Journal of Mathematics Research; Vol. 9, No. 2; April 2017
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

The Cardinality of the Set of Zeros of Homogeneous Linear Recurring Sequences over Finite Fields

Yasanthi Kottegoda[1], Robert W. Fitzgerald[2]

[1]Department of Mathematics and Physics, University of New Haven, USA

[2] Department of Mathematics, Southern Illinois University Carbondale, USA

Correspondence: Yasanthi Kottegoda, Department of Mathematics and Physics, University of New Haven, USA. Tel: 1-203-500-9634. E-mail: YKottegoda@newhaven.edu

Received: February 14, 2016 Accepted: March 8, 2017 Online Published: March 14, 2017

doi:10.5539/jmr.v9n2p56 URL: https://doi.org/10.5539/jmr.v9n2p56

Abstract

Consider homogeneous linear recurring sequences over a finite field $\mathbb{F}_q$, based on the irreducible characteristic polynomial of degree d and order m. We give upper and lower bounds, and in some cases the exact values of the cardinality of the set of zeros of the sequences within its least period. We also prove that the cyclotomy bound introduced here is the best upper bound as it is reached in infinitely many cases. In addition, the exact number of occurrences of zeros is determined using the correlation with irreducible cyclic codes when $(q^d - 1)/m$ follows the quadratic residue conditions and also when it has the form $q^{2a} - q^a + 1$ where $a \in \mathbb{N}$.

Keywords: linear recurring sequences, irreducible cyclic codes, weights of cyclic codes.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements where $q = p^m$ for prime p. Let k be a positive integer, and let $a_0, a_1, \ldots, a_{k-1}$ be given elements of $\mathbb{F}_q$. A sequence $s_0, s_1, \ldots$ of elements of $\mathbb{F}_q$ satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n \qquad for\ n = 0, 1, \ldots \tag{1}$$

is called a (kth-order) homogeneous linear recurring sequence in $\mathbb{F}_q$. The terms $s_0, s_1, \ldots s_{k-1}$, which determine the complete sequence uniquely, are referred to as the initial values. A relation in the form of (1) is called a (kth-order) homogeneous linear recurrence relation. Let $s_0, s_1, \ldots$ be a kth order homogeneous linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation (1), where $a_j \in \mathbb{F}_q$ for $0 \le j \le k-1$. The polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0 \in \mathbb{F}_q[x]$$

is called a *characteristic polynomial* of the linear recurring sequence. For $s_0, s_1, \ldots$ homogeneous linear recurring sequence in $\mathbb{F}_q$, $m(x) \in \mathbb{F}_q[x]$ is said to be the minimal polynomial of the sequence if it has the following property: a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of positive degree is a characteristic polynomial of $s_0, s_1, \ldots$ if and only if $m(x)$ divides $f(x)$.

Definition *Let $f \in \mathbb{F}_q[x]$ be a non zero polynomial. If $f(0) \neq 0$, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the order of f which is denoted by ord(f).*

Theorem 1. (Lidl & Niederreiter, 1994) *Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$ with minimal polynomial $m(x) \in \mathbb{F}_q[x]$. Then the least period of the sequence is equal to ord($m(x)$).*

Linear recurring sequences were discussed for many years with a substantial development in the study of examining zeros and determining effective bounds for the set of zeros over infinite fields (Everest, Poorten, Shparlinski & Ward, 2003). Here we will consider homogeneous linear recurring sequences over finite fields based on irreducible minimal polynomials of certain degree d and order m. Let $P(d, m)$ be the set of all irreducible polynomials over $\mathbb{F}_q$ of degree d and order m. For $f \in P(d, m)$ and $I \in (\mathbb{F}_q^d)^* = (\mathbb{F}_q^d) \setminus \{0\}$, let $S(I, f) := \{s_n(I, f) | 1 \le n \le m\}$ be the first m terms (terms within the least period) of the homogeneous linear recurring sequence S over $\mathbb{F}_q$. Let $\mathcal{A} := \{Z(S(I, f)) | I \in (\mathbb{F}_q^d)^*, f \in P(d, m)\}$ be the set of zeros. Let $t = (q^d - 1)/m$. We will always assume that $t > 1$. If $t = 1$ then the polynomials in $P(d, m)$ are primitive and the number of zeros in the sequence is $q^{d-1} - 1$ (Lidl & Niederreiter, 1994). However, in the general case such an equitable distribution of zeros cannot be expected. Theorem 6.84 in Lidl and Niederreiter (1994) provides an estimate for the number of occurrences of zeros based on Gaussian sums and Mullen and Panario (2013) provides an improved bound. Table 1 gives some observations on the number of zeros of some linear recurring sequences over $\mathbb{F}_2$ computed via MAPLE (Kottegoda, 2010, Appendix I-VIII) with the degrees and orders of their corresponding irreducible

minimal polynomials. In this paper, in addition to explaining why there are so few choices for the number of zeros, we will give an accurate bound for the cardinality of the set of zeros, also providing formulas for the exact number of zeros when t has the form $q^{2a} - q^a + 1$ where $a \in \mathbb{N}$.

Table 1. Zeros of some homogeneous linear recurring sequences over $\mathbb{F}_2$ based on degree d and order m irreducible minimal polynomials.

d	m	Number of zeros	Cardinality
8	51	27, 19	2
8	85	37, 45	2
9	73	33, 37, 45	3
10	93	45, 61	2
10	341	181, 165	2
11	89	49, 41, 33	3
12	65	39, 37, 35, 33, 31, 29, 27, 25	8
12	91	55, 51, 47, 43, 39	5
12	105	73, 57, 49	3
12	195	107, 99, 91	3
12	273	153, 141, 133, 129	4
12	315	155, 187	2
12	455	231, 199	2
12	585	305, 289, 281	3
12	819	435, 403	2
12	1365	693, 661	2
14	381	253, 189	2
14	5461	2773, 2709	2
15	1057	573, 553, 537, 525, 517, 513	6
15	4681	2361, 2345, 2265	3
16	3855	1807, 1935	2
16	771	411, 395, 387, 379, 363, 355	6
16	1285	669, 653, 645, 637, 621, 613, 581	7
16	4369	2225, 2185, 2177, 2169, 2097	5

Section 2 proves that the cardinality of the set of zeros is at most the number of q-cyclotomy classes in $\mathbb{Z}_t$, namely, the cyclotomy bound.

In section 3, results on irreducible cyclic codes are used to show $|\mathcal{A}| = 2$ if t has the form $q^{2a} - q^a + 1$ and also gives the exact values for $\mathcal{A}$ in this case. We also get a lower bound on $|\mathcal{A}|$ when $q = 2$ using results from Wolfmann (2005). Exact values for $|\mathcal{A}|$ when t follows the quadratic residue conditions are also discussed. Lastly, we show that the cyclotomy bound given in section 2 is the best bound as it is reached infinitely often, assuming the Generalized Riemann Hypothesis.

2. Cyclotomy Bound

2.1 Construction of the Cyclotomy Bound

First we will define the following equivalence relation on $\mathbb{Z}_t$.

Definition *For $a, b \in \mathbb{Z}_t$ define $a \sim b$ iff $q^u a \equiv b \pmod{t}$ for some $u \in \mathbb{Z}$.*

Definition *Let t be relatively prime to q. The cyclotomy class of q (or q-cylcotomy coset) modulo t containing i is defined by*

$$C_i = \{(iq^j \pmod{t}) \in \mathbb{Z}_t \mid j = 0, 1, \ldots\}$$

which is the equivalence class that contains i in the above mentioned equivalence relation.

Let C denote the set of all equivalence classes. The following theorem explains that when the characteristic polynomial is irreducible, a suitable trace form can be used to represent the terms of the linear recurring sequence S.

Theorem 2. (Lidl & Niederreiter, 1994) *Let $s_0, s_1, \ldots$ be a kth-order homogeneous linear recurring sequence in $K = \mathbb{F}_q$ whose characteristic polynomial $f(x)$ is irreducible over K. Let α be a root of $f(x)$ in the extension field $F = \mathbb{F}_{q^k}$. Then there exists a uniquely determined $\theta \in F$ such that*

$$s_n = Tr_{F/K}(\theta\alpha^n) \qquad for\ n = 0, 1, \ldots$$

Theorem 3 below gives the upper bound for the cardinality of the set of zeros.

Theorem 3. *Consider the homogeneous linear recurring sequences over $\mathbb{F}_q$ based on an irreducible minimal polynomial of degree d and order m. Set $t = (q^d - 1)/m$. Then for the set of numbers of zeros $\mathcal{A}$, we have $| \mathcal{A} | \leq | C |$.*

Proof.

Let $f \in P(d, m)$. By Theorem 2, there exists a root of f, $\beta \in \mathbb{F}_{q^d}$ and $\theta \in \mathbb{F}_{q^d}^*$ such that the nth term of the sequence S is given by,

$$s_n(I, f) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\theta\beta^n), \quad for\ all\ \ n, \quad 1 \leq n \leq m.$$

Fix a primitive element $\alpha \in \mathbb{F}_{q^d}$. Then order of $\beta = m$ and hence $\beta = \alpha^{rt}$ where $t = (q^d - 1)/m$ and $(r, m) = 1$. Define

$$s_n(\theta, t) := Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\theta\alpha^{tn}).$$

Hence

$$s_n(I, f) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\theta\beta^n) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\theta\alpha^{rtn}) = s_n(\theta, rt).$$

Therefore,

$$\mathcal{A} = \{Z(S(\theta, rt)) \mid \theta \in \mathbb{F}_{q^d}^*, t = (q^d - 1)/m, (r, m) = 1\} \tag{2}$$

Lemma 1. First Reduction : *For $(r, m) = 1$, $Z(S(\theta, t)) = Z(S(\theta, rt))$.*

Proof. Since $(r, m) = 1$, there exists a u such that $ur \equiv 1 \pmod{m}$ and then $urt \equiv 1 \pmod{q^n - 1}$. Hence

$$s_k(\theta, t) = Tr_{K/F}(\theta\alpha^{tk}) = Tr_{K/F}(\theta\alpha^{kurt}) = s_{ku}(\theta, rt)$$

and $s_k(\theta, rt)$ is simply $s_k(\theta, t)$ in a new order. Therefore

$$Z(S(\theta, t)) = Z(S(\theta, rt)).$$

□

Now $\mathcal{A}$ in (2) can be given as follows:

$$\mathcal{A} = \{Z(S(\theta, t)) \mid \theta \in \mathbb{F}_{q^d}^*,\ t = (q^d - 1)/m\} \tag{3}$$

Define

$$r_n(a, t) := Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{a+tn}), \quad for\ some\ \ a \in \mathbb{N}.$$

Since $\theta \in \mathbb{F}_{q^d}^*$, let $\theta = \alpha^k$. Then

$$s_n(\theta, t) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\theta\alpha^{nt}) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{k+tn}) = r_n(k, t).$$

Hence $\mathcal{A}$ in (3) can be written as the following

$$\mathcal{A} = \{Z(R(k, t)) \mid t = (q^d - 1)/m,\ 0 \leq k \leq q^d - 1\} \tag{4}$$

where R denotes the sequence $r_1, r_2, \ldots$

Lemma 2. Second Reduction : *If $k_1 \equiv k_2 (mod\ \ t)$ then $Z(R(k_1, t)) = Z(R(k_2, t))$.*

Proof. If $k_2 = k_1 + tu$ for some $u \in \mathbb{Z}$, then

$$r_n(k_2, t) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{k_2+tn}) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{k_1+(n+u)t}) = r_{n+u}(k_1, t)$$

Hence $r_n(k_2, t)$ is a shifted version of $r_n(k_1, t)$. Therefore,

$$Z(R(k_1, t)) = Z(R(k_2, t)).$$

□

Using Lemma 2, $\mathcal{A}$ in (4) can be given as follows:

$$\mathcal{A} = \{Z(R(k,t)) \mid t = (q^d - 1)/m,\ 0 \le k < t\}$$

Therefore

$$\mid \mathcal{A} \mid \le t.$$

Lemma 3. Third Reduction : *Z(R(k,t)) = Z(R(qk,t)).*

Proof.

$$r_n(k,t) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{k+tn}) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}((\alpha^{k+tn})^q) = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha^{qk+qnt}) = r_{qn}(qk,t)$$

Hence

$$Z(R(k,t)) = Z(R(qk,t)).$$

Therefore

$$\mathcal{A} = \{Z(R(k,t)) \mid t = (q^d - 1)/m \ \ and \ \ C_k \in C\}.$$

Hence $\mid \mathcal{A} \mid \le \mid C \mid$.

2.2 Properties of Cyclotomy Classes

Here we discuss some properties of the cyclotomy classes where we will be able to find the exact value for the cyclotomy bound and give the exact upper bound for the cardinality of the set of zeros $\mid \mathcal{A} \mid$, under specific conditions. Let $ord_a(b)$ be the smallest positive integer c such that $a^c \equiv 1 \pmod a$. By the equivalence relation defined in section 2, $C_1 = \{1, q, q^2, \ldots, q^{k-1}\} \pmod t$ where $k = ord_t(q)$. Hence $\mid C_1 \mid = ord_t(q)$.

Proposition 1. *If t is a composite and l | t, then there exists $C_l \in C$.*

Proof. Let $l \in C_a$ for some $a \in \mathbb{Z}_t$. Then by the definition of C_a, $l \ge a$ and $l \equiv q^r a \pmod t$ for some $r \in \mathbb{Z}$. Since $l \mid t \Rightarrow l \mid q^r a$ and $t \mid q^d - 1 \Rightarrow (t,q) = 1$, hence $(l,q) = 1$. Therefore $l \mid a$ and hence $l \le a$. Hence $l = a$ and $C_l \in C$.

□

The following well known result and the corollaries give the exact values for the cyclotomy bound $\mid C \mid$ and hence the exact upper bound for the cardinality of the set of zeros $\mid \mathcal{A} \mid$.

Proposition 2. *Let $t \in \mathbb{N}$ and t and q are relatively prime. Then*

$$\mid C \mid = \sum_{d \mid t} \frac{\varphi(t/d)}{ord_{t/d}(q)}.$$

Corollary 1. *If t is a prime then* $\mid C \mid = \frac{t-1}{k} + 1$.

Corollary 2. *Let t be a prime power (say p^k) where p is an odd prime. If 2 is a primitive root of $\mathbb{Z}^*_{p^2}$, then* $\mid C \mid = k + 1$.

3. Coding Theory Approach

Weight distributions of irreducible cyclic codes were studied by Baumert and McEliece (1972), Baumert and Mykkeltveit (1973), Aubrey and Langevin (2005), Wolfmann (2005), Vega (2007), Aubrey and Langevin (2008) and Ding (2009). We will use these results to determine the exact occurrences of zeros in some cases, and determine the cardinality of the set of zeros of homogeneous linear recurring sequences based on irreducible minimal polynomials of fixed degree and order. First we set notations and review the basic facts as found on Lidl and Niederreiter (1994).

Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree d and order m. Let $S = \{s_n\}$ be a homogeneous linear recurring sequence over $\mathbb{F}_q$ based on f as its minimal polynomial. By Theorem 2, $s_n = Tr_{K/F}(\theta\alpha^n)$, where $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^d}$, $\alpha \in K$ is a root of f and $\theta \in K^*$. Define the vector

$$c(\theta, \alpha) = [Tr_{K/F}(\theta\alpha), Tr_{K/F}(\theta\alpha^2), \ldots, Tr_{K/F}(\theta\alpha^m)],$$

where the entries represent the terms of the sequence S within its least period m. Set

$$C(\alpha) = \{c(\theta, \alpha) : \theta \in K\}.$$

$C(\alpha)$ is then a cyclic code whose words represent the terms of each sequence S within its least period, based on $f(x)$. Thus $C(\alpha)$ has length m and dimension d. The generator polynomial of $C(\alpha)$ is the reciprocal of $(x^m - 1)/f(x)$, so that $C(\alpha)$ is in fact an irreducible cyclic code.

Note that the weight $wt(c(\theta, \alpha))$, the number of non zero entries of the code word $c(\theta, \alpha)$ is $m - Z(S)$. The reductions of Theorem 3 show that all sequences based on irreducible minimal polynomials of degree d and order m have the same number of zeros. Hence

$$number\ of\ non-zero\ weights\ of\ C(\alpha) =\mid \mathcal{A} \mid .$$

We say a code is a *N-weight* code if it has N non-zero weights and hence for this case, $N =\mid \mathcal{A} \mid$.

3.1 Lower Bounds for the Cardinality of the Set of Number of Zeros of Hhomogeneous Linear Recurring Sequences

Theorem 4. (Wolfmann, 2005) *Let C be an $[n, k]$ linear code over $\mathbb{F}_q$. If C is a 1-weight code with weight w and if the weight of the dual code is at least 2, then there exists $\lambda \in \mathbb{N}$ such that*

$$n = \lambda \frac{q^k - 1}{q - 1}, \quad w = \lambda q^{k-1}.$$

Corollary 3. *Let C be an irreducible cyclic 1-weight code with length m and dimension d. Set $t = (q^d - 1)/m$. Then t divides $q - 1$.*

Proof. We first check that the dual code $C^\perp$ does not have minimal weight one. Suppose it has a minimal weight of one. As $C^\perp$ is also cyclic, the existence of a codeword of weight 1 in $C^\perp$ implies that all vectors of weight 1 are in $C^\perp$ and hence $C^\perp = \mathbb{F}_q^m$. But then $C = \{0\}$, which is not a 1-weight code.

We can thus apply Theorem 4 to get $m = \lambda(q^d - 1)/(q - 1)$ for some λ. Hence $q - 1 = \lambda(q^d - 1)/m = \lambda t$.

□

Corollary 4. *For $q = 2$, $\mid \mathcal{A} \mid \geq 2$ unless the minimal polynomial is primitive.*

Proof. Let $f(x)$ be an irreducible polynomial of degree d and order m. Set $t = (2^d - 1)/m$. If $\mid \mathcal{A} \mid = 1$ then $C(\alpha)$, where α is a root of $f(x)$, is a 1-weight irreducible cyclic code. By Corollary 3, t divides $q - 1 = 1$ so that $t = 1$ and f is primitive.

□

3.2 Kasami-Welch approach

Theorem 5. (Wolfmann, 2005) *Let C be an irreducible cyclic code of length m over $\mathbb{F}_q$. Let $\mathbb{F}_{q^d}$ be the splitting field of $x^m - 1$ over $\mathbb{F}_q$. Let t be the integer such that $mt = q^d - 1$. If $d = 2e$ and if there exists a divisor r of e such that $q^r \equiv -1 \pmod t$, then C is a 2-weight code with weights*

$$w_1 = (q - 1)q^{e-1}\left(\frac{q^e + (t - 1)\epsilon}{t}\right) \qquad w_2 = (q - 1)q^{e-1}\left(\frac{q^e - \epsilon}{t}\right),$$

where ϵ is 1 or -1.

Theorem 6. *Let $q = 2$. Consider sequences based on an irreducible, non-primitive polynomial of degree d and order m. Set $t = (2^d - 1)/m$. Suppose t is prime and 2 is a primitive root modulo t. Then*

$$\mid \mathcal{A} \mid = 2 =\mid C \mid$$

where C is the set of 2-cylcotomic classes in $\mathbb{Z}_t$. In fact, d is even (say $d = 2e$) and $\mathcal{A}$ consists of

$$m - \frac{2^{e-1}(2^e + (t - 1)\epsilon)}{t} \quad and \quad m - \frac{2^{e-1}(2^e - \epsilon)}{t},$$

where ϵ is 1 or -1, determined by $2^e \equiv \epsilon \pmod t$.

Proof. C_1 is the subgroup of $\mathbb{Z}_t^*$ generated by 2, hence $C_1 = \mathbb{Z}_t^*$. So there are exactly two cyclotomy classes, represented by 0 and 1. We have $ord_t(2) = t - 1$ is even and $2^d \equiv 1 \pmod t$ so that $t - 1$ divides d. Write $d = 2e$. For $r = \frac{t-1}{2}$ we have $r \mid e$ and $2^r \equiv -1 \pmod t$. So by Theorem 5, $\mid \mathcal{A} \mid = 2$ and its values are as given.

□

Example 1. Let $q = 2$. Consider sequences based on an irreducible polynomials of degree 10 and order 93 ($f(x) = x^{10} + x^5 + x^4 + x^2 + 1$ is one such polynomial). Then $t = (2^{10} - 1)/93 = 11$. As 2 is a primitive root modulo 11, Theorem 6 gives $\mid \mathcal{A} \mid = 2$. In fact, using $e = 5$ and $\epsilon = -1$, we have $\mathcal{A} = \{45, 61\}$. This explains the result on line 4 in Table 1.

Assuming the Generalized Riemann Hypothesis (GRH), Hooley (1967) proved the Artin Conjecture and in particular, that there are infinitely many primes t such that 2 is a primitive root modulo t. Together with Theorem 6, we thus get the following corollary that proves the cyclotomy bound determined in section 2 is the best bound for $|\mathcal{A}|$.

Corollary 5. *Assume the GRH. For $q = 2$, the cyclotomy bound is achieved infinitely often.*

Theorem 7. (Kasami-Welch case) *Consider sequences based on an irreducible polynomial over $\mathbb{F}_q$ of degree d and order m. Set $t = (q^d - 1)/m$. If t has the form $q^{2a} - q^a + 1$ for some integer a ($a \geq 2$ if $q = 2$) then $d = 2e$ is even and $|\mathcal{A}| = 2$. In fact: $\mathcal{A}$ consists of*

$$m - (q-1)q^{e-1}\left(\frac{q^e + (t-1)\epsilon}{t}\right) \qquad m - (q-1)q^{e-1}\left(\frac{q^e - \epsilon}{t}\right),$$

where $\epsilon = \pm 1$.

Proof.

Let $k = ord_t(q)$. We **Claim** that $k = 6a$. The basic equation is:

$$q^{3a} + 1 = (q^a + 1)(q^{2a} - q^a + 1) = (q^a + 1)t. \tag{5}$$

Then $q^{6a} \equiv 1 \pmod{t}$ and so $k \mid 6a$. Thus k has the form $x, 2x, 3x$ or $6x$ for some divisor x of a. Note that if $k = x$ or $3x$ then $q^{3a} \equiv 1 \pmod{t}$ while (5) gives $q^{3a} \equiv -1 \pmod{t}$. Hence $k = 2x$ or $6x$.

Suppose k has the form $2x$. Then $q^{2a} \equiv 1 \pmod{t}$ and since $t = q^{2a} - q^a + 1$, we have $q^{2a} \equiv q^a - 1 \pmod{t}$. So t divides $q^a - 2$. If $q = 2$, we assume that $a \geq 2$ and hence $q^a - 2 \neq 0$. Therefore,

$$t = q^{2a} - q^a + 1 \leq q^a - 2 \Rightarrow q^{2a} \leq 2q^a - 3 < 2q^a \Rightarrow q^a < 2,$$

which is impossible.

Thus k has the form $6x$. Write $a = xy$. We have $(q^{3x})^2 \equiv 1 \pmod{t}$ and by (2), $(q^{3x})^y \equiv -1 \pmod{t}$. Then y must be odd and $q^{3x} \equiv -1 \pmod{t}$. Then

$$t = q^{2a} - q^a + 1 \leq q^{3x} + 1 \Rightarrow q^a < q^a(q^a - 1) \leq q^{3x}.$$

Hence $a = xy < 3x$ and $y < 3$. Suppose $y = 2$. Then

$$q^{2x}(q^{2x} - 1) \leq q^{3x} \Rightarrow q^{2x} - 1 \leq q^x \Rightarrow q^x \leq 1 + q^{-x} < 2,$$

which is impossible. So $y = 1$, $a = x$ and $k = 6a$, proving the **Claim**.

Fix an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d and order m. Let α be a root of f. We wish to apply Theorem 5 to $C(\alpha)$. Now $t \mid q^d - 1$ so that the order of q modulo t, namely $6a$, divides d. So d is even; write $d = 2e$. Set $r = 3a$. Then r divides e and by (2), $q^r \equiv -1 \pmod{t}$. Thus $C(\alpha)$ is a 2-weight code and $|\mathcal{A}| = 2$. We have $wt[c(\theta, \alpha)] = m - Z(S(\theta, \alpha))$ so Theorem 5 proves the elements of $|\mathcal{A}|$ are as stated.

□

Remark 1 When F is a finite field of even characteristic, the terms of the homogeneous linear recurring sequence take the form of the well known Kasami-Welch function $Tr_{K/F}(x^{2^{2a}-2^a+1})$.

Example 2. Let $q = 2$. Consider sequences based on an irreducible polynomial of degree 12 and order 315 ($f = x^{12} + x^4 + x^2 + x + 1$ is one such polynomial). Then $t = (2^{12} - 1)/315 = 13$ has the form $2^{2a} - 2^a + 1$ for $a = 2$. The number of zeros in such a sequence is thus

$$315 - 2^5\left(\frac{2^6 + 12\epsilon}{13}\right) \qquad \text{or} \quad 315 - 2^5\left(\frac{2^6 - \epsilon}{13}\right),$$

where $\epsilon = \pm 1$. To get integers we must take $\epsilon = -1$. We get $|\mathcal{A}| = \{155, 187\}$. This explains the values on line 12 in Table 1.

Theorem 8. *Consider sequences based on an irreducible polynomial over $\mathbb{F}_q$ of degree d and order m. Set $t = (q^d - 1)/m$. Suppose*

1. *t is a prime where* $t \equiv 1 \pmod 4$,
2. $ord_t(q) = \frac{1}{2}(t-1)$.

Then $d = 2e$ *is even and* $|\mathcal{A}| = 2$ *and* $\mathcal{A}$ *consists of*

$$m - (q-1)q^{e-1}\left(\frac{q^e + (t-1)\epsilon}{t}\right) \qquad m - (q-1)q^{e-1}\left(\frac{q^e - \epsilon}{t}\right),$$

where $\epsilon = \pm 1$.

Proof.

Fix an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d and order m. Let α be a root of f. We will apply Theorem 5 to $C(\alpha)$. Now $t \mid q^d - 1$ and hence $ord_t(q) = \frac{1}{2}(t-1)$ divides d. Since $t \equiv 1 \pmod 4$, $ord_t(q)$ is even and hence d is even;

$$d = \frac{1}{2}(t-1)k = 2e$$

where $e = \frac{1}{4}(t-1)k$. Set $r = \frac{1}{4}(t-1)$. Then $r \mid e$. By the definition of t, $t \mid (q^{\frac{q-1}{2}} - 1)$ and since $(t, \frac{q-1}{4} + 1) = 1$, $t \mid (q^{\frac{q-1}{4}} + 1)$. Therefore $q^r \equiv -1 \pmod t$.

Then $C(\alpha)$ is a 2-weight code by Theorem 5 and $|\mathcal{A}| = 2$. We have $wt[c(\theta, \alpha)] = m - Z(S(\theta, \alpha))$ and Theorem 5 gives the elements of $\mathcal{A}$ as stated above.

□

Example 3. Let $q = 2$. Consider sequences based on an irreducible polynomial of degree 16 and order 3855. Then $t = (2^{16} - 1)/3855 = 17$ and $ord_{17}(2) = \frac{1}{2}(17-1)$. A particular polynomial that can be considered is $f = x^{16} + x^{14} + x^{11} + x^3 + 1$. To get integers, take $\epsilon = 1$. Hence the values for $\mathcal{A}$ are:

$$3855 - 2^7\left(\frac{2^8 + 16}{17}\right) = 1807$$

$$3855 - 2^7\left(\frac{2^8 - 1}{17}\right) = 1935.$$

Hence $|\mathcal{A}| = 2$ which is explains another observation in Table 1.

So far we have only computed $\mathcal{A}$ using Theorem 5 which gives $|\mathcal{A}| = 2$. We will now discuss two other cases providing conditions for which $|\mathcal{A}| = 3$.

Theorem 9. *Let* $q = 2$. *Consider sequences based on an irreducible polynomial of degree d and order m. Set* $t = (2^d - 1)/m$. *Suppose*

1. *t is a prime not equal to 3,*
2. $t \equiv 3 \pmod 4$,
3. $ord_t(2) = \frac{1}{2}(t-1)$.

Then $|\mathcal{A}| = 3$.

Proof. We have $|C| = 3$ by Corollary 1 and hence $|\mathcal{A}| \leq 3$ by Theorem 3. $|\mathcal{A}| \neq 1$ by Corollary 4. Pick a particular polynomial f of degree d and order m. Let α be a root of f. The three conditions on t imply $C(\alpha)$ is not a 2-weight code by Proposition 2 in Aubrey and Langevin (2005). Hence $|\mathcal{A}| \neq 2$ and therefore $|\mathcal{A}| = 3$.

□

Example 4. Let $q = 2$ Consider sequences based on an irreducible polynomial of degree 9 and order 73 ($x^9 + x + 1$ is one such polynomial). Then $t = (2^9 - 1)/73 = 7$, which satisfies all three conditions of Theorem 9. Hence $|\mathcal{A}| = 3$. As given in the third observation of Table 1, a computer computation yields that in fact $\mathcal{A} = \{33, 37, 45\}$.

Theorem 10. *Consider sequences based on an irreducible polynomial of degree d and order m over* $\mathbb{F}_q$. *Set* $t = (q^d - 1)/m$. *Suppose*

1. *t is a prime not equal to 3,*
2. $t \equiv 3 \pmod 4$,
3. $ord_t(q) = \frac{1}{2}(t-1)$.

Then $|\mathcal{A}| = 2$ *or* 3.

Proof. By Corollary 1, $|C| = 3$. Hence $|\mathcal{A}| \leq 3$. Let f be a polynomial of degree d and order m and let α be a root of f. If the irreducible cyclic code $C(\alpha)$ of length m and dimension d is 1-weight, then by Corollary 3, $t \mid q-1$. Hence $ord_t(q) = \frac{t-1}{2} = 1 \Longrightarrow t = 3$ which contradicts the first condition above. Therefore $|\mathcal{A}| = 2$ or 3.

□

The following result can be given using Theorem 10 and Theorem 8 in Aubrey and Langevin (2008).

Corollary 3.4. *Suppose t satisfies the conditions given in Theorem 10. If* $t \equiv 7 \pmod 8$ *then* $|\mathcal{A}| = 3$.

4. Conclusion

The main purpose here was to give an accurate bound for the cardinality of the set of zeros of homogeneous linear recurring sequences over $\mathbb{F}_q$ based on irreducible minimal polynomials of given degree and order. This was achieved by the cyclotomy bound defined here and it was proved to be the best bound as it is reached in infinitely many cases. Besides determining a lower bound for sequences over $\mathbb{F}_2$, the exact number of zeros were given for Kasami Welch and the quadratic residue cases based on results on weights of irreducible cyclic codes. The work here was restricted to analyzing the conditions for the existence of $\mathcal{A} = 2$ and 3. This will be extended to an investigation of higher cardinality in the future.

Acknowledgments

The authors would like to thank the editor and the anonymous reviewers for their positive and constructive comments.

References

Aubrey, Y., & Langevin, P. (2005). *On the weights of binary irreducible cyclic codes*, 161-169. Workshop on Coding and Cryptography, Bergen, Norway.

Aubrey, Y., & Langevin, P. (2008). *On the semiprimitivity of cyclic codes*, 284–293. Symposium on Algebraic Geometry and its Applications, Tahiti.

Baumert, L. D., & McEliece, R. J. (1972). Weights of Irreducible Cyclic Codes. *Information and Control, 20.* https://doi.org/10.1016/S0019-9958(72)90354-3

Baumert, L. D., & Mykkeltveit, J. (1973) Weights Distributions of Some Irreducible Cyclic Codes *JPL Technical report,* 32-1526.

Ding, C. (2009). The weight distribution of some irreducible cyclic codes. *IEEE Transactions on Information Theory, 55*, 955-960.

Everest, G., van der Poorten, A., Shparlinski, I., & Ward, T. (2003). Recurrence Sequences. *Mathematical Surveys and Monographs, 104*, American Mathematical Society, Providence, RI.

Hooley, C. (1967). *On Artin's Conjecture*, 209 - 220. J. Reine Angew. Math. 225.

Kottegoda, Y. (2010). *The number of zeros in a linear recurrence sequence over a finite field* (Master's thesis, Southern Illinois University Carbondale, Illinois, United States).

Lidl, R., & Niederreiter, H. (1994). Introduction to finite fields and their applications *Cambridge University Press,* Cambridge. https://doi.org/10.1017/CBO9781139172769

Mullen, G. L., & Panario, D. (2013). *Handbook of Finite Fields* Chapman & Hall/CRC Press.

Vega, G. (2007). *Determining the number of one-weight cyclic codes when length and dimension are given*, 284 -293. Arithmetic of Finite Fields 4547, Lecture notes in Computer Science.

Wolfmann, J. (2005). Are 2-Weight Projective Cyclic Codes Irreducible? *IEEE Transactions on Information Theory, 51*, 733-737, https://doi.org/10.1109/TIT.2004.840882