A new family of quantum codes from duadic codes

Reza Dastbasteh and Petr Lisoněk

Simon Fraser University
rdastbas@sfu.ca plisonek@sfu.ca

Abstract. We present a new family of binary quantum codes constructed from quaternary linear Hermitian self-dual codes. We provide a minimum distance lower bound for our quantum codes using the theory of duadic codes. Many new record-breaking quantum codes obtained from our construction are also presented.

Keywords: quantum code, duadic code, quadratic residue code, self-dual code, minimum distance bound

1 Background

Quantum error-correcting codes or simply quantum codes are applied to protect quantum information from corruption by noise (decoherence) on the quantum channel in a way that is similar to that of classical error-correcting codes. The parameters of a binary quantum code that encodes k logical qubits into n physical qubits and has minimum distance d are denoted by $[[n, k, d]]$.

An important class of quantum codes is quantum stabilizer codes. Binary stabilizer codes were introduced in the works by Calderbank et al. [3] and Gottesman [5]. Each binary stabilizer code is a quaternary additive code (an additive subgroup of $\mathbb{F}_4^n$) which is self-orthogonal with respect to a certain trace inner product [3]. For more information about the structure of quantum codes and their algebraic constructions we refer to the recent survey [7]. In this work, we only restrict our attention to $\mathbb{F}_4$-linear subspaces of $\mathbb{F}_4^n$ and the following theorem gives the connection between quaternary linear codes and quantum codes.

Theorem 1. *[3, Theorem 2] Let C be a linear $[n, k, d]$ code over $\mathbb{F}_4$ such that $C^{\perp_h} \subseteq C$, where $C^{\perp_h}$ is the Hermitian dual of C. Then we can construct an $[[n, 2k - n, d']]$ binary quantum code, where $d' \geq d$.*

If the quantum code of Theorem 1 has minimum distance $d' = d$, then the code is called a pure quantum code. There are several secondary constructions for quantum codes which take a quantum code and produce a new quantum codes applying standard constructions such as puncturing, lengthening, and shortening of the original code. The next theorem provides two of such constructions.

Theorem 2. *[3, Theorem 6] Suppose that an $[[n, k, d]]$ quantum code exists.*

1. *If $n \geq 2$ and the code is pure, then there exists an $[[n-1, k+1, d-1]]$ quantum code.*
2. *If $n \geq 2$, then an $[[n-1, k, d-1]]$ quantum code exists.*

Duadic codes are an important class of linear cyclic codes and they are thoroughly discussed in [10, Chapter 6] and [9, Section 2.7]. We briefly recall several important properties of this class of linear codes below.

Let q be a prime power and $\mathbb{F}_q$ be the field of q elements. Throughout this extended abstract, n is always a positive integer such that $\gcd(n, q) = 1$.

A linear code $C \subseteq \mathbb{F}_q^n$ is called *cyclic* if for every $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, the vector $(c_{n-1}, c_0, \cdots, c_{n-2})$ obtained by a cyclic shift of the coordinates of c is also in C. It is well known that there is a one-to-one correspondence between cyclic codes of length n over $\mathbb{F}_q$ and ideals of the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, for example see [10, Section 4.2]. Under this correspondence, each cyclic code can be uniquely represented by a monic polynomial $g(x)$, where $g(x)$ is the minimal degree generator of the corresponding ideal. The polynomial $g(x)$ is called the *generator polynomial* of such cyclic code. Let α be a primitive n-th root of unity. Alternatively, we can represent the above cyclic code by its unique *defining set*

$$\{t : 0 \leq t \leq n-1 \text{ and } g(\alpha^t) = 0\}.$$

For each $a \in \mathbb{Z}_n$, the set $Z_a = \{(aq^j) \mod n : 0 \leq j \leq m-1\}$, where m is the smallest positive integer such that $aq^m \equiv a \pmod{n}$ is called a *q-cyclotomic coset* modulo n. The q-cyclotomic cosets partition $\mathbb{Z}_n$ and each defining set of a linear cyclic code is a union of cyclotomic cosets.

For any integer a such that $\gcd(n, a) = 1$, the function μ_a defined on $\mathbb{Z}_n$ by $\mu_a(x) = (ax) \bmod n$ is called a *multiplier*. Clearly a multiplier is a permutation of $\mathbb{Z}_n$.

Definition 1. *[9, Section 2.7] Let S_1 and S_2 be unions of non-zero q-cyclotomic cosets modulo n such that*

1. *$0 \notin S_1 \cup S_2$*
2. *$S_1 \cup S_2 \cup \{0\} = \mathbb{Z}_n$ and $S_1 \cap S_2 = \emptyset$,*
3. *there is a multiplier μ_b such that $\mu_b S_1 = S_2$ and $\mu_b S_2 = S_1$.*

Then the pair $\{S_1, S_2\}$ is called a splitting of $\mathbb{Z}_n$ given by μ_b over $\mathbb{F}_q$.

A vector $(x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$ is called *even-like* provided that

$$\sum_{i=1}^{n} x_i = 0$$

and it is called *odd-like* otherwise. A linear code is called *even-like* if it has only even-like codewords; a linear code is called *odd-like* if it is not even-like. In the binary case an even-like code has only even weights.

Binary duadic codes were first introduced by Leon et al. [13], and later they were generalized to larger fields by Pless [15, 16].

Definition 2 (Duadic codes). *[10, Theorem 6.1.5] [9, Section 2.7] Let $\{S_1, S_2\}$ be a splitting of $\mathbb{Z}_n$ over $\mathbb{F}_q$. Then the linear cyclic codes with the defining sets $S_1 \cup \{0\}$ and $S_2 \cup \{0\}$ are called a pair of even-like duadic codes. The linear cyclic codes with the defining sets S_1 and S_2 are called a pair of odd-like duadic codes.*

A comprehensive list of important properties of duadic codes is provided below.

Theorem 3. *[18, Theorem 3.1][10, Theorem 6.1.3] Let (C_1, C_2) and (D_1, D_2) be pairs of even-like and odd-like duadic codes of length n over $\mathbb{F}_q$, respectively, such that $C_1 \subseteq D_1$ and $C_2 \subseteq D_2$. Then*

1. *C_1 and C_2 (respectively D_1 and D_2) are permutation equivalent codes.*
2. *$C_1 \cap C_2 = \{0\}$ and $C_1 + C_2$ is the cyclic code generated by $x - 1$.*
3. *$D_1 \cap D_2 = H$ and $D_1 + D_2 = \mathbb{F}_q^n$, where H is the subspace of $\mathbb{F}_q^n$ with all ones vector as a basis.*
4. *$\dim C_1 = \dim C_2 = (n-1)/2$ and $\dim D_1 = \dim D_2 = (n+1)/2$.*
5. *C_1 is the subcode of D_1 containing all even-like vectors. The same holds for C_2 as the subcode of D_2.*
6. *$D_1 = C_1 \oplus H$ and $D_2 = C_2 \oplus H$.*
7. *If C_1 is Hermitian self-orthogonal, then $C_1^{\perp_h} = D_1$ and $C_2^{\perp_h} = D_2$.*

Now we briefly mention the class of quadratic residue codes which are special cases of duadic codes. Let p be an odd prime number. Let Q_p be the set of nonzero squares (quadratic residues) modulo p and N_p be the set of nonsquares (quadratic nonresidues) modulo p. The sets Q_p and N_p satisfy the following properties:

1. $|Q_p| = |N_p| = \frac{p-1}{2}$.
2. $aQ_p = Q_p$ and $aN_p = N_p$ for any $a \in Q_p$. Also, $bQ_p = N_p$ and $bN_p = Q_p$ for any $b \in N_p$.

If $q \in Q_p$ then each q-cyclotomic coset modulo p different from $\{0\}$ either is a subset of Q_p or it is a subset of N_p. Thus Q_p and N_p give a splitting of $\mathbb{Z}_p$ given by μ_b for any $b \in N_p$. The duadic codes corresponding to such splitting are called *quadratic residue codes,* abbreviated *QR codes,* of length p over $\mathbb{F}_q$.

Self-orthogonal duadic codes and QR codes over $\mathbb{F}_4$ with respect to the Hermitian inner products are discussed below.

Theorem 4. *[10, Theorem 6.4.4] Let C be a linear cyclic code over $\mathbb{F}_4$ with parameters $[n, \frac{n-1}{2}]$. Then C is Hermitian self-orthogonal if and only if C is an even-like duadic code with the multiplier μ_{-2}.*

Theorem 5. *[10, Section 6.6.1] Let p be an odd prime. The even-like QR codes of length p over $\mathbb{F}_4$ are Hermitian self-orthogonal if and only if $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$.*

Let D be an odd-like duadic code with the even-like subcode C. The *minimum odd-like weight* of D is defined by

$$d_o = \min\{\mathrm{wt}(v) : v \in D \setminus C\}.$$

Several minimum distance conditions for duadic and QR codes are provided below. Let $d(C)$ denote the minimum distance of C.

Theorem 6. *[10, Theorems 6.5.2, 6.6.6, and 6.6.22] Let D be an odd-like duadic code of length n over $\mathbb{F}_q$. Let d_o be the minimum odd-like weight of D. Then*

1. $d_o^2 \geq n$.
2. *If the splitting is given by μ_{-1}, then* $d_o^2 - d_o + 1 \geq n$.
3. *Furthermore, if n is a prime number and D is a QR code, then*
   a. $d(D) = d_o$.
   b. *If $q = 2$ or $q = 4$ and $n \equiv -1 \pmod 8$, then $d(D) \equiv 3 \pmod 4$.*

An extended version of this result is provided in [10, Theorems 6.5.2, 6.6.22]. In general, although the square root bound is a nice theoretical result, our computations given in Table 1 show that it does not provide a tight bound for the minimum distance.

We conclude this section with some useful information regarding when a splitting over $\mathbb{F}_4$ is given by μ_{-2}, or in other words when a duadic code over $\mathbb{F}_4$ is Hermitian self-orthogonal by Theorem 4.

Theorem 7. *[10, Theorems 6.4.9 and 6.4.10] Let p be an odd prime number.*

1. *If $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$, then every splitting of $\mathbb{Z}_p$ over $\mathbb{F}_4$ is given by μ_{-2}.*
2. *If $p \equiv 3 \pmod 8$, then there is no splitting of $\mathbb{Z}_p$ given by μ_{-2} over $\mathbb{F}_4$.*
3. *If $p \equiv 1 \pmod 8$, then μ_{-2} may or may not give a splitting of $\mathbb{Z}_p$ over $\mathbb{F}_4$.*

Moreover, if μ_{-2} and μ_{-1} give the same splitting of $\mathbb{Z}_p$ over $\mathbb{F}_4$, then $p \equiv \pm 1 \pmod 8$. In particular, if $p \equiv -1 \pmod 8$, then μ_{-2} and μ_{-1} give the same splitting of $\mathbb{Z}_p$ over $\mathbb{F}_4$.

2 A new class of good binary quantum codes

A 0-dimensional quantum code with length n has parameters $[[n, 0, d]]$. Such a quantum code represents a single quantum state capable of correcting any $(d-1)/2$ errors. In practice, 0-dimensional quantum codes can be useful for example in testing whether certain storage locations for qubits are decohering faster than they should [3]. Moreover, higher-dimensional quantum codes can be constructed by applying Theorem 2 part 1 to a 0-dimensional quantum code.

In this section, we provide a new infinite family of 0-dimensional quantum codes using duadic codes over $\mathbb{F}_4$. Our construction targets nearly self-orthogonal duadic codes and also bounds the minimum distance of the constructed quantum code using minimum distances of an odd-like and an even-like duadic code.

Through this section, n always is a positive odd integer. For any integer a such that $\gcd(a, n) = 1$, we denote the multiplicative order of a modulo n by $\mathrm{ord}_n(a)$.

Constructions of 1-dimensional quantum codes can be found in the literature. One such construction is provided below which is obtained by applying the CSS construction to binary duadic codes.

Theorem 8. *[1, Theorems 4 and 10] Let n be a positive odd integer. Then there exists a quantum code with parameters $[[n, 1, d]]$, where $d^2 \geq n$. If $\mathrm{ord}_n(2)$ is odd, then $d^2 - d + 1 \geq n$.*

Moreover, Guenda in [8] proved that the distance bound $d^2 - d + 1 \geq n$ in Theorem 8 is still valid when $\mathrm{ord}_n(4)$ is odd. She also found the following new family of quantum codes when $\mathrm{ord}_n(4)$ is even.

Theorem 9. *[8, Theorem 16] Let $n = p^m$ be a prime power power, $\gcd(p, 2) = 1$, and $\mathrm{ord}_n(4)$ be even. Then there exists an $[[n, 1, d]]$ quantum code with $d^2 \geq n$.*

For $u, v \in \mathbb{F}_4^n$ let $\langle u, v\rangle_h$ denote their Hermitian inner product. The next theorem gives some useful information about the weights in certain even-like and odd-like quaternary duadic codes.

Theorem 10. *Let n be a positive odd integer and C_o be an odd-like duadic code of length n with the multiplier μ_{-2} over $\mathbb{F}_4$. Let C_e be the Hermitian dual of the code C_o. Then all vectors in C_e have even weights and all vectors in $C_o \setminus C_e$ have odd weights.*

Proof. First note that by Theorem 4, $C_e \subset C_o$ and C_e is Hermitian self-orthogonal. Let $v = (v_0, v_1, \cdots, v_{n-1})$ be an arbitrary codeword of C_e. Then

$$\langle v, v\rangle_h = \sum_{i=0}^{n-1} v_i^3 = 0.$$

Since C_e is self-orthogonal, $\mathrm{wt}(v)$ is even. This proves the first part.

Let j be the all-ones vector of length n and H be the subspace spanned by j over $\mathbb{F}_4$. Now, toward a contradiction, suppose that $C_o \setminus C_e$ has an even weight vector. By Theorem 3 part 6, $C_o = C_e \oplus H$. Thus there exists $0 \neq a = (a_0, a_1, \cdots, a_{n-1}) \in C_e$ such that $j + a$ has an even weight. Let $\mathrm{wt}(a) = k_1 + k_2$, where k_1 is the number of coordinates of a equal to 1 and k_2 is the number of coordinates equal to ω or ω^2, where ω is a primitive cube root of unity in $\mathbb{F}_4$. Note that $\mathrm{wt}(j + a) = n - k_1$ and the facts that n is odd and $j + a$ has an even weight imply that k_1 is odd. Moreover, since $a \in C_e$ has an even weight, k_2 must be odd too. Now we have

$$0 = \langle a, j\rangle_h = \sum_{i=0}^{n-1} a_i = k_1 + m\omega + (k_2 - m)\omega^2 \tag{1}$$

for some integer m. Since $1 = \omega + \omega^2$ and $k_1 = 1$ over $\mathbb{F}_4$, (1) equals to $(m+1)\omega + (k_2 - m + 1)\omega^2$. However, this is a contradiction as $m + 1$ and $k_2 - m + 1$ have different parities modulo 2 which implies that the right side of (1) is non-zero. So $C_o \setminus C_e$ cannot contain an even weight codeword. □

The *nearly self-orthogonality* of a linear code C with respect to the Hermitian inner product is defined by $e = \dim(C) - \dim(C \cap C^{\perp_h})$ in [14]. Next, we classify all the odd-like duadic codes having the nearly self-orthogonality $e = 1$ with respect to the Hermitian inner product.

Theorem 11. *Let C be an odd-like duadic code. Then C has the nearly self-orthogonality parameter $e = 1$ if and only if C has multiplier μ_{-2}.*

Proof. First suppose that μ_{-2} is a multiplier of C. Thus there exists a splitting of $\mathbb{Z}_n$ given by μ_{-2} in the form (S_1, S_2) such that S_1 is the defining set of C. The code $C^{\perp_h}$ has the defining set $\mathbb{Z}_n \setminus (-2S_1) = \mathbb{Z}_n \setminus S_2 = S_1 \cup \{0\}$. Hence $C^{\perp_h}$ is the even-like duadic subcode of C and

$$e = \dim(C) - \dim(C \cap C^{\perp_h}) = 1.$$

Conversely let (S_1', S_2') be a splitting of $\mathbb{Z}_n$ given by μ_a and C be an odd-like duadic code with the defining set S_1' and assume that $e = 1$. Then

$$\begin{aligned} e = \dim(C) - \dim(C \cap C^{\perp_h}) &= n - |S_1'| - \Big(n - |S_1' \cup \big(\mathbb{Z}_n \setminus (-2S_1')\big)|\Big) \\ &= |S_1' \cup \big(\mathbb{Z}_n \setminus (-2S_1')\big)| - |S_1'|. \end{aligned} \tag{2}$$

Now if $-2S_1' \neq S_2'$, then $\{0, s\} \subseteq \mathbb{Z}_n \setminus (-2S_1')$ for some $s \in S_2'$. Thus (2) implies that $e \geq 2$ which is a contradiction. Therefore, $-2S_1' = S_2'$ and μ_{-2} is a multiplier of C. □

Next, we use the following construction of quantum codes from linear codes which is called *nearly self-orthogonal construction of quantum codes* [14]. This construction extends a linear code, which is not necessarily Hermitian self-orthogonal, to a Hermitian self-orthogonal linear code of a larger length. The next theorem states a slight modification of this construction.

Theorem 12. *Let C be an $[n, n-k]$ linear code over $\mathbb{F}_4$ and $e = n-k-\dim(C \cap C^{\perp_h})$. Then there exists a quantum code with parameters $[[n+e, 2k-n+e, d]]$, where*

$$d \geq \min\{d(C^{\perp_h}), d(C + C^{\perp_h}) + 1\}.$$

Proof. The result follows from applying Theorem 2 of [14] to the code $C^{\perp_h}$ which is an $[n, k]$ linear code over $\mathbb{F}_4$.

Now, we state our main result of this section which provides a construction of a new family of 0-dimensional quantum codes.

Theorem 13. *Let n be a positive odd integer and C_o be an odd-like duadic code of length n with the multiplier μ_{-2} over $\mathbb{F}_4$. Then there exists a binary quantum code with parameters $[[n+1, 0, d]]$, where*

1. *$d \geq \min\{d(C_e), d(C_o) + 1\}$, where C_e is the even-like subcode of C_o.*
2. *d is even.*

3. *If $d(C_o)$ is odd, then $d \geq \sqrt{n}+1$. Moreover, if also μ_{-1} is a multiplier for C_o, then $d^2 - 3(d-1) \geq n$.*

Proof. Let (S_1, S_2) be a splitting of $\mathbb{Z}_n$ given by μ_{-2} over $\mathbb{F}_4$ and C_o and C_e be the odd-like and even-like duadic code with the defining sets S_1 and $S_1 \cup \{0\}$, respectively. By Theorem 11, the code C_o has the nearly self-orthogonality $e = 1$.

The code C_o has parameters $[n, n - \frac{n-1}{2}]$. Now applying the quantum construction given in Theorem 12 to C_o results in an Hermitian self-dual linear code Q which is also a quantum code with parameters $[[n+1, 0, d]]$, where $d \geq \min\{d(C_e), d(C_o)+1\}$. The facts that Q is linear and Hermitian self-dual imply that all weights in Q are even, as was shown in the proof of Theorem 10.

Note that Theorem 10 implies that if $d(C_o) = d_o$ is odd, then $d_o < d(C_e)$. Thus d_o satisfies the square root bound provided in Theorem 6. The facts that $d \geq d_o + 1$ and $d_o \geq \sqrt{n}$ show that $d \geq \sqrt{n}+1$.

Finally, if the same splitting is given by μ_{-1} and $d(C_o) = d_o$ is odd, then by Theorem 6, $d_o^2 - d_o + 1 \geq n$. Now combining $d - 1 \geq d_o$ with the previous inequality gives the result. □

The lower bound that we provided in case 1 of Theorem 13 appears to be very good and almost all of our computational results rely on this lower bound.

Restricting the code lengths to prime numbers in the form $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$ leads to an infinite family of 0-dimensional quantum codes of length $p+1$.

Corollary 1. *Let p be a prime number such that $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$. Then there exists a $[[p+1, 0, d]]$ quantum code with an even minimum distance d and*

$$d \geq \min\{d(C_e), d(C_o)+1\},$$

where C_o is an odd-like duadic code of length p and C_e is the even-like subcode of C_o. If C_o is also a QR code, $p \equiv -1 \pmod 8$, and $d = d(C_o)+1$, then $d \equiv 0 \pmod 4$.

Proof. The proof follows from Theorems 13 and Theorem 7 part 1. The last fact about the minimum distance follows from Theorem 6 part 3b which implies that $d(C_o) \equiv 3 \pmod 4$. □

For each positive odd integer n, we have $\mathrm{ord}_n(4) \mid \mathrm{ord}_n(2)$ and if $\mathrm{ord}_n(2)$ is odd, then $\mathrm{ord}_n(4) = \mathrm{ord}_n(2)$. In the latter case, the binary and quaternary cyclotomic cosets modulo n are the same. Thus the binary and quaternary duadic codes have the same defining sets. In this special case, the following result helps to compute the minimum distance of quaternary duadic codes much faster by only using the binary duadic code with the same defining set.

Theorem 14. *[15, Theorem 4] Let C be a quaternary linear code of minimum distance d which is generated by a set of binary vectors. Then the binary linear code generated by the same set of generators has the minimum distance d.*

Another advantage of the above result is that binary duadic codes have been studied extensively in the literature. For instance, the exact or probable minimum distance of all binary duadic codes of length $n \leq 241$ are determined in [19], [17], and [10, Section 6.5].

3 Minimum distance lower bound for cyclic codes using the fixed subcodes

In general, computing the true minimum distance for linear codes is NP-hard [22] and very difficult for linear codes with large lengths and dimensions. In [12], the authors used the fixed subcode by the action of multipliers to find an upper bound (or even the exact value) for the minimum distance of certain linear cyclic codes. In this section, we use this idea to bound the minimum distance of odd-like duadic codes.

Proposition 1. *Let $C \subseteq \mathbb{F}_4^n$ be a linear cyclic code of an odd length n, with a symmetric defining set, and C_f be the fixed subcode of C under the action of μ_{-1} (as the permutation on $\mathbb{Z}_n$). Then $d(C_f)/2 + 1 \leq d(C)$.*

Proof. Let v be a minimum weight vector in C. Since C is cyclic, without loss of generality, we assume that v has a non-zero entry in the 0th position (coordinate indices are from $\mathbb{Z}_n$). If v is fixed by the map μ_{-1}, then $d(C_f) = d(C)$. Otherwise $v + \mu_{-1}(v)$ is an element of C_f and $d(C_f) \leq \mathrm{wt}(v + \mu_{-1}(v)) \leq 2d(C) - 2$ since both v and $\mu_{-1}(v)$ have the same 0th entry. Hence $d(C_f)/2 + 1 \leq d(C)$. □

In some examples, the minimum distance of the fixed subcode is computed much faster, while the minimum distance computation for the original duadic code required a much longer time. We use this property and the result of Proposition 1 to prove the existence of new quantum codes from the constructions given in Theorem 13.

4 Numerical results

The constructions given in Section 2 lead to many new quantum codes with minimum distances much higher than the previously best-known codes. In some cases the increase is by as much as 10. Table 1 shows parameters of such quantum codes. In the table, the first two columns show the length and the coset leaders of each odd-like duadic code. The third column records whether the original duadic code is a QR code or not.

In Table 1, we used the probable minimum distances provided in [10, Section 6.5] for duadic codes of length 217, 233, and 239, where the binary and quaternary generator polynomials are the same for all these three codes. The probable minimum distance d for each of these values is denoted by d^{ap} in the table. All the other minimum distances given in the table are the true minimum distance obtained from the bound given in Theorem 13 part 1.

When the exact value of minimum distance is not known, its lower and upper bounds are separated by a dash. Some of the minimum distance upper bounds presented in Table 1 are computed using functions implemented in Magma [2] to attack the McEliece cryptosystem.

The "source" column in the table provides information about the way the minimum distance of each code is computed. Most minimum weights are computed by the computer algebra system Magma [2], and a reference for each remaining one is provided in the source column.

Finally, the last column shows the minimum distance of the current best known quantum code of the same length and dimension as shown in [6]. In cases where the code that we list in our table has a strictly higher minimum distance than the current best known quantum code shown in [6], we list the distance of our code in boldface in the last column.

It should be noted that we can apply the secondary construction given in Theorem 2 part 2 to the codes listed in Table 1 and produce many more record-breaking codes. For instance:

- the quantum code $[[224, 0, 32]]$ generates 9 new quantum codes with parameters $[[224 - i, 0, 32 - i]]$ for each $1 \leq i \leq 9$.
- the quantum code $[[200, 0, 32]]$ generates 7 new quantum codes with parameters $[[200 - i, 0, 32 - i]]$ for each $1 \leq i \leq 7$.
- the quantum code $[[240, 0, 32]]$ generates 6 new quantum codes with parameters $[[240 - i, 0, 32 - i]]$ for each $1 \leq i \leq 6$.
- the quantum code $[[192, 0, 28]]$ generates 5 new quantum codes with parameters $[[192 - i, 0, 28 - i]]$ for each $1 \leq i \leq 5$.

The above codes obtained from secondary constructions are not listed in Table 1.

length	coset leaders	type	mod 8	parameters	source	best distance
$n = 5$	1	QR	-3	$[[6, 0, 4]]$	Magma	4
$n = 7$	1	QR	-1	$[[8, 0, 4]]$	Magma	4
$n = 13$	1	QR	-3	$[[14, 0, 6]]$	Magma	6
$n = 17$	$1, 3$		1	$[[18, 0, 8]]$	Magma	8
$n = 23$	1	QR	-1	$[[24, 0, 8]]$	Magma	8
$n = 29$	1	QR	-3	$[[30, 0, 12]]$	Magma	12
$n = 31$	$1, 5, 7$	QR	-1	$[[32, 0, 8]]$	Magma	10
$n = 37$	1	QR	-3	$[[38, 0, 12]]$	Magma	12
$n = 41$	$1, 3$		1	$[[42, 0, 12]]$	Magma	12
$n = 47$	1	QR	-1	$[[48, 0, 12]]$	Magma	14
$n = 49$	$1, 7$		1	$[[50, 0, 4]]$	Magma	14
$n = 53$	1	QR	-3	$[[54, 0, 16]]$	Magma	16
$n = 61$	1	QR	-3	$[[62, 0, 18]]$	Magma	18
$n = 71$	1	QR	-1	$[[72, 0, 12]]$	Magma	18
$n = 73$	$1, 3, 5, 13$		1	$[[74, 0, 10]]$	Magma	18
$n = 79$	1	QR	-1	$[[80, 0, 16]]$	Magma	20
$n = 89$	$1, 3, 5, 13$		1	$[[90, 0, 12]]$	Magma	20
$n = 97$	$1, 5$		1	$[[98, 0, 18]]$	Magma	22
$n = 101$	1	QR	-3	$[[102, 0, 22]]$	Magma	22
$n = 103$	1	QR	-1	$[[104, 0, 20]]$	[10] & Theorem 14	20
$n = 109$	$1, 3, 9$	QR	-3	$[[110, 0, 22]]$	Magma	26
$n = 113$	$1, 3, 9, 10$		1	$[[114, 0, 24]]$	Magma	**24**
$n = 119$	$1, 2, 3, 6, 7, 21, 51$		-1	$[[120, 0, 20]]$	Magma	**20**
$n = 127$	$1, 9, 11, 13, 15,$ $19,\ 21,\ 31,\ 47$	QR	-1	$[[128, 0, 20]]$	[19] & Theorem 14	22
$n = 137$	$1, 3$		1	$[[138, 0, 20 - 32]]$	Magma	**20**
$n = 145$	$1, 3, 5, 7, 11, 29$		1	$[[146, 0, 18 - 32]]$	Magma	18
$n = 149$	1	QR	-3	$[[150, 0, 18 - 30]]$	Magma	18
$n = 151$	$1, 3, 7, 11, 15$		-1	$[[152, 0, 24]]$	[4] & Theorem 14	**24**
$n = 155$	$1, 2, 3, 5, 6, 9, 11,$ $15, 25, 31$		3	$[[156, 0, 18 - 20]]$	Magma	18
$n = 157$	$1, 3, 9$	QR	-3	$[[158, 0, 20 - 36]]$	Magma & Proposition 1	**20**
$n = 161$	$5, 11, 35, 69$		1	$[[162, 0, 16]]$	Magma & Theorem 14	20
$n = 167$	1	QR	-1	$[[168, 0, 24]]$	[21] & Theorem 14	**24**
$n = 173$	1	QR	-3	$[[174, 0, 20 - 36]]$	Magma & Proposition 1	21
$n = 181$	1	QR	-3	$[[182, 0, 22 - 38]]$	Magma & Proposition 1	**22**
$n = 191$	1	QR	-1	$[[192, 0, 28]]$	[20] & Theorem 14	**28**
$n = 193$	$1, 5$		1	$[[194, 0, 20 - 42]]$	Magma	22
$n = 197$	1	QR	-3	$[[198, 0, 22 - 40]]$	Magma & Proposition 1	22
$n = 199$	1	QR	-1	$[[200, 0, 32]]$	[20] & Theorem 14	**32**
$n = 203$	$2, 3, 7, 29$		3	$[[204, 0, 14 - 24]]$	Magma	22
$n = 205$	$1, 3, 5, 7, 9, 11, 15,$ $17, 21, 31, 41$		-3	$[[205, 0, 20 - 36]]$	Magma & Proposition 1	20
$n = 217$	Many codes		1	$[[218, 0, 24^{ap}]]$	[10] & Theorem 14	**24**
$n = 221$	$1, 2, 3, 5, 6, 9, 10,$ $13, 17, 18, 39$		-3	$[[222, 0, 14 - 36]]$	Magma	20
$n = 223$	$1, 9, 19$	QR	-1	$[[224, 0, 32]]$	[11] & Theorem 14	**32**
$n = 229$	$1, 3, 5$	QR	-3	$[[230, 0, 14 - 48]]$	Magma	22
$n = 233$	$1, 3, 7, 27$		1	$[[234, 0, 30^{ap}]]$	[10] & Theorem 14	**30**
$n = 235$	$1, 2, 5, 47$		3	$[[236, 0, 14 - 24]]$	Magma	20
$n = 239$	1	QR	-1	$[[240, 0, 32^{ap}]]$	[10] & Theorem 14	**32**
$n = 241$	$1, 3, 5, 7, 9, 11,$ $13, 21, 25, 35$		1	$[[242, 0, 14 - 56]]$	Magma	20

Table 1. Parameters of self-dual quantum codes obtained from duadic codes.

Bibliography

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. In *2006 IEEE International Symposium on Information Theory*, pages 1105–1108, 2006.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[3] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.

[4] P. Gaborit, C.-S. Nedeloaia, and A. Wassermann. On the weight enumerators of duadic and quadratic residue codes. *IEEE Trans. Inform. Theory*, 51(1):402–407, 2005.

[5] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54(3):1862, 1996.

[6] M. Grassl. Code Tables: Bounds on the parameters of various types of codes. `http://www.codetables.de/`.

[7] M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. *Int. J. Comput. Math. Comput. Syst. Theory*, 6(4):243–259, 2021.

[8] K. Guenda. Quantum duadic and affine-invariant codes. *International Journal of Quantum Information*, 7(01):373–384, 2009.

[9] W. C. Huffman, J.-L. Kim, and P. Solé. *Concise encyclopedia of coding theory*. Chapman and Hall/CRC, 2021.

[10] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.

[11] A. Joundan, S. Nouh, and A. Namir. New efficient techniques to catch lowest weights in large quadratic residue codes. In *Proc. of the 5th International Conference on Advances in Computing, Electronics and Communication*, 2017.

[12] I. A. Joundan, S. Nouh, M. Azouazi, and A. Namir. A new efficient way based on special stabilizer multiplier permutations to attack the hardness of the minimum weight search problem for large BCH codes. *International Journal of Electrical and Computer Engineering*, 9(2):1232, 2019.

[13] J. Leon, J. Masley, and V. Pless. Duadic codes. *IEEE Transactions on Information Theory*, 30(5):709–714, 1984.

[14] P. Lisoněk and V. Singh. Quantum codes from nearly self-orthogonal quaternary linear codes. *Designs, Codes and Cryptography*, 73(2):417–424, 2014.

[15] V. Pless. Q-codes. *Journal of Combinatorial Theory, Series A*, 43(2):258–276, 1986.

[16] V. Pless. Duadic codes and generalizations. In *Eurocode '92*, pages 3–15. Springer, 1993.

[17] V. Pless, J. M. Masley, and J. S. Leon. On weights in duadic codes. *Journal of Combinatorial Theory, Series A*, 44(1):6–21, 1987.

[18] J. J. Rushanan. *Topics in integral matrices and abelian group codes*. PhD thesis, California Institute of Technology, 1986.

[19] M. Smid. Duadic codes. *IEEE Transactions on Information Theory*, 33(3):432–433, 1987.

[20] W. K. Su, P. Y. Shih, T. C. Lin, and T. K. Truong. On the minimum weights of binary extended quadratic residue codes. In *2009 11th International Conference on Advanced Communication Technology*, volume 03, pages 1912–1913, 2009.

[21] T. K. Truong, C. Lee, Y. Chang, and W. K. Su. A new scheme to determine the weight distributions of binary extended quadratic residue codes. *IEEE Transactions on Communications*, 57(5):1221–1224, 2009.

[22] A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Transactions on Information Theory*, 43(6):1757–1766, 1997.