Extending Construction X for Quantum Error-Correcting Codes

Akshay Degwekar
Indian Institute of Technology Madras

Kenza Guenda
University of Science and Technology of Algiers(Algeria)

T. Aaron Gulliver
University of Victoria(Canada)

ken.guenda@gmail.com

Abstract

In this paper we extend the work of Lisonek and Singh on construction X for quantum error-correcting codes to finite fields of order p^2 where p is prime. The results obtained are applied to the dual of Hermitian cyclic codes to generate new quantum error-correcting codes.

Keywords
quantum codes; construction X; optimal codes; cyclic codes

1 Introduction

Quantum error correcting codes have been introduced as an alternative to classical codes for use in quantum communication channels. Since the landmark papers of Shor [6] and Steane [7], this field of research has grown rapidly. Recently, Lisonek and Singh [5] gave a variant of Construction X that produces binary stabilizer quantum codes from arbitrary linear codes. In their construction, the requirement on the duality of the linear codes was relaxed. In this paper, we extend their work on construction X to obtain quantum error-correcting codes over finite fields of order p^2 where p is a prime number. We apply our results to the dual of Hermitian repeated root cyclic codes to generate new quantum error-correcting codes.

The remainder of the paper is organized as follows. In Section 2, we present our main result on the extension of the quantum construction X. Section 3 characterizes the generator polynomial of the Hermitian dual of a repeated root cyclic code. We also give the structure of cyclic codes of length $3p^s$ over $\mathbb{F}_{p^2}$ as well as the structure of the dual codes. Our interest in this class of codes comes from the importance of relaxing the condition $(n, p) = 1$, which allows us to consider codes other than the simple root codes.

2 Extending Construction X for $\mathbb{F}_p$

Let $\mathbb{F}_p$ denote the finite field with p elements and $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$. For $x \in \mathbb{F}_{p^2}$ we denote the *conjugate* of x by $\overline{x} = x^p$. Let $\langle x, y\rangle = \sum_{i=1}^n x_i \overline{y_i}$ be the Hermitian inner product. Then the *norm* of x is defined as $||x|| = \langle x, x\rangle = \sum_{i=1}^n x^{p+1}$, and the *trace* of x as $\mathrm{Tr}(x) = x + \overline{x}$. Both the trace and norm are mappings from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$.

Usually a dual contained condition is required to construct CSS quantum code as given by the following result.

Proposition 1. *([4]) If there exists an $\mathbb{F}_{p^2}$-linear $[n, k, d]_{p^2}$ code B such that $B^{\perp h} \subset B$, then there exists an $[[n, 2k - n, d]]_p$ quantum code.*

In the remainder of this section, we give some important lemmas which will be useful in the proof of our main result.

Lemma 2. *Let S be a subspace of $\mathbb{F}_{p^2}^n$ such that there exist x, y with $\langle x, y\rangle \neq 0$. Then for all $k \in \mathbb{F}_p$, there exists $z \in S$ with $||z|| = k$.*

Lemma 3. *Let D be a subspace of $\mathbb{F}_{p^2}^n$ and assume that M is a basis for $D \cap D^{\perp_h}$. Then there exists an orthonormal set B such that $M \cup B$ is a basis for D.*

Theorem 4. *For an $[n, k]_{p^2}$ linear code C, let $e = n - k - \dim(C \cap C^{\perp_h})$. Then there exists a quantum code with parameters $[[n + e, 2k - n, d]]_p$ with $d \geq \min(\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_h}) + 1)$.*

Proof. We start with the observation that the equation $x^2 + 1 = 0$ always has a solution in $\mathbb{F}_{p^2}$. This can be proven using the fact that $\mathbb{F}_{p^2}^* = \mathbb{F}_{p^2} \setminus \{0\}$ is a cyclic group. Let β be a generator of $\mathbb{F}_{p^2}^*$. Then $\beta^k = -1$ for some k, and since $(-1)^2 = 1$, $\beta^{2k} = 1$ and $(p^2 - 1)|2k$, so that k is even. Thus, $\beta^{\frac{k}{2}}$ is the required solution.

As defined previously

$$e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = \dim(C + C^{\perp_h}) - \dim(C).$$

Let $s = \dim(C \cap C^{\perp_h})$, and G be the matrix

$$G = \begin{pmatrix} M_{s\times n} & 0_{s\times e} \\ A_{(n-e-2s)\times n} & 0_{(n-e-2s)\times e} \\ B_{e\times n} & \beta^{k/2} I_{e\times e} \end{pmatrix}, \tag{1}$$

where the size of the matrix is indicated by the subscripts, and 0 and I denote the zero matrix and identity matrix, respectively.

For a matrix P, let $r(P)$ denote the set of rows of P. The matrix G is constructed such that $r(M)$ is a basis for $C \cap C^{\perp_h}$, $r(M) \cup r(A)$ is a basis for C, $r(M) \cup r(B)$ is a basis for C, and $r(B)$ is an orthonormal set. The existence of such a matrix B follows from Lemma 3. Note that $r(M) \cup r(A) \cup r(B)$ is a basis for $C + C^{\perp_h}$.

Let E be the linear code for which G is a generator matrix. Further, let S denote the union of the first s rows of G and the last e rows of G, i.e., S is the set of rows of the matrix

$$S = \begin{pmatrix} M_{s\times n} & 0_{s\times e} \\ B_{e\times n} & \beta^{k/2} I_{e\times e} \end{pmatrix}. \tag{2}$$

We observe that each row of S is orthogonal to each row of G because any row from the first s rows of S represents a vector in $C \cap C^{\perp_h}$, and hence is orthogonal with all codewords in $C + C^{\perp_h}$, the code represented by G.

Consider a row from the last e rows in S. This row is orthogonal to the first $n - e - s$ rows of G because they represent the code C while the matrix B represents codewords from $C^{\perp_h}$. These rows of the matrix are orthogonal to each other because the rows of B are orthogonal and $\beta^{k/2} I$ will contribute 0. Any row z is self-orthogonal since from the construction $||z|| = 1$ and the identity matrix will contribute -1, giving an inner product of 0. This completes the proof of the observation. Thus, each vector from S belongs to $E^{\perp_h}$, and the vectors in S are linearly independent because

$$\dim(E^{\perp_h}) = n + e - (n - s) = e + s = |S|.$$

Hence S is a basis for $E^{\perp_h}$. Since S is a subset of G by construction, it follows that $E^{\perp_h} \subseteq E$.

Let x be a non-zero vector in E and due to the vertical block structure of G, we can write $x = (x^1|x^2)$ where $x^1 \in \mathbb{F}_{p^2}^n$ and $x^2 \in \mathbb{F}_{p^2}^e$. Thus x is a linear combination of rows of G. If none of the last e rows of G are contained in this linear combination with a non-zero coefficient, then $x^1 \in C \setminus \{0\}$, and so $\mathrm{wt}(x) = \mathrm{wt}(x^1) \geq \mathrm{wt}(C)$. If some of the last e rows of G are in this linear combination with a non-zero coefficient, then $x^1 \in C + C^{\perp_h}$ and $\mathrm{wt}(x) = \mathrm{wt}(x^1) + \mathrm{wt}(x^2) \geq \mathrm{wt}(C + C^{\perp_h}) + 1$. Thus E is an $[n + e, k + e, d]_{p^2}$ code with $d \geq \min(\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_h}) + 1)$ and $E^{\perp_h} \subseteq E$. The code E is such that $E^{\perp} \subset E$, and thus the result follows from Proposition 1. □

Many constructions of quantum codes use self-orthogonal codes [1, 2], which corresponds to the case when $e = 0$. The results in the next section are required to construct the quantum codes in subsequent sections. Note that many of the results in the next section can easily be generalized to constacyclic codes.

3 The Hermitian Dual of Repeated Roots Cyclic Codes

Let p be a prime number and C a cyclic code of length n over the finite field $\mathbb{F}_{p^2}$. Then C is given by the principal ideal $g(x)$ in $\frac{\mathbb{F}_{p^2}[x]}{\langle x^n-1\rangle}$, and so $g(x)$ is called the generator polynomial for C. When the length n divides p, C is called a repeated root cyclic code.

In this section, we obtain the generator polynomial of the Hermitian dual of a repeated root cyclic code. We also give the structure of the cyclic codes of length $3p^s$ over $\mathbb{F}_{p^2}$ as well as the structure of the dual code. Our interest in this class of codes comes from the importance of relaxing the condition $(n,p)=1$, which allows us to consider codes other than simple root codes.

Let $f(x)=a_0+a_1x+\ldots+a_rx^r$ be a polynomial in $\mathbb{F}_{q^2}[x]$, and $\overline{f(x)}=\overline{a_0}+\overline{a_1}x+\ldots+\overline{a_r}x^r$. The polynomial inverse of f is denoted by $f^\star(x)=x^rf(x^{-1})=a_r+a_{r-1}x+\ldots+a_0x^r$, so then $f^\perp(x)=\overline{a_r}+\overline{a_{r-1}}x+\ldots+\overline{a_0}x^r$.

The following properties can easily be verified.

Lemma 5. *Let $f(x)$ and $g(x)$ be polynomials over $\mathbb{F}_{p^m}$. Then*

1. *conjugation is additive: $\overline{f(x)+g(x)}=\overline{f(x)}+\overline{g(x)}$;*
2. *conjugation is multiplicative: $\overline{f(x)g(x)}=\overline{f(x)}\,\overline{g(x)}$;*
3. *polynomial inversion is additive if the polynomials have the same degree: $(f(x)+g(x))^\star=f(x)^\star+g(x)^\star$;*
4. *polynomial inversion is multiplicative: $(f(x)g(x))^\star=f(x)^\star\,g(x)^\star$;*
5. *inversion and conjugation commute with each other: $\overline{(f(x)^\star)}=(\overline{f(x)})^\star$; and*
6. *both operations are self-inverses: $(f(x)^\star)^\star=f(x)$ and $\overline{\overline{f(x)}}=f(x)$.*

Lemma 6. *Let $a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ and $b(x)=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$ be polynomials in $\frac{\mathbb{F}_{p^2}[x]}{\langle x^n-1\rangle}$. Then $a(x)\overline{b(x)}=0$ in $\frac{\mathbb{F}_{p^2}[x]}{\langle x^n-1\rangle}$ if and only if $(a_0,a_1,\ldots,a_{n-1})$ is orthogonal to $(\overline{b_{n-1}},\overline{b_{n-2}},\ldots,\overline{b_0})$ and all its cyclic shifts. That is $\langle a,\overline{b^\star}\rangle=0 \iff a(x)b(x)^\perp=0$.*

We now use Lemma 6 to derive an expression for the Hermitian dual of a cyclic code. Let $S\subseteq R$ and let the annihilator be $\mathrm{ann}(S)=\{g\in R|fg=0,\ \forall f\in S\}$. Then $\mathrm{ann}(S)$ is also an ideal of the ring and hence is generated by a polynomial.

Lemma 7. *If $g(x)$ generates the code C, then $C^{\perp_h}=\mathrm{ann}(\overline{g(x)}^\star)$.*

Lemma 8. *Assume that $C=\langle g(x)\rangle$ is a cyclic code of length n over $\mathbb{F}_{p^2}$ with generator polynomial $g(x)$. Define $h(x)=\frac{x^n-1}{g(x)}$. Then we have that $C^{\perp_h}=\langle h^\perp(x)\rangle$.*

Proof. From Lemma 7 it is known that $C^{\perp_h}=\mathrm{ann}(g(x)^\perp)$. Thus, we must show that $\mathrm{ann}(g^\perp(x))=\langle h^\perp(x)\rangle$. One way containment is easy since $\langle h^\perp(x)\rangle\subseteq\mathrm{ann}(g^\perp(x))$, which is true because $h^\perp(x)g^\perp(x)=(h(x)g(x))^\perp=(x^n-1)^\perp=0$ by Lemma 5. For containment the other way, we observe that since $\mathrm{ann}(g^\perp(x))$ is an ideal of the polynomial ring $\frac{\mathbb{F}_{p^2}[x]}{\langle x^n-1\rangle}$, it is generated by a polynomial, say $b^\perp(x)$. Then $b^\perp(x)g^\perp(x)=x^n-1=\lambda(x^n-1)^\perp$ (because $b(x)$ is the smallest polynomial, so it is an equality). Hence $b(x)g(x)=x^n-1$, so it must be that $b(x)=h(x)$ since both are unitary polynomials. This completes the proof. □

Theorem 9. *Let $p>3$ be a prime. Then*

1. *there exists $\omega\in\mathbb{F}_{p^2}$ such that $\omega^3=1$ and the factorization of $x^{3p^s}-1$ into irreducible factors over $\mathbb{F}_{p^2}[x]$ is*
$$x^{3p^s}-1=(x-1)^{p^s}(x-\omega)^{p^s}(x-\omega^2)^{p^s};$$
2. *the cyclic codes of length $3p^s$ are always of the form*
$$\langle(x-1)^i(x-\omega)^j(x-\omega^2)^k\rangle,$$
where $0\le i,j,k\le p^s$, and the code has $p^{2(3p^s-i-j-k)}$ codewords; and

3. the Hermitian dual of the codes have the form

$$C^{\perp_h} = \begin{cases} \langle (x-1)^{p^s-i}(x-\omega)^{p^s-j}(x-\omega^2)^{p^s-k}\rangle & \text{if } p \equiv 1 \mod 3, \\ \langle (x-1)^{p^s-i}(x-\omega^2)^{p^s-j}(x-\omega)^{p^s-k}\rangle & \text{if } p \equiv 2 \mod 3. \end{cases} \tag{3}$$

Proof.

1. Since p is a prime number, $p \neq 0 \mod 3$, and $p^2-1 = (p+1)(p-1)$, so either $p+1 = 0 \mod 3$ or $p-1 = 0 \mod 3$. Therefore an element of order 3 exists in $\mathbb{F}_{p^2}$. Let this element be ω, so then $(x-1)(x-\omega)(x-\omega^2) = x^3-1$. In a field of characteristic p, it is known that $x^n-1 = (x^m-1)^p$ if $n = mp$. Therefore we have that $x^{3p^s}-1 = (x^3-1)^{p^s} = ((x-1)(x-\omega)(x-\omega^2))^{p^s}$.

2. From the previous part we know that the irreducible factors are $(x-1)$, $(x-\omega)$ and $(x-\omega^2)$, each of multiplicity p^s. As the generator polynomial divides $x^{3p^s}-1$, the statement follows.

3. We know from Lemma 8 that
$$C^{\perp_h} = \langle h^{\perp}(x)\rangle,$$
and hence
$$\begin{aligned} C^{\perp_h} &= \overline{\langle \frac{(x-1)^{p^s}(x-\omega)^{p^s}(x-\omega^2)^{p^s}}{(x-1)^i(x-\omega)^j(x-\omega^2)^k}\rangle^{\star}} \\ &= \overline{\langle (x-1)^{p^s-i}(x-\omega)^{p^s-j}(x-\omega^2)^{p^s-k}\rangle^{\star}} \\ &= \overline{\langle [(x-1)^{p^s-i}]^{\star}[(x-\omega)^{p^s-j}]^{\star}[(x-\omega^2)^{p^s-k}]^{\star}\rangle} \\ &= \overline{\langle [-(x-1)^{p^s-i}][-\omega(x-\omega^{-1})^{p^s-j}]^{\star}[-\omega^2(x-\omega^{-2})^{p^s-k}]^{\star}\rangle} \\ &\text{Further } (x-1)^{\star} = -x+1 = -(x-1), (x-\omega)^{\star} = -\omega x+1 = -\omega(x-\omega^2) \\ &= \overline{\langle [(x-1)^{p^s-i}][(x-\omega^2)^{p^s-j}][(x-\omega)^{p^s-k}]\rangle} \\ &= \langle [(\overline{x-1})^{p^s-i}][(\overline{x-\omega^2})^{p^s-j}][(\overline{x-\omega})^{p^s-k}]\rangle \\ &= \langle [(x-1)^{p^s-i}][(x-\omega^{2p})^{p^s-j}][(x-\omega^p)^{p^s-k}]\rangle \\ &= \begin{cases} \langle (x-1)^{p^s-i}(x-\omega^2)^{p^s-j}(x-\omega)^{p^s-k}\rangle & \text{if } p \equiv 1 \mod 3, \\ \langle (x-1)^{p^s-i}(x-\omega)^{p^s-j}(x-\omega^2)^{p^s-k}\rangle & \text{if } p \equiv 2 \mod 3, \end{cases} \end{aligned} \tag{4}$$
$$\text{then } \omega^p = \omega \text{ if } p \equiv 1 \mod 3, \text{ and } \omega^p = \omega^2 \text{ if } p \equiv 2 \mod 3, \tag{5}$$

which completes the proof. □

4 Extension to Simple Root Cyclic Codes

This section considers cyclic codes of length n over $\mathbb{F}_{p^2}$ such that $(p,n) = 1$. In this case, a cyclic code can be represented by its defining set Z. If m has order p^2 modulo n, then $\mathbb{F}_{p^{2m}}$ is the splitting field of x^n-1 containing a primitive nth root of unity. Consider a primitive root β. Then $\{k | g(\beta^k) = 0,\ 0 \leq k < n\}$ is a defining set of C. Note that this set depends on the choice of β. We can make a canonical choice for β by fixing a primitive element α of $\mathbb{F}_{p^{2m}}$ and letting $\beta = \alpha^{\frac{p^{2m}-1}{n}}$. Let α be defined by the PrimitiveElement function in Magma. This will be used in the code constructions in the next section.

For n and m as defined above and $a \in \{0, \ldots, n-1\}$, the set $\{aq^j \mod n | 0 \leq j < m\}$ is called a *cyclotomic coset modulo n*. It is well known that a defining set of a cyclic code of length n is the union of *cyclotomic cosets modulo n*. Let $\mathbb{Z}_n$ denote the set of integers modulo n. Clearly defining sets can be considered as subsets of $\mathbb{Z}_n$. For $S \subset \mathbb{Z}_n$, denote $\overline{S} = \mathbb{Z}_n \backslash \{S\}$ and $-p^2S = \{-p^2 s \mod n | s \in S\}$.

We now prove the following lemma.

Lemma 10. *If C is a linear cyclic code with defining set Z, then* $\dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = |Z \cap -pZ|$.

Proof. Let C be a linear cyclic code of length n, and $\prod_{k \in Z}(x-\beta^k)$ be the generator polynomial for C. Then from Lemma 8 the generator polynomial for $C^{\perp_h}$ is $\prod_{k \in -p\overline{Z}}(x-\beta^k)$, and the generator polynomial for $C \cap C^{\perp_h}$ is $\prod_{k \in Z \cap -p\overline{Z}}(x-\beta^k)$, which gives that

$$\dim(C^{\perp_h}) - dim(C \cap C^{\perp_h}) = n - |-p\overline{Z}| - (n - |Z \cup -p\overline{Z}|) = |Z \cup -p\overline{Z}| - |-p\overline{Z}| = |Z \cap -pZ|.$$

□

Theorem 11. *Assume n is divisible by p^2-1 and let C be an $[n,k]_{p^2}$ cyclic code with defining set Z such that $(Z \cap -pZ) \subseteq T = \{\frac{nk}{p^2-1} | k \in \{1,\ldots,p^2-1\}\}$. If $e = |Z \cap -pZ|$, then there exists an $[[n+e, 2k-n+e, d]]_p$ quantum code with $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C_u)+1, \mathrm{wt}(C+C^{\perp_h})+2\}$ where the minimum is taken over the cyclic codes C_u with defining set $Z\backslash\{u\}$ for each $u \in Z \cap -pZ$.*

Proof. The proof requires a modification to the proof of Theorem 4, in particular the set of orthonormal vectors used is changed. First we observe that each of the elements in T is a cyclotomic coset and contains only one element. Let $q = p^2-1$, $n = (p^2-1)l = ql$, and ω be a (p^2-1)-th root of unity. Consider the polynomials

$$b_t(x) = \frac{x^n-1}{x-\omega^t} = \sum_{i=0}^{l-1}(x^{qi+q-1} + \omega^t x^{qi+q-2} + \ldots + \omega^{(q-1)t}x^{qi}).$$

For convenience, we let $\{b_i | i \in 0,1,\ldots,l\}$ also denote the corresponding codewords. This is an orthonormal set because

$$\langle b_u, b_v\rangle = q\sum_{i=0}^{l-1}(\omega^{i(u+vp)}) = q\sum i = 0^{l-1}(\omega^{i(u-v)}) = \begin{cases} 0 & u \neq v \\ ql & u = v \end{cases}.$$

To mitigate the ql factor, we can multiply each element by a constant. Thus, to add the rows for B to the matrix, we add $U = \{b_t | \frac{tn}{q} \in Z \cap -pZ\}$.

To prove the claim about the distance, we have 3 cases: no row from B is a linear combination, exactly one row from U is a linear combination with a non-zero coefficient, and at least two rows are a combination. The proof of the first and the last cases is the same as in the proof of Theorem 4. For the second case, let b_t be the row with non-zero coefficient. Then the code generated would be $span(C, b_t)$, which is precisely the cyclic code with defining set $Z\backslash\{\frac{tn}{q-1}\}$. This completes the proof. □

References

[1] K. Guenda, Sur l'équivalence des codes, Ph.D. Thesis, Faculty of Mathematics USTHB, Algiers. 2010.

[2] K. Guenda and T. A. Gulliver, "Symmetric and asymmetric quantum codes," *Int. J. Quantum Inform.*, vol. 11, no. 5, 2013.

[3] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, New York, 2003.

[4] A. Ketkare, A. Klappenecker, S. Kumar and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," arXiv:quant-ph/0508070.

[5] P. Lisonek and V.K. Singh, "Construction X for quantum error-correcting codes," in *Proc. Int. Workshop on Coding and Crypt.*, Bergen, Norway, Apr. 2013.

[6] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 52, no. 4, pp. 2493–2493, Oct. 1995.

[7] A. Steane, "Multiple particle interference and quantum error correction," *Proc. Royal Soc. A*, vol. 452, pp. 2551–2577, Nov. 1996.