly, we can detect and recover any (single) state which was corrupted by bit flip errors, by means of the measurement of the observables Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8 and Z_8Z_9.

Second Case - Correcting phase flip errors Assume that an error occurs in the second qubit for example. Due to the properties of tensor product, the first block of three qubits $|000\rangle + |111\rangle$ becomes $|000\rangle - |111\rangle$ and $|000\rangle - |111\rangle$ becomes $|000\rangle + |111\rangle$. In other words, the two basis states now read as

$$|0_L\rangle \xrightarrow{channel} \frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

and

$$|1_L\rangle \xrightarrow{channel} \frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

After this, we compare the sign of the first and the second blocks of qubits, i.e., $|000\rangle|111\rangle$ is compared with $|000\rangle + |111\rangle$ (has distinct sign) and $|000\rangle + |111\rangle$ is compared with $|000\rangle - |111\rangle$ (has distinct sign). Here, we consider that the block has the same sign in the cases $(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$ and $(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$ and they have different signs in the cases $(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)$ and $(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$. Next, we perform a comparison between the sign of the second and the third blocks of qubits, i.e. $(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$ (has the same sign) and $(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$ (has the same sign). Thus, we know that the phase flip has corrupted one of the three first qubits. To recover the initial encoded state it suffices to flip the sign of the first block of three qubits.

Such procedure to detect phase flip errors presented above is similar to perform the measurement of the observables $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6$ $X_7X_8X_9$.

Third Case - Phase flip and bit flip on the same qubit This case is a direct application of the previous ones. More precisely, it suffices to apply the procedure shown in the **First Case** to recover the qubit affected by the bit flip action of the channel after applying the **Second Case** to correct the phase flip error occurred. These facts are true because both error-correction process are independent.

Therefore, the stabilizer for the Shors nine qubit code is

- $Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$
- $I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$
- $I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I$
- $I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I$
- $I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I$
- $I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z$
- $X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I$
- $I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X$

The Shor code has parameters $[[9, 1, 3]]$, that is, the code utilizes nine qubits to encode a qubit, and it is capable of correcting one arbitrary quantum error.

Until now we have seen only errors of the types phase and bit flip. But the question is: Is the Shor code capable of correcting an arbitrary error? The answer for this question is yes!

To see this, note that the Pauli matrices I, X, Y, Z span $M_2(\mathbb{C})$, the vector space of the matrices of order 2 with complex entries. Since $XZ = -iY$ then the matrices I, X, Z, XZ also span $M_2(\mathbb{C})$. Thus, given an error matrix E in one qubit we can write $E = a_1 I + a_2 X + a_3 Z + a_4 XZ$, where $a_i \in \mathbb{C}$ for all $i = 1, 2, 3, 4$. Therefore, if $|v\rangle$ is a qubit, we have the quantum state $E|v\rangle = a_1|v\rangle + a_2 X|v\rangle + a_3 Z|v\rangle + a_4 XZ|v\rangle$.

By the measurement of the error syndrome the state $E|v\rangle$ collapses to one of the states $|v\rangle, X|v\rangle, Z|v\rangle$ or $XZ|v\rangle$. Since these operators are invertible, we then apply the inverse operator to recover the initial quantum state. In other words, if the code is capable of correcting errors of the type bit flip, phase flip and bit-phase flip combined, in a given qubit then the code is capable of correcting all arbitrary errors in such a qubit. This is an interesting feature of quantum codes: if the code C corrects a suitable discrete subset of errors then C corrects all type of (*continuum*) errors. This fact is essential in quantum error-correction; based on this property, it is possible to construct efficient quantum codes against arbitrary quantum errors.

Theorem **1.1** *(Quantum error-correction conditions) Let C be a quantum code, and let P be the projector onto C. Suppose $\mathcal{E}$ is a quantum operation with operation elements $\{E_i\}$. A necessary and sufficient condition for the existence of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C is that*

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix α of complex numbers. We call the operation elements $\{E_i\}$ for the noise $\mathcal{E}$ errors, and if such an $\mathcal{R}$ exists we say that $\{E_i\}$ constitutes a correctable set of errors for the code.

This previous discussion can be summarized in the next result.

Theorem **1.2** *(Error Discretization) Suppose C is a quantum code and $\mathcal{R}$ is the error-correction operation constructed from Theorem 1.1 to recover from a noise process $\mathcal{E}$ with operation elements $\{E_i\}$. Suppose $\mathcal{F}$ is a quantum operation with operation elements $\{F_j\}$ which are linear combinations of the E_i, that is, $F_j = \sum_i m_{ji} E_i$ for some matrix m_{ji} of complex numbers. Then the error-correction operation $\mathcal{R}$ also corrects for the effects of the noise process $\mathcal{F}$ on the code C.*

In other words, it is possible to discretize quantum errors, that to fight the continuum of errors possible on a single qubit it is sufficient merely to win the war against a finite set of errors, the four Pauli matrices.

2 Binary Stabilizer Formalism

There exist some matrices that play a fundamental role in quantum mechanics, namely, the Pauli matrices

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Let us consider the Pauli matrices $\{I, X, Y, Z\}$. Then the set $G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ endowed with the operation of matrix multiplication is a group.

Definition **2.1** *The Pauli group on* 1 *qubit is defined by the group* $(G_1, \cdot_m)$, *where* $\cdot_m$ *is the product of matrices.*

More generally, we can define the general Pauli group on n qubits.

Definition **2.2** *The general Pauli group on* n *qubits, denoted by* G_n, *is the group* $(G_n, \cdot_m)$, *such that the elements of* G_n *are* n*-tensor products of Pauli matrices with coefficients* ± 1 *or* $\pm i$.

Suppose S is a subgroup of G_n and define V_S to be the set of n-qubit states which are fixed by every element of S. Then V_S is the vector space stabilized by S, and S is said to be the stabilizer of the space V_S, since every element of V_S is stable under the action of elements in S.

Theorem **2.1** V_S *is non-trivial if and only if*

(a) the elements of S *commute;*

(b) $-I$ *is not an element of* S.

Definition **2.3** *We say that the generators* $g_1, \ldots, g_l$ *of a group are independent in the sense that removing any generator* g_i *makes the group generated smaller, i.e.,* $\langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_l \rangle \subsetneqq \langle g_1, \ldots, g_l \rangle$.

Proposition **2.1** *Let* $S = \langle g_1, \ldots, g_{n-k} \rangle$ *be generated by* $n - k$ *independent and commuting elements from* G_n, *and such that* $-I$ *does not belong to* S. *Then* V_S *is a* 2^k*-dimensional vector space.*

2.1 Steane's code

The Steane's $[[7, 1, 3]]$ seven qubit code is an example of the application of the Calderb-ank-Shor-Steane (CSS) quantum code construction that will be presented in the next section.

The basis states for this code are given in the sequence:

$$\begin{aligned}|0_L\rangle := \frac{1}{\sqrt{8}}[&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle]\end{aligned}$$

and

$$\begin{aligned}|1_L\rangle := \frac{1}{\sqrt{8}}[&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle]\end{aligned}$$

The stabilizer for the seven qubit code due to Steane is

- $I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X$
- $I \otimes X \otimes X \otimes I \otimes I \otimes X \otimes X$
- $X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X$
- $I \otimes I \otimes I \otimes Z \otimes Z \otimes Z \otimes Z$
- $I \otimes Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z$
- $Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z$

The code has parameters $[[7, 1, 3]]$, that is, it can correct an arbitrary error in a single qubit and utilizes seven quibits in the encoding process. The classical self-orthogonal code utilized in the encoding process is the $[7, 4, 3]$ Hamming code with parity check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

3 Binary CSS construction

The Calderbank-Shor-Steane (CSS) code construction is one of the most interesting code constructions shown in the literature [15]. In fact, it is the first construction method exhibited in the literature in the sense that one can derive families of quantum codes by applying the CSS construction, and not only few codes with specific parameters. Such a method utilizes two classical linear nested codes (or one Euclidean self-orthogonal linear code) to address to problem of correcting phase and qubit flip errors. The CSS codes form a subclass of the class of the stabilizer codes [15]. We next presented a detailed construction of these codes.

The process starts with two binary linear codes C_1 and C_2 with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $C_2 \subset C_1$ and both C_1 and $C_2^{\perp}$ correct t errors. Based on these classical codes we define a quantum code CSS(C_1, C_2) (this notation is not usual in the literature but we prefer adopt it here to maintain the notation of the textbook [15]) as follows.

Assume that $c, c^{'} \in C_1$ are two codewords of C_1. Define the following relation on C_1: $c \approx c^{'} \Longleftrightarrow c - c^{'} \in C_2$. It is easy to see that $\approx$ is an equivalence relation on C_1. Moreover, it is not difficult to see that the equivalence class $\overline{c}$ determined by a codeword $c \in C_1$ is equal to $\overline{c} = c + C_2 := \{c + x | x \in C_2\}$. Thus, the cosets $c + C_2$ form a partition of C_1. Since we are working with quantum states (qubits or tensor product of qubits) then we must adapt the notation. We then define the quantum state $|c+C_2\rangle$ (already normalized) as

$$|c+C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} |c+x\rangle,$$

where $+$ denotes the componentwise addition modulo 2.

Suppose c and $c^{'}$ belong the disjoint cosets of C_2; this implies that there is no $x, x^{'} \in C_2$ such that $c+x = c^{'} + x^{'}$ otherwise

$$c - c^{'} = x^{'} - x \in C_2 \Longrightarrow c + C_2 = c^{'} + C_2,$$

which is a contradiction. Hence, for distinct $c \neq c^{'}$, the corresponding quantum states $|c+C_2\rangle$ and $|c^{'}+C_2\rangle$ are orthonormal. Thus, we define the quantum code CSS(C_1, C_2) to be the vector space spanned by the states $|c+C_2\rangle$ for all $c \in C_1$. Since the number of cosets is $\frac{|C_1|}{|C_2|}$, the dimension of CSS(C_1, C_2) equals $\frac{|C_1|}{|C_2|} = 2^{k_1-k_2}$. Therefore, the quantum code CSS(C_1, C_2) has parameters $[n, k_1 - k_2]$, capable to correct errors on t qubits.

Let us see how the code works to the error correction. Assume that the initial state of a quantum system is $|c+C_2\rangle$. After passing through the channel, the original state can suffer some kind of error (bit flip and/or phase flip). In the error model it is assumed that bit flip errors e_b are binary vectors of length n (the code length) such that the component is 1 where the bit flip occurs and 0 otherwise. The error of the type phase flip are also binary vectors e_p of length n with 1 in the coordinate that a phase flip occurs and 0 otherwise. Note that both binary vectors cannot have more than t ones. Adopting this model we know that the corrupted state is

$$|c+C_2\rangle \xrightarrow{channel} \frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(c+x)\cdot e_p} |c+x+e_b\rangle,$$

Bit flip Detection. We introduce a sufficient large ancilla system capable of storing the syndrome for C_1 which is initially in the all zero state $|0\rangle$. Applying the parity check matrix H_1 of C_1 to all state $|c+x+e_b\rangle$, since $H_1(c+x) = 0$ we have

$$|c+x+e_b\rangle|0\rangle \longrightarrow |c+x+e_b\rangle|H_1(c+x+e_b)\rangle = |c+x+e_b\rangle|H_1 e_b\rangle,$$

that is, the error was isolated. Thus, we obtain the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(c+x)\cdot e_p} |c+x+e_b\rangle|H_1 e_b\rangle.$$

Performing the measurement of the ancilla, we obtain $H_1 e_b$; discarding the ancilla we return to the quantum state

$$\frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(c+x)\cdot e_p} |c + x + e_b\rangle.$$

Since the classical syndrome $H_1 e_1$ is known, then C_1 tells us the vector error e_b. To recover the state, we apply the NOT gate in all the qubits corrupted by the error, which leads to the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(c+x)\cdot e_p} |c + x\rangle.$$

Our next task is to detect the qubits corrupted by the phase flip error.

Phase flip Detection. Starting from the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(c+x)\cdot e_p} |c + x\rangle,$$

the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

is applied to each qubit producing the state

$$\frac{1}{\sqrt{|C_2| 2^n}} \sum_{v \in \mathbb{F}_2^n} \sum_{x \in C_2} (-1)^{(c+x)\cdot(e_p+v)} |v\rangle,$$

which can be written as

$$\frac{1}{\sqrt{|C_2| 2^n}} \sum_{w \in \mathbb{F}_2^n} \sum_{x \in C_2} (-1)^{(c+x)\cdot w} |w + e_p\rangle,$$

where $w = v + e_p$ (notice that $e_p + e_p$ is the zero vector). Let us now compute the sum $\sum\limits_{x \in C_2} (-1)^{xw}$. If $w \in C_2^{\perp}$ then $w \cdot x = 0$ for all $x \in C_2$; so

$$\sum_{x \in C_2} (-1)^{xw} = \underbrace{1 + 1 + \ldots + 1}_{|C_2| \text{ times}} = |C_2|.$$

On the other hand, if $w \notin C_2^{\perp}$ then it is easy to see that

$$\sum_{x \in C_2} (-1)^{xw} = 0.$$

Hence, the state can be written as

$$\frac{1}{\sqrt{2^n/|C_2|}}\sum_{w\in C_2^{\perp}}(-1)^{c\cdot w}|w+e_p\rangle,$$

which is similar to a bit flip type of error. To correct it, we proceed analogously to the correction of e_b, i.e., we introduce an ancilla and apply the parity check matrix G_2 for $C_2^{\perp}$ (which is a generator matrix for the code C_2) as done previously, to obtain G_2e_p and to correct the error e_p the quantum state

$$\frac{1}{\sqrt{2^n/|C_2|}}\sum_{w\in C_2^{\perp}}(-1)^{c\cdot w}|w\rangle,$$

Applying the Hadamard gate to each qubit results in the original state

$$|c+C_2\rangle := \frac{1}{\sqrt{|C_2|}}\sum_{x\in C_2}|c+x\rangle.$$

Therefore, the resulting quantum code $\mathrm{CSS}(C_1, C_2)$ has parameters $[[n, k_1 - k_2]]$ and can correct arbitrary errors up to t qubits.

In the following we present the CSS construction to qubits.

Lemma **3.1** *[4, 9] Let C_1 and C_2 denote two classical binary linear codes with parameters $[n, k_1, d_1]_2$ and $[n, k_2, d_2]_2$, respectively, such that $C_2 \subset C_1$. Then there exists an $[[n, K = k_1 - k_2, D]]_2$ CSS quantum code where $D = \min\{wt(c) : c \in (C_1 \backslash C_2) \cup (C_2^{\perp} \backslash C_1^{\perp})\}$.*

3.1 Nonbinary Stabilizer codes

It is interesting to note that until now we have dealt with quantum bits or tensor product of quantum bits. Hence we can only construct quantum codes for qubits. Because of this limitation, the authors have such a theory to construct quantum codes for non-binary alphabets, i.e., quantum digits (qudits). A giant step towards this generalization was the work by Calderbank et al. [4] and after by Ketkat et al. [9]. In the latter paper, the authors generalized in several ways the formalism of stabilizers for binary and non-binary alphabets by applying Galois theory.

Notation. We denote p a prime number, q a prime power, $\mathbb{F}_q$ is the finite field with q elements, $\mathbb{C}^q$ is the complex vector space of dimension q (quantum mechanical system scenario), $|x_i\rangle$ are the vectors of an orthonormal basis of

$\mathbb{C}^q$, where x_i range over all elements of $\mathbb{F}_q$, and $\mathbb{C}^{q^n}$ denotes the n-tensor product $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$.

Let us recall the concept of trace map.

Definition **3.1** *The trace map* $\mathrm{tr}_{q^m/q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ *is defined as*

$$\mathrm{tr}_{q^m/q}(a) := \sum_{i=0}^{m-1} a^{q^i}.$$

Definition **3.2** *A quantum error-correcting code is a K-dimensional subspace of* $\mathbb{C}^{q^n} = \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n \text{ times}}$.

We next present the error model utilized in quantum mechanics. The error model is a natural generalization of Pauli matrices to non-binary alphabets, as we will see in the sequence.

Let $q = p^m$ be a prime power and assume that a and b are elements of $\mathbb{F}_q$. We then define two unitary operators:

$$X(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q$$

$$|x_i\rangle \longrightarrow X(a)|x_i\rangle = |x_i + a\rangle$$

and

$$Z(b) : \mathbb{C}^q \longrightarrow \mathbb{C}^q$$

$$|x_i\rangle \longrightarrow Z(b)|x_i\rangle = \omega^{\mathrm{tr}(bx_i)}|x_i\rangle,$$

where $\mathrm{tr} : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_p$ is the trace map and $\omega = \exp(2\pi i/p)$ is a primitive pth root of unity.

Remark **3.1** *Note that the definitions of operators $X(a)$ and $Z(b)$ are natural generalizations of the Pauli matrices X and Z, respectively, to q-ary alphabets. In fact, $X(a)$ acts by changing the vectors of the orthonormal basis, and $Z(b)$ changes the phase of the vectors of the basis.*

We can now define the set of error operators.

Definition **3.3** *Let $X(a)$ and $Z(b)$ defined as above. The set*

$$\varepsilon = \{X(a)Z(b)|a, b \in \mathbb{F}_q\}$$

is called the set of error operators.

In the sequence we define the concept of nice error basis.

Definition **3.4** *Let β be a set of q^2 unitary matrices. We say that β is a* nice error basis *if β satisfies the following conditions:*

(1) *$I_q \in \beta$, where I_q is the identity matrix of order q;*

(2) *if $A, B \in \beta$ then AB is a scalar multiple of another element of β;*

(3) *if $A, B \in \beta$, with $A \neq B$, then $\mathrm{Tr}(A^\dagger B) = 0$, where* Tr *denotes the trace of the matrix.*

The set ε given in Definition 3.3 is a nice error basis.

Proposition **3.1** *The set $\varepsilon = \{X(a)Z(b)|a, b \in \mathbb{F}_q\}$ satisfies the three conditions of Definition 3.4, i.e., ε is a nice error basis on $\mathbb{C}^q$.*

Example **3.1** *[9] Let us consider the finite field with four elements $\mathbb{F}_4 = \{0, 1, \alpha, \overline{\alpha}\}$. According to the notation adopted above, a basis for $\mathbb{C}^4$ can be written as $|0\rangle$, $|1\rangle$, $|\alpha\rangle$ and $|\overline{\alpha}\rangle$. Let*

$$\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

By a simple computation we have
$X(0) = \mathbb{I}_2 \otimes \mathbb{I}_2, X(1) = \mathbb{I}_2 \otimes \sigma_X, X(\alpha) = \mathbb{I}_2 \otimes \mathbb{I}_2, X(\overline{\alpha}) = \sigma_X \otimes \sigma_X,$
$Z(0) = \mathbb{I}_2 \otimes \mathbb{I}_2, Z(1) = \sigma_Z \otimes \mathbb{I}_2, Z(\alpha) = \sigma_Z \otimes \sigma_Z, X(\overline{\alpha}) = \mathbb{I}_2 \otimes \sigma_Z.$

We must know how the errors act on multiple qudits. In other words, it is necessary to know if the tensor products of a finite number of nice error basis is also a nice error basis. Fortunately this is true.

Proposition **3.2** *Let β_1 and β_2 be two sets of nice error bases on $\mathbb{C}^q$. Then the set*

$$\beta = \{E_1 \otimes E_2 | E_1 \in \beta_1, \quad E_2 \in \beta_2\}$$

is also a nice error basis.

By applying induction, we know that Proposition 3.2 also holds for a finite number of tensor products. Assuming that $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ is a vector in $\mathbb{F}_q^n$, then we denote $\mathcal{X}(\mathbf{a}) = X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $\mathcal{Z}(\mathbf{a}) = Z(a_1) \otimes Z(a_2) \otimes \cdots \otimes Z(a_n)$ for tensor products of n error operators.

Corollary **3.1** *Assume the notation above. Then the set*

$$\varepsilon_n = \{\mathcal{X}(\boldsymbol{a})\mathcal{Z}(\boldsymbol{b}) | \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n\}$$

is a nice error basis on the complex vector space $\mathbb{C}^{q^n}$.

Hence, we have a complete characterization (the model) of the errors that can corrupt the quantum digits.

In the sequence we will define a stabilizer code. We start with the group G_n generated by the matrices of ε_n:

$$G_n = \{\omega \mathcal{X}(\mathbf{a})\mathcal{Z}(\mathbf{b}) | \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\},$$

which is called *error group* associated with ε_n. A stabilizer code is the joint eigenspace with eigenvalue 1 of some subgroup of G_n, as we see in the following.

Definition **3.5** *Let S be a subgroup of the error group G_n. A stabilizer code $\mathcal{Q} \neq \{0\}$ is a subspace of $\mathbb{C}^{q^n}$ satisfying the equality*

$$\mathcal{Q} = \bigcap_{E \in S} \{|v\rangle \in \mathbb{C}^{q^n} : E|v\rangle = |v\rangle\}.$$

We need to define the weight of an element in the error group G_n. To this end, let $\mathbf{a}, \mathbf{b}$ be two vectors in $\mathbb{F}_q^n$ and consider the vector $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$.

Definition **3.6** *The symplectic weight* $\mathrm{swt}((\boldsymbol{a}|\boldsymbol{b}))$ *of* $(\boldsymbol{a}|\boldsymbol{b})$ *is the number of nonzero ordered pairs of the form* (a_i, b_i)*, where* $i = 1, 2, \ldots, n$*, i.e.,*

$$\mathrm{swt}((\boldsymbol{a}|\boldsymbol{b})) = |\{i \ |(a_i, b_i) \neq (0, 0)\}|.$$

Definition **3.7** *Let* $E = \omega^c \mathcal{X}(\boldsymbol{a})\mathcal{Z}(\boldsymbol{b})$ *be an element in the error group* G_n*. Then the weight* $\mathrm{wt}(E)$ *of* E *is defined as* $\mathrm{wt}(E) = \mathrm{swt}((\boldsymbol{a}|\boldsymbol{b}))$.

It is interesting to note that $(a_i, b_i) \neq (0, 0)$ if and only if $(X(a_i), Z(b_i)) \neq (I_q, I_q)$. Thus, from Definition 3.7, the weight $\mathrm{wt}(E)$ of E can be interpreted as the number of nonidentity tensor components, as expected.

Definition **3.8** *A quantum error-correcting code (QC) Q is a K-dimensional subspace of $\mathbb{C}^{q^n}$. If Q has minimum distance d, then we say that Q is an $((n, K, d))_q$ code. If $K = q^k$ we write $[[n, k, d]]_q$. The length n, the dimension K and minimum distance d are the parameters of Q. The code Q is said to be* pure *to l if and only if its stabilizer group does not contain non-scalar matrices of weight less than l; Q is pure if and only if it is pure to its minimum distance.*

Definition **3.9** *We say that a quantum code Q has minimum weight d if it can detect all errors in G_n of weight less than d, but it cannot detect some error of weight d.*

A QC with minimum distance d corrects all errors of weight $\lfloor (d-1)/2 \rfloor$ or less.

The center $Z(G_n)$ of the group G_n is the subgroup given by

$$Z(G_n) = \{E \in G_n | EF = FE, \ \forall \ F \in G_n\}.$$

In words, $Z(G_n)$ consists of the elements in G_n that commute with all elements of G_n.

Let S be a subgroup of G_n. The centralizer $C_{G_n}(S)$ of S in G_n is defined as

$$C_{G_n}(S) = \{E \in G_n | EF = FE, \ \forall \ F \in S\}.$$

Analogously, the elements of $C_{G_n}(S)$ are the elements of G_n that commute with all elements of S. Further, let us consider $SZ(G_n)$ as the group generated by S and $Z(G_n)$. The following result gives necessary and sufficient conditions for error-detection.

Theorem **3.1** *Let S be a subgroup of G_n such that S is the stabilizer group of a stabilizer code Q of dimension greater than* 1*. A necessary and sufficient condition in order to Q detects an error $E \in G_n$ is either $E \in SZ(G_n)$ or $E \notin C_{G_n}(S)$.*

Lemma **3.2** *If Q is a nonzero subspace of $\mathbb{C}^{q^n}$, then its stabilizer S is an abelian subgroup satisfying $S \cap Z(G_n) = \{I\}$.*

In the following we present the Calderbank-Shor-Steane (CSS) construction to non-binary alphabets, which is a particular case of stabilizer codes.

Lemma **3.3** *[4, 9] Let q be a prime power. Let C_1 and C_2 denote two classical linear codes both over the field $\mathbb{F}_q$, with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, such that $C_2 \subset C_1$. Then there exists an $[[n, K = k_1 - k_2, D]]_q$ CSS quantum code where $D = \min\{wt(c) : c \in (C_1 \backslash C_2) \cup (C_2^{\perp} \backslash C_1^{\perp})\}$.*

Remark **3.2** *As it was said previously, the CSS codes shown in Lemma 3.3 are constructed over non-binary alphabets. In fact, the original version of the CSS code construction (as we have presented in this subsection) was presented in binary alphabets. For non-binary alphabets, a quantum state is called quantum digits or qudits (for short).*

There exist some well known bounds with respect to the parameters of a quantum code.

Lemma **3.4** *[9] Let C be an $[[n, k, d]]_q$ quantum code. Then the quantum Singleton bound asserts that the parameters of C satisfy $k + 2d \leq n + 2$. If C attains the quantum Singleton bound, i.e., $k + 2d = n + 2$, then it is called a quantum maximum distance separable (MDS) code.*

More generally we have the following result to stabilizer codes.

Lemma **3.5** *(Quantum Singleton bound)[9, Corollary 28] The parameters of an $((n, K, d))_q$ stabilizer code with $K > 1$ satisfy the inequality*

$$K \leq q^{n-2d+2}.$$

4 Linear block codes

In this section we recall basic concepts on linear codes. For more details we refer the reader to [8, 14]. *Notation*: p denotes a prime number, q is a prime power and $\mathbb{F}_q$ is the finite field with q elements. In this subsection the vectors are written in bold.

Definition **4.1** *Assume that $\mathbb{F}_q^n$ is the vector space (over $\mathbb{F}_q$) of all n-tuples in $\mathbb{F}_q$. Then an (n, M) code C over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M. If $\boldsymbol{c} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ is such that $\boldsymbol{c} \in C$, then the vector $\boldsymbol{c}$ is called codeword of C.*

To work with codes without structures is really hard. Hence, we work with linear codes.

Definition **4.2** *A linear code C over $\mathbb{F}_q$ of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$. Linear codes of length n and dimension k are denoted by $[n, k]$; we say that $[n, k]$ are the parameters of the code.*

There exist two usual ways of defining a linear code: by means of generator matrices or based on parity check matrices.

Definition **4.3** *Let C be a linear code over $\mathbb{F}_q$ with parameters $[n, k]$. A generator matrix G for C is a $k \times n$ matrix with entries in $\mathbb{F}_q$ such that the rows of G form a basis for C.*

In general, a generator matrix of a linear code is not unique. However, in the case below one has the uniqueness.

Definition **4.4** *Let C be a linear code over $\mathbb{F}_q$ with parameters $[n, k]$. If the first k coordinates form an information set, then C has a unique generator matrix of the form $[I_k|A]$ with entries in $\mathbb{F}_q$, where I_k is the identity matrix of order k. This matrix is said to be in standard form.*

Another way of defining a linear code is by means of parity check matrices.

Definition **4.5** *Let C be a linear code over $\mathbb{F}_q$ with parameters $[n, k]$. A parity check matrix for C is an $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$ defined by*

$$C = \{\boldsymbol{c} \in \mathbb{F}_q^n | H\boldsymbol{c}^T = \boldsymbol{0}\},$$

where $\boldsymbol{c}^T$ denotes the transpose of vector $\boldsymbol{c}$.

The rows of H are also linearly independent (they form a basis for the (Euclidean) dual $C^\perp$ of C). Evidently, in general, a parity check matrix of a given code is not unique.

Theorem **4.1** *Let C be a linear code over $\mathbb{F}_q$ with parameters $[n, k]$. If $G = [I_k|A]$ is a generator matrix for C then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Example **4.1** *An example of a linear code is the well-known binary Hamming code with parameters $[7, 4]$ with generator matrix (in standard form)*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

and parity check matrix (in standard form)

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

As we will see later, the Hamming code has minimum distance three (see Proposition 4.2).

Another important parameter of a linear code is the minimum distance. To define this concept we need first to define Hamming distance.

Definition **4.6** *The Hamming distance* $\mathrm{d}(\boldsymbol{v}, \boldsymbol{w})$ *between two vectors* $\boldsymbol{v}, \boldsymbol{w}$ *in* $\mathbb{F}_q^n$ *is the number of coordinates in which* $\boldsymbol{v}$ *and* $\boldsymbol{w}$ *differ.*

We are now ready to define the minimum distance of a code, which is totally correlated with the power of error-correction of the code.

Definition **4.7** *The minimum distance of a code* C *(not necessarily linear) is the smallest Hamming distance between distinct codewords of* C*.*

Definition **4.8** *Let* $\boldsymbol{v} \in \mathbb{F}_q^n$*. The Hamming weight* $\mathrm{wt}(\boldsymbol{v})$ *of* $\boldsymbol{v}$ *is defined as the number of nonzero coordinates in* $\boldsymbol{v}$*.*

It is easy to see that for all vectors $\mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$ it follows that

$$\mathrm{d}(\mathbf{v}, \mathbf{w}) = \mathrm{wt}(\mathbf{v} - \mathbf{w}).$$

Since in the case of linear codes for every $\mathbf{v}, \mathbf{w} \in C$ implies that $\mathbf{v} - \mathbf{w} \in C$ we have the following result.

Proposition **4.1** *Let* C *be a linear code over* $\mathbb{F}_q$*. Then the minimum distance of* C *is equal to the minimum weight of all nonzero codewords of* C*.*

Hence, if the code is linear, then its minimum distance is also called the minimum weight of the code.

We have now the complete set of parameters of a linear code, i.e., length, dimension and minimum distance: a linear code C of length n, dimension k and minimum distance d over $\mathbb{F}_q$, is denoted by $[n, k, d]_q$.

There exists a well-known way to find the minimum distance of a linear code.

Proposition **4.2** *Let C be a linear code over $\mathbb{F}_q$ with parity check matrix H. Then C has minimum weight d if and only if H has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.*

The minimum distance of a code is totally correlated with the error-correcting capacity of the code.

Theorem **4.2** *A code C having minimum distance d can correct $\left\lfloor \frac{(d-1)}{2} \right\rfloor$ errors. If d is even, the code can simultaneously correct $\frac{(d-2)}{2}$ errors and detect $d/2$ errors.*

By applying Proposition 4.2 in the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

of the binary $[7,4]$ Hamming code of Example 4.1, we see that the code has minimum distance 3, i.e., the Hamming code is a single-error-correcting code due to Theorem 4.2.

4.1 Dual codes

Let C be an $[n,k,d]_q$ linear code over $\mathbb{F}_q$ with parity check matrix H. Since the rows of H are linearly independent, H is a generator matrix of some code, called *Euclidean dual code* of C, denoted by $C^{\perp}$. The dual code $C^{\perp}$ has length n and dimension $n-k$.

The dual code can be also defined by an alternative way by means of the usual (Euclidean) inner product on $\mathbb{F}_q^n$ in the following way. Recall that if $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ and $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ are two vectors in $\mathbb{F}_q^n$ then the Euclidean inner product $\mathbf{v} \cdot \mathbf{w}$ of $\mathbf{v}$ and $\mathbf{w}$ is defined as

$$\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^{n} v_i w_i.$$

Based on Definition 4.5, we have the following.

Definition **4.9** *The Euclidean dual code $C^{\perp}$ of o linear code C is defined as*

$$C^{\perp} = \{\boldsymbol{v} \in \mathbb{F}_q^n | \, \boldsymbol{v} \cdot \boldsymbol{c} = \boldsymbol{0} \ \forall \ \boldsymbol{c} \in C\}.$$

It is easy to see that if G and H are generator and parity check matrices, respectively, for a given code C, then it follows that H and G are generator and parity check matrices, respectively, for the dual $C^{\perp}$.

Let $C \subseteq \mathbb{F}_{q^2}^n$ be a linear code defined over $\mathbb{F}_{q^2}$. In this case we can also define the dual code $C^{\perp_H}$ of C with respect to the *Hermitian inner product.* To do this, let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_{q^2}^n$ be two vectors.

Definition **4.10** *The Hermitian inner product* $\langle \boldsymbol{v}|\boldsymbol{w}\rangle_H$ *of* $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_{q^2}^n$ *is defined as*

$$\langle \boldsymbol{v}|\boldsymbol{w}\rangle_H = \boldsymbol{v}^q \cdot \boldsymbol{w} = \sum_{i=1}^{n} v_i^q w_i,$$

where $\boldsymbol{v}^q = (v_1^q, v_2^q, \ldots, v_n^q)$.

Based on the Hermitian inner product, one has the *Hermitian dual code* $C^{\perp_H}$ of C.

Definition **4.11** *Let* $C \subseteq \mathbb{F}_{q^2}^n$ *be a linear code. The Hermitian dual code* $C^{\perp_H}$ *of* C *is defined by*

$$C^{\perp_H} = \{\boldsymbol{v} \in \mathbb{F}_{q^2}^n | \boldsymbol{v}^q \cdot \boldsymbol{c} = 0 \quad \forall \ \boldsymbol{c} \in C\}.$$

4.2 Cyclic codes

In this part, we review the concept of cyclic and Bose-Chaudhuri-Hocquenghem (BCH) codes. For more details the reader can consult the textbooks [8, 14].

We assume that q is a prime power and $\mathbb{F}_q$ is the finite field with q elements. Cyclic codes form an important class of linear codes. In this work we always assume that $\gcd(q, n) = 1$, where n is the length of the code. Recall that he multiplicative order of q modulo n $\mathrm{ord}_n(q)$ is the smallest positive integer m such that $n|(q^m - 1)$.

Definition **4.12** *The minimal polynomial over* $\mathbb{F}_q$ *of* $\beta \in \mathbb{F}_{q^m}$ *is the monic polynomial of smallest degree,* $M(x)$*, with coefficients in* $\mathbb{F}_q$ *such that* $M(\beta) = 0$*. If* $\beta = \alpha^i$ *for some primitive element* $\alpha \in \mathbb{F}_{q^m}$ *then the minimal polynomial of* $\beta = \alpha^i$ *is denoted by* $M^{(i)}(x)$*.*

Irreducible polynomials are generated in the following way.

Theorem **4.3** $x^{q^m} - x$ *= product of all monic, irreducible polynomials over* $\mathbb{F}_q$*, whose degree divides* m*.*

Cyclotomic cosets are fundamental for the development of the quantum code constructions presented in this book.

Definition **4.13** *The q-ary cyclotomic coset (or q-ary coset or even q-coset) modulo n containing an element s, is defined by* $\{s, sq, sq^2, sq^3, \ldots, sq^{m_s-1}\}$, *where* m_s *is the smallest positive integer such that* $sq^{m_s} \equiv s \mod n$. *If s is the smallest number in coset, this coset is denoted by* $\mathbb{C}_s$.

The following result is well known.

Theorem **4.4** $x^n - 1 = \prod_j M^{(j)}(x)$, *where* $M^{(j)}(x)$ *denotes the minimal polynomial of* $\alpha^j \in \mathbb{F}_{q^m}$ *and j runs through the coset representatives mod n.*

Let $\mathbb{F}_q[x]$ denote the ring of polynomials in $\mathbb{F}_q$ and consider the quotient ring $R_n = \mathbb{F}_q[x]/(x^n - 1)$. From this context we define the concept of cyclic code.

Definition **4.14** *A cyclic code of length n over* $\mathbb{F}_q$ *is a nonzero ideal in* R_n.

It is well known that there exists only one polynomial $g(x)$ with minimal degree in C; $g(x)$ is a generator polynomial of C. Moreover, $g(x)$ is a factor of $x^n - 1$. The dimension of a cyclic code C is equal to $n - \deg(g(x))$, where $\deg(g(x))$ is the degree of the polynomial $g(x)$.

The dual code $C^{\perp}$ of a cyclic code C is also cyclic and has generator polynomial given by

$$g(x)^{\perp} = x^{\deg h(x)} h(x^{-1}), \tag{1}$$

where $h(x) = (x^n - 1)/g(x)$.

Definition **4.15** *Two codes C and* C^* *are called equivalent if they differ only in the arrangement of symbols. More precisely, if C is the row space of a matrix G, then* C^* *is a code equivalent to C if and only if* C^* *is the row space of a matrix* G^* *that is obtained from G by rearranging columns.*

Based on Definition 4.15 and from Eq. (1), it follows that the code with generator polynomial $h(x)$ is equivalent to the (Euclidean) dual code $C^{\perp}$.

Let us recall the well-known BCH bound theorem.

Theorem **4.5** *(The BCH bound) Let q be a prime power and α a primitive nth root of unity. Let C be a cyclic code with generator polynomial $g(x)$ such that, for some integers $b \geq 0$ and $\delta \geq 1$, and for $\alpha \in \mathbb{F}_q$, we have*

$$g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+\delta-2}) = 0,$$

that is, the code has a sequence of $\delta - 1$ consecutive powers of α as zeros. Then the minimum distance of C is greater than or equal to δ.

In the sequence we present the definition of a BCH code.

Definition **4.16** *[2, 3, 7] Let q be a prime power and let n be a positive integer such that $\gcd(q, n) = 1$. Assume that α is a primitive nth root of unity. A cyclic code C of length n over $\mathbb{F}_q$ is a BCH code with designed distance δ if, for some integer $b \geq 0$, we have*

$$g(x) = \text{l. c. m.}\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the monic polynomial of smallest degree over $\mathbb{F}_q$ having α^b, α^{b+1}, $\ldots, \alpha^{b+\delta-2}$ as zeros.

Therefore, $c \in C$ if and only if $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+\delta-2}) = 0$. Thus the code has a string of $\delta - 1$ consecutive powers of α as zeros, Hence, from the BCH bound, its minimum distance is at least δ. If $n = q^l - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense. A parity check matrix for C is given by

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{(b+1)} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \cdots & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix},$$

where each entry is replaced by the corresponding column of $l = \text{ord}_n(q)$ elements from $\mathbb{F}_q$, then removing any linearly dependent rows. The rows of the resulting matrix over $\mathbb{F}_q$ are the parity checks satisfied by C.

5 Quantum code constructions

Quantum codes are fundamental to the error protection in quantum computers. We present here some constructions of quantum codes derived from classical BCH codes by means of the CSS construction.

5.1 BCH codes - part I

The material contained in this subsection can be found in [11, 12]. In this subsection we present five constructions of nonbinary quantum BCH codes:

- the first two ones are based on non-primitive BCH codes
- the third construction is based on Steane's enlargement of nonbinary CSS codes applied to suitable nonprimitive non-narrow-sense BCH codes.
- the fourth construction is obtained from suitable Hermitian dual-containing nonprimitive non-narrow-sense BCH codes constructed here.
- the fifth one is based on finding cyclic codes whose defining set consists of only one coset with at least two consecutive integers.

To be more precise, our families of quantum BCH codes have parameters described in the sequence:

- $[[n, n-4(c-2)-2, d \geq c]]_q$, where $q \geq 4$ is a prime power, n is an integer with $\gcd(q,n)=1$, $(q-1) \mid n$, $m = \operatorname{ord}_n(q) = 2$ and $2 \leq c \leq r$, where r is such that $n = r(q-1)$;
- $[[n, n-2mr, d \geq r+2]]_q$, where $m = \operatorname{ord}_n(q) \geq 2$, n is a prime number and r is the number of cosets satisfying suitable conditions (see Theorem 5.4);
- $[[n, n-m(2r-1), d \geq r+2]]_q$, where $m = \operatorname{ord}_n(q) \geq 2$, n is a prime number and $q \geq 3$;
- $[[n, n-4c, d \geq c+2]]_q$, where $n > q$ is an integer with $\gcd(q,n)=1$, $(q-1) \mid n$, $m = \operatorname{ord}_n(q) = 2$, $1 \leq c \leq r-3$ and $r > 3$ satisfies $n = r(q-1)$;
- $[[n, n-4c-2, d \geq c+2]]_q$, where $2 \leq c \leq r-2$, $q > 3$, $n = r(q^2-1)$, $r > 1$ and $m = \operatorname{ord}_n(q^2) = 2$;
- $[[n, n-2mr, d \geq r+2]]_q$, where $q \geq 3$ is a prime power, $n > q^2$ is a prime number such that $\gcd(q,n)=1$, $m = \operatorname{ord}_n(q^2) \geq 2$ and r is the number of cosets satisfying suitable conditions (see Theorem 5.9).

- $[[n, n-2m^*, d \geq r+2]]_q$, where $q \geq 3$ is a prime power and $n > m$ ($m = \operatorname{ord}_n(q) \geq r+2$) is a positive integer such that $\gcd(q,n) = 1$, $\gcd(q^{a_i} - 1, n) = 1$ for every $i = 1, 2, \ldots, r$, where $1 \leq r, a_1, a_2, \ldots, a_r < m$ are integers, and $n | \gcd(t_2, \ldots, t_r)$, where $t_j = [(j-(j-1)q^{a_j})(q^{a_j}-1)^{-1} - (q^{a_1}-1)^{-1}]$ for every $j = 2, \ldots, r$ (the operations are performed modulo n).

We always assume that $\gcd(q,n) = 1$ because this condition ensures that C has simple roots. Additionally, we utilize the notation $\mathbb{C}_{[a]}$ to denote the cyclotomic coset containing a, where a is not necessarily the smallest number in $\mathbb{C}_{[a]}$.

5.1.1 Construction I - Nonprimitive Codes

We start by showing Lemma 5.1.

Lemma **5.1** *Let $q \geq 3$ be a prime power and let $n > q$ be an integer such that* $\gcd(q,n) = 1$. *Assume also that $(q-1) \mid n$ and $m =$ $\operatorname{ord}_n(q) \geq 2$ hold. Then each of the q-ary cosets $\mathbb{C}_{[lr]}$ has only one element, where r is given by $n = r(q-1)$, and $1 \leq l \leq q-2$ is an integer.*

Proof: Since $rq = n + r$ holds, one has

$$(lr)q = l(n+r) \equiv lr \mod n;$$

hence

$$(lr)q^t \equiv lr \mod n$$

for each $1 \leq t \leq m-1$, proving the lemma. □

Lemma 5.1 is applied in the proof of Theorem 5.1.

Theorem **5.1** *Assume that $q > 3$ is a prime power and $n > q$ is an integer relatively prime with q. Assume also that $(q-1) \mid n$ and $m =$ $\operatorname{ord}_n(q) = 2$ are true. Then there exists a quantum code with parameters $[[n, n-4(r-2)-2, d \geq r]]_q$, where r is such that $n = r(q-1)$.*

Proof: Since $n \mid (q^2 - 1)$ and because we consider only nonprimitive BCH codes, it follows that $r \leq q$. As $\gcd(q,n) = 1$, one has $r < q$, so the inequalities $(r-2)q < n$ and $r + (r-2)q < n$ hold. We next show that all the q-ary cosets (modulo n of course) given by $\mathbb{C}_{[0]} = \{0\}, \mathbb{C}_{[1]} = \{1, \ \ q\}, \mathbb{C}_{[2]} = \{2, \ \ 2q\}, \mathbb{C}_{[3]} = \{3, \ \ 3q\}, \ldots, \mathbb{C}_{[r-2]} = \{r-2, \ \ (r-2)q\}, \mathbb{C}_{[r]} = \{r\}, \mathbb{C}_{[r+1]} =$

$\{r{+}1,\ r{+}q\}, \mathbb{C}_{[r+2]} = \{r{+}2,\ r{+}2q\}, \ldots, \mathbb{C}_{[2r-2]} = \{2r{-}2,\ r{+}(r{-}2)q\}$, are mutually disjoint and, with exception of the cosets $\mathbb{C}_{[0]} = \{0\}$ and $\mathbb{C}_{[r]} = \{r\}$, each of them has two elements.

The cosets $\mathbb{C}_{[0]}$ and $\mathbb{C}_{[r]}$ have only one element. Let us show that each of the other cosets has two elements. Since $(r-2)q < n$, then the congruence $l \equiv lq \mod n$ implies that $l = lq$, where $1 \leq l \leq r-2$, which is a contradiction. If $r+s \equiv (r+s)q \mod n$, where $1 \leq s \leq r-2$, then $r+s = r+sq$, which is a contradiction.

From now on, we show that all these cosets given above and $\mathbb{C}_{[0]}$ and $\mathbb{C}_{[r]}$ are mutually disjoint. We only consider the case $\mathbb{C}_{[r+l]} = \mathbb{C}_{[r-s]}$, where $1 \leq l, s \leq r-2$, since the other cases are similar to this one. Seeking a contradiction, we assume that $\mathbb{C}_{[r+l]} = \mathbb{C}_{[r-s]}$, where $1 \leq l, s \leq r-2$. If the congruence $(r+l) \equiv (r-s) \mod n$ holds, we obtain

$$(r+l) \equiv (r-s) \mod n \Longrightarrow n \mid (l+s).$$

If $l+s \neq 0$, one has $n \leq l+s$, which is a contradiction. If $l+s = 0$, this implies $l = -s$, which is a contradiction.

On the other hand, if $(r+l)q \equiv r-s \mod n$ holds, we have

$$\begin{aligned}(r+l)q \equiv r-s \Longrightarrow lq &\equiv -s \mod n\\ &\Longrightarrow n \mid (lq+s).\end{aligned}$$

Since $l, s \leq r-2$ and $r < q$ are true, if $lq+s \neq 0$ holds. it follows that $lq+s < n$, which is a contradiction. If $lq+s = 0$ then $lq = -s$, which is a contradiction. Thus all the q-ary cosets $\mathbb{C}_{[0]},\ \mathbb{C}_{[1]}, \ldots, \mathbb{C}_{[r-2]}$, are disjoint from each of the q-ary cosets $\mathbb{C}_{[r]},\ \mathbb{C}_{[r+1]}, \ldots, \mathbb{C}_{[2r-2]}$. Additionally, all the q-ary cosets $\mathbb{C}_{[0]},\ \mathbb{C}_{[1]}, \ldots, \mathbb{C}_{[r-2]}$, are mutually disjoint and all the q-ary cosets $\mathbb{C}_{[r]},\ \mathbb{C}_{[r+1]}, \ldots, \mathbb{C}_{[2r-2]}$ are also mutually disjoint.

Let C_1 be the cyclic code generated by the product of the minimal polynomials

$$M^{(0)}(x)M^{(1)}(x) \cdot \ldots \cdot M^{(r-2)}(x),$$

and C_2 be the cyclic code generated by $g_2(x)$, that is the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where $i \notin \{r, r+1, \ldots, 2r-2\}$ and i runs through the coset representatives mod n. From construction it follows that $C_2 \subsetneq C_1$. From the BCH bound, the minimum distance of C_1 is greater than or equal to r, because its defining set contains the sequence $0, 1, \ldots, r-2$, of $r-1$ consecutive integers. Similarly, the defining set of the code C generated by the polynomial $h(x) = \frac{x^n-1}{g_2(x)}$ contains the sequence $r, r+1, \ldots, 2r-2$, of $r-1$ consecutive integers and so, from the BCH bound, C also has minimum distance greater than or equal to r. Since the code $C_2^{\perp}$ is equivalent to C, $C_2^{\perp}$ also has minimum distance greater than or equal to r. Therefore, the resulting CSS code has minimum distance greater than or equal to r.

Next we compute the dimension of the corresponding CSS code. We know that the degree of the generator polynomial of a cyclic code is equal to the cardinality of its defining set. Furthermore, the defining set Z_1 of C_1 has $r-1$ disjoint cyclotomic cosets. Moreover, all of them (except coset $\mathbb{C}_0$) have two elements; hence Z_1 has $2(r-2)+1$ elements. Therefore, C_1 has dimension $k_1 = n - 2(r-2) - 1$. Similarly, C_2 has dimension $k_2 = 2(r-2)+1$. Thus the dimension of the corresponding CSS code is $n - 4(r-2) - 2$. Applying the CSS construction to the codes C_1 and C_2, one can get a quantum code with parameters $[[n, n-4(r-2)-2, d \geq r]]_q$. The proof is complete. $\square$

We illustrate Theorem 5.1 by means of a graphical scheme:

$$\overbrace{\underbrace{\mathbb{C}_{[0]}\mathbb{C}_{[1]}\ \mathbb{C}_{[2]}\ \ldots\ \mathbb{C}_{[r-2]}}_{C_2}}^{C_1}$$

$$\overbrace{\mathbb{C}_{[r]}\ \mathbb{C}_{[r+1]}\ldots\ \mathbb{C}_{[2r-2]}}^{C}\ \underbrace{\mathbb{C}_{[a_1]}\ldots\mathbb{C}_{[a_n]}}_{C_2}.$$

Observe that the union of the q-cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \ldots, \mathbb{C}_{[r-2]}$ is the defining set of code C_1; the union of the cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \ldots, \mathbb{C}_{[r-2]}, \mathbb{C}_{[a_1]}, \ldots, \mathbb{C}_{[a_n]}$ is the defining set of C_2, where $\mathbb{C}_{[a_1]}, \ldots, \mathbb{C}_{[a_n]}$ are the remaining cosets in order to complete the set of all q-cosets. Finally, the union of the cosets $\mathbb{C}_{[r]}, \mathbb{C}_{[r+1]}, \ldots, \mathbb{C}_{[2r-2]}$ is the defining set of C.

As an immediate result we have:

Corollary **5.1** *Assume that all the hypotheses of Theorem 5.1 are valid. Then there exists a quantum code with parameters* $[[n, n-4(c-2)-2, d \geq c]]_q$, *where* $2 \leq c < r$.

Proof: Let C_1 be the cyclic code generated by the product of the minimal polynomials

$$M^{(0)}(x)M^{(1)}(x) \cdot \ldots \cdot M^{(c-3)}(x)M^{(c-2)}(x),$$

and C_2 be the cyclic code generated by the product of the minimal polynomials

$$\prod_i M^{(i)}(x),$$

where $i \notin \{r, r+1, \ldots, r+c-2\}$ and i runs through the coset representatives mod n. Proceeding similarly as in the proof of Theorem 5.1, the result follows. $\square$

Example **5.1** *As an example, let us consider that* $q = 9$ *and* $n = 40$*; then* $\gcd(9, 40) = 1$*,* $8 \mid 40$ *and* $ord_{40}(9) = 2$*. In this case we have* $r = 5$*. Theorem 5.1 asserts the existence of a quantum code with parameters* $[[40, 26, d \geq 5]]_9$*. Consider next* $q = 11$ *and* $n = 30$*. Let* C_1 *be the cyclic code generated by the product of the minimal polynomials* $M^{(0)}(x)M^{(1)}(x) \ldots M^{(6)}(x)$ *and* C_2 *be the cyclic code generated by the product of the minimal polynomials* $\prod_i M^{(i)}(x)$*, where* $i \notin \{7, 10, 15, 16, 18, 19, 21\}$ *and* i *runs through the coset representatives mod* 30*. Proceeding similarly as in the proof of Theorem 5.1, an* $[[30, 8, d \geq 8]]_{11}$ *quantum code can be constructed.*

5.1.2 Construction II - Codes of prime length

Here the attention is focused on cyclic codes of prime length. Among the contributions exhibited in this subsection, we prove there exists at least one q-ary coset containing two consecutive integers (see Lemma 5.2). In order to proceed further, let us recall a well-known result from number theory.

Theorem **5.2** *A linear congruence* $ax \equiv b$ *(mod* m*), where* $a \neq 0$*, admits an integer solution if and only if* $d = \gcd(a, m)$ *divides* b*.*

Applying Theorem 5.2 we prove Lemma 5.2.

Lemma **5.2** *Assume that* $q \geq 3$ *is a prime power,* $n > q$ *is a prime number and consider that* $m = \operatorname{ord}_n(q) \geq 2$*. Then there exists at least one* q*-ary coset containing two consecutive integers.*

Proof: Note first that $\gcd(q, n) = 1$. In order to prove this lemma, it suffices to show that the congruence $xq \equiv x + 1(\mod n)$ has at least one solution for some $0 \leq x \leq n-1$ or, equivalently, the congruence $(q-1)x \equiv 1 \pmod n$ has at least one solution. We know that $\gcd(q-1, n) = 1$, because $n > q$ and n is prime. Since $q - 1 \neq 0$, it follows from Theorem 5.2 that $(q-1)x \equiv 1$

(mod n) has an integer solution x_0. Applying the division algorithm for x_0 and n we have $x_0 = ns_0 + r_0$, where r_0 and s_0 are integers and $0 \leq r_0 \leq n-1$. Since $(q-1)x_0 \equiv 1$ (mod n) holds then the congruence $(q-1)r_0 \equiv 1$ (mod n) also holds. Therefore, the result follows. □

Remark **5.1** *Note that in Lemma 5.2 it is not necessary to assume that n is a prime number. In fact, we need only to suppose that $\gcd(q-1,n)=1$ and $\gcd(q,n)=1$ hold. However, since the corresponding q-ary cosets of BCH codes of prime length have nice properties, we have assumed that n is prime. However, if one assumes that $\gcd(q-1,n)=1$ and $\gcd(q,n)=1$ hold, more good quantum codes can be constructed.*

Theorem **5.3** *Let $q \geq 3$ be a prime power, $n > q$ be a prime number and consider $m = \operatorname{ord}_n(q) \geq 2$. Suppose also that the q-cosets $\mathbb{C}_{[s]}$ and $\mathbb{C}_{[-s]}$ are disjoint, where $\mathbb{C}_{[s]}$ is a q-coset containing two consecutive integers. Then there exists an $[[n, n-2m, d \geq 3]]_q$ quantum code.*

Proof: Note that $\gcd(q,n)=1$. Let C_1 be the code generated by $M^{(s)}(x)$ and C_2 generated by $\prod_i M^{(i)}(x)$, where $i \neq -s$ and i runs through the coset representatives mod n. It is easy to see that the cosets $\mathbb{C}_{[s]}$ and $\mathbb{C}_{[-s]}$ contain m elements. Proceeding similarly as in the proof of Theorem 5.1, the result follows. □

Theorem **5.4** *Let $q \geq 3$ be a prime power, $n > q$ be a prime and consider that $m = \operatorname{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the q-coset containing s and $s+1$. Suppose also that all the q-ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \ldots, \mathbb{C}_{[s+r]}, \mathbb{C}_{[-s]}, \mathbb{C}_{[-s-2]}, \ldots, \mathbb{C}_{[-s-r]}$, are mutually disjoint. Then there exists a quantum code with parameters $[[n, n-2mr, d \geq r+2]]_q$.*

Proof: We know that $\gcd(q,n)=1$ and the coset $\mathbb{C}_{[-s]}$ also contains two consecutive integers, namely, $-s-1$ and $-s$. Let C_1 be the cyclic code generated by

$$M^{(s)}(x)M^{(s+2)}(x)\cdot \ldots \cdot M^{(s+r)}(x),$$

and let C_2 be the cyclic code generated by the polynomial $g_2(x)$, that is the product of the minimal polynomials

$$g_2(x) = \prod_j M^{(j)}(x),$$

where $j \notin \{-s-r, \ldots, -s-2, -s\}$ and j runs through the coset representatives mod n.

From the BCH bound, the minimum distance of C_1 is greater than or equal to $r+2$ because its defining set contains the sequence of $r+1$ consecutive integers given by $s, s+1, s+2, \ldots, s+r$. Similarly, the defining set of the code C generated by the polynomial $h_2(x) = (x^n - 1)/g_2(x)$, contains a sequence of $r+1$ consecutive integers given by $-s-r, \ldots, -s-2, -s-1, -s$. Again, from the BCH bound, C has minimum distance greater than or equal to $r+2$. Since C is equivalent to $C_2^{\perp}$, it follows that $C_2^{\perp}$ also has minimum distance greater than or equal to $r+2$. Therefore, the resulting CSS code have minimum distance greater than or equal to $r+2$. If $s \in [1, n-1]$ satisfies $\gcd(s, n) = 1$ then the coset $\mathbb{C}_s$ has cardinality m. In fact, if $|\mathbb{C}_s| = c < m$ it follows that $n | s(q^c - 1)$, so $n | (q^c - 1)$, a contradiction. Thus, since n is prime, each of the cosets $\mathbb{C}_s$, where $s \in [1, n-1]$, has cardinality m. Additionally, from the hypotheses, all the q-ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \ldots, \mathbb{C}_{[s+r]}$, are mutually disjoint. Thus C_1 has dimension $k_1 = n - mr$ and C_2 has dimension $k_2 = mr$, since there exist r disjoint q-cosets not contained in the defining set of C_2, where each of them has cardinality m. Therefore, the corresponding CSS code has dimension $K = n - 2mr$. Since the cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \ldots, \mathbb{C}_{[s+r]}, \mathbb{C}_{[-s]}, \mathbb{C}_{[-s-2]}, \ldots, \mathbb{C}_{[-s-r]}$, are mutually disjoint, it follows that $C_2 \subsetneq C_1$. Applying the CSS construction to C_1 and C_2, one obtains an $[[n, n-2mr, d \geq r+2]]_q$ quantum code, and we are done. □

Example **5.2** *Theorem 5.4 has variants as follows: to construct an* $[19, 13, d \geq 3]]_7$ *quantum code, let us consider that* $q = 7$, $n = 19$ *and* $m = 3$. *The cosets are given by* $\mathbb{C}_2 = \{2, 14, 3\}$ *and* $\mathbb{C}_{16} = \{5, 16, 17\}$. *Let* C_1 *be generated by* $M^{(2)}(x)$ *and* C_2 *generated by* $g_2(x) = \prod_i M^{(i)}(x)$, *where* $i \notin \{16\}$ *and* i *runs through the coset representatives mod* 19. *Then an* $[[19, 13, d \geq 3]]_7$ *quantum code can be constructed. Proceeding similarly, one can get quantum codes with parameters* $[[31, 25, d \geq 3]]_5$, $[[71, 61, d \geq 3]]_5$, $[[11, 1, d \geq 4]]_3$, $[[31, 19, d \geq 4]]_5$, $[[31, 13, d \geq 5]]_5$, $[[71, 51, d \geq 4]]_5$, $[[71, 41, d \geq 6]]_5$.

5.1.3 Construction III - Codes Derived from Steane's Construction

In this subsection we construct families of quantum BCH codes of prime length by applying Steane's enlargement of nonbinary CSS construction [6, Corollary 4]. These new families have parameters better than the parameters of the quantum BCH codes available in the literature. Let us recall the Steane's enlargement code construction applied to nonbinary alphabets.

Corollary **5.2** *[6, Corollary 4] Assume that we have an $[N_0, K_0]$ linear code L which contains its Euclidean dual, $L^{\perp} \leq L$, and which can be enlarged to an $[N_0, K_0^{'}]$ linear code $L^{'}$, where $K_0^{'} \geq K_0 + 2$. Then there exists a quantum code with parameters $[[N_0, K_0 + K_0^{'} - N_0, d \geq \ min\{d, \lceil \frac{q+1}{q} d^{'} \rceil\}]]$, where $d = w(L \backslash L^{'\perp})$ and $d^{'} = w(L^{'} \backslash L^{'\perp})$.*

Euclidean dual-containing cyclic codes can be derived from Lemma 5.3:

Lemma **5.3** *[1, Lemma 1] Assume that* $\gcd(q, n) = 1$. *A cyclic code of length n over $\mathbb{F}_q$ with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1} = \emptyset$, where $Z^{-1} = \{-z \ mod \ n \mid z \in Z\}$.*

In Lemma 5.2 of Section 5.1.2 we have shown the existence of, at least, one q-ary cyclotomic coset containing two consecutive integers provided the code length is prime. In what follows, we show how to construct good quantum codes of prime length by applying Steane's code construction. We begin by presenting an illustrative example:

Example **5.3** *Assume that $n = 31$ and $q = 5$. From Lemma 5.2, there exists a coset containing at least two consecutive integers; here it is the coset $\mathbb{C}_8 = \{8, 9, 14\}$. Let C be the cyclic code generated by the product of the minimal polynomials $C = \langle g(x) \rangle = \langle M^{(4)}(x) M^{(8)}(x) \rangle$. C has defining set $Z = \mathbb{C}_4 \cup \mathbb{C}_8 = \{4, 7, 8, 9, 14, 20\}$ and has parameters $[31, 25, d \geq 4]_5$. From Lemma 5.3, it is easy to check that C is Euclidean dual-containing. Furthermore, C can be enlarged to a code $C^{'}$ with parameters $[31, 28, d \geq 3]_5$, whose generator polynomial is $M^{(8)}(x)$. Applying Corollary 5.2 to C and $C^{'}$, we obtain an $[[31, 22, d \geq 4]]_5$ quantum code.*

Theorem **5.5** *Let $q \geq 3$ be a prime power, $n > q$ be a prime and consider that $m = \ \operatorname{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the q-ary coset containing s and $s+1$ and let $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]}$, where $\mathbb{C}_s \neq \mathbb{C}_{[s+2]}$. Assume also that $Z \cap Z^{-1} = \emptyset$ holds. Then there exists an $[[n, n - 3m, d \geq 4]]_q$ code.*

Proof: We know that $\gcd(q, n) = 1$. Let C be the cyclic code generated by $\langle M^{(s)}(x) M^{(s+2)}(x) \rangle$. By hypothesis and from Lemma 5.3, we know that C is Euclidean dual-containing; C has parameters $[n, n - 2m, d \geq 4]_q$. Let $C^{'}$ be the cyclic code generated by $M^{(s)}(x)$. We know that $C^{'}$ is an enlargement of C and it has parameters $[n, n - m, d \geq 3]_q$. Since $m \geq 2$, it follows that $k^{'} - k = m \geq 2$, where $k^{'}$ is the dimension of $C^{'}$ and k is the dimension of C. Applying the Steane's code construction to C and $C^{'}$, since $\frac{q+1}{q} > 1$, we get an $[[n, n - 3m, d \geq 4]]_q$ quantum code. □

Theorem 5.5 can be generalized in the following way:

Theorem **5.6** *Assume that $q \geq 3$ is a prime power, $n > q$ is a prime number and consider that $m = \operatorname{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the coset containing s and $s+1$. Assume that $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]} \cup \ldots \cup \mathbb{C}_{[s+r]}$, where all the q-cosets $\mathbb{C}_{[s+i]}$, $i = 0, 2, 3, \ldots, r$, are mutually disjoint. Assume also that $Z \cap Z^{-1} = \emptyset$. Then there exists an $[[n, n - m(2r-1), d \geq r+2]]_q$ quantum code.*

Proof: We know that $\gcd(q, n) = 1$. Let C be the cyclic code generated by

$$M^{(s)}(x)M^{(s+2)}(x) \cdot \ldots \cdot M^{(s+r)}(x).$$

Since $Z \cap Z^{-1} = \emptyset$, it follows from Lemma 5.3 that C is Euclidean dual-containing. From the hypotheses, all the q-ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \ldots, \mathbb{C}_{[s+r]}$ are mutually disjoint; hence, C has dimension $k = n - mr$ and its minimum distance is lower bounded by $d \geq r+2$, i.e., C is an $[n, n-mr, d \geq r+2]_q$ code. Let $C^{'}$ be the cyclic code generated by

$$M^{(s)}(x)M^{(s+2)}(x) \cdot \ldots \cdot M^{(s+r-1)}(x).$$

We know that $C^{'}$ is an enlargement of C and it has parameters $[n, n-m(r-1), d \geq r+1]_q$. Since $m \geq 2$, we have $k^{'} - k = m \geq 2$, where $k^{'}$ is the dimension of $C^{'}$ and k is the dimension of C. Applying the Steane's construction to C and $C^{'}$ we obtain an $[[n, n-m(2r-1), d \geq r+2]]_q$ code, as required. □

Example **5.4** *In this example we construct an $[[31, 16, d \geq 5]]_5$ quantum code. For this purpose we take $n = 31$ and $q = 5$; then $m = \operatorname{ord}_n(q) = 3$. Let C be the cyclic code generated by $M^{(4)}(x)M^{(6)}(x)M^{(8)}(x)$. It is easy to see that C is Euclidean dual-containing and has parameters $[31, 22, d \geq 5]_5$. Let $C^{'}$ be the cyclic code generated by $M^{(4)}(x)M^{(8)}(x)$. The code $C^{'}$ has parameters $[31, 25, d \geq 4]_5$. Thus there exists an $[[31, 16, d \geq 5]]_5$ quantum code.*

We next establish Theorem 5.7, an analogous to Theorem 5.1.

Theorem **5.7** *Suppose that $q \geq 5$ is a prime power and $n > q$ is an integer such that $\gcd(q, n) = 1$. Assume also that $(q-1) \mid n$ and $m = \operatorname{ord}_n(q) = 2$ hold. Then there exists a quantum code with parameters $[[n, n-4c, d \geq c+2]]_q$, where $1 \leq c \leq r-3$ and $r > 3$ is such that $n = r(q-1)$.*

Proof: We only prove the existence of an $[[n, n-4(r-3), d \geq r-1]]_q$ code, since the constructions of the other codes are quite similar.

Let C be the cyclic code generated by

$$M^{(r)}(x)M^{(r+1)}(x) \cdot \ldots \cdot M^{(2r-3)}(x).$$

From Lemma 5.1 and from the proof of Theorem 5.1, we know that the q-cosets given by $\mathbb{C}_{[r]} = \{r\}, \mathbb{C}_{[r+1]} = \{r+1, \quad r+q\}, \mathbb{C}_{[r+2]} = \{r+2, \quad r+2q\}, \ldots, \mathbb{C}_{[2r-3]} = \{2r-3, \quad r+(r-3)q\}$ are mutually disjoint and each of them has two elements. Therefore, C has dimension $k = n - 2(r-3) - 1$ and minimum distance $d \geq r-1$.

Let us prove that C is Euclidean dual-containing. In fact, if $(r+i) \equiv -(r+j) \mod n$, where $0 \leq i, j \leq r-3$, it follows that $2r + i + j \equiv 0 \mod n$. Since the inequality $2r + i + j < n$ holds because $q \geq 5$, one has a contradiction. On the other hand, if $(r+i)q \equiv -(r+j) \mod n$ holds then

$$\begin{aligned} (iq+j)(q-1) &\equiv 0 \mod n \Longrightarrow \\ i(q^2-q) + j(q-1) &\equiv 0 \mod n \Longrightarrow \\ j(q-1) &\equiv i(q-1) \mod n, \end{aligned}$$

where the latter congruence holds because $\mathrm{ord}_n(q) = 2$. Then the unique solution is when $i = j$. Let us investigate this case. Seeking a contradiction, we assume that the congruence $(r+i)q \equiv -(r+i) \mod n$ is true. Then we obtain

$$\begin{aligned} (r+i)q &\equiv -(r+i) \mod n \Longrightarrow \\ 2r + i(q+1) &\equiv 0 \mod n \Longrightarrow \\ r(q-3) &\equiv i(q+1) \mod n. \end{aligned}$$

If $0 \leq i \leq r-4$, then

$$r(q-3) - i(q+1) \geq r(q-3) - (r-4)(q+1) = 4q - 4r + 4 > 0,$$

where the latter inequality holds because $r < q$ since we only consider non-primitive BCH codes. Moreover, the inequality $r(q-3) - i(q+1) < n$ also holds, which is a contradiction. If $i = r-3$ then the congruence $r(q-3) \equiv (r-3)(q+1) \mod n$ holds, that is, $4r \equiv 3(q+1) \mod n$ holds. Since $r \mid (q+1)$ and $q+1 > r$ hold, it implies that $q+1 \geq 2r$ so, $3(q+1) - 4r \geq 2r > 0$. Moreover, the inequality $3(q+1) - 4r < n$ holds, which is a contradiction. Therefore, C is Euclidean dual-containing.

Let $C^{'}$ be the cyclic code generated by

$$M^{(r)}(x)M^{(r+1)}(x) \cdot \ldots \cdot M^{(2r-4)}(x).$$

$C^{'}$ is an enlargement of C; $C^{'}$ has dimension $k^{'} = n-2(r-4)-1$ and minimum distance $d^{'} \geq r-2$. Since $m = 2$ then $k^{'} - k = 2$, where $k^{'}$ denotes the dimension of $C^{'}$ and k is the dimension of C. We know that $\lceil \frac{q+1}{q} d^{'} \rceil \geq r-1$. Thus, applying the Steane's construction one has an $[[n, n-4(r-3), d \geq r-1]]_q$

quantum code, as required. □

Recall that an $[[n,k,d]]_q$ code C satisfies the quantum Singleton bound given by $k + 2d \leq n + 2$. If C attains the quantum Singleton bound, i.e., $k + 2d = n + 2$, then it is called a quantum maximum distance separable (MDS) code. In the following two examples we construct quantum MDS-BCH codes:

Example **5.5** *Applying Theorem 5.7 for* $q = 9$ *and* $n = 40$ *one has* $r = 5$. *Thus there exists an* $[[40, 36, 3]]_9$ *quantum MDS-BCH code. Analogously, applying Theorem 5.7 for* $q = 11$ *and* $n = 60$ *one obtains an* $[[60, 56, 3]]_{11}$ *quantum MDS-BCH code. Additionally, an* $[[60, 48, d \geq 5]]_{11}$ *and an* $[[60, 52, d \geq 4]]_{11}$ *quantum codes can be constructed.*

5.1.4 Construction IV - Hermitian dual-containing BCH Codes

In this subsection we present the fourth proposed construction, which is based on finding good Hermitian dual-containing BCH codes. Let us recall some useful concepts.

Lemma **5.4** *[1, Lemma 13] Assume that* $\gcd(q, n) = 1$. *A cyclic code of length* n *over* $\mathbb{F}_{q^2}$ *with defining set* Z *contains its Hermitian dual code if and only if* $Z \cap Z^{-q} = \emptyset$, *where* $Z^{-q} = \{-qz \text{ mod } n \mid z \in Z\}$.

Lemma **5.5** *[1, Lemma 17c] (Hermitian Construction) If there exists a classical linear* $[n, k, d]_{q^2}$ *code* D *such that* $D^{\perp_H} \subset D$, *then there exists an* $[[n, 2k - n, \geq d]]_q$ *stabilizer code that is pure to* d. *If the minimum distance* $d^{\perp_H}$ *of* $D^{\perp_H}$ *exceeds* d, *then the stabilizer code is pure and has minimum distance* d.

Let us start with an example of how Lemma 5.1 can be applied together the Hermitian construction in order to construct good codes. Assume that $q = 7$, $n = 144$, $m = 3$ and $r = 3$; the q^2-ary cosets $\mathbb{C}_3$, $\mathbb{C}_6$, $\mathbb{C}_9$ and $\mathbb{C}_{12}$ contain only one element. The other q-cosets are $\mathbb{C}_4 = \{4, 52, 100\}$, $\mathbb{C}_5 = \{5, 101, 53\}$, $\mathbb{C}_7 = \{7, 55, 103\}$, $\mathbb{C}_8 = \{8, 104, 56\}$, $\mathbb{C}_{10} = \{10, 58, 106\}$, $\mathbb{C}_{11} = \{11, 107, 59\}$. Let C be the cyclic code generated by $M^{(3)}(x)M^{(4)}(x)M^{(5)}(x)M^{(6)}(x)M^{(7)}(x)$ $M^{(8)}(x)M^{(9)}(x) \cdot M^{(10)}(x)M^{(11)}(x)M^{(12)}(x)$. It is straightforward to show that C is Hermitian dual-containing and has parameters $[144, 122, d \geq 11]_{7^2}$. Thus, applying the Hermitian construction, we obtain an $[[144, 100, d \geq 11]]_7$ quantum code. Similarly one can construct quantum codes with parameters $[[144, 102, d \geq 10]]_7$, $[[144, 108, d \geq 9]]_7$, $[[144, 114, d \geq 8]]_7$, $[[144, 116, d \geq 7]]_7$,

$[[144, 122, d \geq 6]]_7$, $[[144, 128, d \geq 5]]_7$, $[[144, 130, d \geq 4]]_7$ and $[[144, 136, d \geq 3]]_7$.

Theorem **5.8** *Suppose that $q > 3$ is a prime power and $n > q^2$ is an integer such that* $\gcd(q^2, n) = 1$*. Assume also that $(q^2 - 1) \mid n$ and $m = \text{ord}_n(q^2) = 2$ hold. Then there exists a quantum code with parameters* $[[n, n - 4(r-2) - 2, d \geq r]]_q$*, where r satisfies $n = r(q^2 - 1)$.*

Proof: Let C be the cyclic code generated by

$$M^{(r)}(x)M^{(r+1)}(x) \cdot \ldots \cdot M^{(2r-2)}(x).$$

We first show that C is Hermitian dual-containing. For this, let us consider the defining set Z of C consisting of the q^2-ary cyclotomic cosets given by $\mathbb{C}_{[r]} = \{r\}, \mathbb{C}_{[r+1]} = \{r+1, \quad r+q^2\}, \mathbb{C}_{[r+2]} = \{r+2, \quad r+2q^2\}, \ldots, \mathbb{C}_{[2r-2]} = \{2r-2, \quad r+(r-2)q^2\}$.

We know that $\gcd(q, n) = 1$ holds. From Lemma 5.4, it suffices to show that $Z \cap Z^{-q} = \emptyset$. Seeking a contradiction, we assume that $Z \cap Z^{-q} \neq \emptyset$. Then there exist i, j, where $0 \leq i, j \leq r-2$, such that $(r+j)q^l \equiv -q(r+i) \mod n$, where $l = 0$ or $l = 2$. If $l = 0$, one has $r + j \equiv -q(r+i) \mod n$, so $q(r+i)+r+j \equiv 0 \mod n$. Since both $q(r+i)+r+j < n$ and $q(r+i)+r+j \neq 0$ are true, one has a contradiction. If $l = 2$, it implies that $(r+j)q^2 \equiv -q(r+i) \mod n$ and since $\gcd(q^2, n) = 1$ and $rq^2 \equiv r \mod n$ one obtains

$$\begin{aligned}
(r+j)q^2 &\equiv -q(r+i) \mod n\\
\Longrightarrow r + jq^2 &\equiv -q(r+i) \mod n\\
\Longrightarrow (q+1)r &\equiv -q(i+jq) \mod n\\
\Longrightarrow -q(i+jq)(q-1) &\equiv 0 \mod n\\
\Longrightarrow n &\mid q(i+jq)(q-1)\\
\Longrightarrow r(q+1) &\mid q(i+jq).
\end{aligned}$$

Since $\gcd(r, q) = 1$ and $\gcd(q+1, q) = 1$ hold it implies that $r(q+1) \mid (i+jq)$, which is a contradiction because $i + jq < r(q+1)$. Thus C is Hermitian dual-containing.

It is easy to see that these cosets are mutually disjoint. With exception of $\mathbb{C}_{[r]}$, the other q-cosets have two elements. Thus, C has dimension $k = n - 2(r-2) - 1$. By construction, the defining set of C contains the sequence $r, r+1, \ldots, 2r-2$, of $r-1$ consecutive integers and, so the minimum distance of C is greater than or equal to r, that is, C is an $[n, n-2(r-2)-1, d \geq r]_{q^2}$ code. Applying the Hermitian construction to the code C, one can get an $[[n, n-4(r-2)-2, d \geq r]]_q$ code, as desired.
□

Corollary **5.3** *Suppose $q > 3$ is a prime power and $n > q^2$ is an integer such that* $\gcd(q^2, n) = 1$*. Assume also $(q^2 - 1) \mid n$ and $m = \operatorname{ord}_n(q^2) = 2$. Then there exist quantum codes with parameters $[[n, n - 4c - 2, d \geq c + 2]]_q$, where $2 \leq c < r - 2$ and $n = r(q^2 - 1)$.*

Proof: Let C be the BCH code generated by

$$M^{(r)}(x)M^{(r+1)}(x) \cdot \ldots \cdot M^{(r+c)}(x).$$

Proceeding similarly as in the proof of Theorem 5.8, the result follows. □

Theorem **5.9** *Let $q \geq 3$ be a prime power, $n > q^2$ be a prime number and consider that $m = \operatorname{ord}_n(q^2) \geq 2$. Let $\mathbb{C}_{[s]}$ be the q-coset containing s and $s + 1$. Assume that $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]} \cup \ldots \cup \mathbb{C}_{[s+r]}$, where all the q-ary cosets $\mathbb{C}_{[s+i]}$, $i = 0, 2, 3, \ldots, r$, are mutually disjoint, and suppose that $Z \cap Z^{-q} = \emptyset$. Then there exists an $[[n, n - 2mr, d \geq r + 2]]_q$ quantum code.*

Proof: We know that $\gcd(q, n) = 1$ holds. Let C be the cyclic code generated by

$$M^{(s)}(x)M^{(s+2)}(x) \cdot \ldots \cdot M^{(s+r)}(x).$$

Since $Z \cap Z^{-q} = \emptyset$ holds, it follows from Lemma 5.4 that C is Hermitian dual-containing. From the BCH bound, the minimum distance of C is greater than or equal to $r + 2$. It is easy to see that all the cosets $\mathbb{C}_{[s+i]}$, where $i = 0, 2, 3, \ldots, r$, have m elements and they are mutually disjoint. Thus C has parameters $[n, n - mr, d \geq r + 2]_{q^2}$. Applying the Hermitian construction one can get an $[[n, n - 2mr, d \geq r + 2]]_q$ quantum code. □

We finish this subsection by showing how Lemma 5.2 works for constructing quantum MDS-BCH codes.

Example **5.6** *Let us consider $q = 5$ and $n = 13$. Since* $\gcd(13, 24) = 1$*, the linear congruence $(q^2 - 1)x \equiv 1 \bmod n$ has a solution, so there exists at least one q^2-ary coset containing two consecutive integers, namely, the coset $\mathbb{C}_{[6]} = \{6, 7\}$. Let $C = \langle M^{(6)}(x) \rangle$. Since $\mathbb{C}_{[4]}$ and $\mathbb{C}_{[6]}$ are disjoint, C is Hermitian dual-containing and has parameters $[13, 11, d \geq 3]_5$. Applying the Hermitian construction, an $[[13, 9, 3]]_5$ quantum MDS-BCH code is constructed. Similarly, we can also construct an $[[17, 13, 3]]_4$ and an $[[17, 9, 5]]_4$ quantum MDS-BCH code.*

5.1.5 Construction V - Codes obtained from a single coset

In this subsection show the existence of (classical) cyclic codes whose defining set consists of only one cyclotomic coset containing at least two consecutive integers. This fact allows us to construct quantum codes with good parameters.

Lemma 5.6 in the following is a particular case of the CSS construction.

Lemma **5.6** *[1, Lemma 17] If there exists a classical linear $[n, k, d]_q$ code C such that $C^{\perp} \subset C$, then there exists an $[[n, 2k-n, \geq d]]_q$ stabilizer code that is pure to d.*

Theorem 5.10 establishes conditions for the existence of a cyclic code whose defining set consists of only one q-coset containing at least two consecutive integers. This fact produces conditions to construct quantum codes with good parameters (in the sense of the QSB).

Theorem **5.10** *Let $q \geq 3$ be a prime power and $n > m$ be a positive integer such that $\gcd(q, n) = 1$ and $\gcd(q^{a_i} - 1, n) = 1$ for every $i = 1, 2, \ldots, r$, where $m = \operatorname{ord}_n(q) \geq r + 2$ and $1 \leq r, a_1, a_2, \ldots, a_r < m$ are integers. If $n | \gcd(t_2, \ldots, t_r)$, where $t_j = [(j-(j-1)q^{a_j})(q^{a_j}-1)^{-1} - (q^{a_1}-1)^{-1}]$ for every $j = 2, \ldots, r$ (the operations are performed modulo n), then there exists an $[n, n-m^*, d \geq r+2]_q$ cyclic code, where m^* is the cardinality of the q-coset containing $r+1$ consecutive integers.*

Proof: We will investigate the following system of congruences

$$\begin{aligned} xq^{a_1} &\equiv (x+1) \mod n \\ (x+1)q^{a_2} &\equiv (x+2) \mod n \\ (x+2)q^{a_3} &\equiv (x+3) \mod n \\ &\vdots \\ (x+r-1)q^{a_r} &\equiv (x+r) \mod n, \end{aligned}$$

where $1 \leq r, a_1, a_2, \ldots, a_r < m$. Since $\gcd(q^{a_i} - 1, n) = 1$ for every $i = 1, 2, \ldots, r$, it follows that such system is equivalent to

$$\begin{aligned} x &\equiv (q^{a_1}-1)^{-1} \mod n \\ x &\equiv (2-q^{a_2})(q^{a_2}-1)^{-1} \mod n \\ x &\equiv (3-2q^{a_3})(q^{a_3}-1)^{-1} \mod n \\ &\vdots \\ x &\equiv [r-(r-1)q^{a_r}](q^{a_r}-1)^{-1} \mod n, \end{aligned}$$

where $(q^{a_i}-1)^{-1}$ denotes the multiplicative inverse of $(q^{a_i}-1)$ modulo n.

We know that the last system has a solution if and only if

$$[j-(j-1)q^{a_j}](q^{a_j}-1)^{-1} \equiv [i-(i-1)q^{a_i}](q^{a_i}-1)^{-1} \mod n$$

for all $i, j = 2, \ldots, r$ and

$$(q^{a_1}-1)^{-1} \equiv [i-(i-1)q^{a_i}](q^{a_i}-1)^{-1} \mod n$$

for all $i = 2, \ldots, r$. This fact means that

$$n | [(j-(j-1)q^{a_j})(q^{a_j}-1)^{-1} - (q^{a_1}-1)^{-1}]$$

for every $j = 2, \ldots, r$, i.e., $n | \gcd(t_2, \ldots, t_r)$, where

$$t_j = [(j-(j-1)q^{a_j})(q^{a_j}-1)^{-1} - (q^{a_1}-1)^{-1}]$$

for all $j = 2, \ldots, r$.

Let C be the cyclic code whose defining is the q-coset $\mathbb{C}_x$. From construction, the defining set of C, i.e., the coset $\mathbb{C}_x$, contains the sequence $x, x+1, \ldots, x+r$ of $r+1$ consecutive integers. From the BCH bound, the minimum distance d of C satisfies $d \geq r+2$. Since $|\mathbb{C}_x| = m^*$, C has dimension $n-m^*$. We then obtain an $[n, n-m^*, d \geq r+2]_q$ code, as required. □

If the code length is prime we have the following particular case of Theorem 5.10.

Corollary **5.4** *Let* $q \geq 3$ *be a prime power and* $n > m$ *be a prime number such that* $\gcd(q, n) = 1$*, where* $m = \text{ord}_n(q) \geq r+2$ *and* $1 \leq r, a_1, a_2, \ldots, a_r < m$ *are integers. Assume that* $n | \gcd(t_2, \ldots, t_r)$*, where* $t_j = [(j-(j-1)q^{a_j})$ $(q^{a_j}-1)^{-1} - (q^{a_1}-1)^{-1}]$ *for every* $j = 2, \ldots, r$ *and* $a_1, a_2, \ldots, a_r$ *are integers such that* $1 \leq a_1 + a_2 + \ldots + a_r < m$ *(the operations are performed modulo* n*). Then there exists an* $[n, n-m^*, d \geq r+2]_q$ *cyclic code.*

Proof: Notice that since n is prime, it follows that $\gcd(q^{a_i}-1, n) = 1$ for every $i = 1, 2, \ldots, r$, because $a_1, a_2, \ldots, a_r < m$. We next apply Theorem 5.10 to obtain the desired result. □

In order to proceed further, we will denote by $\mathbb{C}_{-x}$ the coset of $-x$, where $-x$ is taken modulo n. With this notation we have the following result.

Theorem **5.11** *Assume all hypotheses of Theorem 5.10 hold. Let* C *be the cyclic code with defining set* $\mathbb{C}_x$*, where* $\mathbb{C}_x$ *is a coset containing* $r+1$ *consecutive integers. If* $\mathbb{C}_x \neq \mathbb{C}_{-x}$ *then there exists an* $[[n, n-2m^*, d \geq r+2]]_q$ *quantum code.*

Proof: From [1, Lemma 1], C contains its Euclidean dual code $C^{\perp}$. The dimension and the minimum distance of the corresponding quantum code follow directly from Theorem 5.10 and from Lemma 5.6. □

Let us present some examples of how our construction works.

Example **5.7** *Consider that $q = 5$ and $n = 11$; hence $m = \mathrm{ord}_{11}(5) = 5$. The 5-cosets are given by $\mathbb{C}_0 = \{0\}$, $\mathbb{C}_1 = \{1, 5, 3, 4, 9\}$ and $\mathbb{C}_2 = \{2, 10, 6, 8, 7\}$. If C_1 is the cyclic code with defining set $\mathbb{C}_1$, then C_1 is a dual-containing code with parameters $[11, 6, d \geq 4]_5$. From Lemma 5.6, one can get an $[[11, 1, d \geq 4]]_5$ code.*

Let us now take $q = 17$ and $n = 19$; so $m = \mathrm{ord}_{19}(17) = 9$. If C_1 is the code with defining set $\mathbb{C}_1 = \{1, 17, 4, 11, 16, 6, 7, 5, 9\}$ we obtain an $[[19, 1, d \geq 5]]_{17}$ code.

Similarly, we can construct an $[61, 56, d \geq 3]_9$ code C_2 with defining set $\mathbb{C}_8 = \{8, 11, 38, 37, 28\}$. We know that C_2 is a dual-containing code, so an $[[61, 51, d \geq 3]]_9$ quantum code exists.

We can also construct an $[67, 64, d \geq 3]_{29}$ dual-containing code with defining set $\mathbb{C}_{12} = \{12, 13, 42\}$. Hence, there exists an $[[67, 61, d \geq 3]]_{29}$ quantum code.

The existence of an $[35, 31, d \geq 3]_{13}$ dual-containing code generates an $[[35, 27, d \geq 3]]_{13}$ quantum code. An $[35, 31, d \geq 3]_{27}$ dual-containing code with defining set $\mathbb{C}_3 = \{3, 11, 17, 4\}$ guarantees the existence of an $[[35, 27, d \geq 3]]_{27}$ quantum code. An $[73, 70, d \geq 3]_{64}$ dual-containing code with defining set $\mathbb{C}_{21} = \{22, 21, 30\}$ exists, so there exists an $[[73, 67, d \geq 3]]_{64}$ quantum code.

Example **5.8** *In this example, we construction cyclic codes whose defining set consists of two q-cosets (the idea is the same as that presented in Theorem 5.10). An $[35, 27, d \geq 4]_{27}$ dual-containing code C with defining set consisting of $\mathbb{C}_2$ and $\mathbb{C}_3$ ensures the existence of an $[[35, 19, d \geq 4]]_{27}$ quantum code. Taking the cosets $C_{14} = \{14, 20, 30\}$ and C_{21} one has an $[[73, 61, d \geq 4]]_{64}$ quantum code. Similarly, an $[[63, 51, d \geq 3]]_{11}$ quantum code (coset C_{43}) and an $[[63, 39, d \geq 4]]_{11}$ code (cosets C_{43} and C_{20}) can be constructed. Analogously, an $[[63, 51, d \geq 3]]_{23}$ and an $[[63, 45, d \geq 4]]_{23}$ quantum code (cosets C_4 and C_{27}) can be constructed.*

In this section we compare the parameters of our quantum BCH codes with the ones available in the literature. The codes available in the literature derived from Steane's code construction are generated by the same method presented in [16, Table I] by considering the criterion for classical Euclidean dual-containing BCH codes given in [1, Theorems 3 and 5].

Let us fix the notation:

- $[[n, k, d]]_q$ are the parameters of the new quantum codes;
- $[[n^{'}, k^{'}, d^{'}]]_q =$ $[[n^{'}, n^{'} - 2m(\lceil(\delta - 1)(1 - 1/q)\rceil), d^{'} \geq \delta]]_q$ are the parameters of quantum codes available in [1];
- $[[n^{''}, k^{''}, d^{''}]]_q$ are the parameters of quantum BCH codes derived from Steane's code construction shown in [6, Corollary 4].

Table 1 displays a comparison of the parameters of some CSS codes constructed here with the parameters of the CSS codes shown in [1], and Table 2 shows a comparison between our CSS codes with the quantum codes derived from the nonbinary Steane's construction (see Corollary 5.2).

Tables 3 and 4 show our codes obtained from Construction I and from Theorem 5.4 in Construction II, respectively. Table 5 presents some codes generated from Construction III, and Table 6 displays some codes generated from Construction IV. Finally, Table 7 exhibited some codes derived from Construction V.

Checking the parameters of the our quantum BCH codes tabulated, one can see that our codes have parameters better than the ones available in the literature. In other words, fixing the code length n and the minimum distance d (or the lower bound for the minimum distance d, since the true minimum distance of BCH are not known in general), the quantum BCH codes constructed here achieve greater values of the number of qudits than the quantum BCH codes available in the literature.

Remark **5.2** *The procedure of code comparison exhibited above will be adopted throughout the entire book in order to perform the comparison among the parameters of the quantum codes constructed here with the parameters of the quantum codes available in the literature. In other words: to compare the parameters of an $[n, k_1, d]_q$ quantum code $\mathbb{Q}_1$ constructed here, we perform a searching for a quantum code of length n and minimum distance d. If such code $\mathbb{Q}_2$ is an $[n, k_2, d]_q$ code with $k_1 > k_2$, then $\mathbb{Q}_1$ is better than $\mathbb{Q}_2$; if $k_2 > k_1$ it implies that $\mathbb{Q}_2$ is better than $\mathbb{Q}_1$. In many cases we fix the code length and the lower bound for the minimum distance as it was said above (see Tables 1 to 7 to see this), after comparing the code dimension, as was done earlier. This criterion of code comparison is usual in the literature.*

Note that our $[[1093, 1079, d \geq 3]]_3$ code has the same parameters of the corresponding Hamming code; our $[[71, 61, d \geq 3]]_5$ code can be compared with distance three codes obtained by shortening Hamming codes.

Table 1: Code Comparison

Our CSS codes	CSS codes in [1]
$[[n,k,d]]_q$	$[[n^{'},k^{'},d^{'}]]_q$
$[[40,30,d\geq 4]]_9$	$[[40,28,d^{'}\geq 4]]_9$
$[[40,20,d\geq 7]]_9$	—
$[[30,7,d\geq 8]]_{11}$	—
$[[61,55,d\geq 3]]_{13}$	$[[61,49,d^{'}\geq 3]]_{13}$
$[[84,74,d\geq 4]]_{13}$	$[[84,72,d^{'}\geq 4]]_{13}$
$[[84,70,d\geq 5]]_{13}$	$[[84,68,d^{'}\geq 5]]_{13}$
$[[84,66,d\geq 6]]_{13}$	$[[84,64,d^{'}\geq 6]]_{13}$
$[[91,85,d\geq 3]]_{16}$	$[[91,79,d^{'}\geq 3]]_{16}$
$[[144,126,d\geq 6]]_{17}$	$[[144,124,d^{'}\geq 6]]_{17}$
$[[144,122,d\geq 7]]_{17}$	$[[144,120,d^{'}\geq 7]]_{17}$
$[[144,118,d\geq 8]]_{17}$	$[[144,116,d^{'}\geq 8]]_{17}$
$[[127,121,d\geq 3]]_{19}$	$[[127,115,d^{'}\geq 3]]_{19}$

Table 2: Code Comparison

Our CSS codes	q-ary Steane's construction
$[[n,k,d]]_q$	$[[n^{''},k^{''},d^{''}]]_q$
$[[19,13,d\geq 3]]_7$	—
$[[13,7,d\geq 3]]_9$	—
$[[19,13,d\geq 3]]_{11}$	—
$[[61,55,d\geq 3]]_{13}$	$[[61,52,d^{''}\geq 3]]_{13}$
$[[91,85,d\geq 3]]_{16}$	$[[91,82,d^{''}\geq 3]]_{16}$
$[[127,121,d\geq 3]]_{19}$	$[[127,118,d^{''}\geq 3]]_{19}$
$[[13,5,d\geq 3]]_5$	—
$[[13,5,d\geq 3]]_8$	—
$[[13,7,d\geq 3]]_3$	—
$[[43,31,d\geq 3]]_7$	—
$[[73,61,d\geq 3]]_9$	—
$[[1093,1079,d\geq 3]]_3$	$[[1093,1072,d^{''}\geq 3]]_3$

Table 3: Code Comparison

Our CSS codes	CSS codes in [1]
$[[n,k,d]]_q$	$[[n',k',d']]_q$
$[[11,1,d\geq 4]]_3$	—
$[[13,1,d\geq 4]]_3$	—
$[[1093,1079,d\geq 3]]_3$	$[[1093,1065,d'\geq 3]]_3$
$[[31,19,d\geq 4]]_5$	$[[31,13,d'\geq 4]]_5$
$[[31,13,d\geq 5]]_5$	$[[31,7,d'\geq 5]]_5$
$[[71,61,d\geq 3]]_5$	$[[71,51,d'\geq 3]]_5$
$[[71,51,d\geq 4]]_5$	$[[71,41,d'\geq 4]]_5$
$[[73,61,d\geq 4]]_8$	$[[73,55,d'\geq 4]]_8$
$[[73,55,d\geq 5]]_8$	$[[73,49,d'\geq 5]]_8$
$[[73,49,d\geq 6]]_8$	$[[73,43,d'\geq 6]]_8$
$[[73,43,d\geq 7]]_8$	$[[73,37,d'\geq 7]]_8$

Table 4: Code Comparison

Our CSS codes	Steane's code construction
$[[n,k,d]]_q$	$[[n'',k'',d'']]_q$: L, L'
$[[31,19,d\geq 4]]_5$	$[[31,16,d''\geq 4]]_5$: $[31,22,4]_5$, $[31,25,3]_5$
$[[31,13,d\geq 5]]_5$	$[[31,10,d''\geq 5]]_5$: $[31,19,5]_5$, $[31,22,4]_5$
$[[73,61,d\geq 4]]_8$	$[[73,58,d''\geq 4]]_8$: $[73,64,4]_8$, $[73,67,3]_8$
$[[73,55,d\geq 5]]_8$	$[[73,52,d''\geq 5]]_8$: $[73,61,5]_8$, $[73,64,4]_8$
$[[73,49,d\geq 6]]_8$	$[[73,46,d''\geq 6]]_8$: $[73,58,6]_8$, $[73,61,5]_8$
$[[73,43,d\geq 7]]_8$	$[[73,40,d''\geq 7]]_8$: $[73,55,7]_8$, $[73,58,6]_8$

Table 5: Code Comparison

Our codes (Construction III)	Steane's code construction
$[[n,k,d]]_q$	$[[n'',k'',d'']]_q$
$[[31,22,d\geq 4]]_5$	$[[31,16,d''\geq 4]]_5$
$[[31,16,d\geq 5]]_5$	$[[31,10,d''\geq 5]]_5$
$[[71,56,d\geq 4]]_5$	$[[71,46,d''\geq 4]]_5$
$[[73,64,d\geq 4]]_8$	$[[73,58,d''\geq 4]]_8$
$[[73,58,d\geq 5]]_8$	$[[73,52,d''\geq 5]]_8$
$[[40,36,3]]_9$ (MDS)	
$[[60,56,3]]_{11}$ (MDS)	

Table 6: Code Comparison

Our Hermitian Codes (Construction IV)	Hermitian Codes in [1]
$[[n,k,d]]_q$	$[[n^{'},k^{'},d^{'}]]_q$
$[[17,13,3]]_4$ (MDS)	
$[[17,9,5]]_4$ (MDS)	
$[[13,9,3]]_5$ (MDS)	
$[[312,298,d \geq 5]]_5$	$[[312,296,d^{'} \geq 5]]_5$
$[[312,294,d \geq 6]]_5$	$[[312,292,d^{'} \geq 6]]_5$
$[[312,290,d \geq 7]]_5$	$[[312,288,d^{'} \geq 7]]_5$
$[[312,286,d \geq 8]]_5$	$[[312,284,d^{'} \geq 8]]_5$
$[[312,282,d \geq 9]]_5$	$[[312,280,d^{'} \geq 9]]_5$
$[[312,278,d \geq 10]]_5$	$[[312,276,d^{'} \geq 10]]_5$
$[[312,274,d \geq 11]]_5$	$[[312,272,d^{'} \geq 11]]_5$
$[[312,270,d \geq 12]]_5$	$[[312,268,d^{'} \geq 12]]_5$
$[[144,128,d \geq 5]]_7$	$[[144,120,d \geq 5]]_7$
$[[144,122,d \geq 6]]_7$	$[[144,114,d \geq 6]]_7$
$[[144,116,d \geq 7]]_7$	$[[144,108,d \geq 7]]_7$
$[[144,114,d \geq 8]]_7$	$[[144,102,d \geq 8]]_7$
$[[144,108,d \geq 9]]_7$	$[[144,96,d \geq 9]]_7$
$[[144,102,d \geq 10]]_7$	$[[144,90,d \geq 10]]_7$
$[[144,100,d \geq 11]]_7$	$[[144,84,d \geq 11]]_7$

The codes $[[67, 61, d \geq 3]]_{29}$ and $[[73, 67, d \geq 3]]_{64}$ shown in Table 7 have parameters satisfying $n + 2 - k - 2d \leq 2$; the parameters of the codes $[[11, 1, d \geq 4]]_5$, $[[35, 27, d \geq 3]]_{13}$ and $[[35, 27, d \geq 3]]_{27}$, satisfy $n+2-k-2d \leq 4$. The $[[11, 1, d \geq 4]]_5$ code is comparable to the $[[17, 9, 4]]_5$ code shown in [5], and the $[[61, 51, d \geq 3]]_9$ code is comparable to the $[[65, 51, 4]]_9$ code shown in [5].

5.2 BCH codes - part II

In this section we construct more families of quantum codes derived from BCH codes. The codes constructed here can be found in our paper [10].

The first construction generates quantum codes with parameters

(i) $[[n, n - 4(c - 2) - 2, d \geq c]]_q$, where $n = q^4 - 1$, and $3 \leq c \leq q^2$;

The second one produces codes with parameters

Table 7: Our quantum codes

Parameters of the new codes
$[[11, 1, d \geq 4]]_5$
$[[19, 1, d \geq 5]]_{17}$
$[[35, 27, d \geq 3]]_{13}$
$[[35, 27, d \geq 3]]_{27}$
$[[35, 19, d \geq 4]]_{27}$
$[[51, 35, d \geq 3]]_{32}$
$[[61, 51, d \geq 3]]_9$
$[[63, 51, d \geq 3]]_{11}$
$[[63, 39, d \geq 4]]_{11}$
$[[63, 51, d \geq 3]]_{23}$
$[[63, 45, d \geq 4]]_{23}$
$[[67, 61, d \geq 3]]_{29}$
$[[73, 67, d \geq 3]]_{64}$
$[[73, 61, d \geq 4]]_{64}$

(ii) $[[n, n - 2mc - 2, d \geq c + 2]]_q$, for all $1 \leq\ c \leq q^2 - 2$;

(iii) $[[n, n - 2m(q^2 - 1) - 2, d \geq q^2 + 2]]_q$;

(iv) $[[n, n - 2m(c - 1) - 2, d \geq c + 2]]_q$, for all $q^2 + 1 \leq c \leq 2q^2 + 2$;

(v) $[[n, n - 4m(q^2 - 1) - 2, d \geq 2q^2 + 2]]_q$, for all $q^2 + 1 \leq c \leq 2q^2 + 2$, where $n = q^{2m} - 1$, $q \geq 4$ is a prime power, and $m = \mathrm{ord}_n(q^2) \geq 3$.

The third construction generates families of quantum codes with parameters

(vi) $[[n, n - m(2c - 1) - 2, d \geq c + 2]]_q$, for all $1 \leq\ c \leq q - 2$;

(vii) $[[n, n - m(2q - 3) - 2, d \geq q + 1]]_q$;

(viii) $[[n, n - m(2q - 1) - 1, d \geq q + 3]]_q$;

(ix) $[[n, n - m(2c - 4) - 2, d \geq c + 2]]_q$;

(x) $[[n, n - m(4q - 8) - 2, d \geq 2q]]_q$;

(xi) $[[n, n - m(4q - 5) - 2, d \geq 2q + 2]]_q$, where $q + 1 < c < 2q - 2$; where $n = q^m - 1$, $q \geq 4$ is a prime power, and $m = \mathrm{ord}_n(q) \geq 3$.

We need to recall three useful lemmas from [1].

Lemma **5.7** *[1, Lemma 1] Assume that* $\gcd(q, n) = 1$. *A cyclic code of length* n *over* $\mathbb{F}_q$ *with defining set* Z *contains its Euclidean dual code if and only if* $Z \cap Z^{-1} = \emptyset$, *where* $Z^{-1} = \{-z \bmod n | z \in Z\}$.

Lemma **5.8** *Assume that* $\gcd(q, n) = 1$. *A cyclic code of length* n *over* $\mathbb{F}_{q^2}$ *with defining set* Z *contains its Hermitian dual code if and only if* $Z \cap Z^{-q} = \emptyset$, *where* $Z^{-q} = \{-qz \bmod n | z \in Z\}$.

Lemma **5.9** *(Hermitian Construction) If there exists a classical linear* $[n, k, d]_{q^2}$ *code* D *such that* $D^{\perp_H} \subset D$, *then there exists an* $[[n, 2k - n, \geq d]]_q$ *stabilizer code that is pure to* d. *If the minimum distance* $d^{\perp_H}$ *of* $D^{\perp_H}$ *exceeds* d, *then the stabilizer code is pure and has minimum distance* d.

We utilize the notation $\mathbb{C}_{[a]}$ to denote the cyclotomic coset containing a, where a is not necessarily the smallest number in $\mathbb{C}_{[a]}$.

5.2.1 Construction I: Codes of length $q^4 - 1$ over $\mathbb{F}_{q^2}$

Let us prove the first result.

Lemma **5.10** *Let* $n = q^4 - 1$, *where* $q \geq 3$ *is a prime power, and consider the first* $q^2 - 1$ q^2*-ary cosets modulo* n *given by*

$$\begin{aligned} &\mathbb{C}_{[q^2+1]}, \\ \mathbb{C}_{[q^2+2]} &= \{q^2 + 2, \quad 1 + 2q^2\}, \\ &\vdots \\ \mathbb{C}_{[2q^2-1]} &= \{2q^2 - 1, \quad 1 + (q^2 - 1)q^2\}. \end{aligned}$$

Then the following hold:

(a) $\mathbb{C}_{[q^2+1]}$ *contains only one element;*

(b) *each of the other cosets contains two elements;*

(c) *each of these cosets are mutually disjoint.*

Proof: Note first that the inequality $n > 1 + (q^2 - 1)q^2$ holds.

(a) This follows from the fact that $(q^2 + 1)q^2 \equiv q^2 + 1 \bmod n$.

(b) We prove that each of the cosets $\mathbb{C}_{[q^2+2]}$, $\mathbb{C}_{[2q^2-1]}$ has exactly two elements. To do this, assume that $q^2 + j \equiv 1 + jq^2 \bmod n$, where $j = 2, \ldots, q^2 + 1$. Because $1 + jq^2 < n$, we have $q^2 + j = 1 + jq^2$; hence, $j - 1 = (j - 1)q^2$, which is a contradiction.

(c) It is clear that coset $\mathbb{C}_{[q^2+1]}$ is disjoint of the other cosets, since it has only one element. Assume next that $\mathbb{C}_{[q^2+i]} = \mathbb{C}_{[q^2+j]}$, where $2 \leq i, j \leq q^2 - 1$, where $i \neq j$, Thus either $q^2 + i \equiv q^2 + j \bmod n$ or $q^2+i \equiv (q^2+j)q^2 \bmod n$, where $2 \leq i, j \leq q^2-1$. Since $2q^2+1 < q^4-1$ and $1+(q^2-1)q^2 < q^4-1$ hold, such inequalities imply that $q^2+i = q^2+j$ or $q^2 + i = 1 + jq^2$. The first case implies $i = j$, a contradiction, and the second implies $q^2|(i-1)$, which is also a contradiction. Therefore, all these cosets are mutually disjoint. The proof is complete.

□

In the sequence we use Lemma 5.10 to show how to construct quantum codes of length $n = q^4 - 1$.

Theorem **5.12** *Let $q \geq 3$ be a prime power and $n = q^4 - 1$. Then there exists an $[[n, n - 4(q^2 - 2) - 2, d \geq q^2]]_q$ quantum error-correcting code.*

Proof: Let us consider C as the cyclic code generated by the product of the minimal polynomials

$$g(x) = M^{(q^2+1)}(x)M^{(q^2+2)}(x) \cdot \ldots \cdot M^{(q^2+j)}(x),$$

where $1 \leq j \leq q^2 - 1$. We show first that C is Hermitian dual-containing. Seeking a contradiction, we suppose $Z \bigcap Z^{-q} \neq \emptyset$. Thus there exist i, j, where $1 \leq i, j \leq q^2 - 1$ such that $\mathbb{C}_{[q^2+j]} = \mathbb{C}_{[-q(q^2+i)]}$. Hence, $q^2 + j \equiv -q(q^2+i)q^{2k}$, where $k = 0$ or $k = 1$. If $k = 0$, we have $q^3+qi+q^2+j < q^4-1$, so $q^2 + j = -q^3 - qi$, a contradiction. If $k = 1$, since $\gcd(q^2, n) = 1$ and $q^4 \equiv 1 \bmod n$, we have

$$\begin{aligned} q^2 + j \equiv -q^3(q^2 + i) \bmod n \Longrightarrow \\ q^5 + q^3 i \equiv -(q^2 + j) \bmod n \Longrightarrow \\ q + q^3 i \equiv -(q^2 + j) \bmod n, \end{aligned}$$

where $1 \leq i, j, q^2 - 1$.

If $i < q$ then $iq^3+q+q^2+j < q^4-1$, so $q+q^3i = -(q^2+j)$, a contradiction. On the other hand, if $i \geq q$, from the division algorithm we write $i = lq + r$, where r, l are integers such that $0 \leq r \leq q-1$. We also have $0 \leq l \leq q-1$; hence,

$$q + q^3 i = q + q^3(lq + r) \equiv q + l + q^3 r \bmod n.$$

Computing $q + l + q^3 r + q^2 + j$ we obtain

$$q + l + q^3 r + q^2 + j < q^3(q-1) + 2q + 2q^2 = q^4 - q^3 + 2q + 2q^2.$$

Since $q^3 > 2q^2 + 2q + 1$, it follows that $q + l + q^3 r + q^2 + j < q^4 - 1$; hence, $q + l + q^3 r = -q^2 - j$, a contradiction. Consequently, C is Hermitian dual containing.

We next compute the minimum distance and the dimension of C. Since the defining set of C contains the sequence $q^2+1, q^2+2, \ldots, 2q^2-1$, it follows from the BCH bound that C has minimum distance greater than or equal to q^2. On the other hand, from Lemma 5.10, the defining set of C has $2(q^2-2)+1$ elements. Hence, $g(x)$ has degree $\deg(g(x)) = 2(q^2-2)+1$, so C has dimension $n - 2(q^2-2) - 1$, i.e., C is an $[n, n-2(q^2-2)-1, d \geq q^2]_{q^2}$ code. Applying Lemma 5.5, there exists an $[[n, n-4(q^2-2)-2, d \geq q^2[]_q$ quantum code. The proof is complete. □

Corollary **5.5** *Let $q \geq 3$ be a prime power and $n = q^4 - 1$. Then there exists an $[[n, n-4(c-2)-2, d \geq c[]_q$, where $3 \leq c \leq q^2 - 1$*

Proof: It suffices to consider C as the cyclic code generated by

$$M^{(q^2+1)}(x) M^{(q^2+2)}(x) \cdot \ldots \cdot M^{(q^2+c-1)}(x),$$

after proceeding similarly to the proof of Theorem 5.12. □

Example **5.9** *As an example, let us consider $m = 2$ and $q = 3$. Let C be generated by $M^{(10)}(x) M^{(11)}(x)$. Applying Theorem 5.12 we have an $[[80, 74, d \geq 3]]_3$ code.*

5.2.2 Construction II: Hermitian non-narrow-sense BCH codes

In this subsection we construct suitable Hermitian dual-containing non-narrow-sense BCH codes with good parameters in order to obtain good quantum codes derived from them.

We start with the following result.

Lemma **5.11** *Let $q \neq 2$ be a prime power and $n = q^{2m} - 1$, where $m = \operatorname{ord}_n(q^2) \geq 3$. If $s = \sum_{i=0}^{m-1} (q^2)^i$, then the q^2-coset $\mathbb{C}_{[s]}$ has only one element.*

Proof: We know that $\gcd(q^2, n) = 1$ and $q^{2m} \equiv 1 \bmod n$. The result follows from direct computation.

$$
\begin{aligned}
sq^{2j} = \left(\sum_{i=0}^{m-1} (q^2)^i \right) q^{2j} & \\
&= q^{2j}(q^2)^{m-1} + q^{2j}(q^2)^{m-2} + \cdots + q^{2j}q^2 + q^{2j} = \\
&= q^{2j}q^{2m}q^{-2} + q^{2j}q^{2m}q^{-4} + \cdots + q^{2j}q^{2m}q^{-2j+2} + \\
&+ q^{2j}q^{2m}q^{-2j} + q^{2j}q^{2m}q^{-2j-2} + \cdots + q^{2j}q^2 + q^{2j} \\
&\equiv (\operatorname{mod} n) q^{2j}q^{-2} + q^{2j}q^{-4} + \cdots + q^{2j}q^{-2j+2} + \\
&+ q^{2j}q^{-2j} + q^{2m-2} + q^{2m-4} + \cdots + q^{2j}q^2 + q^{2j} = \\
&= (q^2)^{m-1} + (q^2)^{m-2} + \cdots + (q^2)^{j+1} + (q^2)^j + \\
&+ (q^2)^{j-1} + (q^2)^{j-2} + \cdots + q^2 + 1 = \\
&= \sum_{i=0}^{m-1} (q^2)^i = s
\end{aligned}
$$

□

Lemma **5.12** *Let $q \neq 2$ be a prime power and $n = q^{2m} - 1$, where $m = \operatorname{ord}_n(q^2) \geq 3$. Let $s = \sum_{i=0}^{m-1} (q^2)^i$. Then the following results hold:*

(a) *the q^2-ary cosets of the form $\mathbb{C}_{[s+i]}$ are mutually disjoints, where $1 \leq i \leq q^2 - 1$;*

(b) *the q^2-ary cosets of the form $\mathbb{C}_{[s-j]}$ are mutually disjoints, where $1 \leq j \leq q^2 - 1$;*

(c) *the q^2-ary cosets of the form $\mathbb{C}_{[s+i]}$ are mutually disjoints with the q^2-ary cosets of the form $\mathbb{C}_{[s-j]}$, where $1 \leq i, j \leq q^2 - 1$.*

Proof: We only show Item (a). Items (b) and (c) are left to the reader.

(a) Assume that there exist $i \neq j$, where $1 \leq i, j \leq q^2 - 1$ such that $\mathbb{C}_{[s+i]} = \mathbb{C}_{[s+j]}$. The there exists $0 \leq t \leq m - 1$ such that $s + i \equiv$

$(s+j)q^{2t} \bmod n$. From Lemma 5.11, we know that $sq^{2t} \equiv s \bmod n$. Since $\gcd(q^2, n) = 1$ and $q^{2m} \equiv 1 \bmod n$, then one has

$$\begin{aligned} s + i \equiv (s+j)q^{2t} &\equiv s + jq^{2t} \bmod n \\ &\Longrightarrow i \equiv jq^{2t} \bmod n. \end{aligned}$$

Because $1 \leq i, j \leq q^2 - 1$, it follows that

$$i \equiv jq^{2t} \bmod n \Longrightarrow i = jq^{2t}.$$

If $t = 0$, then $i = j$, a contradiction; if $t \geq 1$, the equality $i = jq^{2t}$ does not hold. Therefore, it follows that the cosets $\mathbb{C}_{[s+i]}$ and $\mathbb{C}_{[s+j]}$ are disjoint. The proof is complete. □

Lemma **5.13** *Let $q \geq 4$ be a prime power and $n = q^{2m} - 1$, where $m =$ $\mathrm{ord}_n(q^2) \geq 3$. Let $s = \sum_{i=0}^{m-1} (q^2)^i$. Then the following hold:*

(a) *the cosets of the form $\mathbb{C}_{[s+i]}$, where $1 \leq i \leq q^2 - 1$, contain m elements;*

(b) *the cosets of the form $\mathbb{C}_{[s-j]}$, $1 \leq j \leq q^2 - 1$, contain m elements.*

Proof: We prove Item (a). Item (b) is left as exercise.

(a) The elements of $\mathbb{C}_{[s+i]}$ are of the form $(s+i)q^{2t}$, where $0 \leq t \leq m-1$ for all $1 \leq i \leq q^2 - 1$. Since $\gcd(q^2, n) = 1$, $q^{2m} \equiv 1 \bmod n$ and $sq^{2t} \equiv s \bmod n$, it follows that

$$(s+i)q^{2t} \equiv s + iq^{2t} \bmod n.$$

Let us consider that $0 \leq t \leq m-2$. We then have

$$\begin{aligned} & s + iq^{2t} \\ & \quad < (q^{2m} - 1)/(q^2 - 1) + q^{2m-2} \\ & \quad \leq (q^{2m} - 1)/15 + (q^{2m} - 1)/15 \\ & \quad < q^{2m} - 1. \end{aligned}$$

Hence, the first $m - 1$ elements belonging to $\mathbb{C}_{[s+i]}$ are distinct, for all $1 \leq i \leq q^2 - 1$, i.e., the cosets $\mathbb{C}_{[s+i]}$ contain m elements, because $m - 1 > m/2$. □

Lemma **5.14** *Let* $q \geq 4$ *be a prime power and* $n = q^{2m} - 1$*, where* $m = \mathrm{ord}_n(q^2) \geq 3$*. Let* $s = \sum_{i=0}^{m-1} (q^2)^i$*. If* C *is the cyclic code generated by the product of the minimal polynomials*

$$M^{(s)}(x)M^{(s+1)}(x)\cdots M^{(s+i)}(x)M^{(s-1)}(x)\cdots M^{(s-j)}(x),$$

where $1 \leq i, j \leq q^2 - 1$*, then* C *is Hermitian dual-containing.*

Proof: According to Lemma 5.4,we have to show that $Z \bigcap Z^{-q} = \emptyset$. Forcing a contradiction, we assume that $Z \bigcap Z^{-q} \neq \emptyset$. The cases concerning the coset $\mathbb{C}_{[s]}$ are immediate. Assume first that $\mathbb{C}_{[s+j]} = \mathbb{C}_{[-q(s+i)]}$, $1 \leq i, j \leq q^2 - 1$. Then there exists $0 \leq h \leq m - 1$ such that

$$s + j \equiv -q(s + i)q^{2h} \bmod n.$$

Because $\gcd(q^2, n) = 1$, $q^{2m} \equiv 1 \bmod n$ and $sq^{2t} \equiv s \bmod n$ for all $0 \leq t \leq m - 1$, we obtain

$$s + j \equiv -qs - qiq^{2h} \bmod n,$$

where $0 \leq h \leq m - 1$. We now compute the expression $s + j + q(s + iq^{2h})$, $0 \leq h \leq m - 1$. If $h \leq m - 2$, one has

$$\begin{aligned} s + j + q(s + iq^{2h}) & \\ &\leq \frac{q^{2m} - 1}{q^2 - 1} + j + q\frac{q^{2m} - 1}{q^2 - 1} + iq^{2m-3} \\ &\leq \frac{q^{2m} - 1}{q - 1} + (q^2 - 1)(1 + q^{2m-3}). \end{aligned}$$

It is easy to see that

$$\frac{q^{2m} - 1}{q - 1} + (q^2 - 1)(1 + q^{2m-3}) < q^{2m} - 1.$$

Since $s + j = -qs - iq^{2h+1}$ does not hold, we have a contradiction.

If $h = m - 1$, we will verify the equivalence $s + j \equiv -q(s + i)q^{2m-2} \bmod n$:

$$\begin{aligned} s + j \equiv -q(s + i)q^{2m-2} \bmod n & \\ &\Longrightarrow \; j(q^2 - 1) \equiv -iq^{2m-1}(q^2 - 1) \bmod n \\ &\Longrightarrow \; (j + iq^{2m-1})(q^2 - 1) \equiv 0 \bmod n. \end{aligned}$$

Applying the algorithm of division for i and q we have $i = aq + r$, where $0 \leq r < q$. Because $1 \leq i \leq q^2 - 1$ we also have $0 \leq a < q$; hence,

$$\begin{aligned}
&(j + iq^{2m-1})(q^2 - 1) \\
&\qquad \equiv \quad [j + (aq + r)q^{2m-1}](q^2 - 1) \\
&\qquad \equiv \quad (j + a)(q^2 - 1) + r(q^2 - 1)q^{2m-1} \\
&\qquad \equiv \quad (j + a)(q^2 - 1) + rq - rq^{2m-1} \equiv 0 \bmod n \\
&\qquad \Longrightarrow \quad rq^{2m-1} - rq - (j + a)(q^2 - 1) \equiv 0 \bmod n.
\end{aligned}$$

If $r = 0$, it follows that $(j+a)(q^2-1) < q^{2m}-1$, so $(j+a)(q^2-1) \not\equiv 0 \bmod n$. If $r > 0$, then $0 < rq^{2m-1} - rq - (j + a)(q^2 - 1) < q^{2m} - 1$, which is a contradiction.

The cases $\mathbb{C}_{[s+j]} = \mathbb{C}_{[-q(s-i)]}$, $\mathbb{C}_{[s-j]} = \mathbb{C}_{[-q(s+i)]}$ and $\mathbb{C}_{[s-j]} = \mathbb{C}_{[-q(s-i)]}$ are analogous to the previous one, so the proof is omitted. Therefore, C is Hermitian dual-containing, as required. □

Theorem 5.13 given in the following is the main result of this subsection.

Theorem **5.13** *Let $q \geq 4$ be a prime power and $n = q^{2m} - 1$, where $m = \mathrm{ord}_n(q^2) \geq 3$. Then there exists an $[[n, n - 4m(q^2 - 1) - 2, d \geq q^2 + 2]]_q$ quantum error-correcting code.*

Proof: Let C be the cyclic code generated by

$$M^{(s)}(x)M^{(s+1)}(x) \cdot \ldots \cdot M^{(s+q^2-1)}(x)M^{(s-1)}(x) \cdot \ldots \cdot M^{(s-q^2+1)}(x).$$

From Lemmas 5.12 and 5.13, it is easy to see that C is an $[n, n-2m(q^2-1)-1, d \geq 2q^2 + 2]_{q^2}$ code. From Lemma 5.14, C is Hermitian dual containing. Applying the Hermitian construction, an $[[n, n-4m(q^2-1)-2, d \geq 2q^2+2]]_q$ quantum code can be constructed. The proof is complete. □

Corollary **5.6** *Let $q \geq 4$ be a prime power and $n = q^{2m} - 1$, where $m = \mathrm{ord}_n(q^2) \geq 3$. Then there exist quantum codes with parameters*

- $[[n, n - 2mc - 2, d \geq c + 2]]_q$, *where* $1 \leq c < q^2 - 1$;
- $[[n, n - 2m(q^2 - 1) - 2, d \geq q^2 + 2]]_q$;
- $[[n, n - 2m(c - 1) - 2, d \geq c + 2]]_q$, *where* $q^2 + 1 \leq c \leq 2q^2 - 2$.

5.2.3 Construction III: Euclidean non-narrow-sense BCH code

The result given in the sequence is analogous to Lemma 5.11.

Lemma **5.15** *Let* $q \neq 2$ *be a prime power and* $n = q^m - 1$*, where* $m = \mathrm{ord}_n(q) \geq 3$*. If* $s = \sum_{i=0}^{m-1} q^i$*, then the* q*-coset* $\mathbb{C}_{[s]}$ *has only one element.*

Proof: Left to exercise. □

The following two results are analogous to Lemmas 5.12 and 5.13, respectively.

Lemma **5.16** *Let* $q \geq 3$ *be a prime power and* $n = q^m - 1$*, where* $m = \mathrm{ord}_n(q) \geq 3$*. Let* $s = \sum_{i=0}^{m-1} q^i$*. Then the following are true:*

(a) *the* q*-cosets of the form* $\mathbb{C}_{[s+i]}$ *are mutually disjoints, where* $1 \leq i \leq q-1$*;*

(b) *the* q*-cosets of the form* $\mathbb{C}_{[s-j]}$ *are mutually disjoints, where* $1 \leq j \leq q-1$*;*

(c) *the* q*-cosets of the form* $\mathbb{C}_{[s+i]}$ *are mutually disjoints to the* q*-cosets of the form* $\mathbb{C}_{[s-j]}$*, where* $1 \leq i, j \leq q-1$*.*

Lemma **5.17** *Let* $q \geq 4$ *be a prime power and* $n = q^m - 1$*, where* $m = \mathrm{ord}_n(q) \geq 3$*. Let* $s = \sum_{i=0}^{m-1} q^i$*. Then the following hold:*

(a) *the cosets of the form* $\mathbb{C}_{[s+i]}$*, where* $1 \leq i \leq q-1$*, contain* m *elements;*

(b) *the cosets of the form* $\mathbb{C}_{[s-j]}$*, where* $1 \leq j \leq q-1$*, contain* m *elements.*

Lemma **5.18** *Let* $q \geq 4$ *be a prime power and* $n = q^m - 1$*, where* $m = \mathrm{ord}_n(q) \geq 3$*. Let* $s = \sum_{i=0}^{m-1} q^i$*. Let* C *be the cyclic code generated by*

$$M^{(s)}(x)M^{(s+1)}(x) \cdot \ldots \cdot M^{(s+j)}(x)M^{(s-1)}(x) \cdot \ldots \cdot M^{(s-j)}(x),$$

where $1 \leq j \leq q-1$*. Then* C *is Euclidean dual-containing.*

Proof: From Lemma 5.3, it is sufficient to prove that $Z \bigcap Z^{-1} = \emptyset$. Forcing a contradiction, we assume the $Z \bigcap Z^{-1} \neq \emptyset$. The cases concerning the coset $\mathbb{C}_{[s]}$ are trivial.

(1) Assume first that $\mathbb{C}_{[s+i]} = \mathbb{C}_{[-(s+j)]}$, where $1 \leq i, j \leq q-1$. Then there exists $0 \leq t \leq m-1$ such that $s + i \equiv -(s+j) \bmod n$. Since $\gcd(q, n) = 1$, $q^m \equiv 1 \bmod n$ and $sq^t \equiv s \bmod n$, $0 \leq t \leq m-1$, we have

$$s + i \equiv -s - jq^t \bmod n \Longrightarrow 2s \equiv -(i + jq^t).$$

If $0 \leq t \leq m-2$ and because $q \geq 4$, it follows that

$$\begin{aligned} 2s + i + jq^t & \\ &\leq \frac{2q^m - 2}{q-1} + (q-1)(1 + q^{m-2}) \\ &< q^m - 1 \\ &\Longrightarrow 2s + i + jq^t < q^m - 1. \end{aligned}$$

Hence $s + i = -s - jq^t$, a contradiction.

Let us next consider the case $t = m-1$. We know that for each $1 \leq i, j \leq q-3$ we have $2s + i + jq^{m-1} < q^m - 1$; since $s + i = -s - jq^{m-1}$ does not hold, this implies in a contradiction. Analogously, if $j = q-3$ and $1 \leq i \leq q-1$, it follows that $2s + i + jq^{m-1} < q^m - 1$, and because $s + i \neq -s - jq^{m-1}$, we have a contradiction.

If $j \geq q-2$, we have $2s + i + jq^t > q^m - 1$. Let us compute the equivalence $2s \equiv -(i + jq^{m-1}) \bmod n$ for $j = q-2$ and $1 \leq i \leq q-1$.

$$2s \equiv -[i + (q-2)q^{m-1}] \bmod n \Longrightarrow 2s \equiv -i - 1 + 2q^{m-1} \bmod n.$$

As $0 < 2s + i + 1 - 2q^{m-1} < q^m - 1$ and also $2s \neq -i - 1 + 2q^{m-1}$ are true, one has a contradiction.

Let $j = q-1$ and $1 \leq i \leq q-1$. Computing the equivalence $2s \equiv -(i + jq^{m-1}) \bmod n$ we obtain

$$2s \equiv -[i + (q-1)q^{m-1}] \bmod n \Longrightarrow 2s \equiv -i - 1 + q^{m-1} \bmod n.$$

Because $0 < 2s + i + 1 - q^{m-1} < q^m - 1$ and $2s \neq -i - 1 + q^{m-1}$ hold, then the equivalence $2s \equiv -[i + (q-1)q^{m-1}] \bmod n$ does not hold, a contradiction.

(2) Suppose $\mathbb{C}_{[s-i]} = \mathbb{C}_{[-(s-j)]}$, where $1 \leq i, j \leq q-1$. Then there exists $0 \leq t \leq m-1$ such that $s - i \equiv -(s-j)q^t \bmod n$. We have

$$s - i \equiv -s + jq^t \bmod n \Longrightarrow 2s \equiv i + jq^t \bmod n.$$

If $0 \leq t \leq m-2$ then the inequalities $2s < q^m - 1$ and $2s > i + jq^t$ hold, which is a contradiction. If $t = m-1$, then

$$\begin{aligned} 2s \equiv i + jq^{m-1} \bmod n & \\ & \Longrightarrow \ 2(q^m - 1) \equiv (q-1)(i + jq^{m-1}) \bmod n \\ & \Longrightarrow \ (q-1)i + (q-1)jq^{m-1} \equiv 0 \bmod n \\ & \Longrightarrow \ (q-1)i + j - jq^{m-1} \equiv 0 \bmod n \\ & \Longrightarrow \ jq^{m-1} - i(q-1) - j \equiv 0 \bmod n. \end{aligned}$$

Since $0 < jq^{m-1} - i(q-1) - j < q^m - 1$, the equivalence $2s \equiv i + jq^t \bmod n$ does not hold, a contradiction.

(3) Assume that $\mathbb{C}_{[s+i]} = \mathbb{C}_{[-(s-j)]}$, where $1 \leq i, j \leq q-1$. Then there exists $0 \leq t \leq m-1$ such that $s+i \equiv -(s-j)q^t \bmod n$, so $2s \equiv jq^t - i \bmod n$. If $t = 0$ nd $i = j$ we have $2s \equiv 0 \bmod n$, a contradiction. If $0 \leq t \leq m-2$ and $i \neq j$, we know that

$$2s \equiv jq^t - i \bmod n \Longrightarrow (q-1)(jq^t - i) \equiv 0 \bmod n;$$

hence, $-(q^m - 1) < (q-1)(jq^t - i) < q^m - 1$ and $(q-1)(jq^t - i) \neq 0$, a contradiction.

If $t = m-1$, we obtain

$$(q-1)(jq^{m-1} - i) \equiv 0 \bmod n \Longrightarrow jq^{m-1} + i(q-1) - j \equiv 0 \bmod n.$$

Since $0 < jq^{m-1} + i(q-1) - j < q^m - 1$, the equivalence $s+i \equiv -(s-j)q^t \bmod n$ does not hold, a contradiction.

(4) Suppose finally that $\mathbb{C}_{[s-i]} = \mathbb{C}_{[-(s+j)]}$; then $s - i \equiv -(s+j)q^t \bmod n$ for some $0 \leq t \leq m-1$. Thus, $2s \equiv i - jq^t \bmod n$. As in the previous case, if $t = 0$ nd $i = j$ we have $2s \equiv 0 \bmod n$, a contradiction. If $0 \leq t \leq m-2$ and $i \neq j$ we then know that

$$2s \equiv i - jq^t \bmod n \Longrightarrow (q-1)(i - jq^t) \equiv 0 \bmod n,$$

which is a contradiction. Moreover, it is easy to see that the last equivalence does not hold, a contradiction.

Therefore, C is Euclidean dual-containing code, as required. The proof is complete. □

We next recall Corollary 5.2 shown in [6].

Corollary **5.7** *Assume that we have an $[N_0, K_0]$ linear code L which contains its Euclidean dual, $L^{\perp} \leq L$, and which can be enlarged to an $[N_0, K_0^{'}]$ linear code $L^{'}$, where $K_0^{'} \geq K_0 + 2$. Then there exists a quantum code with parameters $[[N_0, K_0 + K_0^{'} - N_0, d \geq \ min\{d, \lceil \frac{q+1}{q} d^{'} \rceil\}]]$, where $d = w(L \backslash L^{'\perp})$ and $d^{'} = w(L^{'} \backslash L^{'\perp})$.*

We are now ready to state the main results of this subsection.

Theorem **5.14** *Let $q \geq 4$ be a prime power and $n = q^m - 1$, where $m = \operatorname{ord}_n(q) \geq 3$. Then there exists an $[[n, n-m(2c-1)-2, d \geq c+2]]_q$ quantum code, for all $1 \leq c \leq q-2$.*

Proof: Let C be the cyclic code generated by

$$M^{(s)}(x)M^{(s+1)}(x) \cdot \ldots \cdot M^{(s+i)}(x)M^{(s-1)}(x) \cdot \ldots \cdot M^{(s-j)}(x),$$

where $1 \leq i+j = c \leq q-2$. It is easy to see that C is an $[n, n-mc-1, d \geq c+2]_q$ code, where $1 \leq c \leq q-2$. Moreover, from Lemma 5.3, C is Euclidean dual-containing.

Let $C^{'}$ be the code generated by

$$M^{(s)}(x)M^{(s+1)}(x) \cdot \ldots \cdot M^{(s+i)}(x)M^{(s-1)}(x) \cdot \ldots \cdot M^{(s-j+1)}(x).$$

We know that $C^{'}$ is an enlargement of C and has parameters $[n, n-m(c-1)-1, d^{'} \geq c+1]_q$. Applying Corollary 5.2 to C and $C^{'}$ we obtain an $[[n, n-m(2c-1)-2, d \geq c+2]]_q$ code, as required. The proof is complete. □

Theorem **5.15** *Let $q \geq 4$ be a prime power and $n = q^m - 1$, where $m = \operatorname{ord}_n(q) \geq 3$. Then there exist quantum codes with parameters*

- $[[n, n-m(2q-3)-2, d \geq q+1]]_q$;
- $[[n, n-m(2q-1)-1, d \geq q+3]]_q$;
- $[[n, n-m(2c-4)-2, d \geq c+2]]_q$;
- $[[n, n-m(4q-8)-2, d \geq 2q]]_q$;
- $[[n, n-m(4q-5)-2, d \geq 2q+2]]_q$, *where $q+1 < c < 2q-2$.*

We now compare the parameters of our codes with the ones shown in the literature

In Table 8, our Hermitian quantum codes have parameters $[[n, n-4(c-2)-2, d \geq c]]_q$, where $3 \leq c \leq q^2$ and $n = q^4 - 1$; $[[n^{'}, k^{'}, d^{'}]]_q = [[n^{'}, n^{'} - 2m\lceil(\delta-1)(1-1/q^2)\rceil, d^{'} \geq \delta]]_q$ are the parameters of the Hermitian quantum codes shown in Theorem 21 in [1], where $m = \operatorname{ord}_n(q^2) = 2$ and $2 \leq \delta \leq \lfloor n(q^m-1)/(q^{2m}-1)\rfloor$.

In Table 9, our quantum codes are obtained from Subsection 5.2.2 and have parameters $[[n, k, d]]_q$ given by

- $[[n, n-2mc-2, d \geq c+2]]_q$, where $1 \leq c < q^2-1$;
- $[[n, n-2m(q^2-1)-2, d \geq q^2+2]]_q$;
- $[[n, n-2m(c-1)-2, d \geq c+2]]_q$, where $q^2+1 \leq c \leq 2q^2-2$.
- $[[n, n-4m(q^2-1)-2, d \geq 2q^2+2]]_q$, where $n = q^{2m}-1$, $q \geq 4$ is a prime power, $m = \text{ord}_n(q^2) \geq 3$;

$[[n^{'}, k^{'}, d^{'}]]_q = [[n^{'}, n^{'} - 2m\lceil(\delta-1)(1-1/q^2)\rceil, d^{'} \geq \delta]]_q$ are the parameters of the Hermitian quantum codes shown in Theorem 21 in [1], where $m = \text{ord}_n(q^2) \geq 3$ and $2 \leq \delta \leq \lfloor n(q^m-1)/(q^{2m}-1)\rfloor$.

In Table 10, our codes are derived from Subsection 5.2.3 and have parameters $[[n, k, d]]_q$ given by

- $[[n, n-m(2c-1)-2, d \geq c+2]]_q$, where $1 \leq c \leq q-2$;
- $[[n, n-m(2q-3)-2, d \geq q+1]]_q$;
- $[[n, n-m(2q-1)-1, d \geq q+3]]_q$;
- $[[n, n-m(2c-4)-2, d \geq c+2]]_q$;
- $[[n, n-m(4q-8)-2, d \geq 2q]]_q$;
- $[[n, n-m(4q-5)-2, d \geq 2q+2]]_q$, where $q+1 < c < 2q-2$.

The parameters $[[n^{''}, k^{''}, d^{''}]]_q$ are the parameters of quantum BCH codes derived from q-ary Steane's construction (see Corollary 5.2) applied to narrow-sense BCH codes. These codes were obtained by the same method presented in Table I in [16] by considering the criterion for classical Euclidean dual-containing BCH codes of Theorems 3 and 5 in [1].

As we can see in Tables 8 to 10, according to the procedure described in Remark 5.2, our quantum codes have parameters better than the ones exhibited in the literature.

References

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

[2] Bose, R.C., Ray-Chaudhuri, D.K.: On a class of error correcting binary group codes. Information and Control **3**, 68-79 (1960)

Table 8: Code Comparison

Our Hermitian codes		Hermitian codes in [1]
$[[n, n-4(c-2)-2, d \geq c]]_q$		$[[n^{'}, k^{'}, d^{'}]]_q$
	$m = 2$, $q = 3$	
$[[80, 74, d \geq 3]]_3$		$[[80, 72, d^{'} \geq 3]]_3$
$[[80, 70, d \geq 4]]_3$		$[[80, 68, d^{'} \geq 4]]_3$
$[[80, 66, d \geq 5]]_3$		$[[80, 64, d^{'} \geq 5]]_3$
$[[80, 62, d \geq 6]]_3$		$[[80, 60, d^{'} \geq 6]]_3$
$[[80, 58, d \geq 7]]_3$		$[[80, 56, d^{'} \geq 7]]_3$
$[[80, 54, d \geq 8]]_3$		$[[80, 52, d^{'} \geq 8]]_3$
$[[80, 50, d \geq 9]]_3$		
	$m = 2$, $q = 4$	
$[[255, 249, d \geq 3]]_4$		$[[255, 247, d^{'} \geq 3]]_4$
$[[255, 245, d \geq 4]]_4$		$[[255, 243, d^{'} \geq 4]]_4$
$[[255, 241, d \geq 5]]_4$		$[[255, 239, d^{'} \geq 5]]_4$
$[[255, 237, d \geq 6]]_4$		$[[255, 235, d^{'} \geq 6]]_4$
$[[255, 233, d \geq 7]]_4$		$[[255, 231, d^{'} \geq 7]]_4$
$[[255, 229, d \geq 8]]_4$		$[[255, 227, d^{'} \geq 8]]_4$
$[[255, 225, d \geq 9]]_4$		$[[255, 223, d^{'} \geq 9]]_4$
$[[255, 221, d \geq 10]]_4$		$[[255, 219, d^{'} \geq 10]]_4$
$[[255, 217, d \geq 11]]_4$		$[[255, 215, d^{'} \geq 11]]_4$
$[[255, 213, d \geq 12]]_4$		$[[255, 211, d^{'} \geq 12]]_4$
$[[255, 209, d \geq 13]]_4$		$[[255, 207, d^{'} \geq 13]]_4$
$[[255, 205, d \geq 14]]_4$		$[[255, 203, d^{'} \geq 14]]_4$
$[[255, 201, d \geq 15]]_4$		$[[255, 199, d^{'} \geq 15]]_4$
$[[255, 197, d \geq 16]]_4$		
	$m = 2$, $q = 5$	
$[[624, 618, d \geq 3]]_5$		$[[624, 616, d^{'} \geq 3]]_5$
$[[624, 614, d \geq 4]]_5$		$[[624, 612, d^{'} \geq 4]]_5$
$[[624, 610, d \geq 5]]_5$		$[[624, 608, d^{'} \geq 5]]_5$
$[[624, 606, d \geq 6]]_5$		$[[624, 604, d^{'} \geq 6]]_5$
$[[624, 602, d \geq 7]]_5$		$[[624, 600, d^{'} \geq 7]]_5$
$[[624, 598, d \geq 8]]_5$		$[[624, 596, d^{'} \geq 8]]_5$
$[[624, 594, d \geq 9]]_5$		$[[624, 592, d^{'} \geq 9]]_5$
$[[624, 590, d \geq 10]]_5$		$[[624, 588, d^{'} \geq 10]]_5$
$[[624, 586, d \geq 11]]_5$		$[[624, 584, d^{'} \geq 11]]_5$
$[[624, 582, d \geq 12]]_5$		$[[624, 580, d^{'} \geq 12]]_5$

Table 9: Code Comparison

Our Hermitian codes		Hermitian codes in [1]
$[[n,k,d]]_q$		$[[n^{'},k^{'},d^{'}]]_q$
	$m=3$, $q=4$	
$[[4095,4087,d\geq 3]]_4$		$[[4095,4083,d^{'}\geq 3]]_4$
$[[4095,4081,d\geq 4]]_4$		$[[4095,4077,d^{'}\geq 4]]_4$
$[[4095,4075,d\geq 5]]_4$		$[[4095,4071,d^{'}\geq 5]]_4$
$[[4095,4069,d\geq 6]]_4$		$[[4095,4065,d^{'}\geq 6]]_4$
$[[4095,4063,d\geq 7]]_4$		$[[4095,4059,d^{'}\geq 7]]_4$
$[[4095,4057,d\geq 8]]_4$		$[[4095,4053,d^{'}\geq 8]]_4$
$[[4095,4051,d\geq 9]]_4$		$[[4095,4047,d^{'}\geq 9]]_4$
$[[4095,4045,d\geq 10]]_4$		$[[4095,4041,d^{'}\geq 10]]_4$
$[[4095,4039,d\geq 11]]_4$		$[[4095,4035,d^{'}\geq 11]]_4$
$[[4095,4033d\geq 12]]_4$		$[[4095,4029,d^{'}\geq 12]]_4$
$[[4095,4027,d\geq 13]]_4$		$[[4095,4023,d^{'}\geq 13]]_4$
$[[4095,4021,d\geq 14]]_4$		$[[4095,4017,d^{'}\geq 14]]_4$
$[[4095,4015,d\geq 15]]_4$		$[[4095,4011,d^{'}\geq 15]]_4$
$[[4095,4009,d\geq 16]]_4$		$[[4095,4005,d^{'}\geq 16]]_4$
$[[4095,4003,d\geq 18]]_4$		$[[4095,3999,d^{'}\geq 18]]_4$
$[[4095,3997,d\geq 19]]_4$		$[[4095,3993,d^{'}\geq 19]]_4$
$[[4095,3949,d\geq 27]]_4$		$[[4095,3945,d^{'}\geq 27]]_4$
$[[4095,3925,d\geq 31]]_4$		$[[4095,3921,d^{'}\geq 31]]_4$
$[[4095,3919,d\geq 32]]_4$		$[[4095,3915,d^{'}\geq 32]]_4$
$[[4095,3913,d\geq 34]]_4$		$[[4095,3909,d^{'}\geq 34]]_4$

Table 10: Code Comparison

Our codes - construction III		Codes derived from [6]
$[[n,k,d]]_q$		$[[n^{''},k^{''},d^{''}]]_q$
	$m=3$, $q=4$	
$[[63,58,d \geq 3]]_4$		$[[63,54,d^{'} \geq 4]]_4$
$[[63,52,d \geq 4]]_4$		$[[63,48,d^{'} \geq 4]]_4$
$[[63,41,d \geq 7]]_4$		$[[63,39,d^{'} \geq 7]]_4$
$[[63,28,d \geq 10]]_4$		$[[63,24,d^{'} \geq 10]]_4$
	$m=3$, $q=5$	
$[[124,119,d \geq 3]]_5$		$[[124,115,d^{'} \geq 3]]_5$
$[[124,113,d \geq 4]]_5$		$[[124,109,d^{'} \geq 4]]_5$
$[[124,107,d \geq 5]]_5$		$[[124,103,d^{'} \geq 5]]_5$
$[[124,96,d \geq 8]]_5$		$[[124,94,d^{'} \geq 8]]_5$
$[[124,92,d \geq 9]]_5$		$[[124,88,d^{'} \geq 9]]_5$
$[[124,86,d \geq 10]]_5$		$[[124,82,d^{'} \geq 10]]_5$
$[[124,77,d \geq 12]]_5$		$[[124,73,d^{'} \geq 12]]_5$
	$m=3$, $q=7$	
$[[342,337,d \geq 3]]_7$		$[[342,333,d^{'} \geq 3]]_7$
$[[342,331,d \geq 4]]_7$		$[[342,327,d^{'} \geq 4]]_7$
$[[342,325,d \geq 5]]_7$		$[[342,321,d^{'} \geq 5]]_7$
$[[342,319,d \geq 6]]_7$		$[[342,315,d^{'} \geq 6]]_7$
$[[342,313,d \geq 7]]_7$		$[[342,309,d^{'} \geq 7]]_7$
$[[342,302,d \geq 10]]_7$		$[[342,300,d^{'} \geq 10]]_7$
$[[342,298,d \geq 11]]_7$		$[[342,294,d^{'} \geq 11]]_7$
$[[342,292,d \geq 12]]_7$		$[[342,288,d^{'} \geq 12]]_7$
$[[342,286,d \geq 13]]_7$		$[[342,282,d^{'} \geq 13]]_7$
$[[342,271,d \geq 16]]_7$		$[[342,267,d^{'} \geq 16]]_7$
	$m=4$, $q=4$	
$[[255,249,d \geq 3]]_4$		$[[255,243,d^{'} \geq 3]]_4$
$[[255,241,d \geq 4]]_4$		$[[255,235,d^{'} \geq 4]]_4$
$[[255,226,d \geq 7]]_4$		$[[255,223,d^{'} \geq 7]]_4$
$[[255,209,d \geq 10]]_4$		$[[255,203,d^{'} \geq 10]]_4$
	$m=4$, $q=5$	
$[[624,618,d \geq 3]]_5$		$[[624,612,d^{'} \geq 3]]_5$
$[[624,610,d \geq 4]]_5$		$[[624,604,d^{'} \geq 4]]_5$
$[[624,602,d \geq 5]]_5$		$[[624,596,d^{'} \geq 5]]_5$
$[[624,587,d \geq 8]]_5$		$[[624,584,d^{'} \geq 8]]_5$
$[[624,582,d \geq 9]]_5$		$[[624,576,d^{'} \geq 9]]_5$
$[[624,574,d \geq 10]]_5$		$[[624,568,d^{'} \geq 10]]_5$
$[[624,562,d \geq 12]]_5$		$[[624,556,d^{'} \geq 12]]_5$

[3] Bose, R.C., Ray-Chaudhuri, D.K.: Further results on error correcting binary group codes. Information and Control **3**, 279-290 (1960)

[4] Calderbank, A. R., Rains, E. M., Shor, P. W., Sloane, N. J. A.: Quantum error correction via codes over $GF(4)$. IEEE Trans. Inform. Theory **44**, 1369–1387 (1998)

[5] Edel, Y.: Table of quantum twisted codes. electronic address: www.mathi.uni-heidelberg.de/ yves/Matritzen/QTBCH/QTBCHIndex.html

[6] Hamada, M.: Concatenated quantum codes constructible in polynomial time: efficient decoding and rrror correction. IEEE Trans. Inform. Theory **54**, 5689–5704 (2008)

[7] Hocquenghem, A.: Codes correcteurs derreurs. Chiffres **2**, 147-156 (1959)

[8] Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge Univ. Press, Cambridge (2003)

[9] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inform. Theory **52**, 4892–4914 (2006)

[10] La Guardia, G.G.: Constructions of new families of nonbinary quantum codes. Phys. Rev. A. **80**, 042331:1–11 (2009)

[11] La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inform. Theory **60**, 1528–1535 (2014)

[12] La Guardia, G.G.: Quantum codes derived from cyclic codes. Intern. J. Theor. Physics **56**, 24792484 (2017)

[13] La Guardia, G.G., Alves, M.M.S.: On cyclotomic cosets and code constructions. Linear Algebra Appl. **488**, 302-319 (2016)

[14] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, (1977)

[15] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

[16] Steane, A.: Enlargement of Calderbank-Shor-Steane quantum codes. IEEE Trans. Inform. Theory **45**, 2492–2495 (1999)

[17] Yue, D.W., Feng, G.Z.: Minimal cyclotomic coset representatives and their applications to BCH codes and Goppa codes. IEEE Trans. Inform. Theory **46**, 2625–2628 (2000)

[18] Yue, D.W., Hu, Z.M.: On the dimension and minimum distance of BCH codes over $GF(q)$. Chin. J. Electron. **18**, 263-269 (1996)