Polyadic Constacyclic Codes

Bocong Chen[1,2], Hai Q. Dinh[3], Yun Fan[1], San Ling[2]

[1] School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China

[2] School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore

[3] Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA

Abstract

For any given positive integer m, a necessary and sufficient condition for the existence of Type-I m-adic constacyclic codes is given. Further, for any given integer s, a necessary and sufficient condition for s to be a multiplier of a Type-I polyadic constacyclic code is given. As an application, some optimal codes from Type-I polyadic constacyclic codes, including generalized Reed-Solomon codes and alternant MDS codes, are constructed.

Keywords: Polyadic constacyclic code, p-adic valuation, generalized Reed-Solomon code, alternant code, Berlekamp-Welch decoding algorithm.

1 Introduction

The class of duadic cyclic codes over finite fields, which includes the important family of quadratic residue codes, was introduced by Leon *et al.* [15], and then studied by several authors such as in [21], [25], [11], [10] and [13].

Motivated by the good properties of duadic cyclic codes, Pless and Rushanan [22] moved on to study triadic cyclic codes. The class of polyadic cyclic codes (or m-adic cyclic codes) was later introduced by Brualdi and Pless [7]. Subsequently, Rushanan *et al.* generalized duadic cyclic codes to duadic abelian codes ([23], [27]). Zhu *et al.* further studied duadic group algebra codes ([31], [30], [2]). Results on the existence conditions of these codes have been obtained by these authors. Ling and Xing [18] extended the definition of polyadic cyclic codes to include noncyclic abelian codes, and obtained necessary and sufficient conditions for the existence of nondegenerate polyadic codes; some interesting examples arising from this family of codes were also given. Sharma *et al.* [24] removed the

Email addresses: bocong_chen@yahoo.com (B. Chen), hdinh@kent.edu (H. Q. Dinh), yfan@mail.ccnu.edu.cn (Y. Fan), lingsan@ntu.edu.sg (S. Ling).

"nondegenerate" condition considered by Ling and Xing in [18], and determined necessary and sufficient conditions for the existence of polyadic cyclic codes of prime power length.

Another direction of generalization for the notion of duadic cyclic codes is the study of polyadic constacyclic codes over finite fields. Constacyclic codes can be studied with tools which have been proved efficient for cyclic codes, e.g., polynomial techniques, as well as encoding and decoding algorithms for cyclic codes, can be easily modified to treat constacyclic codes. In practice, constacyclic codes can also be implemented by feedback shift registers. In the semisimple case, self-dual constacyclic codes do exist (see Blackford [5]), whereas such a phenomenon is impossible for cyclic codes.

In [16], polyadic cyclic codes were generalized to polyadic consta-abelian codes, and some sufficient conditions for the existence of this class of codes were established. Duadic negacyclic codes, which is a special class of polyadic constacyclic codes, were considered by Blackford [5]. Recently, Blackford [6] continued to study Type-I duadic constacyclic codes (see Definition 2.1 for detail). Necessary and sufficient conditions for the existence of Type-I duadic constacyclic codes were given and, for a given integer s, equivalent conditions were also obtained to determine whether or not s can be a multiplier for a Type-I duadic code. However, to the best of our knowledge, there are no known solutions to the following general questions: for n a positive integer and λ a nonzero element of the underlying field,

1. For any given positive integer m, do Type-I m-adic λ-constacyclic codes of length n exist?

2. For any given integer s, can s be a multiplier of a Type-I polyadic λ-constacyclic code of length n?

In this paper, a necessary and sufficient condition for the existence of Type-I m-adic λ-constacyclic codes is given. Further, a necessary and sufficient condition for s to be a multiplier of a Type-I polyadic λ-constacyclic code is obtained. We also exhibit some optimal polyadic constacyclic codes, including generalized Reed-Solomon codes and alternant MDS codes.

This paper is organized as follows. In Section 2, basic notations and the main results of this paper are presented. In Section 3, we prove some lemmas which play important roles in the proofs of the main results. In Section 4, the proofs of the main results are given. In Section 5, several corollaries are derived from the main results; some optimal codes from Type-I polyadic constacyclic codes are constructed, including generalized Reed-Solomon codes and alternant MDS codes, for which an efficient encoding and decoding method is illustrated through an example.

2 Notations and main results

We denote by $\mathbb{F}_q$ the finite field with cardinality $|\mathbb{F}_q| = q$. Let $\lambda \in \mathbb{F}_q^*$, where $\mathbb{F}_q^*$ denotes the multiplicative group of units of $\mathbb{F}_q$, and let n be a positive integer coprime to q. Any ideal C of the quotient ring $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$ is said to be a λ-*constacyclic code* over $\mathbb{F}_q$ of length n. In particular, it is just the usual cyclic code when $\lambda = 1$; and it is called a *negacyclic code* if $\lambda = -1$. Let $\mathrm{ord}_{\mathbb{F}_q^*}(\lambda) = r$, where $\mathrm{ord}_{\mathbb{F}_q^*}(\lambda)$ denotes the order of λ in the multiplicative group $\mathbb{F}_q^*$; then $r \mid (q-1)$ since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. Thus a constacyclic code C has three parameters q, n, r; in this case we say that C is a (q, n, r)-*constacyclic code*. In this paper we always adopt the following notations:

- q, n, r with $\gcd(q, n) = 1$ and $r|(q-1)$ are the parameters of the constacyclic code C, where $\gcd(q, n)$ denotes the greatest common divisor;
- $\mathbb{Z}_{rn}$ denotes the residue ring of the integer ring $\mathbb{Z}$ modulo rn;
- $\mathbb{Z}_{rn}^*$ denotes the multiplicative group consisting of units of $\mathbb{Z}_{rn}$;
- $1 + r\mathbb{Z}_{rn} = \{1 + rk \mid k = 0, 1, \cdots, n-1\} \subseteq \mathbb{Z}_{rn}$;
- μ_h, where $\gcd(h, rn) = 1$, denotes the permutation of the set $\mathbb{Z}_{rn}$ given by $\mu_h(x) = hx$ for $x \in \mathbb{Z}_{rn}$;
- s is an integer such that $s \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$, and m is a positive integer.

Let e be the multiplicative order of q modulo rn, i.e., $rn \mid (q^e - 1)$ but $rn \nmid (q^{e-1} - 1)$. Then, in the finite field $\mathbb{F}_{q^e}$, there is a primitive rn-th root ω of unity such that $\omega^n = \lambda$. It is easy to check the following facts:

- ▶ *ω^i, $i \in (1 + r\mathbb{Z}_{rn})$, are just all the roots of $X^n - \lambda$.*
- ▶ *For an integer h coprime to rn, the set $1 + r\mathbb{Z}_{rn}$ is μ_h-invariant if and only if $h \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$.*

Since $\gcd(q, n) = 1$ and $r|(q-1)$, it follows that $q \in \mathbb{Z}_{rn}^* \cap (1+r\mathbb{Z}_{rn})$ and $1+r\mathbb{Z}_{rn}$ is μ_q-invariant. Let $(1 + r\mathbb{Z}_{rn})/\mu_q$ denote the set of μ_q-orbits within $1 + r\mathbb{Z}_{rn}$, i.e., the set of q-cyclotomic cosets within $1+r\mathbb{Z}_{rn}$. For any q-cyclotomic coset Q in $\mathbb{Z}_{rn}$, the polynomial $M_Q(X) = \prod_{i \in Q}(X - \omega^i)$ is irreducible in $\mathbb{F}_q[X]$. Thus

$$X^n - \lambda = \prod_{Q \in (1+r\mathbb{Z}_{rn})/\mu_q} M_Q(X)$$

is the monic irreducible decomposition of $X^n - \lambda$ in $\mathbb{F}_q[X]$.

Definition 2.1. If $1 + r\mathbb{Z}_{rn}$ has a partition $1 + r\mathbb{Z}_{rn} = \mathcal{X}_0 \cup \cdots \cup \mathcal{X}_{m-1}$ such that, for some integer s, every $\mathcal{X}_j$ is μ_q-invariant and $\mu_s(\mathcal{X}_j) = \mathcal{X}_{j+1}$ for $j = 0, 1, \cdots, m-1$ (the subscripts are taken modulo m), then

(i) the partition $\{\mathcal{X}_0, \mathcal{X}_1, \cdots, \mathcal{X}_{m-1}\}$ is called a *Type-I m-adic splitting* of $1 + r\mathbb{Z}_{rn}$, and μ_s is said to be a *multiplier* of the Type-I m-adic splitting;

(ii) the constacyclic codes $C_{\mathcal{X}_j}$, with check polynomial $\prod_{Q \in \mathcal{X}_j/\mu_q} M_Q(X)$ for $j = 0, 1, \cdots, m-1$, are called *Type-I m-adic constacyclic codes* given by the multiplier μ_s.

Remark. In the case of Definition 2.1, the following map (denoted by $\hat{\mu}_s$):

$$\hat{\mu}_s : \quad \mathbb{F}_q[X]/\langle X^n - \lambda\rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - \lambda\rangle, \quad \sum_{i=0}^{n-1} a_i X^i \longmapsto \sum_{i=0}^{n-1} a_i X^{is},$$

is an isometry (i.e., $\hat{\mu}_s$ keeps both the algebraic structure and the weight structure, see [9, §3]) of the quotient algebra $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$ such that $\hat{\mu}_s(C_{\mathcal{X}_j}) = C_{\mathcal{X}_{j+1}}$ for $j = 0, 1, \cdots, m-1$ and $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle = \bigoplus_{j=0}^{m-1} C_{\mathcal{X}_j}$. The map $\hat{\mu}_s$ is also called a *multiplier* of the quotient algebra, e.g., see [14, Theorem 4.3.12].

Of course, the notion of an m-adic splitting makes sense in practice only for $m > 1$. We allow that $m = 1$ since it is convenient for the statements of our results. Note that, when $m = 2$, "2-adic" is usually said to be "duadic".

Example 2.2. Taking $q = 5$, $r = 2$ (hence $\lambda = -1$), $n = 6$ and $s = -1$, we have $1 + r\mathbb{Z}_{rn} = 1 + 2\mathbb{Z}_{12} = \{1, 3, 5, 7, 9, 11\}$. Obviously, $\mathcal{X}_0 = \{1, 3, 5\}$ and $\mathcal{X}_1 = \{7, 9, 11\}$ are μ_5-invariant, and $\mu_{-1}(\mathcal{X}_0) = \mathcal{X}_1$, $\mu_{-1}(\mathcal{X}_1) = \mathcal{X}_0$. Hence,

- $\{\mathcal{X}_0, \mathcal{X}_1\}$ is a Type-I duadic splitting of $1 + 2\mathbb{Z}_{12}$ given by μ_{-1};
- the constacyclic codes $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ are Type-I duadic negacyclic codes with check polynomials $X^3 + X^2 + 3X + 2$ and $X^3 + 4X^2 + 3X + 3$, respectively. In fact, both $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ have nice theoretical and practical properties, see Proposition 5.9 and Example 5.11 below.

Example 2.3. However, if we are given $q = 3$, $r = 2$ and $n = 10$, then there are no Type-I polyadic splittings of $1 + 2\mathbb{Z}_{20} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\}$, because $\{5, 15\}$ is a 3-coset which is fixed by any multiplier μ_s. Thus, we have to exclude it and look for duadic splittings of $\{1, 3, 7, 9, 11, 13, 17, 19\}$, which is partitioned into μ_3-invariant subsets $\mathcal{X}_0 = \{1, 3, 7, 9\}$ and $\mathcal{X}_1 = \{11, 13, 17, 19\}$. Obviously, $\mu_{-1}(\mathcal{X}_0) = \mathcal{X}_1$ and $\mu_{-1}(\mathcal{X}_1) = \mathcal{X}_0$. In [5], $\{\mathcal{X}_0, \mathcal{X}_1\}$ is called a *Type-II duadic splitting* of $1 + 2\mathbb{Z}_{20}$ given by μ_{-1}.

As mentioned in Section 1, there are two fundamental questions concerning Type I m-adic constacyclic codes:

- Under what conditions do Type-I m-adic (q, n, r)-constacyclic codes exist?
- For a given integer s, is μ_s a multiplier of a Type-I m-adic splitting for $1 + r\mathbb{Z}_{rn}$?

We address these two questions in this paper.

Let t be a non-zero integer. For any prime p, there is a unique non-negative integer $\nu_p(t)$ such that $p^{\nu_p(t)} \| t$, i.e., $p^{\nu_p(t)}$ is the largest power of p dividing t. The function $\nu_p(t)$ is well known as the *p-adic valuation of t*. Of course, $t = \pm \prod_p p^{\nu_p(t)}$, where p runs over all primes, but $\nu_p(t) = 0$ for all except finitely many primes p. We adopt the convention that $\nu_p(0) = -\infty$ and $|\nu_p(0)| = \infty$.

The following two theorems are the main results of this paper.

Theorem 2.4. *There is a unique integer $M = \prod_p p^{\nu_p(M)}$ such that Type-I m-adic (q, n, r)-constacyclic codes exist if and only if m is a divisor of M, where $\nu_p(M)$ is determined as follows: if $p \nmid r$ or $p \nmid n$, then $\nu_p(M) = 0$; otherwise:*

- **(i)** *if p is odd or $\nu_p(r) \geq 2$, then $\nu_p(M) = \min\{\nu_p(q-1) - \nu_p(r), \nu_p(n)\}$;*
- **(ii)** *if $p = 2$ and $\nu_2(r) = 1$, there are two subcases:*
  - **(ii.1)** *if $\nu_2(q-1) \geq 2$, then $\nu_2(M) = \max\{\min\{\nu_2(q-1)-2, \nu_2(n)-1\}, 1\}$;*
  - **(ii.2)** *if $\nu_2(q-1) = 1$, then $\nu_2(M) = \min\{\nu_2(q+1) - 1, \nu_2(n) - 1\}$.*

Note that $\nu_2(q-1) = 1$ if and only if $q \equiv -1 \pmod 4$, which is equivalent to $\nu_2(q+1) \geq 2$.

Theorem 2.5. *There is a unique integer $M_s = \prod_p p^{\nu_p(M_s)}$ such that μ_s is a Type-I m-adic splitting for $1 + r\mathbb{Z}_{rn}$ if and only if m is a divisor of M_s, where $\nu_p(M_s)$ is determined as follows: if $p \nmid r$ or $p \nmid n$, then $\nu_p(M_s) = 0$; otherwise:*

- **(i)** *if p is odd or $p = 2$ and both $\nu_p(q-1) \geq 2$ and $\nu_p(s-1) \geq 2$ hold, then*

$$\nu_p(M_s) = \max\big\{ \min\{\nu_p(q-1), \nu_p(rn)\} - |\nu_p(s-1)|, 0\big\};$$

- **(ii)** *if $p = 2$, $\nu_2(q-1) = 1$ and $\nu_2(s-1) \geq 2$, then*

$$\nu_2(M_s) = \max\big\{ \min\{\nu_2(q+1) + 1, \nu_2(rn)\} - |\nu_2(s-1)|, 0\big\};$$

- **(iii)** *if $p = 2$, $\nu_2(q-1) \geq 2$ and $\nu_2(s-1) = 1$, then*

$$\nu_2(M_s) = \max\big\{ \min\{\nu_2(q-1), \nu_2(rn)\} - |\nu_2(s+1)|, 1\big\};$$

- **(iv)** *if $p = 2$, $\nu_2(q-1) = 1$ and $\nu_2(s-1) = 1$, then*

$$\nu_2(M_s) = \begin{cases} \max\big\{\min\{\nu_2(q+1) + 1, \nu_2(rn)\} - \min\{|\nu_2(s+1)|, \nu_2(q+1)\}, 0\big\}, \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad \nu_2(s+1) \neq \nu_2(q+1); \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad \nu_2(s+1) = \nu_2(q+1). \end{cases}$$

3 Preparations

Let $\mathcal{X}$ be a finite set and let $\mathrm{Sym}(\mathcal{X})$ be the symmetric group of $\mathcal{X}$ consisting of all permutations of $\mathcal{X}$. If $\mu \in \mathrm{Sym}(\mathcal{X})$, i.e., μ is a permutation of $\mathcal{X}$, then $\langle \mu \rangle = \{\mu^j \,|\, j \in \mathbb{Z}\}$ acts on $\mathcal{X}$, and thus $\mathcal{X}$ is partitioned into a disjoint union of $\langle \mu \rangle$-orbits (abbreviation: μ-orbits). The following result appeared previously in [19, Lemma 3.1].

Lemma 3.1. *Let μ be a permutation of a finite set $\mathcal{X}$ and let m be a positive integer. Then the following statements are equivalent:*

- **(i)** *There is a partition $\mathcal{X} = \mathcal{X}_0 \cup \mathcal{X}_1 \cup \cdots \cup \mathcal{X}_{m-1}$ such that $\mu(\mathcal{X}_i) = \mathcal{X}_{i+1}$ for $i = 0, 1, \cdots, m-1$ (the subscripts are taken modulo m).*
- **(ii)** *The length of every μ-orbit on $\mathcal{X}$ is divisible by m.*

Let a finite group G act on a finite set $\mathcal{X}$. As is well known, for $x \in \mathcal{X}$, the length of the G-orbit containing x is equal to the index $|G : G_x|$, where G_x is the stabilizer of x in G. The action of G on $\mathcal{X}$ is said to be *free* if, for any $x \in \mathcal{X}$, the stabilizer of x is $G_x = \{1\}$. An element $\mu \in G$ is said to be free on $\mathcal{X}$ if the subgroup $\langle \mu \rangle$ generated by μ acts on $\mathcal{X}$ freely; in that case the length of any μ-orbit on $\mathcal{X}$ is equal to the order of μ (cf. [1, Ch.1]).

The proofs of the next two elementary facts are straightforward, so we omit them here.

Lemma 3.2. *Let G, H be finite groups, and let $\mathcal{X}$, $\mathcal{Y}$ be a finite G-set and a finite H-set, respectively. Then $\mathcal{X} \times \mathcal{Y}$ is a finite $(G \times H)$-set with the natural action of $G \times H$, and the following statements hold:*

- **(i)** *For $g \in G$ and $h \in H$, the order of $(g, h) \in G \times H$ is equal to the least common multiple of the order of g in G and the order of h in H, i.e., $\mathrm{lcm}\big(\mathrm{ord}_G(g), \mathrm{ord}_H(h)\big)$.*
- **(ii)** *For $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, the length of the (g, h)-orbit on $\mathcal{X} \times \mathcal{Y}$ containing (x, y) is equal to the least common multiple of the length of the g-orbit on $\mathcal{X}$ containing x and the length of the h-orbit on $\mathcal{Y}$ containing y.*

Lemma 3.3. *Let G act on a finite set $\mathcal{X}$ freely, and let N be a normal subgroup of G. Let $\mathcal{X}/N$ be the set of N-orbits on $\mathcal{X}$. Then the quotient G/N acts on $\mathcal{X}/N$ freely; in particular, the length of any G/N-orbit on $\mathcal{X}/N$ is equal to the index $|G : N|$.*

Remark 3.4. Let t be a positive integer and $u \in \mathbb{Z}_t^*$.

- **(i)** The action of μ_u on $\mathbb{Z}_t$ is not free, e.g., 0 is always fixed by μ_u. However, $\mathbb{Z}_t^*$ is μ_u-invariant and the action of μ_u on $\mathbb{Z}_t^*$ is always free.
- **(ii)** If $t = p^a$ is an odd prime power, then $\mathbb{Z}_{p^a}^*$ is a cyclic group of order $p^{a-1}(p-1)$; the subset $1 + p^b\mathbb{Z}_{p^a}$ with $b \geq 1$ of $\mathbb{Z}_{p^a}^*$ is a cyclic subgroup of order $p^{\max\{a-b,\,0\}}$, and $1 + p^b d$, with d coprime to p, is a generator of the cyclic subgroup $1 + p^b\mathbb{Z}_{p^a}$.

(iii) If $t = 2^a$ with $a \geq 2$, then $\mathbb{Z}_{2^a}^* = \begin{cases} \langle -1 \rangle, & a = 2; \\ \langle -1 \rangle \times \langle 5 \rangle, & a > 2, \end{cases}$ where the order of $\langle 5 \rangle$ is $|\langle 5 \rangle| = 2^{a-2}$. For the subgroup $1 + 2^b \mathbb{Z}_{2^a}$ with $b \geq 1$ of $\mathbb{Z}_{2^a}^*$, there are two subcases:

- **(iii.1)** if $b \geq 2$, then $1 + 2^b \mathbb{Z}_{2^a} \subseteq \langle 5 \rangle$ with order $|1 + 2^b \mathbb{Z}_{2^a}| = 2^{\max\{a-b,\, 0\}}$, and $1 + 2^b d$, with d coprime to 2, is a generator of the cyclic subgroup $1 + 2^b \mathbb{Z}_{2^a}$.
- **(iii.2)** if $b = 1$, then $1 + 2\mathbb{Z}_{2^a} = \mathbb{Z}_{2^a}^*$.

The next two lemmas play important roles in the proofs of our main results.

Lemma 3.5. *Let $u \neq -1$ be an odd integer. In the multiplicative group $\mathbb{Z}_{2^a}^*$ ($a \geq 2$), we have:*

- **(i)** *If $\nu_2(u-1) \geq 2$, then $\langle u \rangle \subseteq \langle 5 \rangle$, $\mathrm{ord}(u) = 2^{\max\{a - \nu_2(u-1),\, 0\}}$, and the quotient group $\mathbb{Z}_{2^a}^* / \langle u \rangle = \langle \overline{-1} \rangle \times \langle \bar{5} \rangle$, where $\overline{-1}$ and $\bar{5}$ denote the images of -1 and 5 in the quotient group, respectively. In particular, $|\langle \bar{5} \rangle| = 2^{\min\{\nu_2(u-1)-2,\, a-2\}}$ and $|\langle \overline{-1} \rangle| = 2$.*
- **(ii)** *If $\nu_2(u-1) = 1$, then $\langle u \rangle \cap \langle 5 \rangle = \langle u^2 \rangle$, $\mathrm{ord}(u^2) = 2^{\max\{a - \nu_2(u+1) - 1,\, 0\}}$, and the quotient group $\mathbb{Z}_{2^a}^* / \langle u \rangle = \langle \bar{5} \rangle$ is a cyclic group of order $2^{\min\{\nu_2(u+1)-1,\, a-2\}}$.*

Proof. Let $u = 1 + 2^b d$, where $b = \nu_2(u-1)$ and d is odd.

(i). If $b \geq a$, then $u = 1 \in \langle 5 \rangle$. Otherwise, $2 \leq b < a$, so $(1 + 2^b d)^{2^{a-b}} = 1$ but $(1 + 2^b d)^{2^{a-b-1}} \neq 1$, which gives $\mathrm{ord}(u) = 2^{a-b}$. In other words, $\mathrm{ord}(u) = 2^{\max\{a-b,\, 0\}}$ $\big($this is just an argument for Remark 3.4 (iii.1)$\big)$. Specifically, $\langle 5 \rangle = 1 + 2^2 \mathbb{Z}_{2^a}$. Therefore, $\langle u \rangle \subseteq \langle 5 \rangle$, $\mathbb{Z}_{2^a}^* / \langle u \rangle = \langle \bar{5} \rangle \times \langle \overline{-1} \rangle$ and

$$|\langle \bar{5} \rangle| = 2^{a-2} / \mathrm{ord}(u) = 2^{\min\{b-2,\, a-2\}}.$$

(ii). In this case $u + 1 = 2(d+1)$, so $\nu_2(u+1) = 1 + \nu_2(d+1) \geq 2$. Writing $d = 2^{\nu_2(u+1)-1}(-u') - 1$ with u' being odd, we get

$$u = 1 + 2d = (-1)(1 + 2^{\nu_2(u+1)} u') \in \langle -1 \rangle \times \langle 5 \rangle, \quad \nu_2(u+1) \geq 2, \quad 2 \nmid u'. \tag{3.1}$$

Note that $u \notin \langle 5 \rangle$, but $u^2 = 1 + 2^{\nu_2(u+1)+1}(u' + 2^{\nu_2(u+1)-1} u'^2) \in \langle 5 \rangle$ and

$$\mathrm{ord}(u^2) = \begin{cases} 2^{a - \nu_2(u+1) - 1}, & \nu_2(u+1) + 1 \leq a; \\ 1, & \nu_2(u+1) + 1 > a. \end{cases}$$

In other words, $\mathrm{ord}(u^2) = 2^{\max\{a - \nu_2(u+1) - 1,\, 0\}}$. Then $\mathbb{Z}_{2^a}^* = \langle 5 \rangle \cdot \langle u \rangle$ and $\langle u \rangle \cap \langle 5 \rangle = \langle u^2 \rangle$, hence

$$\mathbb{Z}_{2^a}^* / \langle u \rangle \cong \langle 5 \rangle / \left(\langle u \rangle \cap \langle 5 \rangle \right) = \langle 5 \rangle / \langle u^2 \rangle$$

is cyclic group. Recalling that $|\langle 5 \rangle| = 2^{a-2}$, we then have

$$|\mathbb{Z}_{2^a}^* / \langle u \rangle| = |\langle 5 \rangle / \langle u^2 \rangle| = 2^{\min\{\nu_2(u+1)-1,\, a-2\}}.$$

We are done. □

Lemma 3.6. *Let h, u be odd integers with $u \neq -1$. We denote by $\bar{h}$ the image of h in the quotient group $\mathbb{Z}_{2^a}^*/\langle u\rangle$, where $a \geq 2$. Let $\mathrm{ord}(\bar{h}) = 2^v$. With the convention that $\nu_2(h+1) = -\infty$ and $|\nu_2(h+1)| = \infty$ when $h = -1$, we have:*

(i) *If both $\nu_2(u-1) \geq 2$ and $\nu_2(h-1) \geq 2$, then*

$$v = \max\big\{\min\{\nu_2(u-1),\, a\} - \nu_2(h-1),\, 0\big\}.$$

(ii) *If $\nu_2(u-1) = 1$ and $\nu_2(h-1) \geq 2$, then*

$$v = \max\big\{\min\{\nu_2(u+1)+1,\, a\} - \nu_2(h-1),\, 0\big\}.$$

(iii) *If $\nu_2(u-1) \geq 2$ and $\nu_2(h-1) = 1$, then*

$$v = \max\big\{\min\{\nu_2(u-1),\, a\} - |\nu_2(h+1)|,\, 1\big\}.$$

(iv) *If both $\nu_2(u-1) = 1$ and $\nu_2(h-1) = 1$, then*

$$v = \begin{cases} \max\big\{\min\{\nu_2(u+1)+1,\, a\} - \min\{|\nu_2(h+1)|,\, \nu_2(u+1)\},\, 0\big\}, \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad \nu_2(h+1) \neq \nu_2(u+1); \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad \nu_2(h+1) = \nu_2(u+1). \end{cases}$$

Proof. Let $\langle h, u\rangle$ be the subgroup of $\mathbb{Z}_{2^a}^*$ generated by h and u. Then $2^v = \big|\langle h, u\rangle/\langle u\rangle\big|$.

(i). By Lemma 3.5(i), both u and h are located in $\langle 5\rangle$. Hence, $2^v = \mathrm{ord}(h)/\mathrm{ord}(u)$ if $\mathrm{ord}(h) > \mathrm{ord}(u)$, and $2^v = 1$ otherwise. However, $\mathrm{ord}(h) = 2^{\max\{a-\nu_2(h-1),\,0\}}$ and $\mathrm{ord}(u) = 2^{\max\{a-\nu_2(u-1),\,0\}}$ by Lemma 3.5(i) again. We get

$$\mathrm{ord}(h) > \mathrm{ord}(u) \quad\Longleftrightarrow\quad \nu_2(h-1) < \min\{\nu_2(u-1), a\}.$$

Thus $2^v = 2^{\max\{\min\{\nu_2(u-1),\,a\}-\nu_2(h-1),\,0\}}$.

(ii). In this case, $\langle h\rangle \subseteq \langle 5\rangle$ but $\langle u\rangle \cap \langle 5\rangle = \langle u^2\rangle$ (see Lemma 3.5(ii)). Then $\langle h\rangle \cap \langle u\rangle = \langle h\rangle \cap \langle 5\rangle \cap \langle u\rangle = \langle h\rangle \cap \langle u^2\rangle$, and hence

$$2^v = \big|\langle h, u\rangle/\langle u\rangle\big| = \big|\langle h\rangle/\langle h\rangle \cap \langle u^2\rangle\big|,$$

which leads to computations in the cyclic group $\langle 5\rangle$ similar to the ones in (i). By Lemma 3.5(ii), $\mathrm{ord}(u^2) = 2^{\max\{a-\nu_2(u+1)-1,\,0\}}$, so

$$2^v = 2^{\max\{\min\{\nu_2(u+1)+1,\,a\}-\nu_2(h-1),\,0\}}.$$

(iii). We can write $h = (-1)(1 + 2^{\nu_2(h+1)}h')$ with $|\nu_2(h+1)| \geq 2$ (the case $\nu_2(h+1) = -\infty$, i.e., $h = -1$, is allowed) and h' being odd (see Eqn (3.1)); set $h'' = 1 + 2^{\nu_2(h+1)}h'$. By Lemma 3.5(i), it follows that $\mathbb{Z}_{2^a}^*/\langle u\rangle = \langle\overline{-1}\rangle \times \langle\bar{5}\rangle$, and $\bar{h} = \overline{-1}\cdot\overline{h''}$ with $\overline{h''} \in \langle\bar{5}\rangle$. Then

$$2^v = \mathrm{ord}(\bar{h}) = \max\{\mathrm{ord}(\overline{-1}),\, \mathrm{ord}(\overline{h''})\}.$$

We know that $\mathrm{ord}(h'') = 2^{\max\{a-|\nu_2(h+1)|,\,0\}}$ (see Lemma 3.5(i), but $h=-1$ is allowed here). With the same argument as in (i), we have

$$\mathrm{ord}(\overline{h''}) = 2^{\max\{\min\{\nu_2(u-1),\,a\}-|\nu_2(h+1)|,\,0\}}.$$

Recalling that $\mathrm{ord}(\overline{-1}) = 2$, we get that $2^v = 2^{\max\{\min\{\nu_2(u-1),\,a\}-|\nu_2(h+1)|,\,1\}}$.

(iv). Similar to the above, we can write

$$\begin{aligned} h &= (-1)h'', \quad h'' = 1 + 2^{\nu_2(h+1)}h', \quad \nu_2(h+1) \geq 2, \quad 2 \nmid h'; \\ u &= (-1)u'', \quad u'' = 1 + 2^{\nu_2(u+1)}u', \quad \nu_2(u+1) \geq 2, \quad 2 \nmid u'. \end{aligned}$$

It is clear that $\langle h, u\rangle = \langle hu, u\rangle$, so

$$2^v = |\langle h, u\rangle/\langle u\rangle| = |\langle hu, u\rangle/\langle u\rangle|.$$

Since $u \notin \langle 5\rangle$, but $u^2 = 1 + 2^{\nu_2(u+1)+1}(u' + 2^{\nu_2(u+1)-1}u'^2) \in \langle 5\rangle$ and

$$hu = h''u'' = 1 + 2^{\nu_2(h+1)}h' + 2^{\nu_2(u+1)}u' + 2^{\nu_2(h+1)+\nu(u+1)}h'u' \ \in \ \langle 5\rangle;$$

this present case can be reduced to the case (ii) above (by replacing h in (ii) with hu). If $\nu_2(h+1) = \nu_2(u+1)$, then $\nu_2(hu-1) \geq \nu_2(u+1)+1$ (see the above formulation of hu), hence $2^v = 1$ by the conclusion in (ii). Otherwise

$$\nu_2(hu-1) = \begin{cases} \min\{\nu_2(h+1), \nu_2(u+1)\}, & h \neq -1; \\ \nu_2(u+1), & h = -1, \end{cases}$$

i.e., $\nu_2(hu-1) = \min\{|\nu_2(h+1)|, \nu_2(u+1)\}$. By the conclusion in (ii) again,

$$2^v = 2^{\max\{\min\{\nu_2(u+1)+1,\,a\}-\min\{|\nu_2(h+1)|,\,\nu_2(u+1)\},\,0\}}.$$

If $\nu_2(h+1) > \nu_2(u+1)$ or $h=-1$, then $\min\{|\nu_2(h+1)|,\, \nu_2(u+1)\} = \nu_2(u+1)$, and hence v can be simplified to:

$$v = \max\{\min\{\nu_2(u+1)+1, a\} - \nu_2(u+1),\, 0\} = \begin{cases} 1, & \nu_2(u+1) < a; \\ 0, & \nu_2(u+1) \geq a. \end{cases}$$

The proof is completed. □

4 Proofs of the main results

We keep the notations of Section 2. Consider the surjective homomorphism

$$\mathbb{Z}_{rn} \longrightarrow \mathbb{Z}_r, \quad x \ (\mathrm{mod}\ rn) \longmapsto x \ (\mathrm{mod}\ r). \tag{4.1}$$

Then $1 + r\mathbb{Z}_{rn}$ is just the inverse image of $1 \in \mathbb{Z}_r$.

Assume that $p_1, \cdots, p_k, p_1', \cdots, p_{k'}', p_1'', \cdots, p_{k''}''$ are distinct primes such that

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} {p_1'}^{\alpha_1'} \cdots {p_{k'}'}^{\alpha_{k'}'}, \quad \text{with } \alpha_1, \cdots, \alpha_k, \alpha_1', \cdots, \alpha_{k'}' \text{ all positive;}$$

$$r = p_1^{\beta_1} \cdots p_k^{\beta_k} {p''_1}^{\beta''_1} \cdots {p''_{k''}}^{\beta''_{k''}}, \quad \text{with } \beta_1, \cdots, \beta_k, \beta''_1, \cdots, \beta''_{k''} \text{ all positive,}$$

i.e., $\alpha_i = \nu_{p_i}(n)$, $\beta_i = \nu_{p_i}(r)$, etc. Then

$$rn = p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k} {p'_1}^{\alpha'_1} \cdots {p'_{k'}}^{\alpha'_{k'}} {p''_1}^{\beta''_1} \cdots {p''_{k''}}^{\beta''_{k''}}.$$

Set $n' = {p'_1}^{\alpha'_1} \cdots {p'_{k'}}^{\alpha'_{k'}}$ and $r'' = {p''_1}^{\beta''_1} \cdots {p''_{k''}}^{\beta''_{k''}}$. Applying the Chinese Remainder Theorem, we rewrite $\mathbb{Z}_{rn}$ as follows:

$$\mathbb{Z}_{rn} \overset{\text{CRT}}{=} \mathbb{Z}_{p_1^{\alpha_1+\beta_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k+\beta_k}} \times \mathbb{Z}_{n'} \times \mathbb{Z}_{r''}.$$

The surjective homomorphism (4.1) may be rewritten as

$$\rho: \quad \mathbb{Z}_{p_1^{\alpha_1+\beta_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k+\beta_k}} \times \mathbb{Z}_{n'} \times \mathbb{Z}_{r''} \longrightarrow \mathbb{Z}_{p_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_k}} \times \mathbb{Z}_{r''}, \quad (4.2)$$

with kernel

$$\text{Ker}(\rho) = p_1^{\beta_1}\mathbb{Z}_{p_1^{\alpha_1+\beta_1}} \times \cdots \times p_k^{\beta_k}\mathbb{Z}_{p_k^{\alpha_k+\beta_k}} \times \mathbb{Z}_{n'} \times \{0\},$$

where $\{0\}$ is the zero ideal of $\mathbb{Z}_{r''}$. Thus, $1 + r\mathbb{Z}_{rn} = 1 + \text{Ker}(\rho)$ can be rewritten as

$$1 + r\mathbb{Z}_{rn} \overset{\text{CRT}}{=} \left(1 + p_1^{\beta_1}\mathbb{Z}_{p_1^{\alpha_1+\beta_1}}\right) \times \cdots \times \left(1 + p_k^{\beta_k}\mathbb{Z}_{p_k^{\alpha_k+\beta_k}}\right) \times \mathbb{Z}_{n'} \times \{1\}. \quad (4.3)$$

Therefore

$$\mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn}) \overset{\text{CRT}}{=} \left(1 + p_1^{\beta_1}\mathbb{Z}_{p_1^{\alpha_1+\beta_1}}\right) \times \cdots \times \left(1 + p_k^{\beta_k}\mathbb{Z}_{p_k^{\alpha_k+\beta_k}}\right) \times \mathbb{Z}_{n'}^* \times \{1\}. \quad (4.4)$$

Thus, any $x \in (1 + r\mathbb{Z}_{rn})$ can be represented as

$$x \overset{\text{CRT}}{=} \left(1 + p_1^{\xi_1}x_1, \ \cdots, \ 1 + p_k^{\xi_k}x_k, \ x', \ 1\right) \quad (4.5)$$

with $\xi_i = \nu_{p_i}(x-1) \geq \beta_i$, $p_i \nmid x_i$ for $i = 1, \cdots, k$, and $x' \in \mathbb{Z}_{n'}$, and hence any $s \in {\mathbb{Z}_{rn}}^* \cap (1 + r\mathbb{Z}_{rn})$ can be represented as

$$s \overset{\text{CRT}}{=} \left(1 + p_1^{\sigma_1}s_1, \ \cdots, \ 1 + p_k^{\sigma_k}s_k, \ s', \ 1\right) \quad (4.6)$$

with $\sigma_i = \nu_{p_i}(s-1) \geq \beta_i$ and $p_i \nmid s_i$ for $i = 1, \cdots, k$, and $s' \in \mathbb{Z}_{n'}^*$. In particular, since $q \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$, we have

$$q \overset{\text{CRT}}{=} \left(1 + p_1^{\tau_1}q_1, \ \cdots, \ 1 + p_k^{\tau_k}q_k, \ q', \ 1\right) \quad (4.7)$$

where $\tau_i = \nu_{p_i}(q-1) \geq \beta_i$ and $p_i \nmid q_i$ for $i = 1, \cdots, k$, and $q' \in \mathbb{Z}_{n'}^*$.

We first need the following observation.

Lemma 4.1. *Let p be a prime. If $p \notin \{p_1, \cdots, p_k\}$, then there is a μ_s-orbit in $1 + r\mathbb{Z}_{rn}$ whose length is not divisible by p.*

Proof. Take $x_0 \in (1 + r\mathbb{Z}_{rn})$ such that (cf. Eqn (4.5)):

$$x_0 \overset{\text{CRT}}{=} \big(1 + p_1^{\xi_1} x_1,\ \cdots,\ 1 + p_k^{\xi_k} x_k,\ 0,\ 1\big).$$

Then the length of the μ_s-orbit in $\mathbb{Z}_{n'}$ containing 0 is 1, and the length of the μ_s-orbit in $1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$ containing $1 + p_i^{\xi_i} x_i$ is a power of p_i. By Lemmas 3.2 and 3.3, we see that the length of the μ_s-orbit in $(1 + r\mathbb{Z}_{rn})/\mu_q$ containing the q-cyclotomic coset $x_0\langle q\rangle$ is not divisible by p. □

Recall that, for any p_i, $1 \le i \le k$, both q and $s \pmod{p_i^{\alpha_i+\beta_i}}$ are contained in the multiplicative group $1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$; we denote by $\langle q, s\rangle_i$ the subgroup of $1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$ generated by q and s.

Theorem 4.2. *Let $M_s = \prod_{i=1}^{k} |\langle q, s\rangle_i : \langle q\rangle_i|$ be the order of s in the quotient group $\prod_{i=1}^{k} \big(1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\big)/\langle q\rangle_i$. Then μ_s is a Type-I m-adic splitting for $1 + r\mathbb{Z}_{rn}$ if and only if $m | M_s$.*

Proof. For any $x \in (1 + r\mathbb{Z}_{rn})$ as in Eqn (4.5), by Lemma 3.3, the length of the μ_s-orbit in the quotient set $\big(1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\big)/\mu_q$ containing $(1 + p_i^{\xi_i} x_i)\langle q\rangle$ is equal to $|\langle q, s\rangle_i : \langle q\rangle_i|$. By Lemmas 3.1, 3.2 and 4.1, the theorem follows at once. □

Now we are ready to prove our main results.

Proof of Theorem 2.4. Take an $\hat{s} \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$ as follows $\big($cf. Eqn (4.6)$\big)$:

$$\hat{s} \overset{\text{CRT}}{=} (1 + p_1^{\hat{\sigma}_1}, \cdots, 1 + p_k^{\hat{\sigma}_k}, 1, 1)$$

such that each component $1 + p_i^{\hat{\sigma}_i} \in 1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$ of $\hat{s}$ becomes an element of maximal order in the quotient group $\big(1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\big)/\langle q\rangle_i$ for $i = 1, \cdots, k$. Set $M = M_{\hat{s}}$ as in Theorem 4.2. Then, for any $s \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$, by Theorem 4.2 we have $M_s \,|\, M$. Thus, for an integer m, an m-adic (q, n, r)-constacyclic code of Type-I exists if and only if m is a divisor of M. It remains to determine M by its p-adic valuations $\nu_p(M)$, for all primes p. If $p \notin \{p_1, \cdots, p_k\}$, then we have seen from Theorem 4.2 that $\nu_p(M) = 0$. For $1 \le i \le k$, by Theorem 4.2 and the choice of $\hat{s}$, we see that $p_i^{\nu_{p_i}(M)}$ is the maximal order of elements of the quotient group $\big(1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\big)/\langle q\rangle_i$; we determine it in the following cases.

Case 1: p_i is odd or $\beta_i = \nu_{p_i}(r) \ge 2$. Then the group $1 + p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$ is a cyclic group of order $p_i^{\alpha_i}$, and the order of q is $p_i^{\max\{\alpha_i+\beta_i-\nu_{p_i}(q-1),\, 0\}}$ $\big($recall that $\nu_{p_i}(q-1) \ge \beta_i$ and the order of q is 1 when $\alpha_i + \beta_i \le \nu_{p_i}(q-1)\big)$. Thus,

the maximal order of the elements of the quotient group $\left(1+p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\right)/\langle q\rangle_i$ is $p_i^{\min\{\nu_{p_i}(q-1)-\beta_i,\,\alpha_i\}}$; hence $\nu_{p_i}(M)=\min\{\nu_{p_i}(q-1)-\nu_{p_i}(r),\,\nu_{p_i}(n)\}$.

Case 2: $p_i=2$ and $\nu_2(r)=1$. Then the group $1+2\mathbb{Z}_{2^{\alpha_i+1}}=\mathbb{Z}^*_{2^{\alpha_i+1}}=\langle -1\rangle\times\langle 5\rangle$ and $|\langle 5\rangle|=2^{\alpha_i-1}$. There are two subcases:

Subcase 2.1: $\nu_2(q-1)\geq 2$. By Lemma 3.5(i), the quotient group $\mathbb{Z}^*_{2^{\alpha_i+1}}/\langle q\rangle$ is the direct product of a cyclic group of order $2^{\min\{\nu_2(q-1)-2,\,\alpha_i-1\}}$ and a group of order 2. Thus

$$\nu_2(M)=\max\{\min\{\nu_2(q-1)-2,\,\nu_2(n)-1\},\,1\}.$$

Subcase 2.2: $\nu_2(q-1)=1$. By Lemma 3.5(ii), the quotient group $\mathbb{Z}^*_{2^{\alpha_i+1}}/\langle q\rangle$ is a cyclic group of order $2^{\min\{\nu_2(q+1)-1,\,\alpha_i-1\}}$. Thus

$$\nu_2(M)=\min\{\nu_2(q+1)-1,\,\nu_2(n)-1\}.$$ □

Proof of Theorem 2.5. For $i=1,\cdots,k$, from Theorem 4.2, in the quotient group $\left(1+p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}\right)/\langle q\rangle_i$, we have seen that

$$\nu_{p_i}(M_s)=|\langle q,s\rangle_i:\langle q\rangle_i|.$$

If p_i is odd, then $1+p_i^{\beta_i}\mathbb{Z}_{p_i^{\alpha_i+\beta_i}}$ is a cyclic group of order $p_i^{\nu_{p_i}(rn)-\nu_{p_i}(r)}$. By Remark 3.4(ii), we get immediately that

$$|\langle q,s\rangle_i:\langle q\rangle_i|=p_i^{\max\{\min\{\nu_{p_i}(q-1),\,\nu_{p_i}(rn)\}-|\nu_{p_i}(s-1)|,\,0\}}.$$

Otherwise, $p_i=2$ and all of the conclusions follow from Lemma 3.6 at once. □

5 Corollaries and examples

Most results on the existence of Type-I polyadic constacyclic codes can follow as consequences from the main theorems immediately. Moreover, with the help of the main results and the arguments, some interesting examples can be constructed from Type-I polyadic constacyclic codes. Here we describe the case when $m=p$ is a prime, which is an interesting case.

5.1 p-adic constacyclic codes

Corollary 5.1. *Let $m=p$ be a prime. Then Type-I p-adic (q,n,r)-constacyclic codes exist if and only if one of the following two conditions holds:*

- **(i)** *$\nu_p(n)\geq 1$ and $\nu_p(q-1)>\nu_p(r)\geq 1$ (the case $p=2$ is allowed);*
- **(ii)** *$p=2$, $\nu_2(r)=1$ and $\min\{\nu_2(q+1),\nu_2(n)\}\geq 2$.*

Proof. Taking $m = p$ in Theorem 2.4, we obtain the desired result. □

Remark 5.2. The case of $p = 2$ in Corollary 5.1, i.e., the necessary and sufficient conditions for the existence of duadic constacyclic codes, was treated in [6, Corollary 17] and stated in different notations.

On the other hand, if the prime p is odd, then (ii) of Corollary 5.1 is not applicable, hence the statement can be shortened; for example, for $p = 3$, the statement can read as

"*Type-I triadic (q, n, r)-constacyclic codes exist if and only if $\nu_3(n) \geq 1$ and $\nu_3(q-1) > \nu_3(r) \geq 1$.*"
This result has been obtained in [19].

Inspired by the conditions of Corollary 5.1, we construct a class of p-adic constacyclic generalized Reed-Solomon codes. For nonzero $v_0, v_1, \cdots, v_{n-1} \in \mathbb{F}_q^*$ and distinct $\alpha_0, \alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q$, the following $[n, k, n-k+1]$ code

$$\Big\{ \Big(v_0 f(\alpha_0), v_1 f(\alpha_1), \cdots, v_{n-1} f(\alpha_{n-1}) \Big) \;\Big|\; f(X) \in \mathbb{F}_q[X],\ \deg f(X) < k \Big\}$$

is called a *generalized Reed-Solomon code*, abbreviated by *GRS code*, with locator $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$; it is an $[n, k, n-k+1]$ MDS code. We denote this GRS code by $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})$, where $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$, cf. [17, Ch.9].

Proposition 5.3. *Assume that $m = p$ is a prime, q is a prime power with $\nu_p(q-1) \geq 2$, and $rn \mid (q-1)$ such that $\nu_p(r) \geq 1$ and $\nu_p(n) \geq 1$ (then Corollary 5.1(i) is satisfied). Let $\omega \in \mathbb{F}_q$ be a primitive rn-th root of unity and $\lambda = \omega^n$. Set*

$$\mathcal{X}_j = \Big\{ 1 + ir \;\Big|\; \tfrac{jn}{p} \leq i < \tfrac{(j+1)n}{p} \Big\}, \qquad j = 0, 1, \cdots, p-1.$$

Then

- **(i)** *$C_{\mathcal{X}_j}$, for $j = 0, 1, \cdots, p-1$, are Type-I p-adic λ-constacyclic codes given by $\mu_{1+\frac{rn}{p}}$;*
- **(ii)** *for any $0 < k < p$, the constacyclic code $C = C_{\mathcal{X}_0} \oplus C_{\mathcal{X}_1} \oplus \cdots \oplus C_{\mathcal{X}_{k-1}}$ is the $[n, \frac{kn}{p}, \frac{(p-k)n}{p}+1]$ GRS code $\mathrm{GRS}_{\frac{kn}{p}}(\boldsymbol{\omega}; \mathbf{v})$ with $\boldsymbol{\omega} = (1, \omega^{-r}, \cdots, \omega^{-(n-1)r})$ and $\mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-(n-1)})$.*

Proof. (i). Let $s = 1 + \frac{rn}{p}$. Noting that $p \mid r$, we have

$$\mu_s(1+ir) = \Big(1 + \frac{rn}{p}\Big)(1+ir) \equiv\ 1 + r\Big(\frac{n}{p} + i\Big) \pmod{rn}.$$

Hence $\mu_s(\mathcal{X}_j) = \mathcal{X}_{j+1}$ for $j = 0, \cdots, p-2$, and $\mu_s(\mathcal{X}_{p-1}) = \mathcal{X}_0$. Thus $\mathcal{X}_0$, $\mathcal{X}_1$, $\cdots$, $\mathcal{X}_{p-1}$ form a Type-I p-adic splitting of $1 + r\mathbb{Z}_{rn}$ given by μ_s.

(ii). Since ω^{-r} is a primitive n-th root of unity, $\boldsymbol{\omega}$ is a locator and $\mathrm{GRS}_{kn/p}(\boldsymbol{\omega}; \mathbf{v})$ is a GRS $[n, \frac{kn}{p}, \frac{(p-k)n}{p} + 1]$ code. We need to show that $C = \mathrm{GRS}_{kn/p}(\boldsymbol{\omega}; \mathbf{v})$. Since $\dim C = \frac{kn}{p}$, it suffices to show that $\mathrm{GRS}_{kn/p}(\boldsymbol{\omega}; \mathbf{v}) \subseteq C$.

Set $\mathcal{K} = \mathcal{X}_0 \cup \cdots \cup \mathcal{X}_{k-1}$ and $\mathcal{K}' = \mathcal{X}_k \cup \cdots \cup \mathcal{X}_{p-1}$. Then $\prod_{Q \in \mathcal{K}/\mu_q} M_Q(X)$ is a check polynomial of C, hence $\{\omega^t \mid t \in \mathcal{K}'\} = \{\omega^{1+ir} \mid \frac{kn}{p} \le i < n\}$ is the set of zeros of the code C.

For $f(X) = \sum_{j=0}^{\frac{kn}{p}-1} f_j X^j$ with $f_i \in \mathbb{F}_q$, the codeword of $\mathrm{GRS}_{kn/p}(\boldsymbol{\omega}; \mathbf{v})$,

$$c'_f = \big(f(1), \omega^{-1} f(\omega^{-r}), \cdots, \omega^{-(n-1)} f(\omega^{-r(n-1)})\big),$$

corresponds to the polynomial $c'_f(X) = \sum_{t=0}^{n-1} \omega^{-t} f(\omega^{-rt}) X^t$ in the polynomial representation of codewords. To prove that $c'_f \in C$, it is enough to show that $c'_f(\omega^{1+ir}) = 0$ for $\frac{kn}{p} \le i < n$. We compute $c'_f(\omega^{1+ir})$ as follows:

$$c'_f(\omega^{1+ir}) = \sum_{t=0}^{n-1} \omega^{-t} \left(\sum_{j=0}^{\frac{kn}{p}-1} f_j \omega^{-rtj} \right) \omega^{(1+ir)t} = \sum_{j=0}^{\frac{kn}{p}-1} f_j \sum_{t=0}^{n-1} \omega^{r(i-j)t}.$$

Since $\frac{kn}{p} \le i < n$ and $0 \le j < \frac{kn}{p}$, we see that $0 < i - j < n$, hence $\omega^{r(i-j)} \neq 1$ as ω^r is a primitive n-th root of unity. Then

$$\sum_{t=0}^{n-1} \omega^{r(i-j)t} = \frac{\omega^{r(i-j)n} - 1}{\omega^{r(i-j)} - 1} = 0, \qquad \text{for } \frac{kn}{p} \le i < n, \;\; 0 \le j < \frac{kn}{p}.$$

Therefore, $c'_f(\omega^{1+ir}) = 0$ for all $1 + ir \in \mathcal{K}'$; we are done. □

Some GRS codes from Proposition 5.3 are exhibited in Table 5.1.

No	m	q	r	n	k	d	GRS code $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})$
(i)	3	19	3	6	4	3	$\boldsymbol{\alpha} = (1, \omega^{-3}, \cdots, \omega^{-15}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-5})$
(ii)	3	2^6	3	21	7	15	$\boldsymbol{\alpha} = (1, \omega^{-3}, \cdots, \omega^{-60}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-20})$
(iii)	2	17	2	8	4	5	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-14}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-7})$
(iv)	2	3^4	2	40	20	21	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-78}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-39})$
(v)	2	5^2	2	12	6	7	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-22}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-11})$
(vi)	2	7^2	2	24	12	13	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-46}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-23})$

Table 5.1: GRS codes from Type-I polyadic constacyclic codes

Example 5.4. An interesting particular case of Proposition 5.3 is as follows: $m = r = 2$, n is an even divisor of $\frac{q-1}{2}$, and the splitting of $1 + 2\mathbb{Z}_{2n}$ is

$$\mathcal{X}_0 = \{1, 3, \cdots, n-1\}, \qquad \mathcal{X}_1 = \{n+1, n+3, \cdots, 2n-1\}, \tag{5.1}$$

(e.g., the codes (iii)-(vi) in Table 5.1 where $n = \frac{q-1}{2}$). It is a Type-I duadic splitting of $1 + 2\mathbb{Z}_{2n}$ given by $\mu_{1+\frac{rn}{2}} = \mu_{n+1}$. However, it is easy to check that

$\mathcal{X}_0, \mathcal{X}_1$ also form a splitting of $1+2\mathbb{Z}_{2n}$ given by μ_{-1}. In other words, both $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ are self-dual duadic negacyclic GRS codes with parameters $[n, \frac{n}{2}, \frac{n}{2}+1]$.

The biggest choice of n is $n = \frac{q-1}{2}$ and, in this case, the self-dual duadic negacyclic GRS code $C_{\mathcal{X}_0}$ has parameters $[\frac{q-1}{2}, \frac{q-1}{4}, \frac{q+3}{4}]$.

Before further analyzing this example, we discuss the particular case of Theorem 2.5 where $m = p$ is a prime.

5.2 p-adic constacyclic codes given by μ_s

When $m = p$ is an odd prime in Theorem 2.5, the case is easy, as shown in the following.

Corollary 5.5. *Assume that $m = p$ is an odd prime, $s \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$ and $s \neq 1$. Then Type-I p-adic splittings of $1 + r\mathbb{Z}_{rn}$ given by μ_s exist if and only if $p \,|\, \gcd(n, r)$ and $\nu_p(s-1) < \min\{\nu_p(q-1), \nu_p(rn)\}$.*

For the remaining case of $m = p = 2$ in Theorem 2.5, we obtain the following consequence.

Corollary 5.6. *Assume that $s \in \mathbb{Z}_{rn}^* \cap (1+r\mathbb{Z}_{rn})$. Then Type-I duadic splittings for $1 + r\mathbb{Z}_{rn}$ given by μ_s exist if and only if both n and r are even and one of the following four conditions holds:*

- **(i)** *$\nu_2(q-1) > |\nu_2(s-1)|$ and $\nu_2(rn) > |\nu_2(s-1)|$;*
- **(ii)** *$\nu_2(q-1) = 1$, $\nu_2(s-1) > 1$, $\nu_2(q+1) + 1 > |\nu_2(s-1)|$ and $\nu_2(rn) > |\nu_2(s-1)|$;*
- **(iii)** *$\nu_2(q-1) = \nu_2(s-1) = 1$, $|\nu_2(s+1)| > \nu_2(q+1)$ and $\nu_2(rn) > \nu_2(q+1)$;*
- **(iv)** *$\nu_2(q-1) = \nu_2(s-1) = 1$, $|\nu_2(s+1)| < \nu_2(q+1)$ and $|\nu_2(s+1)| < \nu_2(rn)$.*

Proof. By Theorem 2.5, we need to look for a condition such that $\nu_2(M_s) \geq 1$. If $\nu_2(q-1) \geq 2$, by (i) and (iii) of Theorem 2.5, we arrive at (i) of the corollary. Furthermore, (ii) of the corollary follows from (ii) of Theorem 2.5, while (iii) and (iv) of the corollary follow from (iv) of Theorem 2.5. □

Remark 5.7. Note that, if $s \in \mathbb{Z}_{rn}^* \cap (1+r\mathbb{Z}_{rn})$ and r is even, then s is odd, i.e., $|\nu_2(s-1)| \geq 1$; hence Condition (i) of Corollary 5.6 implies that $\nu_2(q-1) \geq 2$, or equivalently, $q \equiv 1 \pmod 4$. Hence, Corollary 5.6(i) yields again, but in different notations, the result [6, Theorem 20] for the case when $q \equiv 1 \pmod 4$. Moreover, a special case of Corollary 5.6 (iii) and (iv) was also described in [6, Theorem 20], which, however, contains some inaccuracies. A correction to [6, Theorem 20] has been shown in [8, Theorem 1.3] as follows:

> *Assume $q \equiv 3 \pmod 4$, with $q = -1 + 2^c d$ for some $c \geq 2$ and some odd d. Let $r = 2r'$, $n = 2^b n'$ and $s = 1 + 2r'n'$, with r', n' odd and $b \geq 2$.*

(A) *μ_s is a Type-I duadic splitting for $1 + r\mathbb{Z}_{rn}$ if and only if one of the following conditions holds:* (1) $c > b > \nu_2(1 + r'n')$; (2) $b \geq c > \nu_2(1 + r'n')$.

(B) *For $2 \leq i < 1 + b$, $\mu_{1+2^i r'n'}$ is a Type-I duadic splitting for $1 + r\mathbb{Z}_{rn}$ if and only if $i \leq c$.*

One can see that statement (B) follows from (ii) of Corollary 5.6, while statement (A) follows from (iii) and (iv) of the corollary. Moreover, (ii), (iii) and (iv) of Corollary 5.6 are more extensive than the result of [8] stated above, e.g., the case "$s = -1$" does not appear in [8, Theorem 1.3] but is included in Corollary 5.6: since $\nu_2((-1) - 1) = 1$ and $|\nu_2((-1) + 1)| = \infty$, the following corollary follows at once.

Corollary 5.8. *Type-I duadic splittings for $1 + r\mathbb{Z}_{rn}$ given by μ_{-1} exist if and only if n is even, $r = 2$ and one of the following two conditions holds:*

(i) $\nu_2(q - 1) \geq 2$ *(i.e., $q \equiv 1 \pmod 4$);*

(ii) $\nu_2(q - 1) = 1$ *(i.e., $q \equiv 3 \pmod 4$) and* $\nu_2(q + 1) < \nu_2(rn)$.

As mentioned in [5], Euclidean self-dual negacyclic codes are just Type-I duadic negacyclic codes given by μ_{-1}. In this sense, Corollary 5.8 is just [5, Theorem 3].

5.3 Alternant constacyclic MDS codes

By an *alternant code*, we mean a subfield subcode of a GRS code $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})$ over a large field $\mathbb{F}_{q^e}$, i.e., the code over the ground field $\mathbb{F}_q$, denoted by $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})|_{\mathbb{F}_q}$, obtained by restricting the GRS code $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})$ over $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$ (cf. [17, Ch. 9]).

For the case (i) of Corollary 5.8, we have shown in Example 5.4 a family of self-dual negacyclic GRS codes with parameters $[\frac{q-1}{2}, \frac{q-1}{4}, \frac{q+3}{4}]$. On the other hand, it is easy to see that there are no self-dual negacyclic GRS codes for the case (ii) of Corollary 5.8: since $2n \nmid (q - 1)$, there are no primitive $2n$-th roots of unity in $\mathbb{F}_q$. However, Proposition 5.3 and Example 5.4 provide a way to construct self-dual negacyclic alternant MDS codes for both the cases of Corollary 5.8. An easy modification of the Berlekamp-Welch algorithm can then be applied to carry out decoding for such codes.

Proposition 5.9. *Assume that q is a power of an odd prime. Let $n = \frac{q+1}{\ell}$ with ℓ being an odd divisor of $q + 1$, let $\omega \in \mathbb{F}_{q^2}$ be a primitive $2n$-th root of unity, and let*

$$\mathcal{X}_0 = \{1, 3, \cdots, n - 1\}, \qquad \mathcal{X}_1 = \{n + 1, n + 3, \cdots, 2n - 1\},$$

as in Eqn (5.1). Then

(i) *$\mathcal{X}_0$ and $\mathcal{X}_1$ form a Type-I duadic splitting of $1+2\mathbb{Z}_{2n}$ over $\mathbb{F}_q$ given by μ_{-1};*

(ii) *the duadic negacyclic codes $C_{\mathcal{X}_0}, C_{\mathcal{X}_1}$ over $\mathbb{F}_q$ are self-dual duadic negacyclic MDS $[n, \frac{n}{2}, \frac{n}{2}+1]$ codes;*

(iii) *$C_{\mathcal{X}_0} = \mathrm{GRS}_{n/2}(\boldsymbol{\omega}; \mathbf{v})|_{\mathbb{F}_q}$ is an alternant code restricted from $\mathrm{GRS}_{n/2}(\boldsymbol{\omega}; \mathbf{v})$, which is the GRS code over $\mathbb{F}_{q^2}$ with $\boldsymbol{\omega} = (1, \omega^{-2}, \cdots, \omega^{-2(n-1)})$ and $\mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-(n-1)})$.*

Proof. Note that, for any odd integer t, we have $tn \equiv n \pmod{2n}$. Since $q = \ell n - 1$ with ℓ being odd, we have $q \equiv n-1 \pmod{2n}$. For any $i \in \mathcal{X}_0$, since i is odd, we have

$$qi \equiv (n-1)i = ni - i \equiv n - i \pmod{2n}.$$

Thus $\mu_q(\mathcal{X}_0) = \mathcal{X}_0$, i.e., both $\mathcal{X}_0$ and $\mathcal{X}_1$ are μ_q-invariant, which proves the conclusion (i).

By Proposition 5.3 and Example 5.4, the duadic negacyclic code $\tilde{C}_{\mathcal{X}_0}$ over $\mathbb{F}_{q^2}$ is a self-dual negacyclic GRS code as follows:

$$\begin{aligned}\tilde{C}_{\mathcal{X}_0} &= \mathrm{GRS}_{n/2}(\boldsymbol{\omega}; \mathbf{v}) \\ &= \Big\{ \Big(f(1), \omega^{-1} f(\omega^{-2}), \cdots, \omega^{-(n-1)} f(\omega^{-2(n-1)}) \Big) \,\Big|\, f(X) \in \mathbb{F}_{q^2}[X],\ \deg f(X) < \tfrac{n}{2} \Big\}.\end{aligned}$$

Note that $C_{\mathcal{X}_0} \subseteq \tilde{C}_{\mathcal{X}_0}$, $\omega C_{\mathcal{X}_0} \subseteq \tilde{C}_{\mathcal{X}_0}$, and that $\dim_{\mathbb{F}_q} \tilde{C}_{\mathcal{X}_0} = 2 \dim_{\mathbb{F}_{q^2}} \tilde{C}_{\mathcal{X}_0} = n$. We have the direct sum $\tilde{C}_{\mathcal{X}_0} = C_{\mathcal{X}_0} \oplus \omega C_{\mathcal{X}_0}$. Therefore, $C_{\mathcal{X}_0} = \tilde{C}_{\mathcal{X}_0}|_{\mathbb{F}_q}$ is the desired subfield subcode of the code $\tilde{C}_{\mathcal{X}_0}$. Both the conclusions (ii) and (iii) now follow easily. □

The biggest choice of n in Proposition 5.9 is $n = q+1$. For this choice, the self-dual duadic negacyclic alternant MDS code $C_{\mathcal{X}_0}$ has parameters $[q+1, \frac{q+1}{2}, \frac{q+3}{2}]$. Blackford [5, Corollary 5] has constructed this self-dual negacyclic $[q+1, \frac{q+1}{2}, \frac{q+3}{2}]$ code, but did not show it to be an alternant code. The additional knowledge of the alternant structure of this code implies that, for example, a slight modification of the Berlekamp-Welch algorithm (cf. [28]) can now be used for decoding for this code.

Remark 5.10. The alternant structure of $C_{\mathcal{X}_0} = \mathrm{GRS}_{\frac{n}{2}}(\boldsymbol{\omega}; \mathbf{v})|_{\mathbb{F}_q}$ in Proposition 5.9 is helpful, e.g., the Berlekamp-Welch decoding algorithm can be adapted to decode $C_{\mathcal{X}_0}$.

Let $e = \lfloor \frac{n-k}{2} \rfloor$ (note that $k = \frac{n}{2}$ for $C_{\mathcal{X}_0}$). Assume that a codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in C_{\mathcal{X}_0}$ is transmitted and the word $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1})$ is received. To recover the polynomial $f(X) \in \mathbb{F}_{q^2}[X]$ with $\deg f(X) < k$ such that $c_i = \omega^{-i} f(\omega^{-2i})$, $i = 0, 1, \cdots, n-1$, we proceed in two steps.

S1. Find a polynomial $E(X) = X^e + \eta_{e-1}X^{e-1} + \cdots + \eta_0 \in \mathbb{F}_{q^2}[X]$ and a polynomial $Q(X) = \xi_{e+k-1}X^{e+k-1} + \xi_{e+k-2}X^{e+k-2} + \cdots + \xi_0 \in \mathbb{F}_{q^2}[X]$ such that

$$\omega^i y_i E(\omega^{-2i}) = Q(\omega^{-2i}), \qquad i = 0, 1, \cdots, n-1, \tag{5.2}$$

which is a system of n linear equations and $2e + k$ unknowns (recall that $2e + k \le n$). If the system of linear equations (5.2) has no solution, then output `Fail`; otherwise go to S2.

S2. If $E(X)$ divides $Q(X)$, then output $f(X) = Q(X)/E(X)$; otherwise, output `Fail`.

It is known that, if the Hamming distance $\mathrm{d}(\mathbf{y}, \mathbf{c}) \le e$, then a unique $f(X)$ is output. S1 is implemented by solving the system of linear equations, and S2 is implemented by long division of polynomials. Thus the complexity of the algorithm is $O(n^3)$.

The following example is a continuation of Example 2.2.

Example 5.11. Let $q = 5$, $r = 2$ (hence $\lambda = -1 = 4$), $n = 6$ and $s = -1$. Take a primitive third root θ of unity (in $\mathbb{F}_{25}$), i.e., $\theta \notin \mathbb{F}_5$ and $\theta^2 + \theta + 1 = 0$. Thus any element of $\mathbb{F}_{25}$ is represented uniquely as $a\theta + b$ with $a, b \in \mathbb{F}_5$. Then $\omega = 3\theta$ is a primitive 12-th root of unity such that $\omega^3 = 2$ and $\omega^6 = -1$. By Proposition 5.9, $1 + 2\mathbb{Z}_{12} = \{1, 3, 5, 7, 9, 11\}$ and

- $\mathcal{X}_0 = \{1, 3, 5\}$, $\mathcal{X}_1 = \{7, 9, 11\}$ form a Type-I duadic splitting of $1 + 2\mathbb{Z}_{12}$ given by μ_{-1};
- $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ are Type-I self-dual negacyclic codes with check polynomials $X^3 + X^2 + 3X + 2$ and $X^3 + 4X^2 + 3X + 3$, respectively.

Thus $X^3 + 4X^2 + 3X + 3$ is a generator polynomial of $C_{\mathcal{X}_0}$, and

$$G = \begin{pmatrix} 3 & 3 & 4 & 1 & & \\ & 3 & 3 & 4 & 1 & \\ & & 3 & 3 & 4 & 1 \end{pmatrix}$$

is a generator matrix of $C_{\mathcal{X}_0}$. Since $C_{\mathcal{X}_0}$ is self-dual, G is also a check matrix with which we can do systematic encoding by using feedback shift registers: a message (m_0, m_1, m_2) is encoded into a codeword $\mathbf{c} = (c_0, c_1, c_2, c_3, c_4, c_5)$, where $c_0 = m_0$, $c_1 = m_1$, $c_2 = m_2$, and

$$\begin{pmatrix} 3 & 3 & 4 & 1 & & \\ & 3 & 3 & 4 & 1 & \\ & & 3 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

i.e.,

$$c_3 = -4c_2 - 3c_1 - 3c_0, \quad c_4 = -4c_3 - 3c_2 - 3c_1, \quad c_5 = -4c_4 - 3c_3 - 3c_2.$$

Assume that a message $\mathbf{m} = (1, 0, 0)$ is being transmitted. It is encoded into the codeword $\mathbf{c} = (1, 0, 0, 2, 2, 1)$.

Suppose that the received word is $\mathbf{y} = (y_0, y_1, y_2, y_3, y_4, y_5) = (1, 1, 0, 2, 2, 1)$. then $\mathrm{d}(\mathbf{y}, \mathbf{c}) = 1 \leq e = \lfloor \frac{6-3}{2} \rfloor = 1$. By the algorithm in Remark 5.10, solving the linear system (5.2) (note that $\omega^{-1} = 2\theta^2$) yields

$$E(X) = X + \theta, \qquad Q(X) = (\theta - 2)X^3 + 2\theta X^2 + 2X + (3\theta - 1).$$

Next, by long division of polynomials, we obtain

$$Q(X) = (X + \theta)\big((\theta - 2)X^2 + X - (\theta - 2)\big),$$

from which it follows that $f(X) = (\theta - 2)X^2 + X - (\theta - 2)$. Thus

$$\begin{aligned} &c_0 = f(1) = 1, \qquad c_1 = 2\theta^2 f(-\theta) = 0, \quad c_2 = -\theta f(\theta^2) = 0, \\ &c_3 = 3f(-1) = 2, \quad c_4 = \theta^2 f(\theta) = 2, \qquad c_5 = 2\theta f(-\theta^2) = 1. \end{aligned}$$

Proposition 5.12. *Let q be an odd prime power such that $\nu_2(q-1) \geq 3$. Let $r = \frac{q-1}{2}$, $s = 1 + \frac{q^2-1}{4}$, $n = q + 1$, let $\omega \in \mathbb{F}_{q^2}$ be a primitive rn-*th *root of unity and let*

$$\mathcal{X}_0 = \Big\{1 + \frac{q-1}{2}j \,\Big|\, -\frac{q-1}{4} < j \leq \frac{q-1}{4} + 1\Big\}, \quad \mathcal{X}_1 = (1 + r\mathbb{Z}_{rn}) \setminus \mathcal{X}_0.$$

Then

(i) $\mathcal{X}_0$ and $\mathcal{X}_1$ form a Type-I duadic splitting of $1 + r\mathbb{Z}_{rn}$ over $\mathbb{F}_q$ given by μ_s;

(ii) the duadic constacyclic codes $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ over $\mathbb{F}_q$ are MDS $[n, \frac{n}{2}, \frac{n}{2} + 1]$ codes;

(iii) $C_{\mathcal{X}_1} = \mathrm{GRS}_{n/2}(\boldsymbol{\omega}; \mathbf{v})|_{\mathbb{F}_q}$ is an alternant code, where $\mathrm{GRS}_{n/2}(\boldsymbol{\omega}; \mathbf{v})$ is the GRS code over the field $\mathbb{F}_{q^2}$ with $\boldsymbol{\omega} = \big(1, \omega^r, \cdots, \omega^{(n-1)r}\big)$ and $\mathbf{v} = \big(1, \omega^{\frac{q-1}{4}r-1}, \omega^{\frac{q-1}{4}2r-2}, \cdots, \omega^{\frac{q-1}{4}(n-1)r-(n-1)}\big)$.

Proof. It is clear that $s \in \mathbb{Z}_{rn}^* \cap (1 + r\mathbb{Z}_{rn})$. To prove (i), it is enough to show that $\mathcal{X}_0$ is a union of some q-cyclotomic cosets modulo rn with $|\mathcal{X}_0| = \frac{q+1}{2}$ and $s\mathcal{X}_0 \bigcap \mathcal{X}_0 = \emptyset$. Clearly, $|\mathcal{X}_0| = \frac{q+1}{2}$. To show that $\mathcal{X}_0$ is a union of some q-cyclotomic cosets, it suffices to prove that $q(1 + \frac{q-1}{2}j) \in \mathcal{X}_0$ for any $-\frac{q-1}{4} < j \leq \frac{q-1}{4} + 1$. This is straightforward: $q(1 + \frac{q-1}{2}j) \equiv 1 + \frac{q-1}{2}(2 - j) \pmod{rn}$ and $-\frac{q-1}{4} + 1 \leq 2 - j < \frac{q-1}{4} + 2$. We are left to show that $s\mathcal{X}_0 \bigcap \mathcal{X}_0 = \emptyset$. Assuming otherwise, then two integers j, j' with $-\frac{q-1}{4} < j, j' \leq \frac{q-1}{4} + 1$ can be found such that $1 + \frac{q-1}{2}j \equiv 1 + \frac{q-1}{2}(j' + \frac{q+1}{2}) \pmod{\frac{q^2-1}{2}}$. We then have $j - j' \equiv \frac{q+1}{2} \pmod{q+1}$, which is impossible. Thus $\{\mathcal{X}_0,\ \mathcal{X}_1\}$ is a splitting of $1 + r\mathbb{Z}_{rn}$ given by μ_s, proving (i).

Observe that $\mathrm{ord}_{rn}(q) = 2$. Let $\tilde{C}_{\mathcal{X}_1}$ be the constacyclic code of length $q+1$ over $\mathbb{F}_{q^2}$ with check polynomial $\prod_{Q \in \mathcal{X}_1/\mu_q} M_Q(X)$. Hence, $\{\omega^j \mid j \in \mathcal{X}_0\}$ is the

set of zeros of the code $\tilde{C}_{\mathcal{X}_1}$. Using reasoning similar to that in the proof of Proposition 5.3, one gets

$$\tilde{C}_{\mathcal{X}_1} = \Big\{ \big(f(1), \omega^{\frac{q-1}{4}r-1} f(\omega^r), \cdots, \omega^{\frac{q-1}{4}(n-1)r-(n-1)} f(\omega^{(n-1)r})\big) \\ \Big| \, f(X) \in \mathbb{F}_{q^2}[X], \ \deg f(X) < \tfrac{n}{2} \Big\}.$$

It is easy to see that $\tilde{C}_{\mathcal{X}_1} \bigcap \mathbb{F}_q^n = C_{\mathcal{X}_1}$. We are done. □

We list some examples in Table 5.2. The alternant codes (i)-(iii) correspond to the codes (iv)-(vi) of Table 5.1, respectively, using Proposition 5.9, whereas the alternant codes (iv)-(v) are derived from Proposition 5.12.

No	m	q	r	n	k	d	Alternant code $\mathrm{GRS}_k(\boldsymbol{\alpha}; \mathbf{v})\vert_{\mathbb{F}_q}$
(i)	2	3^2	2	10	5	6	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-18}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-9})$
(ii)	2	5	2	6	3	4	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-10}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-5})$
(iii)	2	7	2	8	4	5	$\boldsymbol{\alpha} = (1, \omega^{-2}, \cdots, \omega^{-14}),\ \mathbf{v} = (1, \omega^{-1}, \cdots, \omega^{-7})$
(iv)	2	3^2	4	10	5	6	$\boldsymbol{\alpha} = (1, \omega^{4}, \cdots, \omega^{36}),\ \mathbf{v} = (1, \omega^{7}, \cdots, \omega^{63})$
(v)	2	17	8	18	9	10	$\boldsymbol{\alpha} = (1, \omega^{8}, \cdots, \omega^{136}),\ \mathbf{v} = (1, \omega^{33}, \cdots, \omega^{527})$

Table 5.2: Alternant MDS codes from Type-I duadic constacyclic codes

We present a tweak of Example 2.3 that leads to the existence of a Type-I polyadic splitting.

Example 5.13. Take $q = 3$, $r = 2$ (hence $\lambda = -1$) and $n = 20$. Unlike in Example 2.3, using Corollary 5.8(ii) in this case, there is a Type-I duadic splitting of

$$1 + 2\mathbb{Z}_{40} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39\}$$

given by μ_{-1} as follows:

$$\mathcal{X}_0 = \{1, 3, 5, 7, 9, 15, 21, 23, 27, 29\}, \quad \mathcal{X}_1 = \{11, 13, 17, 19, 25, 31, 33, 35, 37, 39\}.$$

We obtain self-dual duadic negacyclic ternary codes $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ of parameters $[20, 10, d]$. Since $\mathcal{X}_0$ contains 5 consecutive elements, we see that the minimum distance $d \geq 6$ by the BCH bound. For any self-dual ternary code of length n, by [20, Corollary 3], the minimum distance is bounded from above by $3\left\lfloor \frac{n}{12} \right\rfloor + 3$; and the code is said to be *extremal* when this upper bound is attained. Thus, it follows that both $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$ are extremal self-dual ternary $[20, 10, 6]$ codes.

The following example consists of another pair of extremal self-dual ternary constacyclic codes. With respect to the table in [12], they have the same minimum distance as the best known one to date.

Example 5.14. Take $q = 3$, $r = 2$ and $n = 28$. We have that

$$1 + 2\mathbb{Z}_{56} = Q_1 \bigcup Q_5 \bigcup Q_7 \bigcup Q_{11} \bigcup Q_{29} \bigcup Q_{35},$$

where Q_i are the 3-cyclotomic cosets modulo 56, for $i = 1, 5, 7, 11, 29, 35$. Let

$$\mathcal{X}_0 = Q_1 \bigcup Q_5 \bigcup Q_{35} \quad \text{and} \quad \mathcal{X}_1 = Q_{29} \bigcup Q_{11} \bigcup Q_7.$$

Then we obtain self-dual duadic negacyclic codes $C_{\mathcal{X}_0}$ and $C_{\mathcal{X}_1}$, which are $[28, 14, 9]$ codes.

Acknowledgements

The main results of this work were obtained while the third author was visiting the fourth author at Nanyang Technological University in Jan-Feb 2014. He is grateful for the hospitality and the support. The research of Bocong Chen, Yun Fan and San Ling is supported by NSFC with grant numbers 11271005 and 11171370. The research of Bocong Chen and San Ling is also partially supported by Nanyang Technological University's research grant number M4080456. We sincerely thank the Associate Editor and the anonymous referees for their helpful suggestions which led to significant improvements of the paper.

References

[1] J. L. Alperin, R. B. Bell, Groups and Representations, GTM 162, Springer-Verlag, New York, 1997.

[2] S.A. Aly, A. Klappenecker, P.K. Sarvepalli, Duadic group algebra codes, In: Proc. Int. Symp. Inf. Theory, Adelaide, Australia, (2007), 2096-2100.

[3] N. Aydin, I. Siap, D.J. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr., **24**(2001), 313-326.

[4] E.R. Berlekamp, Goppa codes, IEEE Trans. Inform. Theory, **5**(1973), 590-592.

[5] T. Blackford, Negacyclic duadic codes, Finite Fields Appl., **14**(2008), 930-943.

[6] T. Blackford, Isodual constacyclic codes, Finite Fields Appl., **24**(2013), 29-44.

[7] R.A. Brualdi, V. Pless, Polyadic codes, Discr. Appl. Math., **25**(1989), 3-17.

[8] B. Chen, H.Q. Dinh, A note on isodual constacyclic codes, Finite Fields Appl., **29**(2014), 243-246.

[9] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, Finite Fields Appl., **18**(2012), 1217-1231.

[10] C. Ding, K.Y. Lam, C. Xing, Enumeration and construction of all duadic codes of length p^m, Fund. Inform., **38**(1999), 149-161.

[11] C. Ding, V. Pless, Cyclotomy and duadic codes of prime lengths, IEEE Trans. Inform. Theory, **45**(1999), 453-466.

[12] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de

[13] S. Han, J.-L. Kim, Computational results of duadic double circulant codes, J. Appl. Math. Comput., **40**(2012), 33-43.

[14] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[15] J.S. Leon, J.M. Masley, V. Pless, Duadic codes, IEEE Trans. Inform. Theory, **30**(1984), 709-714.

[16] C. J. Lim, Consta-abelian polyadic codes, IEEE Trans. Inform. Theory, **51**(2005), 2198-2206.

[17] S. Ling, C. Xing, Coding Theory: A First Course, Cambridge University Press, Cambridge, 2004.

[18] S. Ling, C. Xing, Polyadic codes revisited, IEEE Trans. Inform. Theory, **50**(2004), 200-207.

[19] C. Liu, Some special classes of constacyclic codes (in Chinese), Thesis (M. S.), Central China Normal University, 2010.

[20] C.L. Mallows, N.J.A. Sloane, An upper bound for self-dual codes, Inform. Control, **22**(1973), 188-200.

[21] V. Pless, Duadic codes revisited, Congressus Numeratium, **59**(1987), 225-233.

[22] V. Pless, J.J. Rushanan, Triadic codes, Linear Algebra Appl., **98**(1988), 415-433.

[23] J.J. Rushanan, Duadic codes and difference sets, J. Combin. Theory Ser. A, **57**(1991), 254-61.

[24] A. Sharma, G.K. Bakshi, M. Raka, Polyadic codes of prime power length, Finite Fields Appl., **13**(2007), 1071-1085.

[25] M.H.M. Smid, Duadic codes, IEEE Trans. Inform. Theory, **33**(1987), 432-433.

[26] J.H. van Lint, Introduction to Coding Theory, Springer, Berlin, 1982.

[27] H.N. Ward, L. Zhu, Existence of abelian group codes partitions, J. Combin. Theory Ser. A, **67**(1994), 276-281.

[28] Wikipedia, Berlekamp-Welch algorithm, http://en.wikipedia.org/wiki/Berlekamp-Welch_algorithm, 2014.

[29] Y. Yang, W. Cai, On self-dual constacyclic codes over finite fields, Des. Codes Cryptogr., DOI 10.1007/s10623-013-9865-9.

[30] S. Zhang, Existence of certain class of duadic group algebra codes, J. Statist. Plann. Inference, **94**(2001), 405-411.

[31] L. Zhu, Duadic group algebra codes, J. Statist. Plann. Inference, **51**(1996), 395-401.