Quantum Block and Synchronizable Codes Derived from Certain Classes of Polynomials

Tao Zhang and Gennian Ge

Abstract

One central theme in quantum error-correction is to construct quantum codes that have a large minimum distance. In this paper, we first present a construction of classical codes based on certain class of polynomials. Through these classical codes, we are able to obtain some new quantum codes. It turns out that some of quantum codes exhibited here have better parameters than the ones available in the literature. Meanwhile, we give a new class of quantum synchronizable codes with highest possible tolerance against misalignment from duadic codes.

Index Terms

Quantum codes, quantum synchronizable codes, polynomial codes, cyclotomic cosets, duadic codes.

I. INTRODUCTION

Quantum codes were introduced to protect quantum information from decoherence during quantum computations and quantum communications. After the initial work for quantum error-correcting codes [22], [23], researchers have made great progress in developing quantum codes. In [3], the construction of binary quantum codes was diverted into finding classical self-orthogonal codes over GF(4), and then generalized to the nonbinary case [21], [2]. After the establishment of the above connection between quantum codes and classical codes, the construction of quantum codes can be converted to that of classical self-orthogonal codes (see [1], [4], [5], [15], [16], [17], [19], [24] and the references therein). As in classical coding theory, one of the central tasks in quantum coding theory is to construct quantum code with a large minimum distance.

We know that Reed-Solomon code is an MDS (maximum distance separable) code [13], as its parameters meet the Singleton bound. But the length of a q-ary Reed-Solomon code is restricted to be less than or equal to q. By using the principal of evaluation, several successful constructions have been made to construct good q-ary linear codes which have lengths larger than q (see [27], [20], [14], [25]). Motivated by these works, we will give a new construction of linear codes by evaluation. Using these linear codes, we obtain new quantum codes. Some of them have better parameters than the quantum codes listed in tables online [6], [12].

Recently, Fujiwara [11] considered another type of quantum codes, named quantum synchronizable codes, which is a coding scheme that corrects not only the general quantum noise represented by Pauli errors but also misalignment errors. Misalignment is the type of errors that the information processing device misidentifies the boundaries of an information block. For example, assume that each chunk of information is encoded into a block of consecutive three bits in a stream of bits b1 so that the data has a frame structure. If three blocks of information are encoded, we have nine ordered bits (b0, b1, b2, b3, b4, b5, b6, b7, b8) in which each of the three blocks (b0, b1, b2), (b3, b4, b5), (b6, b7, b8) forms an information chunk. If misalignment occurs to the right by one bit when attempting to retrieve the second block of information, the device will wrongly read out b4, b5 and b6 instead of the correct set of bits b3, b4 and b5. The same kind of error in block synchronization may be considered for a stream of qubits.

A theoretical framework of quantum synchronizable coding was first introduced in [11]. Later, the authors of [9] improved the original construction method and gave more examples of quantum synchronizable codes. While we have a theoretical framework of quantum synchronizable coding, there are only a few infinite families of quantum synchronizable codes in the literature. One of the main challenges in the construction of quantum synchronizable codes is that it is quite difficult to find suitable classical codes because the required algebraic structures are very harsh. Particular constraint is the variety of available code parameters. For instance, the lengths of the encoded information blocks of the known quantum synchronizable codes that have highest possible tolerance against misalignment are primes, 2^n – 1 or of the form \( \frac{2^n - 1}{3} \) [9], [10], [26]. In this work, we construct a new infinite family of quantum synchronizable codes by exploiting duadic codes over finite field \( \mathbb{F}_2 \).

This paper is organized as follows. In Section III we recall the basics about quantum codes and quantum synchronizable codes. In Section IV we first give a new construction of classical linear codes. From these linear codes, we obtain some new quantum codes. In Section V we present a new class of quantum synchronizable codes based on duadic codes.
II. Preliminaries

Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, where \( q \) is a prime power. A linear \([n, k]\) code \( C \) over \( \mathbb{F}_q \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \). The weight \( wt(x) \) of a codeword \( x \in C \) is the number of nonzero components of \( x \). The distance of two codewords \( x, y \in C \) is \( d(x, y) := wt(x - y) \). The minimum distance \( d \) between any two distinct codewords of \( C \) is called the minimum distance of \( C \). An \([n, k, d]\) code is an \([n, k]\) code with the minimum distance \( d \).

A linear \([n, k]\) code \( C \) over the finite field \( \mathbb{F}_q \) is called cyclic if \( (c_0, c_1, \cdots, c_{n-1}) \in C \) implies \( (c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C \). If we identify each codeword \( (c_0, c_1, \cdots, c_{n-1}) \) with \( c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1) \), then cyclic code \( C \) is identified with an ideal of the ring \( \mathbb{F}_q[x]/(x^n - 1) \). Note that every ideal of \( \mathbb{F}_q[x]/(x^n - 1) \) is principal, then \( C \) is generated by a monic divisor \( g(x) \) of \( x^n - 1 \). In this case, \( g(x) \) is called the generator polynomial of \( C \) and we write \( C = \langle g(x) \rangle \). Let \( \alpha \) be a primitive \( n \)-th root of unity in some extension field of \( \mathbb{F}_q \), then the set \( Z = \{i|g(\alpha^i) = 0, \ 0 \leq i \leq n-1 \} \) is called the defining set of \( C \).

Given two vectors \( x = (x_0, x_1, \cdots, x_{n-1}), \ y = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^n \), there are two inner products we are interested in. One is the Euclidean inner product which is defined as
\[
\langle x, y \rangle_E = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1}.
\]
When \( q = l^2 \), where \( l \) is a prime power, then we can also consider the Hermitian inner product which is defined by
\[
\langle x, y \rangle_H = x_0^l y_0^l + x_1^l y_1^l + \cdots + x_{n-1}^l y_{n-1}^l.
\]
The Euclidean dual code of \( C \) is defined as
\[
C^\perp_E = \{x \in \mathbb{F}_q^n | \langle x, y \rangle_E = 0 \text{ for all } y \in C \}.
\]
Similarly the Hermitian dual code of \( C \) is defined as
\[
C^\perp_H = \{x \in \mathbb{F}_q^n | \langle x, y \rangle_H = 0 \text{ for all } y \in C \}.
\]
A linear code \( C \) is called Euclidean (Hermitian) dual-containing if \( C^\perp_E \subseteq C \) (\( C^\perp_H \subseteq C \), respectively). A code \( D \) is called \( C \)-containing if \( C \subseteq D \).

A. Quantum Codes

In this subsection, we recall the basics of quantum codes. Let \( q \) be a power of a prime number \( p \). A qubit \( |v\rangle \) is a nonzero vector in \( \mathbb{C}^q : |v\rangle = \sum_{x \in \mathbb{F}_q} c_x |x\rangle \), where \( \{ |x\rangle | x \in \mathbb{F}_q \} \) is a basis of \( \mathbb{C}^q \). For \( n \geq 1 \), the \( n \)-th tensor product \( (\mathbb{C}^q)^\otimes n \cong \mathbb{C}^{q^n} \) has a basis \( \{ |a_1 \cdots a_n\rangle = |a_1\rangle \otimes \cdots \otimes |a_n\rangle | (a_1, \cdots, a_n) \in \mathbb{F}_q^n \} \), then an \( n \)-qubit is a nonzero vector in \( \mathbb{C}^{q^n} : |v\rangle = \sum_{a \in \mathbb{F}_q^n} c_a |a\rangle \), where \( c_a \in \mathbb{C} \).

Let \( \zeta_p \) be a primitive \( p \)-th root of unity. The quantum errors in \( q \)-ary quantum system are linear operators acting on \( \mathbb{C}^q \) and can be represented by the set of error bases: \( E_n = \{ T^a R^b | a, b \in \mathbb{F}_q \} \), where \( T^a R^b \) is defined by
\[
T^a R^b |x\rangle = \zeta_p^{Tr_q(bx)} |x + a\rangle.
\]
The set
\[
E_n = \{ \zeta_p^l T^a R^b | 0 \leq l \leq p-1, a = (a_1, \cdots, a_n), b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n \}
\]
forms an error group, where \( \zeta_p^l T^a R^b \) is defined by
\[
\zeta_p^l T^a R^b |x\rangle = \zeta_p^l T^a R^b |x_1\rangle \otimes \cdots \otimes T^a R^b |x_n\rangle = \zeta_p^{Tr_q(bx)} |x + a\rangle,
\]
for any \( |x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \), \( x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n \). For an error \( e = \zeta_p^l T^a R^b \), its quantum weight is defined by
\[
w_Q(e) = \# \{ 1 \leq i \leq n | (a_i, b_i) \neq (0, 0) \}.
\]
A subspace \( Q \) of \( \mathbb{C}^{q^n} \) is called a \( q \)-ary quantum code with length \( n \). The \( q \)-ary quantum code has minimum distance \( d \) if and only if it can detect all errors in \( E_n \) of quantum weight less than \( d \), but cannot detect some errors of weight \( d \). A \( q \)-ary \([n, k, d]\) quantum code is a \( q^k \)-dimensional subspace of \( \mathbb{C}^{q^n} \) with minimum distance \( d \). There are many methods to construct quantum codes, and the following theorem is one of the most frequently used construction methods.

**Theorem II.1.** (Hermitian Construction) If \( C \) is a \( q^2 \)-ary Hermitian dual-containing \([n, k, d]\) code, then there exists a \( q \)-ary \([n, 2k - n, \geq d]\)-quantum code.

We also mention that quantum codes have propagation rules as classical linear codes.

**Theorem II.2.** (Propagation Rules) Suppose there is a \( q \)-ary \([n, k, d]\) quantum code. Then
1. (Subcode) there exists a \( q \)-ary \([n, k - 1, \geq d]\) quantum code.
2. (Lengthening) there exists a \( q \)-ary \([n + 1, k, \geq d]\) quantum code.
3. (Puncturing) there exists a \( q \)-ary \([n - 1, k, \geq d - 1]\) quantum code.
4. there exists a \( q \)-ary \([n, k, d - 1]\) quantum code.
B. Quantum Synchronizable Codes

A \((c_l, c_r) - [[n, k]]_2\) quantum synchronizable code is an \([[n, k]]_2\) quantum code that corrects not only bit errors and phase errors but also misalignment to the left by \(c_l\) qubits and to the right by \(c_r\) qubits for some nonnegative integers \(c_l\) and \(c_r\). The framework for constructing quantum synchronizable codes involves an algebraic notion in polynomial rings. Let \(f(x) \in \mathbb{F}_2[x]\) be a polynomial over \(\mathbb{F}_2\) such that \(f(0) = 1\). The cardinality \(\text{ord}(f(x)) = |\{x^a \mod f(x) | a \in \mathbb{N}\}|\) is called the order of the polynomial \(f(x)\), where \(\mathbb{N}\) is the set of positive integers.

Theorem II.3. \([9]\) Let \(C\) be a Euclidean dual-containing cyclic \([n, k_1, d_1]\) code with generator polynomial \(h(x)\) and \(D\) be a \(C\)-containing cyclic \([n, k_2, d_2]\) code with generator polynomial \(g(x)\). Define polynomial \(f(x)\) of degree \(k_2 - k_1\) to be the quotient of \(h(x)\) divided by \(g(x)\) over \(\mathbb{F}_q[x]/(x^n - 1)\). Then for every pair \(a_1, a_r\) of nonnegative integers such that \(a_i + a_r < \text{ord}(f(x))\) there exists a quantum synchronizable \((a_1, a_r) - [[n + a_1 + a_r, 2k_1 - n]]_2\) code that corrects at least up to \(\left\lfloor \frac{d_2 - 1}{2} \right\rfloor\) phase errors and at least up to \(\left\lfloor \frac{d_2 - 1}{2} \right\rfloor\) bit errors.

In order to compute the order of the polynomial \(f(x)\), we need the following lemmas.

Lemma II.4. \([18]\) Let \(f(x) \in \mathbb{F}_q[x]\) be an irreducible polynomial over \(\mathbb{F}_q\) of degree \(m\) and with \(f(0) \neq 0\). Then \(\text{ord}(f(x))\) is equal to the order of any root of \(f\) in the multiplicative group \(\mathbb{F}_{q^m}^\times\).

Lemma II.5. \([18]\) Let \(g_1(x), \ldots, g_k(x)\) be pairwise relatively prime nonzero polynomials over \(\mathbb{F}_q\), and let \(f(x) = g_1(x) \cdots g_k(x)\). Then \(\text{ord}(f(x))\) is equal to the least common multiple of \(\text{ord}(g_1(x)), \ldots, \text{ord}(g_k(x))\).

III. New Quantum Codes from Polynomial Codes

This section gives a new construction of classical linear codes and provides a family of quantum codes. The following notations are fixed in this section.

- Let \(q = p^b\) be a prime power, where \(p\) is a prime number.
- Let \(m\) be a positive integer with \(\gcd(q, m) = 1\) and \(\text{ord}_m(q) = p^b\), where \(b \geq 1\) is a positive integer.
- Let \(t = p^b\) and \(s = p^{b-1}\).

A. Polynomial Codes

Note that \(\text{ord}_m(q) = t\). For any \(a \in \mathbb{Z}_m = \{0, 1, \ldots, m - 1\}\), the \(q\)-cyclotomic coset \(C_a\) belonging to \(a\) is defined by

\[C_a := \{aq^j \mod m | 0 \leq j \leq t - 1\}.
\]

Now we choose a representation of the \(q\)-cyclotomic coset with maximum length:

\[A := \{\max(C_a) | 0 \leq a \leq m - 1, |C_a| = t\},
\]

where \(\max(C_a)\) is the maximum element of set \(C_a\). We are ready to define the following polynomials.

Definition III.1. For every \(a \in A\) and every integer \(k\) such that \(0 \leq k \leq s - 1\), let

\[e_{a,k}(x) = \sum_{j=0}^{t-1} \gamma^{q^j+k} x^{q^ja},
\]

where \(\gamma\) is a fixed normal element of \(\mathbb{F}_{q^s}/\mathbb{F}_q\), i.e., \(\gamma, \gamma^q, \ldots, \gamma^{q^{s-1}}\) is an \(\mathbb{F}_q\)-basis of \(\mathbb{F}_{q^s}\).

Let \(B := \{e_{a,k}(x) | a \in A, 0 \leq k \leq s - 1\}\) be the set of all polynomials just defined and \(U_m\) be the subgroup of the \(m\)-th roots of unity in \(\mathbb{F}_{q^s}^\times\). Then we have the following result.

Lemma III.1. The polynomials \(e_{a,k}(x)\) have the following properties:

(i) For \(a \in A\) and \(0 \leq k \leq s - 1\), the polynomial \(e_{a,k}(x)\) has coefficients in \(\mathbb{F}_{q^s}\) and degree equal to \(a\).

(ii) The polynomials \(e_{a,k}(x)\) for \(a \in A\) and \(0 \leq k \leq s - 1\) are linearly independent over \(\mathbb{F}_q\).

(iii) \(e_{a,k}(\beta) \in \mathbb{F}_q\) for all \(\beta \in U_m\).

(iv) \(e_{a,k}(u) = 0\) for all \(u \in (\mathbb{F}_{q^s} \cap U_m) \cup \{0\}\).

(v) \(|B| = \frac{m - \gcd(m, q^{s-1})}{p}\).

Proof: (i) All the assertions are clear.

(ii) If \(a\) and \(b\) are in different \(q\)-cyclotomic cosets, then \(e_{a,k_1}(x)\) and \(e_{b,k_2}(x)\) have different degrees, they are linearly independent. Since \(\gamma, \gamma^q, \ldots, \gamma^{q^{s-1}}\) are an \(\mathbb{F}_q\)-basis of \(\mathbb{F}_{q^s}\), \(e_{a,k}(x)\) for \(0 \leq k \leq s - 1\) are linearly independent over \(\mathbb{F}_q\).
(iii). Let $\beta \in U_m$, then

$$(e_{a,k}(\beta))^q = \left(\sum_{j=0}^{t-1} \gamma^{q^{i+j}} \beta^{q^ja}\right)^q$$

$$= \sum_{j=0}^{t-1} \gamma^{q^{i+j+1}} \beta^{q^j a}$$

$$= \sum_{j=1}^{t-1} \gamma^{q^i} \beta^{q^ja} + \gamma^{q^i} \beta^{q^ja}$$

$$= \sum_{j=0}^{t-1} \gamma^{q^i} \beta^{q^ja},$$

so $e_{a,k}(\beta) \in \mathbb{F}_q$.

(iv). It is clear that $e_{a,k}(0) = 0$. Let $u \in \mathbb{F}_{q^s} \cap U_m$, then

$$e_{a,k}(u) = \sum_{j=0}^{t-1} \gamma^{q^{i+k}} u^{q^j a} = \frac{t}{s} \sum_{j=0}^{s-1} \gamma^{q^{i+k}} u^{q^j a} = \frac{p}{s} \sum_{j=0}^{s-1} \gamma^{q^{i+k}} u^{q^j a} = 0.$$

(v). We can verify that $|C_a| < t$ if and only if $m|a(q^s - 1)$, that is $\frac{m}{\gcd(m,q^s-1)}a$. Since every $q$-cyclotomic coset with $t$ elements corresponds to $s$ polynomials, we have $|B| = \frac{m-\gcd(m,q^s-1)}{p}$. In order to give our construction, let

- $L \subseteq A$, $S := \bigcup_{a \in L} C_a$, $\mathfrak{A} := \bigcup_{a \in A} C_a$,
- $B(S) := \{e_{a,k}(x)|a \in S, 0 \leq k \leq s-1\}$,
- $V(S) := \text{span}_{\mathbb{F}_q}(B(S))$,
- $\{\beta_1, \beta_2, \cdots, \beta_n\}$ be a complete set of representatives of elements from $U_m \backslash \mathbb{F}_{q^s}^*$ which are pairwise nonconjugate over $\mathbb{F}_{q^s}$, where $U_m$ is the subgroup of the $m$-th roots of unity in $\mathbb{F}_{q^s}$.

It is clear that $n = \frac{m-\gcd(m,q^s-1)}{p}$. Our construction is:

**Proposition III.2.** Let

$$C(S) := \{ [f(\beta_1), f(\beta_2), \cdots, f(\beta_n)] | f \in V(S) \}.$$ 

Then $C(S)$ is an $\mathbb{F}_q$-linear $[n,k,d]$ code, where $n = \frac{m-\gcd(m,q^s-1)}{p}$, $k = |B(S)|$, $d \geq \left\lceil \frac{m+1-c}{p} \right\rceil$ and $c$ is the maximum element of set $S$.

**Proof:** We only need to show that $d \geq \left\lceil \frac{m+1-c}{p} \right\rceil$. On one hand, by Lemma [III.1] $f(u) = 0$ for all $u \in (\mathbb{F}_{q^s} \cap U_m) \cup \{0\}$.

On the other hand, if $\beta_i$ is a root of $f(x)$, then so are all the $p$ conjugate elements $\beta_i, \cdots, \beta_i^{p-1}$. Therefore $f(x)$ has at most $\frac{\deg(f(x)) \cdot \gcd(m,q^s-1)-1}{p}$ roots among $\{\beta_1, \beta_2, \cdots, \beta_n\}$. Hence its Hamming weight is at least $n - \frac{\gcd(m,q^s-1)-1}{p} = \frac{m+1-c}{p}$. ■

**B. New Quantum Codes**

In this section, we will construct some new quantum codes from polynomial codes. First of all, we determine the dual of the code $C(S)$. Let $C_a = \{m - i | i \in C_a \}$ and $\overline{S} = \bigcup_{a \in S} \overline{C_a}$, then we have

**Proposition III.3.** The Euclidean dual of $C(S)$ is $C(R)$, where $R = \mathfrak{A} \setminus \overline{S}$.

**Proof:** Since $\dim(C(S)) + \dim(C(R)) = n$, we only need to show that every codeword in $C(S)$ is orthogonal to all codewords of $C(R)$. ■
For $a \in S$, $b \in R$ and $0 \leq k_1, k_2 \leq s - 1$, we have
\[
\sum_{i=1}^{n} e_{a,k_1}(\beta_i) e_{b,k_2}(\beta_i) = \sum_{i=1}^{n} \left( \sum_{j=0}^{t-1} \gamma^{q^j+k_1} \beta^{q^j a} \sum_{l=0}^{t-1} \gamma^{q^l+k_2} \beta^{q^l b} \right)
= \sum_{i=1}^{t-1} \left( \sum_{j=0}^{n} \gamma^{q^j+k_1} + q^2 \sum_{i=1}^{t-1} \gamma^{q^j+k_2} \beta^{q^j a + q^l b} \right)
= \sum_{j=0}^{t-1} \left( \sum_{i=1}^{n} \gamma^{q^j+k_1} + q^2 \sum_{i=1}^{t-1} \beta^{q^j a + q^l b} \right) q^j
= \sum_{j=0}^{t-1} \left( \sum_{i=1}^{t-1} \gamma^{q^j+k_1} + q^2 \sum_{i=1}^{t-1} \beta^{q^j a + q^l b} \right) q^{j+q^k}
= \sum_{j=0}^{t-1} \left( \sum_{i=1}^{n} \gamma^{j+k_1+q^k} + q^2 \sum_{i=1}^{t-1} \beta^{j a + q^l b} q^{j+q^k} \right).
\]
Note that
\[
\sum_{l=0}^{p-1} \left( \sum_{i=1}^{n} \beta^{q^j a + b} q^{j+q^k} \right) q^{j+q^k} = \sum_{\beta \in U_m} \beta^{q^j a + b} - \sum_{\beta \in F_{q^s} \cap U_m} \beta^{q^j a + b} = \begin{cases} 0; & \text{if } \gcd(m, q^s - 1) \nmid q^j a + b, \\
-\gcd(m, q^s - 1); & \text{if } \gcd(m, q^s - 1) \mid q^j a + b. 
\end{cases}
\]
we have
\[
\sum_{i=1}^{n} e_{a,k_1}(\beta_i) e_{b,k_2}(\beta_i) = -\gcd(m, q^s - 1) \sum_{j=0}^{t-1} \sum_{l=0}^{s-1} \gamma^{q^j+k_1+q^k+l+q^k} \gcd(m, q^s - 1) \mid q^j a + b
= -\gcd(m, q^s - 1) p \sum_{j=0}^{t-1} \sum_{l=0}^{s-1} \gamma^{q^j+k_1+q^k+l+q^k} \gcd(m, q^s - 1) \mid q^j a + b
= 0.
\]
Since every codeword of $C(S)$ ($C(R)$) is an $F_q$-linear combination of $(e_{a,k_1}(\beta_i))_i$, ($(e_{b,k_2}(\beta_i))_i$, respectively), where $a \in S$, $b \in R$ and $0 \leq k_1, k_2 \leq s - 1$. We conclude that the Euclidean dual of $C(S)$ is $C(R)$, where $R = \mathfrak{A} \setminus S$.

In order to apply our result to quantum codes, we want to discuss the Hermitian dual of $C(S)$ as well.

**Proposition III.4.** Let $q = l^2$, then the Hermitian dual of $C(S)$ is $C(R)$, where $R = \mathfrak{A} \setminus \overline{S}$, $\overline{S} = \{ls|s \in S\}$.

**Proof:** It is clear that the Hermitian dual of $C(S)$ is the Euclidean dual of $C(lS)$. Then the desired result follows from Proposition III.3.

Now we state our main result.

**Theorem III.5.** Let $q = p^{2e}$ be a prime power, where $p$ is a prime number and $e$ is a positive integer. If there exist an integer $m$ and a finite set $S$ satisfying the following conditions:

1) $\gcd(q, m) = 1$ and $\text{ord}_m(q) = p^b$, where $b \geq 1$ is a positive integer;

2) $L \subseteq A, S = \bigcup_{a \in L} C_a, \quad \mathfrak{A} = \bigcup_{a \in A} C_a, S \cup \overline{S} \supseteq \mathfrak{A}$, where $C_a$ is $q$-cyclotomic coset modulo $m$ and $A = \{ \max(C_a)|0 \leq a \leq m - 1, |C_a| = p^b \}$;

then there exists a $p^e$-ary quantum code $[[n, k, d]]$, where $n = \frac{m - \gcd(m, q^b - 1)}{p}, k = \frac{2|S| - m + \gcd(m, q^b - 1)}{p}$ and $d \geq \left\lceil \frac{m + 1 - c}{p} \right\rceil$

where $c$ is the maximum element of set $S$.

**Proof:** By Proposition III.4, we have $C(\mathfrak{A} \setminus \overline{S}) = C(S)^{\perp_H}$. If $S \cup \overline{S} \supseteq \mathfrak{A}$, then $C(S)^{\perp_H} \subseteq C(S)$. Applying Theorem II.1 and Proposition II.2, the result follows.

Table III lists some quantum codes obtained from Theorem III.5 where max(S) is the maximum element of set S. In order to do comparison in Table III, we use the propagation rule (Theorem II.3) to obtain some of the codes with lengths that are listed in the table online [6]. Tables III and IV show that our quantum codes have larger minimum distance (larger dimension) than the previous quantum codes available when they have the same length and dimension (minimum distance, respectively).

IV. NEW QUANTUM SYNCHRONIZABLE CODES FROM DUADIC CODES

In this section we study a special class of cyclic codes to give a new family of quantum synchronizable codes.
TABLE I
NEW QUANTUM CODES

| $q$ | $m$ | $\text{max}(S)$ | quantum codes | $q$ | $m$ | $\text{max}(S)$ | quantum codes |
|-----|-----|------------------|---------------|-----|-----|------------------|---------------|
| 4   | 15  | 9                | [6, 0, 4]$_2$ | 4   | 15  | 13               | [6, 4, 2]$_2$ |
| 4   | 255 | 229              | [120, 40, 15]$_2$ | 4   | 255 | 229              | [120, 48, 14]$_2$ |
| 4   | 255 | 230              | [120, 92, 13]$_2$ | 4   | 255 | 230              | [120, 96, 12]$_2$ |
| 4   | 255 | 234              | [120, 64, 11]$_2$ | 4   | 255 | 234              | [120, 72, 10]$_2$ |
| 4   | 255 | 241              | [120, 80, 8]$_2$ | 4   | 255 | 242              | [120, 84, 7]$_2$ |
| 4   | 255 | 245              | [120, 92, 6]$_2$ | 4   | 255 | 246              | [120, 96, 5]$_2$ |
| 4   | 255 | 249              | [120, 104, 4]$_2$ | 4   | 255 | 250              | [120, 108, 3]$_2$ |
| 4   | 255 | 253              | [120, 116, 2]$_2$ | 9   | 104 | 90               | [32, 12, 6]$_4$ |
| 9   | 104 | 94               | [32, 16, 4]$_4$ | 9   | 104 | 98               | [32, 22, 3]$_4$ |
| 9   | 104 | 101              | [32, 28, 2]$_4$ | 9   | 104 | 104              | [32, 19, 3]$_4$ |
| 9   | 728 | 728              | [240, 204, 8]$_2$ | 9   | 728 | 704              | [240, 206, 9]$_3$ |
| 9   | 728 | 728              | [240, 214, 6]$_2$ | 9   | 728 | 716              | [240, 220, 5]$_3$ |
| 9   | 728 | 718              | [240, 224, 4]$_3$ | 9   | 728 | 722              | [240, 230, 3]$_3$ |
| 9   | 728 | 725              | [240, 236, 2]$_3$ | 16  | 85  | 67               | [40, 12, 10]$_4$ |
| 16  | 85  | 71               | [40, 16, 8]$_4$ | 16  | 85  | 73               | [40, 20, 7]$_4$ |
| 16  | 85  | 75               | [40, 22, 6]$_4$ | 16  | 85  | 77               | [40, 26, 5]$_4$ |
| 16  | 85  | 79               | [40, 30, 4]$_4$ | 16  | 85  | 81               | [40, 34, 3]$_4$ |
| 16  | 85  | 85               | [40, 38, 2]$_4$ | 16  | 255 | 203              | [120, 36, 27]$_4$ |
| 16  | 255 | 229              | [120, 40, 24]$_4$ | 16  | 255 | 229              | [120, 44, 23]$_4$ |
| 16  | 255 | 235              | [120, 48, 22]$_4$ | 16  | 255 | 235              | [120, 52, 21]$_4$ |
| 16  | 255 | 241              | [120, 56, 20]$_4$ | 16  | 255 | 241              | [120, 60, 19]$_4$ |
| 16  | 255 | 237              | [120, 62, 18]$_4$ | 16  | 255 | 237              | [120, 66, 16]$_4$ |
| 16  | 255 | 257              | [120, 72, 15]$_4$ | 16  | 255 | 257              | [120, 74, 14]$_4$ |
| 16  | 255 | 251              | [120, 78, 13]$_4$ | 16  | 255 | 251              | [120, 82, 12]$_4$ |
| 16  | 255 | 235              | [120, 86, 11]$_4$ | 16  | 255 | 235              | [120, 90, 10]$_4$ |
| 16  | 255 | 241              | [120, 94, 8]$_4$ | 16  | 255 | 243              | [120, 98, 6]$_4$ |
| 16  | 255 | 249              | [120, 102, 6]$_4$ | 16  | 255 | 247              | [120, 106, 6]$_4$ |
| 16  | 255 | 243              | [120, 110, 4]$_4$ | 16  | 255 | 241              | [120, 114, 3]$_4$ |
| 16  | 255 | 233              | [120, 118, 2]$_4$ | 16  | 255 | 233              | [120, 122, 3]$_4$ |

TABLE II
QUANTUM CODES COMPARISON

| quantum codes from Table I | quantum codes from Table II |
|-----------------------------|-----------------------------|
| [120, 40, 15]$_2$           | [120, 40, 14]$_2$           |
| [120, 48, 14]$_2$           | [120, 48, 13]$_2$           |
| [120, 92, 13]$_2$           | [120, 92, 12]$_2$           |
| [120, 60, 12]$_2$           | [120, 60, 11]$_2$           |
| [120, 64, 11]$_2$           | [120, 64, 10]$_2$           |
| [120, 72, 10]$_2$           | [120, 72, 9]$_2$            |

A. Duadic Codes

In this subsection, we recall the definition and basic properties of duadic codes of length $n$ over a finite field $\mathbb{F}_q$ such that $\text{gcd}(n, q) = 1$.

Let $S_0$, $S_1$ be the defining sets of two cyclic codes of length $n$ over $\mathbb{F}_q$ such that

1) $S_0 \cap S_1 = \emptyset$,
2) $S_0 \cup S_1 = \{1, 2, \ldots, n-1\}$, and
3) $a S_i \pmod{n} = S_{i+1} \pmod{2}$ for some $a$ coprime to $n$.

In particular, each $S_i$ is a union of $q$-ary cyclotomic cosets modulo $n$. Then $|S_0| = |S_1|$, we have $|S_i| = \frac{n-1}{2}$. Hence $n$ must be odd.

Let $\omega$ be a primitive $n$-th root of unity over a field $\mathbb{F}_q$. For $i \in \{0, 1\}$, the odd-like duadic code $D_i$ is a cyclic code of length $n$ over $\mathbb{F}_q$ with defining set $S_i$ and generator polynomial

$$g_i(x) = \prod_{j \in S_i} (x - \omega^j).$$

The even-like duadic code $C_i$ is defined as a cyclic code with defining set $S_i \cup \{0\}$ and generator polynomial $(x-1)g_i(x)$. Then the dimension of $D_i$ is $(n+1)/2$ and dimension of $C_i$ is $(n-1)/2$ respectively. Obviously $C_i \subseteq D_i$.

**Lemma IV.1.** [13] Let $C_i$ and $D_i$ be the even-like and odd-like duadic codes of length $n$ over $\mathbb{F}_q$, where $i \in \{0, 1\}$. Then

1) $C_i^\perp = D_i$ if and only if $-S_i \equiv S_{i+1} \pmod{2}$ ($\pmod{n}$).
2) $C_i^\perp = D_{i+1} \pmod{2}$ if and only if $-S_i \equiv S_i \pmod{n}$.

The following well known fact gives a lower bound for the minimum distance of odd-like duadic codes.
Lemma IV.2. \[\text{Let } D_0 \text{ and } D_1 \text{ be a pair of odd-like duadic codes of length } n \text{ over } \mathbb{F}_q. \text{ If } -S_i \equiv S_{i+1} \pmod{2} \pmod{n}, \text{ then their minimum distances in both codes are the same, say } d_0. \text{ We also have } d_0^2 - d_0 + 1 \geq n.\]

B. New Quantum Synchronizable Codes

We now provide a construction for quantum synchronizable codes designed from duadic codes. We first recall the following lemma, which gives a connection between cyclotomic cosets and irreducible polynomials.

Lemma IV.3. \[\text{Let } \omega \text{ be a primitive } n\text{-th root of unity over a field containing } \mathbb{F}_q, \text{ where } \gcd(q, n) = 1. \text{ Then the minimal polynomial of } \omega^i \text{ with respect to } \mathbb{F}_q \text{ is } \]
\[M^{(i)}(x) = \prod_{j \in C_{i,n}} (x - \omega^j),\]
where \(C_{i,n}\) is the unique \(q\)-cyclotomic coset modulo \(n\) containing \(i\).

Now we assume that \(p\) is an odd prime and \(p \equiv -1 \pmod{8}\). Let \(m, n\) be positive integers, \(m \leq n\), \(g\) be a primitive root modulo \(p^n\), and \(\omega\) be a primitive \(p^n\)-th root of unity over a field containing \(\mathbb{F}_2\). Define
\[g_m = g \pmod{p^m}, \quad \omega_m = \omega^{p^n - m}.\]

Then \(g_m\) is a primitive root modulo \(p^n\) and \(\omega_m\) is a primitive \(p^n\)-th root of unity.

Set
\[S_{m0} = \langle g_m^2 \rangle, \quad S_{m1} = g_mS_{m0},\]
where \(\langle g_m^2 \rangle\) denotes the subgroup generated by \(g_m^2\) of \(\mathbb{Z}_{p^n}^\ast\). It is obvious that
\[S_{m0} \cup S_{m1} = \mathbb{Z}_{p^n}^\ast, \quad S_{m0} \cap S_{m1} = \emptyset.\]

We also define polynomials corresponding to \(S_{mj}\), \(j = 0, 1\):
\[d_{mj}(x) = \prod_{i \in S_{mj}} (x - \omega_i^m), \quad j = 0, 1.\]

We can also verify that
\[x^{p^n} - 1 = (x - 1)(\prod_{m=1}^{n} d_{m0}(x))(\prod_{m=1}^{n} d_{m1}(x)).\]

Since \(p \equiv -1 \pmod{8}\), then \(2 \in S_{m0}\), whence \(d_{m0}(x) \in \mathbb{F}_2[x]\) from Lemma IV.3. Let
\[g_m(x) = d_{10}(x)d_{20}(x)\cdots d_{m0}(x),\]
and \(C_m\) denote the cyclic code over \(\mathbb{F}_2\) of length \(p^n\) generated by the polynomial \(g_m(x)\).

Lemma IV.4. \(\text{ord}(d_{m0}(x)) = p^n.\)

Proof: Since all the roots of \(d_{m0}(x)\) are \(p^n\)-th root of unity, and \(d_{m0}(\omega_n) = 0\), where \(\omega_n\) is a primitive \(p^n\)-th root of unity. Then by Lemmas II.4 and II.5 \(\text{ord}(d_{m0}(x)) = p^n.\)

Theorem IV.5. \[\text{Let } n > 1 \text{ be a positive integer, } p \text{ be an odd prime and } p \equiv -1 \pmod{8}. \text{ Then for pair } a_l, a_r \text{ of nonnegative integers such that } a_l + a_r < p^n, \text{ there exists a quantum synchronizable } (a_l, a_r) - \left\lceil \frac{p^n + a_l + a_r - 1}{2} \right\rceil\text{ code that corrects at least up to } \left\lfloor \frac{d_n-1}{2} \right\rfloor \text{ phase errors, where } d_n^2 - d_n + 1 \geq p^n.\]
Proof: Take the code $C_n$ and $C_m$, where $m < n$, then $C_n \subseteq C_m$. By Lemma IV.2, $C_n$ is an odd-like duadic code with parameters $[p^n, p^{n+1}/2, d_n]$, where $d_n - d_m + 1 \geq p^n$. Since $p \equiv -1 \pmod{8}$, we have $S_{n0} = -S_{n1}$. By Lemma IV.1 $C_n \supseteq C_m$. Applying Theorem IV.3, the assertion follows.

In order to get more results, we discuss the factorization of $d_{n0}(x)$.

Lemma IV.6. Let $n > 1$ be a positive integer, $p$ be an odd prime and $p \equiv -1 \pmod{8}$. If $\text{ord}_p(2) = t$, then $d_{n0}(x)$ can be factorized into $\frac{p^n - 1}{2t}$ irreducible polynomials of degree $t$ over $\mathbb{F}_2$.

Proof: Let $S_{i,p^n} = \{1, 2^j \pmod{p^n} | j = 0, 1, \ldots \}$ denoting the 2-cyclotomic coset modulo $p^n$ containing $i$. If $\text{ord}_p(2) = t$, then $t$ is the minimal integer such that $p^n | 2^t - 1$, so $|S_{i,p^n}| = t$ for all $\gcd(i, p^n) = 1$. Since all the roots of $d_{n0}(x)$ are with the form $\omega^j$, where $\gcd(j, p^n) = 1$. Then by Lemma IV.3, $d_{n0}(x)$ can be factorized into $\frac{p^n - 1}{2t}$ irreducible polynomials of degree $t$ over $\mathbb{F}_2$.

Theorem IV.7. Let $n \geq 1$ be a positive integer, $p$ be an odd prime and $p \equiv -1 \pmod{8}$. If $\text{ord}_p(2) = t_m$, $m = 1, 2, \ldots, n$. Then for nonnegative integers $a_i, a_r, u_m \ (m = 1, 2, \ldots, n)$ such that $a_i + a_r < p^n$, $1 \leq u_i \leq \frac{p^n - 1}{2t_m}$, $0 \leq u_l \leq \frac{p^{n-1}(p-1)}{2t_l}$ for $l = 1, 2, \ldots, n - 1$, and $\sum_{i=1}^{n} u_i \geq 1$, there exists a quantum synchronizable $(a_i, a_r) - \frac{[p^n + a_i + a_r, p^n - 2 - 2\sum_{j=1}^{n} u_i]}{2}$ code.

Proof: By Lemma IV.6, $d_{n0}(x) = \prod_{j=1}^{\frac{p^n - 1}{2t_m}} h_{mj}(x)$, where $h_{mj}(x)$, $j = 1, \ldots, \frac{p^{n-1}(p-1)}{2t_l}$, $m = 1, 2, \ldots, n$ are irreducible polynomials over $\mathbb{F}_2$.

Then let

$$f_1(x) = \prod_{i=1}^{n} \prod_{j=1}^{u_i} h_{ij}(x), \quad 1 \leq u_i \leq \frac{p^n - 1}{2t_n}, \quad 0 \leq u_l \leq \frac{p^{n-1}(p-1)}{2t_l} \quad \text{for} \quad l = 1, 2, \ldots, n - 1, \quad \text{and} \quad \sum_{i=1}^{n} u_i \geq 1,$$

$$f_2(x) = \prod_{i=1}^{n} \prod_{j=1}^{u_i} h_{ij}(x), \quad v_n < u_n, v_l \leq u_l \quad \text{for} \quad l = 1, 2, \ldots, n - 1, \quad \text{and} \quad \sum_{i=1}^{n} v_i \geq 1,$$

and $D_1$ ($D_2$) denote the cyclic code of length $p^n$ generated by the polynomial $f_1(x)$ ($f_2(x)$, respectively).

Then applying Theorem IV.3 for nonnegative integers $a_i, a_r$ and $u_m \ (m = 1, 2, \ldots, n)$ such that $a_i + a_r < p^n$, $1 \leq u_i \leq \frac{p^n - 1}{2t_m}$, $0 \leq u_l \leq \frac{p^{n-1}(p-1)}{2t_l}$ for $l = 1, 2, \ldots, n - 1$, and $\sum_{i=1}^{n} u_i \geq 1$, we obtain a quantum synchronizable $(a_i, a_r) - \frac{[p^n, p^n - 2 - 2\sum_{j=1}^{n} u_i]}{2}$ code.

Remark IV.1. It is easy to see that Theorem IV.2 is a generalization of the result in [20].

Example IV.8. Let $p = 31$, $n = 2$. It can be verified that $g = 3$ is a primitive root modulo $31^2$. Take

$$S_{20} = \{9^i \pmod{961} | i \in \mathbb{N} \}, \quad S_{10} = \{9^i \pmod{31} | i \in \mathbb{N} \}.$$

Then $|S_{20}| = 465$ and $|S_{10}| = 15$. We can get that $\text{ord}_{31}(2) = 155$ and $\text{ord}_{31}(2) = 5$, then $S_{20}$ ($S_{10}$) is the union of 3 cyclotomic cosets as follows:

$$S_{20} = T_{21} \cup T_{22} \cup T_{23}, \quad S_{10} = T_{11} \cup T_{12} \cup T_{13},$$

where $T_{21} = \{1, 2, 4, 8, 16, 32, 33, 35, \ldots \}$, $T_{22} = \{5, 9, 10, 18, 20, 36, 40, 41, \ldots \}$, $T_{23} = \{7, 14, 19, 25, 28, 38, 45, 50, \ldots \}$, $T_{11} = \{1, 2, 4, 8, 16 \}$, $T_{12} = \{5, 9, 10, 18, 20 \}$ and $T_{13} = \{7, 14, 19, 25, 28 \}$. Let $\omega$ be a primitive 961-th root of unity over a field containing $\mathbb{F}_2$. Set

$$h_{21}(x) = \prod_{j \in T_{21}} (x - \omega^j), \quad h_{11}(x) = \prod_{j \in T_{11}} (x - \omega^{31j}), \quad i = 1, 2, 3.$$

Then $h_{ij}(x) \in \mathbb{F}_2[x]$ for $i = 1, 2, j = 1, 2, 3$. Applying Theorem IV.7, we obtain the quantum synchronizable $(a_i, a_r) - \frac{[961 + a_i + a_r, k]}{2}$ codes listed in Table IV where $a_i + a_r < 961$.

REFERENCES

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, “On quantum and classical BCH codes,” IEEE Trans. Inform. Theory, vol. 53, no. 3, pp. 1183–1188, 2007.
[2] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” IEEE Trans. Inform. Theory, vol. 47, no. 7, pp. 3065–3072, 2001.
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over GF(4),” IEEE Trans. Inform. Theory, vol. 44, no. 4, pp. 1369–1387, 1998.
[4] H. Chen, S. Ling, and C. Xing, “Quantum codes from concatenated algebraic-geometric codes,” IEEE Trans. Inform. Theory, vol. 51, no. 8, pp. 2915–2920, 2005.
[5] Y. Ding, L. Jin, and C. Xing, “Good linear codes from polynomial evaluations,” IEEE Trans. Commun., vol. 60, no. 2, pp. 357–363, 2012.
[6] Y. Edel, “Some good quantum twisted codes,” Online available at [https://www.mathi.uni-heidelberg.de/~yes/MatritzenQBCH/QBCHIndex.html]
[7] K. Feng, S. Ling, and C. Xing, “Asymptotic bounds on quantum codes from algebraic geometry codes,” IEEE Trans. Inform. Theory, vol. 52, no. 3, pp. 986–991, 2006.
TABLE IV
QUANTUM SYNCHRONIZABLE \(\{a_1, a_r\} - [[961 + a_1 + a_r, k]]_2\) CODES, WHERE \(a_1 + a_r < 961\)

| \(f_1(x)\) | \(f_2(x)\) | \(k_1\) | \(k\) |
|---|---|---|---|
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 481 | 1 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 636 | 311 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 486 | 11 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 641 | 321 |
| \(h_{11}(x)\Pi_{i=1}^2 h_{21}(x)\) | \(h_{11}(x)\Pi_{i=1}^2 h_{21}(x)\) | 491 | 21 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 791 | 621 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 496 | 31 |
| \(h_{11}(x)\Pi_{i=1}^2 h_{21}(x)\) | \(h_{11}(x)\Pi_{i=1}^2 h_{21}(x)\) | 646 | 331 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | 796 | 631 |
| \(\Pi_{i=1}^2 h_i(x)\Pi_{j=1}^3 h_{2j}(x)\) | \(h_{21}(x)\) | 651 | 341 |
| \(h_{11}(x)\Pi_{j=1}^3 h_{21}(x)\) | \(h_{11}(x)\) | 801 | 641 |

[8] K. Feng and C. Xing, “A new construction of quantum error-correcting codes,” Trans. Amer. Math. Soc., vol. 360, no. 4, pp. 2007–2019, 2008.
[9] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, “Algebraic techniques in designing quantum synchronizable codes,” Phys. Rev. A, vol. 88, no. 1, p. 012318, 2013.
[10] Y. Fujiwara and P. Vandyveld, “Quantum synchronizable codes from finite geometries,” IEEE Trans. Inform. Theory, vol. 60, no. 11, pp. 7345–7354, Nov 2014.
[11] Y. Fujiwara, “Block synchronization for quantum information,” Phys. Rev. A, vol. 87, no. 2, p. 022344, 2013.
[12] M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes,” Online available at [http://www.codeatales.de](http://www.codeatales.de), 2007, accessed on 2014-12-21.
[13] W. C. Huffman and V. Pless, Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003.
[14] L. Jin and C. Xing, “A construction of quantum codes via a class of classical polynomial codes,” in Proc. IEEE Int. Symp. Information Theory (ISIT), 2012, pp. 339–342.
[15] ——, “A construction of new quantum MDS codes,” IEEE Trans. Inform. Theory, vol. 60, no. 5, pp. 2921–2925, 2014.
[16] G. G. La Guardia, “On the construction of nonbinary quantum BCH codes,” IEEE Trans. Inform. Theory, vol. 60, no. 3, pp. 1528–1535, 2014.
[17] Z. Li, L. Xing, and X. Wang, “Quantum generalized Reed-Solomon codes: unified framework for quantum maximum-distance-separable codes,” Phys. Rev. A (3), vol. 77, no. 1, p. 012308, 4, 2008.
[18] R. Lidl and H. Niederreiter, Finite fields, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1997, vol. 20, with a foreword by P. M. Cohn.
[19] X. Lin, “Quantum cyclic and constacyclic codes,” IEEE Trans. Inform. Theory, vol. 50, no. 3, pp. 547–549, 2004.
[20] S. Ling, H. Niederreiter, and C. Xing, “Symmetric polynomials and some good codes,” Finite Fields Appl., vol. 7, no. 1, pp. 142–148, 2001, dedicated to Professor Chao Ko on the occasion of his 90th birthday.
[21] E. M. Rains, “Nonbinary quantum codes,” IEEE Trans. Inform. Theory, vol. 45, no. 6, pp. 1827–1832, 1999.
[22] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” Phys. Rev. A, vol. 52, no. 4, p. R2493, 1995.
[23] A. Steane, “Multiple-particle interference and quantum error correction,” Proc. Roy. Soc. London Ser. A, vol. 452, no. 1954, pp. 2551–2577, 1996.
[24] A. M. Steane, “Enlargement of Calderbank-Shor-Steane quantum codes,” IEEE Trans. Inform. Theory, vol. 45, no. 7, pp. 2492–2495, 1999.
[25] M. Steinbach and D. Hachenberger, “A class of quaternary linear codes improving known minimum distances,” Des. Codes Cryptogr., pp. 1–13, 2014. [Online]. Available: [http://dx.doi.org/10.1007/s10623-014-0021-3](http://dx.doi.org/10.1007/s10623-014-0021-3)
[26] Y. Xie, J. Yuan, and Y. Fujiwara, “Quantum synchronizable codes from quadratic residue codes and their supercodes,” in IEEE Inform. Theory Workshop, 2014, pp. 172–176.
[27] C. Xing and S. Ling, “A class of linear codes with good parameters,” IEEE Trans. Inform. Theory, vol. 46, no. 6, pp. 2184–2188, 2000.