Journal of Mathematics Research; Vol. 9, No. 3; June 2017
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Quadratic form Approach for the Number of Zeros of Homogeneous Linear Recurring Sequences over Finite Fields

Yasanthi Kottegoda[1]

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

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

Received: April 14, 2017 Accepted: May 3, 2017 Online Published: May 9, 2017

doi:10.5539/jmr.v9n3p8 URL: https://doi.org/10.5539/jmr.v9n3p8

Abstract

We consider homogeneous linear recurring sequences over a finite field $\mathbb{F}_q$, based on an irreducible characteristic polynomial of degree n and order m. Let $t = (q^n - 1)/m$. We use quadratic forms over finite fields to give the exact number of occurrences of zeros of the sequence within its least period when t has q-adic weight 2. Consequently we prove that the cardinality of the set of zeros for sequences from this category is equal to two.

Keywords: Linear recurring sequences, quadratic forms, finite fields.

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

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

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 rest of the sequence uniquely, are referred to as the initial values. Let $s_0, s_1, \ldots$ be a kth order homogeneous linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation in (1), where $a_j \in \mathbb{F}_q$ for $0 \leq j \leq k-1$. 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 the homogeneous linear recurring sequence $s_0, s_1, \ldots$ 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($m(x)$).*

Discussions on linear recurring sequences took place for many years with a substantial development in the area of examining zeros and determining effective bounds for the set of zeros over infinite fields (Everest, Poorten, Shparlinski & Ward, 2003). Linear recurring sequences over finite fields have appeared sporadically over the years in a variety of contexts in Cryptography, mainly in the area of linear shift registers where determining the exact number of zeros is of higher importance (Lidl & Niederreiter, 1994). Let S be a homogeneous linear recurring sequence over $\mathbb{F}_q$ and let $f(x) \in \mathbb{F}_q[x]$ be the irreducible minimal polynomial of S with degree n and order m and let $t = \frac{q^n-1}{m}$. Kottegoda and Fitzgerald (2017) provided an accurate bound for the number of zeros of S within its least period, also providing formulas for the exact number of zeros when t has the form $q^{2a} - q^a + 1$ where $a \in \mathbb{N}$. Here, we will give the exact number of zeros when $t = q^a + 1$ using applications in quadratic forms over finite fields.

In section 2, we will describe some known results on one-term trace forms over finite fields of even and odd characteristics by Klapper (1993, 1997) and include proofs for the simpler formulation of Klapper's results which were stated by Mullen and Panario (2013)7.2 without proofs.

In section 3, we give our main theorem by providing formulas for the exact number of occurrences of zeros of S within its least period for the case where $t = \frac{q^n-1}{m}$ takes the form $q^a + 1$ where $a \in \mathbb{N}$, using the quadratic form results from section 2. Hence we will also prove that the cardinality of the set of zeros in this case is 2.

2. Results on Quadratic Forms

Let $F = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$ where q is a prime power. Let $Q : K \to F$ be a quadratic form and $N(Q = u)$ be the number of solutions for $Q(x) = u$ in K. General information and the main definitions on quadratic forms can be obtained by Mullen and Panario (2013)7.2.

We now recall what is known about $N(Q = u)$ over finite fields of even and odd characteristic.

Proposition 1. (Klapper, 1993) *Every quadratic form Q of rank m in n variables over $\mathbb{F}_q$ for even q is equivalent to one of the following 3 standard types under a change of co-ordinates :*

Type I: $B_m(\overline{x})$;
Type II: $B_{m-1}(\overline{x}) + x_m^2$;
Type III: $B_{m-2}(\overline{x}) + bx_{m-1}^2 + x_{m-1}x_m + bx_m^2$;
For any $v \in \mathbb{F}_q$, let $\eta(v) = -1$ if $v \neq 0$ and $\eta(0) = q - 1$. The number of solutions to the equation $Q(\overline{x}) = v$ is :
*for **Type I**: $q^{n-1} + \eta(v)q^{n-\frac{m}{2}-1}$;*
*for **Type II**: q^{n-1};*
*for **Type III**: $q^{n-1} - \eta(v)q^{n-\frac{m}{2}-1}$;*

Proposition 2. (Klapper, 1997) *For any quadratic form Q of rank m in n variables over $\mathbb{F}_q$ for odd q is equivalent under a change of coordinates to precisely one of the following quadratic forms:*

Type I: $B_m(\overline{x})$;
Type II: $B_{m-1}(\overline{x}) + bx_m^2$;
Type III: $B_{m-2}(\overline{x}) + x_{m-1}^2 - ax_m^2$; *where $b \in \{1, a\}$ and $1 \neq a \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$.*
and the determinants of Q (i.e $det(Q)$) are as follows:
*for **Type I**: $det(Q) = (-1)^{\frac{m}{2}}$;*
*for **Type II**: $det(Q) = b(-1)^{\frac{m-1}{2}}$;*
*for **Type III**: $det(Q) = a(-1)^{\frac{m}{2}}$;*
Furthermore the number of solutions to the equation $Q(\overline{x}) = u$ is
$q^{n-1} + v(u)\eta((-1)^{\frac{m}{2}} det(Q))q^{n-\frac{m}{2}-1}$ *for Type I and Type III*
$q^{n-1} + \eta((-1)^{\frac{m-1}{2}} u\, det(Q))q^{n-\frac{m+1}{2}}$ *for Type II*
where $v(x) = \begin{cases} -1, & x \neq 0 \\ q-1, & x = 0 \end{cases}$ *and* $\eta(x) = \begin{cases} 1, & x \text{ is a square} \\ -1, & x \text{ is a not a square} \\ 0, & x = 0 \end{cases}$

The following formulation for $N(Q = 0)$ is much simpler to use for computations.

$$N(Q = 0) = \frac{1}{q}[q^n + (q - 1)\Lambda(Q)\sqrt{q^{n+r}}] \tag{2}$$

where $r = \dim \operatorname{rad}(Q)$ and $\Lambda(Q)$ is an invariant defined in terms of the discriminant (if q is odd) or the Arf invariant (if q is even). Let $v_2(x)$ denote the 2-adic valuation of x. Consider the trace form $Q(x) = Tr_{K/F}(\gamma x^{q^a+1})$. Set $d = (n, a)$.

Proposition 3. (Mullen & Panario, 2013) *For even q let $Q(x) = Tr_{K/F}(\gamma x^{q^a+1})$ and $\gamma \in K$.*

1. *If $v_2(n) < v_2(2a)$ then $(r, \Lambda(Q)) = (d, 0)$*

2. *If $v_2(n) = v_2(2a)$ then*

$$(r, \Lambda(Q)) = \begin{cases} (2d, +1), & \text{if } \gamma \text{ is a } (q^a + 1)th \text{ power} \\ (0, -1), & \text{if } \gamma \text{ is not a } (q^a + 1)th \text{ power.} \end{cases}$$

3. *If $v_2(n) > v_2(2a)$ then*

$$(r, \Lambda(Q)) = \begin{cases} (2d, -1), & \text{if } \gamma \text{ is a } (q^a + 1)th \text{ power} \\ (0, +1), & \text{if } \gamma \text{ is not a } (q^a + 1)th \text{ power.} \end{cases}$$

Proof. **Case 1:** $v_2(2a) > v_2(n)$

Since $v_2(a) \geq v_2(n)$, $v_2(d) = v_2(n)$. Hence if n is even then a is even resulting $\frac{n}{d}$ to be odd. If n is odd then $\frac{n}{d}$ is odd. Therefore by Theorem 4.1 (Klapper, 1993), $Q(x)$ is of Type II with rank $Q = n - d + 1$ where $r = 0$ and $\Lambda(Q) = 0$.

Case 2: $v_2(2a) = v_2(n)$

Here n is even and $v_2(a) < v_2(n)$. Hence $\frac{n}{d}$ is even. Since $v_2(2d) = 1 + v_2(a) = v_2(n)$, $\frac{n}{2d}$ is odd. Therefore by Theorem 4.1 (Klapper, 1993), $Q(x)$ is of Type III with rank n if γ is not a $q^a + 1$th power in K and $Q(x)$ is of Type I with rank $n - 2d$ if γ is not a $q^a + 1$th power in K. Hence r take the values 0 and $2d$ respectively and $\Lambda(Q)$ take the values -1 and 1 respectively.

Case 3: $v_2(2a) < v_2(n)$

Here n is even and $v_2(n) \geq 2$. If a is odd, then d is odd and hence both $\frac{n}{d}$ and $\frac{n}{2d}$ are even. If a is even, then d is even and $v_2(d) = v_2(a) < v_2(n)$. Hence both $\frac{n}{d}$ and $\frac{n}{2d}$ are even. Therefore by Theorem 4.1 (Klapper, 1993), $Q(x)$ is of Type I with rank n if γ is not a $q^a + 1$th power in K and $Q(x)$ is of Type III with rank $n - 2d$ if γ is a $q^a + 1$th power in K. Hence r take the values 0 and $2d$ respectively and $\Lambda(Q)$ take the values 1 and -1 respectively.

□

Proposition 4. (Mullen & Panario, 2013) *For odd q let $Q(x) = Tr_{K/F}(\gamma x^{q^a+1})$ and $\gamma \in K$. Let ω be a primitive element of K and write $\gamma = \omega^g$ for some $0 \leq g < q^n - 1$.*

1. *If $v_2(n) < v_2(2a)$ then $r = 0$.*

2. *If $v_2(n) = v_2(2a)$ then*

$$(r, \Lambda(Q)) = \begin{cases} (2d, +1), & \text{if } g \equiv \frac{1}{2}(q^d + 1) \pmod{q^d + 1} \\ (0, -1), & \text{if } g \not\equiv \frac{1}{2}(q^d + 1) \pmod{q^d + 1}. \end{cases}$$

3. *If $v_2(n) > v_2(2a)$ then*

$$(r, \Lambda(Q)) = \begin{cases} (2d, -1), & \text{if } g \equiv 0 \pmod{q^d + 1} \\ (0, +1), & \text{if } g \not\equiv 0 \pmod{q^d + 1}. \end{cases}$$

Proof. **Case 1:** $v_2(n) < v_2(2a)$

Here $v_2(n) = v_2(d)$ and hence $\frac{n}{d}$ is odd. Therefore by theorem 5.2,(Klapper, 1997) rank of $Q = n$ and hence $r = 0$.

Case 2: $v_2(n) = v_2(2a)$

Here $v_2(n) > v_2(a)$ and $v_2(d) = v_2(a)$ and hence $\frac{n}{d}$ is even. Since $v_2(2d) = 1 + v_2(d) = 1 + v_2(a) = v_2(n)$, then $\frac{n}{2d}$ is odd. Therefore by Theorem 5.2 (Klapper, 1997), rank of Q take $n - 2d$ when $g \equiv \frac{1}{2}(q^d + 1) \pmod{q^d + 1}$ and n when $g \not\equiv \frac{1}{2}(q^d + 1) \pmod{q^d + 1}$ giving r the values $2d$ and 0 respectively. By Theorem 5.3 (Klapper, 1997) Q is of type I in the first case and type III in the second providing $\Lambda(Q) = 1, -1$ respectively.

Case 3: $v_2(n) > v_2(2a)$

As in case 2, it can be proved that $\frac{n}{(n,a)}$ is even. Here $v_2((n, a)) = v_2(a)$ and hence $v_2(2(n, a)) = 1 + v_2((n, a)) < v_2(n)$. Therefore $\frac{n}{2(n,a)}$ is even. Hence by Theorem 5.2, 5.3 (Klapper, 1997), rank $(Q) = n - 2d$ and Q is of type III when $g \equiv 0 \pmod{q^d + 1}$ giving $r = 2d$ and $\Lambda(Q) = -1$. When $g \not\equiv \frac{1}{2}(q^d + 1) \pmod{q^d + 1}$, rank $(Q) = n$ and Q is of type I with $r = 0$ and $\Lambda(Q) = 1$.

□

3. Zeros of Homogeneous Linear Recurring Sequences

When the characteristic polynomial of a homogeneous linear recurring sequence is irreducible, each term of the sequence can be expressed in terms of a suitable trace function as given in the following theorem.

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

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

Let $P(n, m)$ be the set of all irreducible polynomials over $\mathbb{F}_q$ of degree n and order m. For $f \in P(n, m)$ and $I \in (\mathbb{F}_q^n)^* = (\mathbb{F}_q^n) \setminus \{0\}$, let $S(I, f) := \{s_k(I, f) | 1 \leq k \leq m\}$ be the first m terms (terms within the least period) of the homogeneous linear recurring sequence S over $\mathbb{F}_q$ with the characteristic polynomial f and the initial values given by the n - tuple I. Let β be a root of f in $\mathbb{F}_q^n$ and hence by Theorem 2, there exists a unique $\theta \in \mathbb{F}_{q^n}^*$ such that the k th term of the sequence is given by,

$$s_k(I, f) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\theta\beta^k) \;\text{ for all }\; k, \;\; 1 \leq k \leq m \tag{3}$$

The main result here is the following theorem that gives the exact values for the number of zeros of $S(I, f)$ when $t = \frac{q^n-1}{m}$ is of the form $q^a + 1$ for some $a \in \mathbb{N}$.

Theorem 3. *The number of zeros $Z(S(I, f))$ of the homogeneous linear recurring sequence $S(I, f)$ over $\mathbb{F}_q$ when t has the form $q^a + 1$ for some $a \in \mathbb{N}$ takes the values $Z((S(I, f))) = \frac{1}{t}(N(Q) - 1)$ for the following $N(Q)$:*
If q is even,

$$N(Q) = \begin{cases} \frac{1}{q}(q^n + (q-1)\sqrt{q^{n+2d}}) \;\; ; \nu_2(n) = \nu_2(2a) \;\; \textit{and} \;\; l \equiv 0 \pmod{q^a + 1} \\ \frac{1}{q}(q^n - (q-1)\sqrt{q^n}) \;\; ; \nu_2(n) = \nu_2(2a) \;\; \textit{and} \;\; l \not\equiv 0 \pmod{q^a + 1} \\ \frac{1}{q}(q^n - (q-1)\sqrt{q^{n+2d}}) \;\; ; \nu_2(n) > \nu_2(2a) \;\; \textit{and} \;\; l \equiv 0 \pmod{q^a + 1} \\ \frac{1}{q}(q^n + (q-1)\sqrt{q^n}) \;\; ; \nu_2(n) > \nu_2(2a) \;\; \textit{and} \;\; l \not\equiv 0 \pmod{q^a + 1} \end{cases}$$

and if q is odd,

$$N(Q) = \begin{cases} \frac{1}{q}(q^n + (q-1)\sqrt{q^{n+2d}}) \, ; \nu_2(n) = \nu_2(2a) \;\; \textit{and} \;\; l \equiv \frac{q^d+1}{2} \pmod{q^a + 1} \\ \frac{1}{q}(q^n - (q-1)\sqrt{q^n}) \, ; \nu_2(n) = \nu_2(2a) \;\; \textit{and} \;\; l \not\equiv \frac{q^d+1}{2} \pmod{q^a + 1} \\ \frac{1}{q}(q^n - (q-1)\sqrt{q^{n+2d}}) \, ; \nu_2(n) > \nu_2(2a) \;\; \textit{and} \;\; l \equiv 0 \pmod{q^a + 1} \\ \frac{1}{q}(q^n + (q-1)\sqrt{q^n}) \, ; \nu_2(n) > \nu_2(2a) \;\; \textit{and} \;\; l \not\equiv 0 \pmod{q^a + 1} \end{cases}$$

where $\theta = \alpha^l \in \mathbb{F}_{q^n}^*$ for a fixed primitive element $\alpha \in \mathbb{F}_{q^n}^*$ and $d = (n, a)$.

Proof. Let $F = \mathbb{F}_q$ and $K = \mathbb{F}_q^n$ and let $f \in P(n, m)$. Fix a primitive element $\alpha \in K$. Then the order of β in equation (3) is m and hence $\beta = \alpha^{rt}$ where $t = (q^n - 1)/m$ and $(r, m) = 1$. Hence equation (3) above can be expressed as

$$s_k(I, f) = \mathrm{Tr}_{K/F}(\theta\alpha^{rtk}) \tag{4}$$

Define

$$s_k(\theta, t) := \mathrm{Tr}_{K/F}(\theta\alpha^{tk})$$

to be the kth term of the homogeneous linear recurring sequence $S(\theta, t)$ over F.

$$\begin{aligned} S(I, f) &= \{\mathrm{Tr}_{K/F}(\theta\beta^k) \mid 1 \leq k \leq m\} \\ &= \{\mathrm{Tr}_{K/F}(\theta\alpha^{rtk}) \mid t = \frac{q^n - 1}{m}, 1 \leq k \leq m, (r, m) = 1\} \\ &= \{s_k(\theta, rt) \mid t = \frac{q^n - 1}{m}, 1 \leq k \leq m, (r, m) = 1\} \\ &= S(\theta, rt) \;\text{ where }\; (r, m) = 1. \end{aligned}$$

Now define $Q : K \to F$ by

$$Q(x) = Tr_{K/F}(\theta x^{q^a+1}).$$

This is known as a trace form. Since α is a primitive element of $K, \beta = \alpha^m$ for any $\beta \in K^*$. Then

$$Q(\beta) = Q(\alpha^m) = Tr_{K/F}(\theta(\alpha^m)^{q^a+1}) = Tr_{K/F}(\theta(\alpha^{q^a+1})^m) = s_m(\theta, t)$$

where $t = q^a + 1$. Hence $Q(\beta)$ gives the mth term of the homogeneous linear recurring sequence $S(\theta, t)$. Let N(Q) denote the number of zeros of Q in K. Then $N(Q) = 1 + tZ(S(\theta, t))$, where the extra 1 comes from including the solution $x = 0$. By Lemma 1 (Kottegoda & Fitzgerald, 2017), $N(Q) = 1 + tZ(S(\theta, rt)) = 1 + tZ(S(I, f))$.

Now we will claim that $ord_t(q) = 2a$. If $ord_t(q) = b$ then $q^b \equiv 1 \pmod{t}$. Considering the form of t (which is $q^a + 1$), $q^{2a} \equiv 1 \pmod{t}$ and hence $t \mid q^{2a} - q^b$ which implies $t \mid q^{2a-b} - 1$. If $2a - b > 0$ then by the definition of $ord_t(q)$, $2a - b > b$ which implies $a > b$ contradicting the fact that $t \mid q^b - 1$. Hence the claim is proved.

Now Q is the trace form associated with a sequence $S(\theta, t)$. $q^n \equiv 1 \pmod{t}$ and by the claim above, $2a \mid n$. Hence $v_2(n) \geq v_2(a)$ and we are in the cases 2 and 3 in Propositions 3 and 4 above that give the number of solutions for $Q(x) = 0$. Hence the result is obtained.

□

As q, n and a are fixed, depending on θ there are only two possible values of $(r, \Lambda(Q))$ by Propositions 3 and 4. Therefore by Theorem 3, there are only two possible values for N(Q) proving the following corollary.

Corollary 1. *The cardinality of the set of zeros of homogeneous linear recurring sequences $S(I, f)$ over $\mathbb{F}_q$ defined above where $t = \frac{q^n-1}{m}$ with a q-adic weight 2 is equal to 2.*

Example 1. Consider the set of all homogeneous linear recurring sequences over $\mathbb{F}_2$, based on irreducible minimal polynomials of degree 8 and order 85. Here $n = 8$, $m = 85$ and $q = 2$ and $t = \frac{2^8-1}{85} = 3 = 2^1 + 1$ where $a = 1$. Observations obtained by a MAPLE program in (Kottegoda, 2010, Appendix I-VIII) explains that there are 2040 such sequences (which are based on the 8 irreducible polynomials of degree 8 and order 85) and the number of zeros within each of their least periods are either 37 or 45. We will apply Theorem 3 and justify these observations. Here $d = (n, a) = 1$ and $v_2(2) = 1$ and $v_2(8) = 3$ and hence $v_2(2a) < v_2(n)$. Therefore by Theorem 3, $N(Q)$ takes the values

$$\frac{1}{q}[q^8 - (q-1)\sqrt{q^{10}}] \text{ and } \frac{1}{q}[q^8 + (q-1)\sqrt{q^8}].$$

Therefore when $q = 2$, $N(Q) = 112$ and 136 and since $N(Q) = 1 + tZ(S)$, we get $Z(S) = \{37, 45\}$.

The next example considers the set of all homogeneous linear recurring sequences over $\mathbb{F}_2$ based on degree 16 and order 3855. There are 8388480 such sequences and computing the zeros via a computer program is a tedious task. A simple computation with the use of Theorem 3 gives the pair of exact values for the number of zeros for this case confirming the 21st observation given in Table 1 (Kottegoda & Fitzgerald, 2017).

Example 2.

Here $n = 16$, $m = 3855$, $q = 2$ and hence $t = \frac{2^{16}-1}{3855} = 17 = 2^4 + 1$ where $a = 4$. This results $d = (n, a) = 4$ and $v_2(2a) < v_2(n)$. Therefore by Theorem 7, $N(Q)$ takes the values

$$\frac{1}{q}[q^{16} - (q-1)\sqrt{q^{24}}] \text{ and } \frac{1}{q}[q^{16} + (q-1)\sqrt{q^{16}}].$$

Therefore when $q = 2$, $N(Q) = 30720$ and 32896 and since $N(Q) = 1 + tZ(S)$, we get $Z(S) = \{1807, 1935\}$.

4. Conclusion

Considering homogeneous linear recurring sequences over $\mathbb{F}_q$ based on irreducible minimal polynomials of given degree (n) and order (m), the main goal here was to examine the number of zeros within its least period when $t = \frac{q^n-1}{m}$ has a q-adic weight 2. This was achieved by Theorem 3 here where the exact number of occurrences of zeros were determined using applications of quadratic forms over finite fields and hence it was also proved that the cardinality of the set of zeros in this case is 2.

Acknowledgments

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

References

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

Klapper, A. (1993) *Cross-Correlations of Geometric Sequences in Characteristic Two* (pp. 347-377) Designs, Codes and Cryptography 3. https://pdfs.semanticscholar.org/e51c/37eb1682ee7e6d491ba90fa9b88fad452210.pdf

Klapper, A. (1997) *Cross-Correlations of Quadratic Form Sequences in Odd Characteristic* (pp. 289-305) Designs, Codes and Cryptography 11. https://pdfs.semanticscholar.org/4b78/5459ce63e82c86cd2467f44b15cd1bee90f0.pdf

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).

Retrieved from http://opensiuc.lib.siu.edu/cgi/viewcontent.cgi?article=1019&context=gs_rp

Kottegoda, Y., Fitzgerald, R. (2017) *The Cardinality of the Set of Zeros of Homogeneous Linear Recurring Sequences over Finite Fields* (pp. 56-64) Journal of Mathematics Research 9, No. 2. http://www.ccsenet.org/journal/index.php/jmr/article/view/66368/36348 https://doi.org/10.5539/jmr.v9n2p56

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.

Copyrights