Walsh Transforms of Some Quadratic Trace Forms with One and Two terms for Even Degree Extension and Related Artin-Schreier Curves

Sankhadip Roy

***Abstract*—In this paper, we present the Walsh transform $f^W : \mathbb{F}_{2^n} \to \mathbb{Z}$ of some quadratic trace forms $f(x) = Tr(\sum_{i=0}^{m} a_i x^{2^i+1})$ over finite fields of characteristic two where the degree of extension n is even. In this article, we consider only trace forms with one or two terms where a_is are coming from base field $\mathbb{F}_2$. We use the Walsh coefficient $f^W(0)$ to investigate the number of rational points on Artin-Schreier curves over $\mathbb{F}_{2^n}$ of the form $\mathcal{X} : y^2 + y = \sum_{i=0}^{m} a_i x^{2^i+1}$. Using these results we also derive some maximal Artin-Scheier curves.**

***Index Terms*—Finite Fields, Quadratic Forms, Walsh transform, Artin-Schreier curves.**

I. Introduction

LET $K = \mathbb{F}_{2^n}$ be the finite field with 2^n elements. Let Tr denote the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$. For a boolean function $f : K \to \mathbb{F}_2$, the Walsh transform of f is the function $f^W : K \to \mathbb{Z}$ defined by

$$f^W(a) = \sum_{x \in K} (-1)^{f(x)+Tr(ax)}.$$

The Walsh spectrum of f is the set $\{f^W(a) : a \in K\}$. The famous examples of functions whose Walsh spectrum is three valued are the Gold functions [8] $f(x) = Tr(x^{2^a+1})$ where $\gcd(a, n) = 1$ and n is odd and the spectrum is $\{0, \pm 2^{\frac{n+1}{2}}\}$. Another important set of functions are the Kasami-Welch functions $f(x) = Tr(x^{4^a - 2^a + 1})$, which have the same transform values under the same hypotheses. Later Lahtonen et al.[17] considered more general form of Kasami-Welch functions, $f(x) = Tr(x^d), d = \frac{2^{ta}+1}{2^a+1}$ and calculated $f^W(1)$ under certain conditions. In his paper, Fitzgerald [6] showed some important results for the trace forms with two terms over characteristic two which explicitly give the two basic invariants of quadratic forms namely $\dim \mathrm{rad}(Q)$ and $\Lambda(Q)$. In this article, we have used some of the techniques introduced in [9] and [21] to find the Walsh transforms of some quadratic trace forms. Cusick and Dobbertin[9] were actually confirming two cojectures of Niho. Besides, one can check [3] for explicit evaluation of Walsh transforms of Gold type functions.

In section 2 we mention the preliminary definitions and symbols used throughout this paper.

In section 3 we introduce some new results for quadratic trace forms with one or two terms. But we stick to the case of n, degree of extension to be even.

Manuscript received March 29, 2021; revised October 17, 2021.

Dr. Sankhadip Roy is an Associate Professor of Mathematics in the Department of Basic Science and Humanities, University of Engineering and Management, Kolkata 700160, India ; email: sankhadiproy@gmail.com.

Algebraic curves over finite fields have various applications in coding theory, cryptography, quasi-random numbers and related areas. For references see [13], [14], [15], [16]. For these applications it is important to know the number of rational points of the curve. In section 4 we investigate the the application of Walsh transform of quadratic functions to obtain the number of rational points on Artin-Schreier curves over $\mathbb{F}_{2^n}$ of the form $\mathcal{X} : y^2 + y = \sum_{i=0}^{m} a_i x^{2^i+1}$. Van der Geer and Van der Vlugt [18] used p-linearlized polynomials to find new maximal Artin-Schreier curves. Later Wilfred and Anbar[19], [20] did a thorough study of the Artin-Schreier curves and described the number of rational points using Walsh transform $f^W(0)$ of quadratic trace forms. In this regard one can also check Bartoli et al.[2]. But most of their works are for $\mathbb{F}_{p^n}$ for p odd. In this section we only consider the case $p = 2$ and use the theorems from section 3 to describe the number of rational points of $\mathcal{X}$ in terms of Walsh coefficients $Q^W(0)$ of the quadratic trace forms $Q(x) = Tr(\sum_{i=0}^{m} a_i x^{2^i+1})$.

II. Preliminaries

Let $F = \mathbb{F}_2, K = \mathbb{F}_{2^n}$ and

$$R(x) = \sum_{i=0}^{m} a_i x^{2^i},$$

where $a_i \in \{0, 1\}$. We consider the trace forms which are the quadratic forms $Q_R^K : K \to F$ given by $Q_R^K(x) = Tr(xR(x))$. These types of trace forms have appeared in many literature and they have been widely used to compute weight enumerators of certain binary codes [1], [4], to construct curves with many rational points and associated trace codes [7] and to construct binary sequences with optimal correlations [10], [11]. In each of these applications we need the number of solutions (in K) to $Q_R^K(x) = 0$, denoted by $N(Q_R^K)$. It has been shown [12, 6.26,6.32], for the different type of quadratic forms:

$$N(Q_R^K) = \frac{1}{2}(2^n + \Lambda(Q_R^K)\sqrt{2^{n+r(Q_R^K)}}),$$

where $r(Q_R^K) = \dim \mathrm{rad}(Q_R^K)$ and

$$\Lambda(Q_R^K) = \begin{cases} 0, & \text{if } Q_R^K \simeq z^2 + \sum_{i=1}^{\nu} x_i y_i \\ 1, & \text{if } Q_R^K \simeq \sum_{i=1}^{\nu} x_i y_i \\ -1, & \text{if } Q_R^K \simeq x_1^2 + y_1^2 + \sum_{i=1}^{\nu} x_i y_i \end{cases}$$

Here $\mathrm{rad}(Q_R^K)$ denotes the radical of the bilinear form $B(x, z)$ of the trace form $Q(x)$ which is defined by

$$B(x, z) = Q(x) + Q(z) + Q(x + z) \text{ for } x, z \in \mathbb{F}_{2^k}.$$

Also $v_p(n)$ denotes the highest power of p dividing n and $\chi(x) = (-1)^{Tr(x)}$.

III. Walsh spectrum of some quadratic forms

The first result we introduce in this section is for the Walsh transform of trace forms with one term where n, the degree of extension is even but $\frac{n}{2}$ is odd.
We define $Tr_L(x) = \sum_{i=0}^{m-1} x^{2^i}$ which will be used in this section. We will also use the fact that for $x, y \in K$, $Tr(x^{2^i} y) = Tr(xy^{2^{-i}})$.

Theorem 1: Let $E = \mathbb{F}_{2^n}, n = 2m, L = \mathbb{F}_{2^m}$, m be odd and $f(x) = Tr(x^{2^k+1})$. Then

$$\begin{aligned} f^W(\alpha) &= \sum_{x \in E} \chi(x^{2^k+1} + \alpha x) \\ &= \begin{cases} 2^m \sum_{\mu \in M} \chi(\mu z_0), & \text{when k is odd} \\ 2^m \sum_{\mu \in M} \chi(\mu^{2^k+1} + \mu z_0), & \text{when k is even,} \end{cases} \end{aligned}$$

where $M = \{\mu \in L | \mu^{2^k} + \mu^{2^{-k}} + z_1 = 0\}$, $GF(4) = \{0, 1, \beta, \gamma\} \subset E = L[\beta]$ and $\alpha = z_0 + \beta z_1 \in E$ for $z_0, z_1 \in L$.
Proof: We have $\mathbb{F}_{2^2} \subset E$. We consider $\mathbb{F}_{2^2} = \{0, 1, \beta, \gamma\}$, where $\beta + \gamma = 1, \beta^2 = \gamma, \gamma^2 = \beta$. Note that $E = L[\beta]$, as m is odd. Further,

$$\beta^{2^i} = \begin{cases} \beta, & \text{when } i \text{ is even} \\ \gamma, & \text{when } i \text{ is odd.} \end{cases}$$

Also $Tr(\lambda + \mu\beta) = Tr(\lambda + \mu\gamma) = Tr_L(\mu)$ for $\lambda, \mu \in L$. Now for $x = \lambda + \mu\beta$,

$$\begin{aligned} f(x) &= Tr(x^{2^k+1}) \\ &= Tr((\lambda + \mu\beta)^{2^k+1}) \\ &= Tr(\lambda^{2^k+1} + \lambda\mu^{2^k}\beta^{2^k} + \lambda^{2^k}\mu\beta + \mu^{2^k+1}\beta^{2^k+1}). \end{aligned}$$

So when k is even

$$\begin{aligned} f(x) &= Tr(\lambda^{2^k+1} + \mu^{2^k}\lambda\beta + \mu\lambda^{2^k}\beta + \mu^{2^k+1}\gamma) \\ &= Tr_L(\mu^{2^k}\lambda + \mu\lambda^{2^k} + \mu^{2^k+1}). \end{aligned}$$

For $\alpha = z_0 + z_1\beta$,

$$f^W(\alpha) = \sum_{\mu, \lambda \in L} \chi(\mu^{2^k}\lambda + \mu\lambda^{2^k} + \mu^{2^k+1} + \lambda z_1 + \mu z_0 + \mu z_1)$$

as

$$\begin{aligned} Tr(\alpha x) &= Tr((z_0 + z_1\beta)(\lambda + \mu\beta)) \\ &= Tr(z_0\lambda + \lambda z_1\beta + z_0\mu\beta + z_1\mu\gamma) \\ &= Tr_L(\lambda z_1 + \mu z_0 + \mu z_1). \end{aligned}$$

So

$$\begin{aligned} f^W(\alpha) &= \sum_{\mu, \lambda \in L} \chi(\mu^{2^k}\lambda + \mu^{2^{-k}}\lambda + \mu^{2^k+1} \\ &\quad + \lambda z_1 + \mu z_0 + \mu z_1) \\ &= \sum_{\mu \in L} \chi(\mu^{2^k+1} + \mu z_0 + \mu z_1) \sum_{\lambda \in L} \chi(\lambda(\mu^{2^k} \\ &\quad + \mu^{2^{-k}} + z_1)) \\ &= 2^m \sum_{\mu \in M} \chi(\mu^{2^k+1} + \mu z_0 + \mu z_1), \end{aligned}$$

where $M = \{\mu \in L | \mu^{2^k} + \mu^{2^{-k}} + z_1 = 0\}$.
For k odd,

$$\begin{aligned} f(x) &= Tr(\lambda^{2^k+1} + \mu^{2^k}\lambda\gamma + \mu\lambda^{2^k}\beta + \mu^{2^k+1}) \\ &= Tr_L(\mu^{2^k}\lambda + \mu\lambda^{2^k}). \end{aligned}$$

So

$$\begin{aligned} f^W(\alpha) &= \sum_{\mu, \lambda \in L} \chi(\mu\lambda^{2^k} + \mu^{2^k}\lambda + \lambda z_1 + \mu z_0 + \mu z_1) \\ &= \sum_{\mu \in L} \chi(\mu z_0 + \mu z_1) \sum_{\lambda \in L} \chi(\lambda(\mu^{2^k} + \mu^{2^{-k}} + z_1) \\ &= 2^m \sum_{\mu \in M} \chi(\mu z_0 + \mu z_1), \end{aligned}$$

For $\mu \in M$ we have $\mu^{2^k} + \mu^{2^{-k}} + z_1 = 0$ which implies $Tr_L(\mu z_1) = 0$.
Hence, for k even

$$\begin{aligned} f^W(\alpha) &= 2^m \sum_{\mu \in M} \chi(\mu^{2^k+1} + \mu z_0 + \mu^{2^k+1} + \mu^{2^{-k}+1}) \\ &= 2^m \sum_{\mu \in M} \chi(\mu^{2^k+1} + \mu z_0) \end{aligned}$$

and for k odd $f^W(\alpha) = 2^m \sum_{\mu \in M} \chi(\mu z_0)$. □

Corollary 1: For Theorem 1, if $\gcd(m, k) = 1$, then Walsh spectrum is $\{0, \pm 2^{m+1}\}$.
Proof: For $\gcd(m, k) = 1$, $\mu^{2^k} + \mu^{2^{-k}} + z_1 = 0$ has solution in L iff $Tr_L(z_1) = 0$. In that case it has two solutions $\{\mu, \mu + 1\}$. So $|M| = 0$ or 2. Therefore, $f^W(a) = 0$ or $\pm\, 2^{m+1}$. □

In the next theorem we will consider trace forms with two terms like $f(x) = Tr(x^{2^a+1} + x^{2^b+1})$. Similar result can be found in [21] but for odd n with restrictions $0 \leq a < b$ and $\gcd(b - a, n) = \gcd(b + a, n) = 1$.

Theorem 2: Let $E = \mathbb{F}_{2^n}, n = 2m, L = \mathbb{F}_{2^m}$, m be odd and $f(x) = Tr(x^{2^a+1} + x^{2^b+1})$. Then
$f^W(\alpha) = \sum_{x \in E} \chi(x^{2^a+1} + x^{2^b+1} + \alpha x)$

$$= \begin{cases} 2^m \sum_{\mu \in M} \chi(\mu^{2^a+1} + \mu^{2^b+1} + \mu z_0), & \text{if } a, b \text{ even} \\ 2^m \sum_{\mu \in M} \chi(\mu z_0), & \text{if } a, b \text{ odd} \\ 2^m \sum_{\mu \in M} \chi(\mu^{2^a+1} + \mu z_0), & \text{if } a \text{ even}, b \text{ odd} \\ 2^m \sum_{\mu \in M} \chi(\mu^{2^b+1} + \mu z_0), & \text{if } a \text{ odd }, b \text{ even} \end{cases}$$

where $M = \{\mu \in L | \mu^{2^a} + \mu^{2^{-a}} + \mu^{2^b} + \mu^{2^{-b}} + z_1 = 0\}$,$GF(4) = \{0, 1, \beta, \gamma\} \subset E = L[\beta]$ and $\alpha = z_0 + \beta z_1 \in E$ for $z_0, z_1 \in L$.
Proof: Using the same arguments as in Theorem 1, we have

$$Tr(\lambda + \mu\beta) = Tr(\lambda + \mu\gamma) = Tr_L(\mu) \text{ for } \lambda, \mu \in L.$$

Case 1: a, b even. For $x = \lambda + \mu\beta$ and $\alpha = z_0 + z_1\beta$,

$$\begin{aligned} f(x) &= Tr((\lambda + \mu\beta)^{2^a+1} + (\lambda + \mu\beta)^{2^b+1}) \\ &= Tr_L(\mu^{2^a+1} + \mu^{2^a}\lambda + \mu\lambda^{2^a} + \mu^{2^b}\lambda \\ &\quad + \mu\lambda^{2^b} + \mu^{2^b+1}) \end{aligned}$$

and $Tr_L(\alpha x) = Tr_L(\lambda z_1 + \mu z_0 + \mu z_1)$. Therefore,

$$\begin{aligned} f^W(\alpha) &= \sum_{\mu,\lambda\in L} \chi(\mu^{2^a+1} + \mu^{2^a}\lambda + \mu^{2^{-a}}\lambda \\ &\quad +\mu^{2^b+1} + \mu^{2^b}\lambda + \mu^{2^{-b}}\lambda \\ &\quad +\lambda z_1 + \mu z_0 + \mu z_1) \\ &= \sum_{\mu\in L} \chi(\mu^{2^a+1} + \mu^{2^b+1} + \mu z_0 + \mu z_1)\cdot \\ &\quad \sum_{\lambda\in L} \chi(\lambda(\mu^{2^a} + \mu^{2^{-a}} + \mu^{2^b} + \mu^{2^{-b}} + z_1)) \\ &= 2^m \sum_{\mu\in M} \chi(\mu^{2^a+1} + \mu^{2^b+1} + \mu z_0 + \mu z_1) \end{aligned}$$

where $M = \{\mu \in L | \mu^{2^a} + \mu^{2^{-a}} + \mu^{2^b} + \mu^{2^{-b}} + z_1 = 0\}$. Now $\mu^{2^a} + \mu^{2^{-a}} + \mu^{2^b} + \mu^{2^{-b}} + z_1 = 0$ implies $Tr_L(\mu z_1) = 0$. Hence $f^W(\alpha) = 2^m \sum_{\mu\in M} \chi(\mu^{2^a+1} + \mu^{2^b+1} + \mu z_0)$.

Case 2: a, b odd.

$$\begin{aligned} f^W(\alpha) &= \sum_{\mu,\lambda\in L} \chi(\mu\lambda^{2^a} + \mu^{2^a}\lambda + \mu\lambda^{2^b} + \mu^{2^b}\lambda + \lambda z_1 \\ &\quad +\mu z_0 + \mu z_1) \\ &= \sum_{\mu\in L} \chi(\mu z_0 + \mu z_1) \sum_{\lambda\in L} \chi(\lambda(\mu^{2^a} + \mu^{2^{-a}} \\ &\quad +\lambda(\mu^{2^b} + \mu^{2^{-b}} \\ &\quad\quad +z_1)) \\ &= 2^m \sum_{\mu\in M} \chi(\mu z_0) \end{aligned}$$

Case 3: a even, b odd.

$$\begin{aligned} f^W(\alpha) &= \sum_{\mu,\lambda\in L} \chi(\mu^{2^a}\lambda + \mu\lambda^{2^a} + \mu^{2^a+1} + \mu\lambda^{2^b} + \mu^{2^b}\lambda \\ &\quad +\lambda z_1 + \mu z_0 + \mu z_1) \\ &= \sum_{\mu\in L} \chi(\mu^{2^a+1} + \mu z_1 + \mu z_0) \sum_{\lambda\in L} \chi(\lambda(\mu^{2^a} + \mu^{2^{-a}} \\ &\quad +\lambda(\mu^{2^b} + \mu^{2^{-b}} \\ &\quad\quad +z_1)) \\ &= 2^m \sum_{\mu\in M} \chi(\mu^{2^a+1} + \mu z_0) \end{aligned}$$

Case 4: a odd, b even. Same as Case 3. □

We can get the following result of [21] as a corollary from the previous theorem.

Corollary 2: For Theorem 2, if $\gcd(b-a, m) = 1 = \gcd(b+a, m)$, then the Walsh spectrum is $\{0, \pm 2^{m+1}\}$.

Proof: when $\gcd(b-a, m) = \gcd(b+a, m) = 1$, we can show that $x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}} + z_1 = 0$ has solution in L iff $Tr_L(z_1) = 0$ and in that case it has two solutions. Hence $f^W(\alpha) = 0$ or 2^{m+1}. □

Using the above theorem and Theorem 1.5 from Fitzgerald's [6], we can find the size of the set M as follows:

Proposition 1: Having the same conditions like Theorem 2 along with the condition $0 \le a < b$, we can describe the size of the set M as $|M| = 0$ or $2^{\gcd(b-a,m)+\gcd(b+a,m)-\gcd(e,m)}$ where $e = \gcd(b-a, b+a)$.

Proof: Consider $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\phi(x) = x^{2^{2b}} + x^{2^{b+a}} + x^{2^{b-a}} + x$.

$v_2(m) = 0 \le \max\{v_2(b-a), v_2(b+a)\}$. From [6, Theorem 1.5], we see $|Ker\phi| = 2^{\gcd(b-a,m)+\gcd(b+a,m)-\gcd(e,m)}$. Hence $|M| = 0$ or $2^{\gcd(b-a,m)+\gcd(b+a,m)-\gcd(e,m)}$ where $e = \gcd(b-a, b+a)$.

□

Lahtonen et al. [17] discussed the Walsh spectrum of $f(x) = Tr(x^{2^a+1})$ over $\mathbb{F}_{2^k}$ for odd k and $\gcd(a, k) = 1$ and described $f^W(\alpha)$ in terms of $f^W(1)$. In the next theorem we determine $f^W(\alpha)$ for k even and $\gcd(k, a) = 1$.

Theorem 3: Let $K = \mathbb{F}_{2^k}$, k be even and $\gcd(a, k) = 1$, $f(x) = Tr(x^{2^a+1})$. Then for $b \in K$,

$$f^W(b) = \begin{cases} 0, & \text{if } Tr(b) = 0 \text{ and } \\ & b \in Im(L) \\ \chi(\beta^{2^a+1} + \beta^{2^a}) f^W(1), & \text{if } Tr(b) = 0 \text{ and } \\ & b \in 1 + Im(L) \\ \chi(\beta^{2^{-a}} + \alpha\beta) f^W(\alpha) & \\ \text{ or } \chi(\beta^{2^{-a}} + \alpha^2\beta) f^W(\alpha^2), & \text{if } Tr(b) = 1 \end{cases}$$

where $\alpha \in K$ such that $\alpha^2 + \alpha + 1 = 0$ with $Tr(\alpha) = 1$, $L(x) = x^{2^a} + x^{2^{-a}}$ and $\beta \in K$ satisfying $L(\beta) = b$ or $1 + b$ or $\alpha + b$ or $\alpha^2 + b$ depending on the cases.

Proof: Consider β an element of K, which will be fixed later.

$$\begin{aligned} f^W(b) &= \sum_{x\in K} \chi(x^{2^a+1} + bx) \\ &= \sum_{x\in K} \chi((x+\beta)^{2^a+1} + b(x+\beta)) \\ &= \sum_{x\in K} \chi(x^{2^a+1} + \beta^{2^a+1} + x^{2^a}\beta + \beta^{2^a}x \\ &\quad +bx + b\beta) \\ &= \sum_{x\in K} \chi(x^{2^a+1} + \beta^{2^a+1} + x\beta^{2^{-a}} + \beta^{2^a}x \\ &\quad +bx + b\beta) \\ &= \chi(\beta^{2^a+1} + b\beta) \sum_{x\in K} \chi(x^{2^a+1} + x(L(\beta) + b)) \end{aligned}$$

where $L(\beta) = \beta^{2^a} + \beta^{2^{-a}}$ and we have used the fact that $Tr(x^{2^i}\beta) = Tr(x\beta^{2^{-i}})$.

Claim: L is linear with Kernel $GF(2^2)$:

$L(\beta) = 0 \implies \beta^{2^a} + \beta^{2^{-a}} = 0 \implies \beta^{2^{2a}} + \beta = 0$. So $\beta \in GF(2^{2a}) \cap GF(2^k) = GF(2^2)$ and $Kernel(L) = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 + \alpha + 1 = 0$. So $K = Im(L) \cup (1 + Im(L)) \cup (\alpha + Im(L)) \cup (\alpha^2 + Im(L))$ and $Tr(\alpha) = 1$.

This follows from $K = K_0 \cup K_0^c$ as $K_0 = Im(L) \cup (1 + Im(L))$ and $K_0^c = (\alpha + Im(L)) \cup (\alpha^2 + Im(L))$.

Now if $Tr(b) = 0$, then $b \in Im(L)$ or $b \in 1 + Im(L)$.

If $b \in Im(L)$, then $\exists\beta$ such that $b = L(\beta) = \beta^{2^a} + \beta^{2^{-a}}$. So $f^W(b) = 0$.

If $b \in 1 + Im(L)$, then $b = 1 + \beta^{2^a} + \beta^{2^{-a}}$ and

$$\begin{aligned} f^W(b) &= \chi(\beta^{2^a+1}+b\beta)\sum_{x\in K}\chi(x^{2^a+1}+x) \\ &= \chi(\beta+\beta^{2^{-a}+1})f^W(1) \\ &= \chi(\beta^{2^a}+\beta^{2^a+1})f^W(1) \end{aligned}$$

If $Tr(b) = 1$, then $b \in \alpha + Im(L)$ or $\alpha^2 + Im(L)$. So $b = \alpha + \beta^{2^a} + \beta^{2^{-a}}$ or $b = \alpha^2 + \beta^{2^a} + \beta^{2^{-a}}$.

If $b = \alpha + \beta^{2^a} + \beta^{2^{-a}}$, then

$$\begin{aligned} f^W(b) &= \chi(\beta^{2^a+1}+b\beta)\sum_{x\in K}\chi(x^{2^a+1}+\alpha x) \\ &= \chi(\alpha\beta+\beta^{2^{-a}+1})f^W(\alpha) \end{aligned}$$

If $b = \alpha^2 + \beta^{2^a} + \beta^{2^{-a}}$, then

$$\begin{aligned} f^W(b) &= \chi(\beta^{2^a+1}+b\beta)\sum_{x\in K}\chi(x^{2^a+1}+\alpha^2 x) \\ &= \chi(\alpha^2\beta+\beta^{2^{-a}+1})f^W(\alpha^2). \end{aligned}$$

IV. Rational points of Artin-Schreier curves

In this section we consider the Artin-Schreier curves as

$$\boldsymbol{\chi} : y^2+y = xR(x), \text{ where } R(x) = \sum_{i=0}^{m} a_i x^{2^i} \text{ with } a_i \in \mathbb{F}_2.$$

The Hasse-Weil bound relates the number of rational points of $\boldsymbol{\chi}$ to its genus. Moreover, it states that for a smooth geometrically irreducible projective curve $\boldsymbol{\chi}$ over $\mathbb{F}_{2^k}$ of genus $g(\boldsymbol{\chi})$ with $N(\boldsymbol{\chi})$ rational points

$$1 + 2^k - 2g(\boldsymbol{\chi})2^{\frac{k}{2}} \leq N(\boldsymbol{\chi}) \leq 1 + 2^k + 2g(\boldsymbol{\chi})2^{\frac{k}{2}}$$

A curve is called maximal (or minimal) if it attains the upper bound (or lower bound).
Here we note that using[13, Proposition 3.7.10], the genus of the curve χ is $g(\boldsymbol{\chi}) = \frac{1}{2}\deg R(x)$. Also by Hilbert's Theorem 90, the number of rational points $N(\boldsymbol{\chi})$ of $\boldsymbol{\chi}$ is

$$N(\boldsymbol{\chi}) = 2N(Q_R^K) + 1 = 2^k + 1 + \Lambda(Q_R^K)\sqrt{2^{k+r}}$$

where $r = \dim rad(Q_R^K)$. The curve is $maximal$ i.e. when the equality holds in the Hasse-Weil upper bound

$$N(\boldsymbol{\chi}) \leq 2^k + 1 + 2g\sqrt{2^k} = 2^k + 1 + \deg R(x)\sqrt{2^k}.$$

Clearly equality holds only if k is even and then $\boldsymbol{\chi}$ is $maximal$ iff

1) $\deg R(x) = 2^{\frac{r}{2}}$ and
2) $\Lambda(Q_R^K) = +1$.

The next lemma whose proof is obvious or we can check the proof in [19], is very usefull for our results.

Lemma 1: Let Q be a quadratic function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. Then

$$|Z| = 2^{k-1} + \frac{1}{2}Q^W(0).$$

The next theorem follows directly from Theorem 1.

Theorem 4: Let $E = \mathbb{F}_{2^n}, n = 2m, L = \mathbb{F}_{2^m}$, m be odd and $f(x) = Tr(x^{2^k+1})$. Then the number of rational points of

$$\boldsymbol{\chi} : y^2 + y = x^{2^k+1}$$

over $\mathbb{F}_{2^n}$ is given by

$$N(\boldsymbol{\chi}) = \begin{cases} 1 + 2^n + 2^m|M|, & \text{when k is odd} \\ 1 + 2^n + 2^m \sum_{\mu\in M}\chi(\mu^{2^k+1}), & \text{when k is even,} \end{cases}$$

where $M = \{\mu \in L|\mu^{2^k} + \mu^{2^{-k}} = 0\}$, $GF(4) = \{0, 1, \beta, \gamma\} \subset E = L[\beta]$.
Proof: From Theorem 1, we get

$$f^W(0) = \begin{cases} 2^m|M|, & \text{when k is odd} \\ 2^m \sum_{\mu\in M}\chi(\mu^{2^k+1}), & \text{when k is even,} \end{cases}$$

where $M = \{\mu \in L|\mu^{2^k} + \mu^{2^{-k}} = 0\}$. The proof follows from Lemma 1. □

Theorem 5: Let $E = \mathbb{F}_{2^n}, n = 2m, m$ odd $, L = \mathbb{F}_{2^m}$. Then the number of rational points of

$$\boldsymbol{\chi} : y^2 + y = x^{2^a+1} + x^{2^b+1}$$

over $\mathbb{F}_{2^n}$ is given by

$$N(\boldsymbol{\chi}) = \begin{cases} \psi_{n,m,1}, & \text{if } a, b \text{ even} \\ 1 + 2^n + 2^m \cdot |M|, & \text{if } a, b \text{ odd} \\ \psi_{n,m,2}, & \text{if } a \text{ even }, b \text{ odd} \\ \psi_{n,m,3}, & \text{if } a \text{ odd }, b \text{ even} \end{cases}$$

where $\psi_{n,m,1} = 1 + 2^n + 2^m \cdot \sum_{\mu\in M}\chi(\mu^{2^a+1} + \mu^{2^b+1})$, $\psi_{n,m,2} = 1+2^n+2^m\cdot\sum_{\mu\in M}\chi(\mu^{2^a+1})$, $\psi_{n,m,3} = 1+2^n+2^m\cdot\sum_{\mu\in M}\chi(\mu^{2^b+1})$ and $M = \{\mu \in L|\mu^{2^a}+\mu^{2^{-a}}+\mu^{2^b}+\mu^{2^{-b}} = 0\}$.
Proof: From Theorem 2, we have

$$f^W(0) = \begin{cases} 2^m \sum_{\mu\in M}\chi(\mu^{2^a+1} + \mu^{2^b+1}), & \text{if } a, b \text{ even} \\ 2^m|M|, & \text{if } a, b \text{ odd} \\ 2^m \sum_{\mu\in M}\chi(\mu^{2^a+1}), & \text{if } a \text{ even }, b \text{ odd} \\ 2^m \sum_{\mu\in M}\chi(\mu^{2^b+1}), & \text{if } a \text{ odd }, b \text{ even} \end{cases}$$

where $M = \{\mu \in L|\mu^{2^a} + \mu^{2^{-a}} + \mu^{2^b} + \mu^{2^{-b}} = 0\}$. The proof follows from Lemma 1.

□

Now we can move towards some maximal Artin-Schreier curves. The following theorem will introduce a collection of maximal Artin-Schreier curves.

Theorem 6: Let $E = \mathbb{F}_{2^n}, n = 2m, L = \mathbb{F}_{2^m}$, m be odd. Then

$$\boldsymbol{\chi} : y^2 + y = x^{2^k+1}$$

over $\mathbb{F}_{2^n}$ is maximal if k is odd and $m = lk$ where $\gcd(l, m) = 1$.
Proof: From Theorem 4, we have
$M = \{\mu \in L|\mu^{2^k} + \mu^{2^{-k}} = 0\} = \{\mu \in L|\mu^{2^{2k}} + \mu = 0\} = \mathbb{F}_{2^m} \cap \mathbb{F}_{2^{2k}} = \mathbb{F}_{2^{(m,2k)}} = \mathbb{F}_{2^{(m,k)}}$. When k is odd
$N(\boldsymbol{\chi}) = 1+2^n+2^m|M|$ which must be equal to $1+2^n+2^m\cdot 2^k$ for maximal curves. So $2^{(m,k)} = 2^k$ and the result follows. □

V. Conclusion

In this article, we have seen Walsh transforms of some quadratic trace forms with one or two terms. Later we have considered some Artin-Schreier curves and describe the number of rational points on the curves using Walsh coefficient $f^W(0)$. Theorem 3 describes the Walsh transform of $Q(x) = Tr(x^{2^a+1})$ for even degree of extension and $\gcd(a, k) = 1$. This theorem can further be used to find $N(\mathcal{X})$ for $\mathcal{X} : y^2 + y = x^{2^a+1} + x$ using the fact that $f^W(1) = Q^W(0)$, where $f(x) = Tr(x^{2^a+1} + x) = Tr(x^{2^a+1} + x^2)$.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York (1968).

[2] Bartoli D., Quoos L., Sayg Z., Explicit maximal and minimal curves of ArtinSchreier type from quadratic forms, AAECC (2020).

[3] Ayhan Cogun, Explicit evaluation of Walsh transforms of a class of Gold type functions, Volume 50, March 2018, Pages 66-83, Finite Fields and Their Applications, Elsevier

[4] P. Delsarte, J. M. Goethals, Irreducible binary codes of even dimension,in: Proc. Second Chapel Hill Conference on Combinatorial Mathematics and its Applications, Univ. North Carolina, Chapel Hill, NC, 1970, pp. 100-113.

[5] R. Fitzgerald, J. Yucas, Pencils of quadratic forms over GF(2), Discrete Math. 283 (2004) 71-79.

[6] R. Fitzgerald, Invariants of trace forms over finite fields of characteristic 2, Finite Fields Appl. 15 (2009) 261-275.

[7] R. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, Finite Fields Appl. 11 (2005) 165-181.

[8] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inform. Theory 14 (1968) 154156.

[9] T. W. Cuisick, H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences, IEEE Trans. Inform. Theory ,42 (4),1996,1238-1240.

[10] K. Khoo, G. Gong, D. R. Stinson, New family of Gold-like sequences, in: Proceesings of IEEE International Symposium on Information Theory,2002, p. 181.

[11] A. Klapper, Cross-correlation of geometric series in characterstic two, Des. Codes Cryptogr. 3 (1993) 348-377.

[12] R. Lidl, H. Niederreiter, Finite Fields, second edition, Encyclopedia Math. Appl., Vol 20, Cambridge University Press, Cambridge, 1997.

[13] H. Stichtenoth, Algebraic Function Fields and Codes, Universitytext, Springer, Berlin, 1993.

[14] H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge Univ. Press, Cambridge, 2001.

[15] H. Niederreiter, C. Xing, Algebraic Geometry in Coding Theory and Cryptography, Princeton Univ. Press, Princeton, 2009.

[16] M.A. Tsfasman, S.G. Vladut, D. Nogin, Algebraic Geometric Codes: Basic Notions American Mathematical Society, Providence, 2007.

[17] J. Lahtonen, G. McGuire, H.N. Ward, Gold and KasamiWelch functions, quadratic forms and bent functions, Adv. Math. Commun. 1 (2) (2007) 243250.

[18] Gerard van der Geer, Marcel van der Vlugt, Fibre products of Artin-Schreier curves and generalized hamming weights of codes, Journal of Combinatorial Theory, Series A, 70(2)(1995) 337-348

[19] W. Meidl,N. Anbar, Quadratic functions and maximal ArtinSchreier curves, Finite Fields and Their Applications, 33 (2014)49-71.

[20] N. Anbar,W. Meidl, More on quadratic functions and maximal Artin-Schreier curves,Applicable Algebra in Engineering, Communication and Computing, 26(5) (2015)409-426.

[21] S. Roy, Generalization of some results on Gold and Kasami-Welch functions, Finite Fields and Their Applications, 18 (2012)894-903.