Good Stabilizer Codes from Quasi-Cyclic Codes over $\mathbb{F}_4$ and $\mathbb{F}_9$

Martianus Frederic Ezerman, San Ling, Buket Özkaya
School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371
Emails: {fredezerman, lingsan, buketozkaya}@ntu.edu.sg

Patrick Solé
Aix-Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France
Email: sole@enst.fr

Abstract—We apply quantum Construction X on quasi-cyclic codes with large Hermitian hulls over $\mathbb{F}_4$ and $\mathbb{F}_9$ to derive good qubit and qudit stabilizer codes, respectively. In several occasions we obtain quantum codes with strictly improved parameters than the current record. In numerous other occasions we obtain quantum codes with best-known performance. For the qudit ones we supply a systematic construction to fill some gaps in the literature.

Index Terms—Construction X, Hermitian hull, quantum stabilizer code, quasi-cyclic code.

I. INTRODUCTION

Turning large scale quantum computing into practical reality remains a huge challenge to engineer. Keeping the errors in the system below the fidelity threshold is key since noise, if can be kept below a certain level, is not an obstacle to resilient quantum computation [10]. The possibility of correcting errors in the qubit systems was shown, e.g., in the early works of Shor [16], Steane [17] and Laflamme et al. [11]. Developments in this active topic up to 2011 is well-documented in [12]. Advances continue to be made as effort intensifies in the race to be among the first to make quantum computing scalable.

Let $F_q$ denote the finite field with $q$ elements, where $q$ is a prime power. The stabilizer formalism, discussed in Gottesman’s thesis [7] and, in the qubit (quantum bit) case, described in the language of group algebra by Calderbank et al. in [3], remains the most widely-studied model of error control. Ketchum et al. generalized the formalism to $q$-ary quantum codes derived from classical codes over $F_{q^m}$ in [9].

Let $V_n = (C^n)^{\otimes n}$ be the $n$-fold tensor power of $C^n$. A $q$-ary quantum code of length $n$ is a subspace $Q$ of $V_n$ with dimension $K \geq 1$. If the code $Q$ is a stabilizer code, we use the notation $Q = [n, k, d]_q$, where $k = \log_q K$. The propagation rules in the next proposition will be useful later.

Proposition 1. ([3, Thm. 6]) Let $Q$ be an $[n, k, d]_q$ code. Then the following quantum codes exist.

i) $[n, k-1, \geq d]_q$ (by subcode construction).
ii) $[n+1, k, \geq d]_q$ (by lengthening).
iii) $[n+1, k, \geq d-1]_q$ (by puncturing).

Lisonek and Singh proposed an interesting modification to the construction of qubit stabilizer codes by relaxing the self-orthogonality requirement in [14]. Their framework, inspired by Construction X in the classical setup (see [15, Chapter 18 §7.1]), yielded a number of better qubit codes than the previous best-known. These better codes came from applying their construction to specifically chosen cyclic codes over $F_4$.

Construction X for qubit codes generalizes naturally to $q$-ary quantum codes. The case of $p$-ary for primes $p$ was shown in [4, Thm. 4]. The first statement in the proof of [14, Prop. 1] holds for any $q$ since the trace mapping $\text{Tr}_{F_{q^2}/F_q}$ is onto. The construction of the orthonormal set $B$ in [14, Prop. 1] can then be replicated and the general version of [14, Thm. 2] follows from the exact same argument as in the original version.

It is unfortunate that the $p$-ary codes, with $p > 2$, in [4, Table 1] are compared to qubit codes. The authors’ claim that the obtained $p$-ary quantum codes improve on the parameters of known qubit codes is incorrect. The codes being compared live from the exact same argument as in the original version.

This work uses self-orthogonal or nearly self-orthogonal quasi-cyclic codes over $F_4$ and $F_9$ as ingredients in the quantum Construction X to derive good qubit and qudit (3-ary quantum) codes. Such codes have a good chance to be implemented in actual quantum processors. We exhibit quantum codes with parameters that strictly improve on the currently best-known ones and list those that match the best-known ones in performance.

Let $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{u} := (u_1, \ldots, u_n)$ be vectors in $F_{q^2}^n$. Their Hermitian inner product $\langle \vec{v}, \vec{u} \rangle_H$ is $\sum_{i=1}^{n} v_i \bar{u}_i$. The weight of $\vec{v}$, denoted by $\text{wt}(\vec{v})$, is the number of nonzero entries in $\vec{v}$. A linear code $C$ over $F_{q^2}$ of length $n$, dimension $k$ and minimum distance $d := d(C)$ is denoted by $[n, k, d]_{q^2}$. We let $A + B := \{ \vec{v} + \vec{u} : \vec{v} \in A, \vec{u} \in B \}$, for subspaces $A$ and $B$ in $F_{q^2}^n$, and use $\text{dim}(A)$ to abbreviate $\text{dim}_{F_{q^2}}(A)$.

Instead of starting with an $[n, k, d]_{q^2}$-code $C$ that contains its Hermitian dual $C^\perp$ with parameters $[n, n-k, d^\perp]_{q^2}$, we will begin with a Hermitian self-orthogonal $[n, k, d]_{q^2}$-code $C$, i.e., $C \subseteq C^\perp$. We end this introduction by restating quantum Construction X in the form that matches our preference.

Theorem 2. ([14, Thm. 2] and [4, Thm. 4]). For an $[n, k]_{q^2}$-linear code $C$, let $e := k - \text{dim}(C \cap C^\perp)$. Then there exists an $[n+e, n-2k+e, d(Q)]_{q^2}$ quantum stabilizer code $Q$ with $d(Q) \geq \min\{d(C^\perp), d(C + C^\perp)+1\}$.

Note that $e = 0$ describes the usual stabilizer construction.
Stabilizer codes from QC codes of index 2 was discussed in [6]. To avoid a sharp drop in \(d\), we would like \(e\) to be small, i.e., the Hermitian hull \(C \cap C^{-1}\) to be large. The search reported in [14] on the family of linear cyclic codes over \(F_4\) found improved qubit codes with \(e \in \{1, 2, 3\}\).

II. QUASI-CYCLIC CODES

Let \(m\) and \(\ell\) be positive integers such that \(\gcd(m, q) = 1\). A linear code \(C\) of length \(mt\) over \(F_q\) is called a quasi-cyclic (QC) code of index \(\ell\) if it is invariant under shift of codewords by \(\ell\) positions and \(\ell\) is the minimal number with this property. The code \(C\) is cyclic when \(\ell = 1\). If we view any codeword of \(C\) as an \(m \times \ell\) array

\[
\vec{c} = \begin{pmatrix}
c_{0,0} & \cdots & c_{0,\ell-1} \\
\vdots & \ddots & \vdots \\
c_{m-1,0} & \cdots & c_{m-1,\ell-1}
\end{pmatrix},
\]

then being invariant under shift by \(\ell\) units in \(F_q^{mt}\) amounts to being closed under row shift in \(F_q^{m\times \ell}\).

Consider the principal ideal \(I = (x^m - 1)\) of \(F_q[x]\) and define the quotient ring \(R := F_q[x]/I\). We associate a vector \(\vec{c} \in F_q^{m\times \ell}\) as in (1) with an element of \(R^\ell\) as

\[
\vec{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell,
\]

where for each \(0 \leq t \leq \ell - 1,

c_t(x) := c_{0,t} + c_{1,t}x + c_{2,t}x^2 + \cdots + c_{m-1,t}x^{m-1} \in R.
\]

Then, the following map is an \(R\)-module isomorphism.

\[
\phi: F_q^{m\times \ell} \rightarrow R^\ell
\]

\[
\vec{c} \rightarrow \vec{c}(x).
\]

For \(\ell = 1\), this is the classical polynomial representation of cyclic codes. Note that the row shift in \(F_q^{m\times \ell}\) corresponds to componentwise multiplication by \(x\) in \(R^\ell\). Thus, a \(q\)-ary QC code \(C\) of length \(mt\) and index \(\ell\) is an \(R\)-submodule in \(R^\ell\).

A QC code over \(F_q\) decomposes into shorter codes over field extensions of \(F_q\). Further details are given in [13]. The self-reciprocal polynomial \(x^m - 1\) factors into irreducible polynomials in \(F_q[x]\) as

\[
x^m - 1 = g_1(x) \cdots g_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x),
\]

where \(g_i\)'s are self-reciprocal and \(h_j^*\) denotes the reciprocal of \(h_j\), for all \(i, j\). Since \(\gcd(m, q) = 1\), there are no repeating factors in (5). By the Chinese Remainder Theorem (CRT),

\[
R \cong \bigoplus_{i=1}^s F_q[x]/(g_i(x)) \oplus \bigoplus_{j=1}^r \left( F_q[x]/(h_j(x)) \oplus F_q[x]/(h_j^*(x)) \right).
\]

Since each \(g_i(x), h_j(x)\) and \(h_j^*(x)\) divides \(x^m - 1\), their roots are powers of some fixed primitive \(m\)-th root of unity \(\xi\). For each \(i \in \{1, \ldots, s\}\), let \(u_i\) be the smallest nonnegative integer such that \(g_i(\xi^{u_i}) = 0\). For each \(j \in \{1, \ldots, r\}\), let \(v_j\) be the smallest nonnegative integer such that \(h_j(\xi^{v_j}) = h_j^*(\xi^{-v_j}) = 0\). Since all factors in (5) are irreducible, direct summands in (6) are isomorphic to field extensions of \(F_q\). Let \(G_i := F_q[\xi^{u_i}] \simeq F_q[x]/(g_i(x)), H_j := F_q[\xi^{v_j}] \simeq F_q[x]/(h_j(x))\) and \(H_j'' := F_q[\xi^{-v_j}] \simeq F_q[x]/(h_j^*(x))\) denote those extensions, for each \(i \) and \(j\), respectively. By CRT, the decomposition of \(R\) in (6) now becomes

\[
R \cong \left( \bigoplus_{i=1}^s F_q[\xi^{u_i}] \right) \oplus \left( \bigoplus_{j=1}^r \left( H_j + \mathbb{H}_j'' \right) \right)
\]

\[
f(x) \rightarrow \left( (f(\xi^{u_i}))_{1 \leq i \leq s}, (f(\xi^{v_j}))_{1 \leq j \leq r}, (f(\xi^{-v_j}))_{1 \leq j \leq r} \right),
\]

This implies that

\[
R^\ell \cong \left( \bigoplus_{i=1}^s G_i^\ell \right) \oplus \left( \bigoplus_{j=1}^r \left( H_j^\ell + \mathbb{H}_j^{''\ell} \right) \right).
\]

\[
\vec{f}(x) \rightarrow \left( (\vec{f}(\xi^{u_i}))_{1 \leq i \leq s}, (\vec{f}(\xi^{v_j}))_{1 \leq j \leq r}, (\vec{f}(\xi^{-v_j}))_{1 \leq j \leq r} \right),
\]

where \(\vec{f}(a)\) denotes the componentwise evaluation at \(a\), for any element \(\vec{f}(x) = (f_0(x), \ldots, f_{\ell-1}(x)) \in R^\ell\). Hence, as an \(R\)-submodule of \(R^\ell\), a QC code \(C \subseteq R^\ell\) decomposes into

\[
C \cong \left( \bigoplus_{i=1}^s C_i \right) \oplus \left( \bigoplus_{j=1}^r \left( C_j + C_j'' \right) \right).
\]

Here \(C_i\)'s are the \(G_i\)-linear codes of length \( \ell \), for all \( i = 1, \ldots, r\), while \(C_j\)'s and \(C_j''\)'s are the \(H_j\)- and \(H_j''\)-linear codes of length \( \ell \), respectively, for all \( j = 1, \ldots, r\). We call these linear codes of length \( \ell \) over various extensions of \(F_q\) the constituents of \(C\).

Let \(C \subseteq R^\ell\) be generated by \(\{\vec{f}_1(x), \ldots, \vec{f}_r(x)\}\), where \(\vec{f}_j(x) = (f_{0,j}(x), \ldots, f_{\ell-1,j}(x)) \in R^\ell\), for each \( 1 \leq j \leq n \). Then, for \( 1 \leq i \leq s \) and \( 1 \leq j \leq r \), we have

\[
C_i = \text{Span}_{G_i}[\vec{f}_j(\xi^{u_i}) : 1 \leq j \leq n],
\]

\[
C_j = \text{Span}_{H_j}[\vec{f}_j(\xi^{v_j}) : 1 \leq j \leq n],
\]

\[
C_j'' = \text{Span}_{H_j''}[\vec{f}_j(\xi^{-v_j}) : 1 \leq j \leq n].
\]

Conversely, let \(C_i \subseteq G_i^\ell\), \(C_j \subseteq H_j^\ell\) and \(C_j'' \subseteq H_j^{''\ell}\) be arbitrary linear codes, for each \( i \in \{1, \ldots, s\}\) and each \( j \in \{1, \ldots, r\}\). Then, by [13, Thm. 5.1], an arbitrary codeword \(\vec{c}\) in the corresponding \(q\)-ary QC code \(C\) described as in (9) can be written as an \(m \times \ell\) array like in (1) such that each row of \(\vec{c}\) is of the form

\[
\vec{c}_g = \frac{1}{m} \left( \sum_{i=1}^s \text{Tr}_{G_i/F_q} (\lambda_i, t^{\xi^{u_i}}) + \sum_{j=1}^r \left[ \text{Tr}_{H_j/F_q} (\lambda_j, t^{\xi^{-v_j}}) + \text{Tr}_{H_j''/F_q} (\lambda_j'', t^{\xi^{-v_j}}) \right] \right),
\]

for \( 0 \leq g \leq m - 1\), where \(\lambda_i = (\lambda_{i,0}, \ldots, \lambda_{i,\ell-1}) \in C_i\), for all \( i \), \(\lambda_j = (\lambda_{j,0}, \ldots, \lambda_{j,\ell-1}) \in C_j\) and \(\lambda_j'' = (\lambda_{j,0}'', \ldots, \lambda_{j,\ell-1}'') \in C_j''\), for all \( j \). Since \(\frac{1}{m} C = C\), we can cancel \(\frac{1}{m}\) out. Note that, in this representation, the row shift invariance of codewords amounts to being closed under multiplication by \(\xi^{-1}\).

The cardinality, say \(q_0\), of each \(G_i\) is an even power of \(q\). Each \(G_i\) is equipped with the Hermitian inner product. For \( 1 \leq j \leq r \), \(H_j\) and \(H_j''\) are equipped with the usual Euclidean inner product. Observe that \(H_j'' = H_j^{''}\) follows from the fact that \(F_q(\alpha^{u_i}) = F_q(\alpha^{v_i-1})\), for any \( a \in \{0, \ldots, m - 1\} \).
The dual of a QC code is also QC. For the proof of the following result we refer to [13].

**Proposition 3.** Let \( C \) be a QC code with CRT decomposition as in (9). Then \( C^{⊥_H} \) is of the form
\[
C^{⊥_H} = \left( \bigoplus_{i=1}^{r} C^t_i \right) \oplus \left( \bigoplus_{j=1}^{r} \left( C_j^{t,E} \oplus C_j^{⊥_E} \right) \right),
\]
where \( ⊥_H \) denotes the Hermitian dual on \( G^t_i \) and \( ⊥_E \) denotes the Euclidean dual on \( H^t_j = H^t_j^\prime \).

By (9) and (12), we characterize self-orthogonal QC codes.

**Theorem 4.** Let \( C \) be a q-ary QC code of length \( ml \) whose CRT decomposition is as in (9). Then \( C \) is Hermitian self-orthogonal if and only if \( C_1 \) is Hermitian self-orthogonal over \( \mathbb{F}_q \), for all \( 1 \leq i \leq s \), and \( C_i^{⊥_E} \subseteq C_i^{⊥_H} \) (or equivalently \( C_i^{⊥_E} \subseteq C_i^{⊥_H} \)) over \( \mathbb{H}^t_j = \mathbb{H}^t_j^\prime \), for all \( 1 \leq j \leq r \).

**III. DESIGNING THE HERMITIAN HULL**

From this point on we consider Hermitian self-orthogonal or nearly self-orthogonal QC codes over \( \mathbb{F}_{q^2} \). As was done in Theorem 4 for self-orthogonality, the CRT decompositions of the QC code \( C \) in (9) and of its Hermitian dual \( C^{⊥_H} \) in (12) characterize nearly self-orthogonal QC codes.

Let \( k \) denote the dimension of \( C \) over \( \mathbb{F}_{q^2} \). Clearly, \( C^{⊥_H} \) has dimension \( ml - k \). Let \( e_i := |G_i : \mathbb{F}_{q^2}| = \deg(g_i(x)) \) and \( k_i := \dim_{\mathbb{F}_{q^2}}(C_i) \), for all \( 1 \leq i \leq s \). Let \( e_j := |H^t_j : \mathbb{F}_{q^2}| = \dim_{\mathbb{F}_{q^2}}(H^t_j) \) and \( k_j := \dim_{\mathbb{F}_{q^2}}(C_j^t) \) and \( k_j := \dim_{\mathbb{F}_{q^2}}(C_j^{⊥_H}) \), for all \( 1 \leq j \leq r \). Then we have
\[
m = \sum_{i=1}^{s} e_i + \sum_{j=1}^{r} 2e_j, \quad k = \sum_{i=1}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k_j' + k_j^\prime).
\]

Clearly, \( x - 1 \) is one of the self-reciprocal divisors of \( x^m - 1 \), for any positive integer \( m \), and \( x + 1 \) is another such divisor if \( m \) is even. Recall that \( x - 1 \) and \( x + 1 \) coincide whenever \( q \) is even. WLOG, let \( g_1(x) := x + 1 \). We have \( G_1 = \mathbb{F}_{q^2} \) and rewrite \( k \) in (13) as
\[
k = \dim(C_1) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k_j' + k_j^\prime).
\]
By using (14) and Proposition 3, we obtain
\[
\dim(C \cap C^{⊥_H}) = \dim(C_1 \cap C_1^{⊥_H}) + \sum_{i=2}^{s} e_i \dim_{\mathbb{F}_{q^2}}(C_i \cap C_i^{⊥_H}) + \sum_{j=1}^{r} e_j \left( \dim_{\mathbb{F}_{q^2}}(C_j^t \cap C_j^{⊥_E}) + \dim_{\mathbb{F}_{q^2}}(C_j^{⊥_E} \cap C_j^{⊥_E}) \right).
\]

Assuming \( C \) to be Hermitian self-orthogonal is equivalent to saying that \( C = C \cap C^{⊥_H} \), where (14) and (15) also coincide. To use Theorem 2 with QC codes in the desired way, we assume that all constituent codes except \( C_1 \) satisfy the requirements of Theorem 4. The code \( C_1 \) has a bit more freedom since we set \( e := \dim(C_1) - \dim(C_1 \cap C_1^{⊥_H}) \). If the remaining constituents \( C_i, C_j^t, C_j^{⊥_E} \) agree with the conditions in Theorem 4, for all \( 2 \leq i \leq s \) and \( 1 \leq j \leq r \), then we obtain \( e = k - \dim(C \cap C^{⊥_H}) \) easily by subtracting (15) from (14).

The next section presents the outcomes of a random search over such constituent codes and the resulting stabilizer codes.

**IV. GOOD QUBIT AND QUANTUM CODES**

For qubit, the most comprehensive record is Grassl’s online table [8]. Systematically constructed (i.e., not in the form of stored values) stabilizer matrices corresponding to the currently best codes in \( (\mathbb{C}^2)^{\otimes n} \), for \( n \leq 96 \), are available for many entries. It is a two-fold challenge to contribute meaningfully. First, for \( n \leq 100 \), many researchers have attempted exhaustive search. Better codes are unlikely to be found without additional clever strategy. Second, for \( n > 100 \), computing the actual distance \( d(Q) \) tends to be prohibitive.

Less attention has been given to qutrit codes, for which there is no publicly available database of comparative extent. A table listing numerous qutrit codes is kept by Y. Edel in [5] based on their explicit construction as quantum twisted codes in [1]. Better codes than many of those in the table have since been found. M. Grassl generously allowed us access to his offline database that contains best-known qutrit codes up to length 50 for comparison. In most of the nontrivial cases, the stabilizer matrices are stored matrices. Adding systematic ways to build them remains a valuable endeavour here.

**Example 5.** For qubits, our search yields a \([31, 9, 7]_2 \) code, which is strictly better than the prior best-known \([31, 9, 6]_2 \) code. Let us describe a quaternary QC code, which gives rise to the better code. Let \( \zeta \) be a primitive element in \( \mathbb{F}_4 \), \( m = 15 \) and \( \ell = 2 \). Over \( \mathbb{F}_4 \), the factorization of \( x^{15} - 1 \) (cf. (5)) is
\[
x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^2 + ζ^2 x + 1)(x + ζ)(x + ζ^2)
\]
\[
(x^2 + x + ζ)(x^2 + ζ^2 x + 2)(x^2 + x + ζ^2)(x^2 + ζ x + ζ + 2).
\]

The first 3 factors are self-reciprocal and the remaining 6 factors are ordered in reciprocal pairs. Hence, we have \( s = r = 3 \) such that \( G_1 = \mathbb{F}_4, G_2 = G_3 = \mathbb{F}_{16}, H_1 = H_2 = \mathbb{F}_4 \) and \( H_j = \mathbb{F}_{16} \) for \( j \in \{2, 3\} \). Assuming this ordering, consider the following constituents of length 2 with their generator matrices corresponding to the ordered factors:
\[
C_1 : (0 \quad 1), \quad C_2 = C_3 : (1 \quad ζ), \quad C_4 : 0_2, \quad C_5 : (1 \quad ξ^{10}), \quad C_1' : (1 \quad 1), \quad C_1' : I_2, \quad C_2' : 0_2, \quad C_2' : I_2,
\]
where \( ξ \) is a primitive element of \( \mathbb{F}_{16} \) satisfying \( ξ^2 + ξ + ζ = 0, ξ^2 + ζ + 1 = 0 \), and \( I_2 \) denotes the \( 2 \times 2 \) identity matrix.

The QC code \( C \subseteq \mathbb{F}_{q^2} \) of index 2 with those constituents has dimension 11, by (13). If \( R = \mathbb{F}_{4}[x]/(x^{15} - 1) \), then \( C \) is generated by \( f_1(x) = (f_{1,0}(x), f_{1,1}(x)) \) and \( f_2(x) = (f_{2,0}(x), f_{2,1}(x)) \) as an \( R \)-submodule in \( R^2 \), with
\[
f_{1,0}(x) = ζ x^{12} + x^{10} + ζ^2 x^9 + ζ^2 x^8 + x^7 + ζ x^3,
\]
\[
f_{1,1}(x) = ζ^2 x^{13} + ζ^2 x^{12} + ζ^2 x^{10} + x^9 + ζ^2 x^7 + x^6 + ζ^2 x^5 + ζ^4 + ζ^2 x^3 + ζ x + 1,
\]
\[
f_{2,0}(x) = 0,
\]
\[
f_{2,1}(x) = ζ^2 x^{14} + ζ x^{13} + ζ^2 x^{12} + ζ^2 x^{11} + ζ x^9 + x^8 + ζ x^7 + ζ^6 + x^4 + ζ^2 x^3 + x^2 + x.
\]
The generator polynomials are found by applying (11) on the constituents given in (16) followed by the map $\phi$ in (4). Conversely, one obtains the constituents listed in (16) by evaluating $f_1(x)$ and $f_2(x)$ at $1, \xi^6, \xi^3, \xi^2, \xi, \xi^{11}, \xi^2, \xi^7$, respectively. It is easy to verify that all constituents except $C_1$ satisfy the requirements of Theorem 4, whereas $\dim(C_1 \cap C^⊥) = 0$, implying $e = 1$. Hence, $C \cap C^⊥$ has dimension 10. The Hermitian dual of $C$ is a $[30, 19, 7]_4$ code, which attains the best-known distance for a quaternary code of this length and dimension, and $d(C + C^⊥) = 6$. Thus, by Theorem 2, we obtain a $[31, 9, 7]_2$ stabilizer code.

The propagation rules in Proposition 1 give codes with parameters $[31, 8, 7]_2$, $[32, 9, 7]_2$ and $[30, 9, 6]_2$. Their performance matches the current best.

Example 6. In the qutrit case we obtain an optimal $[17, 7, 5]_3$ code whose distance reaches the upper bound. The previous best-known was a $[17, 7, 4]_3$ code. Let us explain how to obtain the optimal code. Let $\omega$ be a primitive element in $F_9$, $m = 8$ and $\ell = 2$. The decomposition of $x^8 - 1$ into linear factors over $F_9$ is

$$x^8 - 1 = \prod_{j=0}^{7} (x + \omega^j) = (x+1)(x-1) \prod_{j=1}^{3} [(x+\omega^j)(x+\omega^j)],$$

where the first 2 factors are self-reciprocal and the remaining 6 factors are ordered in reciprocal pairs. We have $s = 2$ and $r = 3$ such that $G_1 = H_{\omega}^{r} = H_{\omega}^{r} = F_9$, for all $i \in \{1, 2\}$ and $j \in \{1, 2, 3\}$. Consider the following constituents of length 2 corresponding to the ordered factors:

$$C_1 : (1 \omega^2), C_2 : (1 \omega^2), C_3 : (1 \omega^2), C_4 : (1 \omega^2), C_5 : (1 \omega^2), C_6 : (1 \omega^2), C_7 : (1 \omega^2), C_8 : (1 \omega^2), C_9 : (1 \omega^2), C_{10} : (1 \omega^2). \quad (17)$$

The QC code $C$ of index 2 over $F_9$ with those constituents has dimension 5. Let $R = F_9[x]/(x^8 - 1)$. Then $C$ is generated by $f_1(x) = (f_{1,0}(x), f_{1,1}(x)), f_2(x) = (f_{2,0}(x), f_{2,1}(x))$ as an $R$-submodule in $R^2$, where

$$f_{1,0}(x) = \omega^3x^7 + \omega^3x^5 + \omega^3x^3 + \omega^2x - 1,$$

$$f_{1,1}(x) = \omega^3x^7 - x^6 - x^4 + 3x^5 + 3x^4 + \omega x^3 + \omega^3x + \omega^3,$$

$$f_{2,0}(x) = 0,$$

$$f_{2,1}(x) = \omega^2x^7 + \omega^2x^6 + \omega^2x^5 + x^4 + \omega^3x^3 + \omega^2x^2 + \omega^7x - 1.$$
| No. | Generators                                      | No. | Generators                                      |
|-----|------------------------------------------------|-----|------------------------------------------------|
| 1   | $\{\omega, \omega^2\}$                        | 17  | $\{\omega^4, \omega^5, \omega^5, \omega^6\}$   |
| 2   | $\{1, \omega^3\}$                              | 18  | $\{\omega^2, \omega^3, \omega^4, \omega^{11}\}$ |
| 3   | $\{\omega^4, \omega^5, \omega^6, \omega^7\}$   | 19  | $\{1, 0, \omega, \omega^2, \omega^3, \omega^5\}$ |
| 4   | $\{\omega^5, \omega^6, \omega^7, \omega^8\}$   | 20  | $\{\omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$ |
| 5   | $\{\omega^6, \omega^7, \omega^8, \omega^9\}$   | 21  | $\{\omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$ |
| 6   | $\{\omega^7, \omega^8, \omega^9, \omega^{10}\}$ | 22  | $\{1, 1, \omega\}$                             |
| 7   | $\{\omega^8, \omega^9, \omega^{10}, \omega^{11}\}$ | 23  | $\{\omega^2, \omega^3, \omega^4, \omega^5\}$    |
| 8   | $\{\omega^9, \omega^{10}, \omega^{11}, \omega^{12}\}$ | 24  | $\{\omega^2, \omega^3, \omega^4, \omega^5\}$    |
| 9   | $\{1, \omega^3, \omega^4, \omega^6\}$          | 25  | $\{\omega^2, \omega^3, \omega^4, \omega^5\}$    |

#### Table II

Generators of the Quasi-Cyclic codes used to construct the qutrit stabilizers in Table I

[2] W. Bosma, J. Cannon and C. Playoust, “The Magma algebra system I. The user language,” *J. Symb. Comput.*, vol. 24, no. 3-4, 235–265, 1997.
[3] A. Calderbank, E. Rains, P. Shor, and N. Sloane, “Quantum error correction via codes over GF(4),” *IEEE Trans. Inf. Theory*, vol. 44, no. 4, 1369–1387, 1998.
[4] A. Deweger, K. Guenda, and T. A. Gulliver, “Extending Constructions X for quantum error-correcting codes,” in *Coding Theory and Applications*. Springer, 2015, 141–152.
[5] Y. Edel, “Parameters of some GF(3)-linear quantum twisted codes,” Online available at https://www.math.uni-heidelberg.de/~yesv/Matrizen/QTBCH/QTBCHTab3.html, 2000, accessed on 2019-01-17.
[6] A. Galindo, F. Hernando, and R. Matsumoto, “Quasi-cyclic constructions of quantum codes,” *Finite Fields Appl.*, vol. 52, 261–280, 2018.
[7] D. E. Gottsman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, 1997.
[8] M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes,” Online available at http://www.codetables.de, accessed on 2019-01-17.
[9] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *IEEE Trans. Inf. Theory*, vol. 52, no. 11, 4892–4914, 2006.
[10] E. Knill, “Resilient quantum computation,” *Science*, vol. 279, no. 5349, 342–345, 1998.
[11] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, “Perfect quantum error correcting code,” *Phys. Rev. Lett.*, vol. 77, no. 1, 198–201, 1996.
[12] D. A. Lidar and T. A. Brun, eds., *Quantum Error Correction*. Cambridge University Press, 2013.
[13] S. Ling and P. Sole, “On the algebraic structure of quasi-cyclic codes I: Finite fields,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, 2751–2760, 2001.
[14] P. Lisoněk and V. Singh, “Quantum codes from nearly self-orthogonal quaternary linear codes,” *Des. Codes Cryptogr.*, vol. 73, no. 2, 417–424, 2014.
[15] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. North-Holland Publ. Co., 1978.
[16] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Phys. Rev. A*, vol. 52, no. 4, R2493–R2496, 1995.
[17] A. Steane, “Multiple-particle interference and quantum error correction,” *Proc. R. Soc. London, Ser. A*, vol. 452, no. 1954, 2551–2577, 1996.