The Number of Solutions of Certain Diagonal Equations over Finite Fields

JACQUES WOLFMANN

G.E.C.T, Université de Toulon, 83130 La Garde, France

Communicated by M. Waldschmidt

Received November 6, 1990; revised April 29, 1991

Let \( F = \text{GF}(q) \) be the finite field of order \( q \). Let \( a_1, a_2, \ldots, a_s \) be in \( F \setminus \{0\} \), with \( s \geq 2 \), and \( b \) in \( F \). Denote by \( N \) the number of solutions \((x_1, x_2, \ldots, x_s)\) in \( F^s \) of the equation \( a_1 x_1^d + a_2 x_2^d + \cdots + a_s x_s^d = b \). We determine \( N \) if \( q \) is a square and \( d \) is a special divisor of \( q - 1 \), and we deduce examples of projective varieties over \( F \) attaining Weil-Deligne bound. In the case of \( q \) even, \( b = 0 \), and \( a_1 = a_2 = \cdots = a_s = 1 \), we express \( N \), for any divisor of \( q - 1 \), by means of the weight distribution of certain irreducible cyclic codes. As a corollary, congruence relations on \( N \) are set up.

1. Introduction

If \( F = \text{GF}(q) \) is the finite field of order \( q \) then diagonal equations over \( F \) are equations of the form \( a_1 x_1^d + a_2 x_2^d + \cdots + a_s x_s^d = b \) with \( a_1, a_2, \ldots, a_s \) in \( F \setminus \{0\} \) and \( b \) in \( F \). They have extensively been studied (see [4, 6, 7, 9, 12, 16]). In this paper we are interested in the case of constant exponent, i.e., \( d_1 = d_2 = \cdots = d_s = d \). This is the example chosen by Weil in [16] to illustrate his famous conjecture on projective varieties over \( F \), which was proved later by Deligne. The non-trivial cases reduce to \( s \geq 2 \) and \( d \) divides \( q - 1 \). Section 2, using a classical method, gives an expression of the number \( N \) of solutions \((x_1, x_2, \ldots, x_s)\) in \( F^s \) of the equation \( a_1 x_1^d + a_2 x_2^d + \cdots + a_s x_s^d = b \), by means of character sums. This result is used in Section 3 to determine \( N \) if \( q \) is a square and \( d \) is a special divisor of \( q - 1 \). We define the case of \( a_1 = a_2 = \cdots = a_s = 1 \) and we deduce examples of projective varieties over \( F \) attaining Weil-Deligne bound. Section 4 is devoted to linking diagonal equations with cyclic codes. This point was first considered by Helleseth [5] and Tietäväinen [14, 15], about the covering radius of a cyclic code. In this work we express the number \( N \) of solutions of \( x_1^d + x_2^d + \cdots + x_s^d = 0 \) when \( p = 2 \), and for any divisor of \( q - 1 \), by means of the weight distribution of an irreducible cyclic code. In this case we deduce a congruence relation on \( N \) in Section 5.
Notations

$F = GF(q)$ denotes the finite field of order $q$, where $q = p^k$ is a power of a prime number $p$. The trace of $z \in F$ over $GF(p)$ is $\text{tr } z = \sum_{i=0}^{k-1} z^{p^i}$. $\psi_a$ is the additive character of $F$ defined by $\psi_a(x) = \exp((2in/p) \text{ tr } ax)$ for $a \in F$ and $S_u = \sum_{x \in F} \psi_u(x^d)$ for $u \in F$.

2. Diagonal Equations with Constant Exponent

For future use we need the following proposition. The proof is classical and given here for convenience.

**Proposition 1.** Let $q$ be a power of a prime number $p$ and $F = GF(q)$ the finite field of order $q$. Let $s$ be an integer, $s > 2$, and $\psi$ the additive character of $F$ defined by $\psi(x) = \exp((2in/p) \text{ tr } ax)$ where $\text{tr}$ denotes the trace of $F$ over $GF(p)$.

If $N$ is the number of solutions $(x_1, x_2, \ldots, x_s)$ in $GF(q^s)$ of the equation $a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = b$ then

$$N = q^{-1} \sum_{a \in F} \psi(-b) \prod_{i=1}^s S_{a_i},$$

where $S_u = \sum_{x \in F} \psi_u(x^d)$.

**Proof.** Let $F(x_1, x_2, \ldots, x_s) = a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d - b$ and consider

$$S = \sum_{(x_1 \ldots x_s) \in F^s} \sum_{a \in F} \psi_a(F(x_1, x_2, \ldots, x_s)).$$

Because of a well-known character sum property, the sum $\sum_{a \in F} \psi_a(F(x_1, x_2, \ldots, x_s))$ is equal to $q$ if $F(x_1, x_2, \ldots, x_s) = 0$ and is equal to $0$ otherwise. Therefore we get $S = qN$. Now by interchanging the two summations it follows that

$$qN = \sum_{a \in F} \sum_{(x_1 \ldots x_s) \in F^s} \psi_a(F(x_1, x_2, \ldots, x_s)).$$

By using the morphism property of $\psi_a$ the second sum is equal to the product of $\psi_a(-b)$ by $\sum_{(x_1 \ldots x_s) \in F^s} (\prod_{i=1}^s \psi_a(a_i x_i^d))$ which obviously is also equal to $\prod_{i=1}^s (\sum_{x \in F} \psi_a(a_i x_i^d))$ hence the result is proved. \qed

3. Special Diagonal Equations

3.1. The Main Result

We now consider the case where $d$ is a special divisor of $q - 1$ and $q$ is a square. The purpose of that section is to prove
THEOREM 1. Let $p$ be a prime number, $q = p^k$, $k = 2t$, and $F = GF(q)$ the finite field of order $q$. Let $a_1, a_2, \ldots, a_s$ in $F \setminus \{0\}$, with $s > 2$, $b$ in $F$, and $d$ a divisor of $q - 1$ with $nd = q - 1$. Denote by $N$ the number of solutions $(x_1, x_2, \ldots, x_s)$ in $F^s$ of the equation $a_1 x_1^d + a_2 x_2^d + \cdots + a_s x_s^d = b$. If there exists a divisor $r$ of $t$ such that $p^r \equiv -1 \pmod{d}$ then:

1. $b = 0,$

$$N = q^s - 1 + \varepsilon^s q^{s/2 - 1} (q - 1) d^{-1} \sum_{0}^{d-1} (1 - d)^{\tau(j)}.$$ 

2. $b \neq 0,$

$$N = q^s - 1 - \varepsilon^s q^{s/2 - 1} \left[ (1 - d)^{\theta(b)} q^{1/2} - (q^{1/2} - \varepsilon) d^{-1} \sum_{0}^{d-1} (1 - d)^{\tau(j)} \right],$$

where

$$\varepsilon = (-1)^{t/r},$$

$\theta(b)$ is the number of $i$, $1 \leq i \leq s$, such that $(a_i)^n = (-b)^n$ 

$\tau(j)$ is the number of $i$, $1 \leq i \leq s$, such that $(a_i)^n = (x^j)^n$ (with $x$ a primitive root of $F$).

Remarks. (1) The result in the case of $r = t$ was already given in [4]. The condition $p^r \equiv -1 \pmod{d}$ implies $(p^r)^{t/r} \equiv (-1)^{t/r} \pmod{d}$, that is, $p^r - \varepsilon \equiv 0 \pmod{d}$. Thus, if $t/r$ is odd then $p^r \equiv -1 \pmod{d}$ and the result is known from [4]. Our theorem is therefore new if $t/r$ is even.

(2) If $d = 2$ the non-trivial situation is $q$ odd. In that case the result was already known (see [7, Chap. 6]).

(3) In the case $s = 2, b = 1, a_1 = 1, a_2 = -1$, and deleting the solutions $(x_1, x_2)$ such that $x_1 = 0$ or $x_2 = 0$, we are able to calculate the cyclotomic numbers of order $d$ over $F$ under the assumptions of the theorem. In that way we find the results of [2].

(4) If $s = 2$ see also [8] about a special case.

In order to prove the theorem we need the two next results which are proved in [17].

PROPOSITION 2. Let $p$, $q$, $F$, and $S_a$ be as in Proposition 1 with $q = p^k$ and $k = 2t$. Let $n$ and $d$ be integers such that $nd = q - 1$.

If there exists a divisor $r$ of $t$ such that $p^r \equiv -1 \pmod{d}$ then the number $S(\gamma, \delta)$ of solutions $x$ in $F$ of the equation $tr(\gamma x^d + \delta) = 0$ ($\gamma \in F \setminus \{0\}$, $\delta \in F$) is given by:
If \( y^n = \varepsilon_1 \) and \( \text{tr}(\delta) = 0 \), \( S(\gamma, \delta) = p^{2t-1} - \varepsilon(p-1)(d-1)p^{t-1} \);

If \( y^n = \varepsilon_1 \) and \( \text{tr}(\delta) \neq 0 \), \( S(\gamma, \delta) = p^{2t-1} + \varepsilon(d-1)p^{t-1} \);

If \( y^n \neq \varepsilon_1 \) and \( \text{tr}(\delta) = 0 \), \( S(\gamma, \delta) = p^{2t-1} + \varepsilon(p-1)p^{t-1} \);

If \( y^n \neq \varepsilon_1 \) and \( \text{tr}(\delta) \neq 0 \), \( S(\gamma, \delta) = p^{2t-1} - \varepsilon p^{t-1} \),

where \( \varepsilon = (-1)^{t/r} \) and \( \varepsilon_1 = \varepsilon^u \) with \( ud = p^r + 1 \).

**Corollary 3.** Let \( p, q, \mathbf{F}, \) and \( S_a \) be as in Proposition 1 with \( q = p^k \) and \( k = 2t, \) \( nd = q - 1, \) \( r \) a divisor of \( t \) such that \( p' \equiv -1 \) (mod \( d \)).

Then \( S_a \) is given by the following formulae where \( c = (1)^{t/r} \) and \( \varepsilon_1 = \varepsilon^u \) with \( ud = p^t + 1 \).

If \( a^n = \varepsilon_1 \), \( S_a = -\varepsilon(d-1)p^t \).

If \( a^n \neq \varepsilon_1 \), \( S_a = \varepsilon p^t \).

**Remarks.** (1) These two previous results are implicit in [2, 3] but Proposition 2 and Corollary 3 specify the parameters \( \varepsilon \) and \( \varepsilon_1 \).

(2) In the case \( a^n = \varepsilon_1 \) in Corollary 3, the Carlitz-Uchiyama bound on character sums is attained.

In the same way, Proposition 2 implies the existence of algebraic curves attaining Weil bound on curves (see [17]).

**Proof of Theorem 1.** Recall the formulae giving \( N \) in Proposition 1 and use the notation of Corollary 3. For \( a \in \mathbf{F} \setminus \{0\} \) let \( \sigma(a) \) be the number of subscripts \( i \) such that \( (a^i)^n = \varepsilon_1 \) and let \( S_1 = -\varepsilon(d-1)p^t, S_2 = \varepsilon p^t \). From Corollary 3, the product \( \prod_{i=1}^d S_{a_i} \) becomes \( S_1^{\sigma(1)}S_2^{-\sigma(1)} \). Therefore, from Proposition 1 and by isolating the contribution of \( a = 0 \),

\[
qN = q^s + (S_2)^s \sum_{a \in \mathbf{F} \setminus \{0\}} (S_1(S_2)^{-1})^{\sigma(a)} \psi_a(-b),
\]

that is

\[
qN = q^s + \varepsilon p^{st} \sum_{a \in \mathbf{F} \setminus \{0\}} (1-d)^{\sigma(a)} \psi_a(-b). \tag{1}
\]

Let \( E_n \) be the multiplicative sub-group of order \( n \) in \( \mathbf{F} \setminus \{0\} \) and let \( C_j \) be the class modulo \( E_n \) defined by \( C_j = \alpha^j E_n \) for \( j = 0, 1, ..., d-1 \) where \( \alpha \) is a primitive root of \( 
\). In other words \( C_j \) is the set of \( y \) in \( \mathbf{F} \setminus \{0\} \) such that \( y^n = \alpha^i \). The summation in (1) can be rewritten as

\[
\sum_{a \in \mathbf{F} \setminus \{0\}} (1-d)^{\sigma(a)} \psi_a(-b) = \sum_{j=0}^{d-1} \sum_{a \in C_j} (1-d)^{\sigma(a)} \psi_a(-b). \tag{2}
\]
Let \( v(j) \) be the number of \( i \) such that \((a^i)^n \ (a_i)^n = \varepsilon_1 \). For all \( a \in C_j \) we have \((aa_i)^n - \varepsilon_1 \) if and only if \( (a^i)^n \ (a_j)^n = \varepsilon_1 \). That means \( \sigma(a) = v(j) \) if \( a \in C_j \), and so it follows from (1) and (2),

\[
qN = q^s + \varepsilon^s p^s \sum_{j=0}^{d-1} (1 - d)^v(j) \sum_{a \in C_j} \psi_a(-b).
\]

First Case. \( b \neq 0 \). For \( \lambda \in GF(p) \) define \( R_j(b, \lambda) = \# \{ a \in C_j : \text{tr}(-ba) = \lambda \} \) and \( T_j(b, \lambda) = \# \{ x \in F \setminus \{0\} : \text{tr}(-bx^d) = \lambda \} \). If \( a \in C_j \) then there are exactly \( d \) elements of \( F \setminus \{0\} \) such that \( a = \alpha x^d \) and so \( dR_j(b, \lambda) = T_j(b, \lambda) \). This implies \( d \sum_{a \in C_j} \psi_a(-b) = T_j(b, 0) + \sum_{j=1}^{p-1} T_j(b, \lambda) \exp((2i\pi/p) \lambda) \).

Proposition 2 shows that \( T_j(b, \lambda) \) only depends on \((-b \alpha^j x^d)\) and thus

\[
d \sum_{a \in C_j} \psi_a(-b) = T_j(b, 0) + T_j(b, 1) \sum_{\lambda=1}^{p-1} \exp((2i\pi/p) \lambda) \\
= T_j(b, 0) + T_j(b, 1) \left( -1 + \sum_{\lambda=0}^{p-1} \exp((2i\pi/p) \lambda) \right) \\
= T_j(b, 0) - T_j(b, 1).
\]

Substituting in (3) we obtain

\[
qN = q^s + d^{-1}\varepsilon^s p^s \sum_{j=0}^{d-1} A_j(b)(1 - d)^v(j)
\]

with \( A_j(b) = T_j(b, 0) - T_j(b, 1) \).

From Proposition 2 and the definition of \( T_j(b, \lambda) \), the number \( A_j(b) \) only depends on \( b \) and \( j \) according to the fact \((-b \alpha^j x^d)\) is equal to \( \varepsilon_1 \) or not. The unique case where \( \varepsilon_1 = -1 \) in Proposition 2 is \( p \) odd and \( u \) odd. In this case the equality \( ud = p' + 1 \) implies \( d \) even. That means \( (\varepsilon_1)^d = (-1)^d = 1 \) and therefore, because \( nd = q - 1 \), there exist exactly \( n \) solutions of \( a^n = \varepsilon_1 \). This is obviously true if \( \varepsilon_1 = 1 \). In all cases there exists one and only one \( j \) with \( 0 < j < d - 1 \), say \( j_0 \), satisfying \((-b \alpha^j)^n = \varepsilon_1 \). With the notations of Proposition 2 and if \( 1 = \text{tr}(v_1), \gamma_0 = b \alpha^{j_0}, \gamma_1 = b \alpha^j \), with \( j \neq j_0 \), we obtain:

If \( j = j_0 \) then \( A_j(b) = A_1 = S(\gamma_0, 0) - 1 - S(\gamma_0, v_1) = -1 - \varepsilon(d - 1)p' \).

If \( j \neq j_0 \) then \( A_j(b) = A_2 = S(\gamma_1, 0) - 1 - S(\gamma_1, v_1) = -1 + \varepsilon p' \).

Now (4) gives

\[
qN = q^s + d^{-1}\varepsilon^s p^s \left[ A_1(1 - d)^v(j_0) + A_2 \sum_{j \neq j_0} (1 - d)^v(j) \right] \\
= q^s + d^{-1}\varepsilon^s p^s \left[ (A_1 - A_2)(1 - d)^v(j_0) + A_2 \sum_{j=0}^{d-1} (1 - d)^v(j) \right] \\
= q^s + d^{-1}\varepsilon^s p^s \left[ (-\varepsilon dp')(1 - d)^v(j_0) + (-1 + \varepsilon p') \sum_{j=0}^{d-1} (1 - d)^v(j) \right].
\]
Finally remark the following property of $v(j)$: By definition, $v(j)$ is the number of $i$ such that $(a_i^n)^n - a_i^n$. On the other hand, $\varepsilon_i$ is an $n$th power as previously seen. Thus, if $0 \leq j \leq d - 1$, $v(j)$ is equal to the number of $a_i$'s belonging to one and only one class modulo $E_n$. Consequently $\tau(j)$ can be written instead of $v(j)$ in the summation above. Furthermore if $j = j_0$ and because $\varepsilon_1 = (bz^0)^n$, the integer $v(j_0)$ is equal to the number of $i$ such that $(a_i^n)^n = (b)^n$. We denote this last number by $\theta(b)$ and this proves the theorem if $b \neq 0$.

**Second Case.** $b = 0$. In this case, (3) becomes

$$qN = q^t + d^{-1}(q - 1) \varepsilon \sum_{j=0}^{d-1} (1 - d)^{v(j)}$$

which is the expected result. \(\blacksquare\)

3.2. \*The Case* $a_1 = a_2 = \cdots = a_s = 1$

This case is related to Waring's problem in a finite field and the covering radius of codes (see [5, 14]). If $d = 2$ see [7, Chapt. 6]. If $d = 3$ or $d = 4$ and $b = 0$ some results are given in [12].

With the notations of Theorem 1 we find:

$$\tau(0) = s \quad \text{and} \quad \tau(j) = 0 \text{ if } j \neq 0$$

$$\theta(b) = s \text{ if } b^n = 1 \quad \text{and} \quad \theta(b) = 0 \text{ if } b^n \neq 1.$$

Hence this gives the following:

**Corollary 4.** Let $p$ be a prime number, $q = p^k$, $k = 2t$, and $F = GF(q)$ the finite field of order $q$. Let $N$ be the number of solutions $(x_1, x_2, \ldots, x_s)$ in $F^t$ of the equation $x_1^d + x_2^d + \cdots + x_s^d = b$, where $s \geq 2$, $b \in F$, and $d$ is a divisor of $q - 1$ with $nd = q - 1$.

If there exists a divisor $r$ of $t$ such that $p^r \equiv -1 \pmod{d}$ then:

1. $b = 0,$

$$N = q^{s-1} + \eta^s q^{s/2 - 1} (q - 1) \ B(d, s).$$

2. $b \neq 0,$

   (i) if $b^n = 1,$

   $$N = q^{s-1} + \eta^{s+1} q^{s/2 - 1} [(d - 1)^s q^{1/2} - (q^{1/2} + \eta) B(d, s)]$$

   (ii) if $b^n \neq 1,$

   $$N = q^{s-1} + \eta^{s+1} q^{s/2 - 1} [(-1)^s q^{1/2} - (q^{1/2} + \eta) B(d, s)],$$

where $\eta = (-1)^{t+1}$ and $B(d, s) = d^{-1} [(d - 1)^s + (-1)^s (d - 1)]$. 
**Remarks.** (1) The method we used in the proof of Corollary 4 is also convenient in the case of \( a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = b \) and \((a_1)^n = (a_2)^n = \cdots = (a_s)^n\), because it leads to the same values for the \( \tau(j) \)'s. In fact, in this case, we can write \( a_i = \alpha^i u_i^d \), and using \( y_i = u_i x_i \), the equation reduces to \( y_1^d + y_2^d + \cdots + y_s^d = \alpha^{-1}b \), and then Corollary 4 holds.

(2) As it can be seen in [6, p. 162] (see also [16]) the zeta function of the hypersurface defined by the homogeneous polynomial \( x_1^d + x_2^d + \cdots + x_s^d \) is of the form \( P(u)^{-1}/(1-u)(1-qu)\cdots(1-q^{r-2}u) \) where \( P(u) \) is a polynomial and the degree of \( P(u) \) is precisely the number \( B(d,s) = d^{-1}[((d-1)^s + (-1)^s(d-1)) \] which appears in the result above. It also appears in the famous Weil–Deligne bound that we recall below.

### 3.3. Projective Varieties Attaining the Weil–Deligne Bound

This well-known bound is as follows in the special case we consider (see [6, 9, 16] for example). Let \( P \) be an homogeneous polynomial of degree \( d \) in \( F[x_1, x_2, \ldots, x_m] \) with \( F = GF(q) \) and \( V \) the projective variety defined by \( P \) over \( F \). Let \( N \) be the number of points of \( V \) over \( F \). If \( V \) is absolutely irreducible and non-singular then

\[
\left| N - \frac{(q^m-1)}{q-1} \right| \leq q^{m/2}B(d,m),
\]

where \( B(d,m) = d^{-1}[((d-1)^m + (-1)^m(d-1)) \]

Now consider \( P = x_1^d + x_2^d + \cdots + x_s^d \) and assume the conditions of Corollary 4 on the parameters. Then \( V \) is absolutely irreducible and non-singular because \( d \) is prime to \( q \) and obviously \( N = 1 + (q-1)N \) where \( N \) is the number of solutions in \( F^s \) of \( x_1^d + x_2^d + \cdots + x_s^d = 0 \). Corollary 4 gives

\[
\frac{(q^r-1)}{q-1} \leq \eta q^{s/2}B(d,s), \quad \text{with} \quad \eta = (1)^{t/r} + 1
\]

and so Weil–Deligne bound (*) is attained.

**Corollary 5.** Let \( V \) be the projective variety defined by \( x_1^d + x_2^d + \cdots + x_s^d \) over \( F = GF(p^k) \) with \( s \geq 2 \), \( p \) is a prime number, \( k = 2t \), and \( d \) divides \( p^k - 1 \). Let \( N \) be the number of points of \( V \) over \( F \). If there exists a divisor \( r \) of \( t \) such that \( p^r \equiv -1 \pmod{d} \), then \( N \) attains Weil–Deligne bound.

If \( t/r \) is even then \( N = (q^r-1)/(q-1) - q^{r/2}B(d,s) \).

If \( t/r \) is odd then \( N = (q^r-1)/(q-1) + q^{r/2}B(d,s) \).

**Remark.** If \( d = p^r + 1 \) this is the well-known case where \( V \) is a Hermitian variety.
4. IRREDUCIBLE CYCLIC CODES

4.1. Codes

The following definitions and results are recalled for readers who are not familiar with coding theory. The references on coding theory can be found in [10].

The irreducible cyclic codes have been studied in [2] (see also [11]).

Let \( K \) be a finite field. If \( x = (a_0, a_1, ..., a_{n-1}) \in K^n \), then the weight of \( x \) is the number \( w(x) = \# \{i : a_i \neq 0\} \). A linear code of length \( n \) over \( K \) is a \( K \)-vector subspace of \( K^n \). Such a code is said to be cyclic if it is invariant by the shift transform of \( K^n \) defined by \( (a_0, a_1, ..., a_{n-1}) \rightarrow (a_{n-1}, a_0, ..., a_{n-2}) \).

Identifying \( K^n \) with the algebra \( A = K[x]/(x^n - 1) \) by means of \( (a_0, a_1, ..., a_{n-1}) \rightarrow \sum_{i=0}^{n-1} a_i x^i \), the cyclic codes are the ideals of \( A \). It follows that a cyclic code \( C \) is the principal ideal generated by a unique divisor of \( x^n - 1 \) over \( K \) which is called the generator of \( C \).

An irreducible cyclic code is a minimal ideal of \( A \). This means that its generator is \( (x^n - 1)/m(x) \) with \( m(x) \) an irreducible divisor of \( x^n - 1 \) over \( K \). Furthermore \( m(x) = m_\beta(x) \) such that \( \beta \) is an \( n \)th root of unity over \( K \) and \( m_\beta(x) \) is the minimal polynomial of \( \beta \) over \( K \). Let us denote such a code by \( C(\beta) \). The code \( C(\beta) \) is called non-degenerate if \( \beta \) is a primitive \( n \)th root of unity.

Let \( L \) be the splitting field of \( x^n - 1 \) over \( K \). It is well known that \( C(\beta) \) is the image of \( L \) by the mapping \( \mu \) from \( L \) into \( K^n \) defined by

\[
\mu(a) = (\text{Tr}(a), \text{Tr}(a\beta), ..., \text{Tr}(a\beta^{n-1}))
\]

with \( \text{Tr} \) the trace of \( L \) over \( K \). If \( C(\beta) \) is non-degenerate then \( \mu \) is one-to-one.

4.2. Binary Cyclic Codes and Diagonal Equations

We return to our diagonal equation in the case \( q = 2^k \) with \( nd = 2^k - 1 \) and \( F = GF(2^k) \). In this case \( \psi_a(x) = (-1)^{\text{tr}(ax^d)} \) and the character sum \( S_a = \sum_{x \in F} \psi_a(x^d) \) can be expressed as

\[
S_a = 2^k - 2N_a,
\]

where \( N_a \) is the number of non-zero \( x \) in \( F \) such that \( \text{tr}(ax^d) = 1 \).

If \( \beta \) is a primitive \( n \)th root of unity over \( GF(2) \) then, because \( nd = 2^k - 1 \), we have

\[
N_a = dn_a,
\]

where \( n_a \) is the number of integers \( i \) in the range \([0, n-1]\) such that \( \text{tr}(a\beta^i) = 1 \).
Let \( L = GF(2^n) \) be the splitting field of \( x^n - 1 \) over \( GF(2) \), i.e., \( v \) is the multiplicative order of 2 modulo \( n \). Let \( T \) and \( \tau \) be the trace functions of \( L \) over \( GF(2) \) and of \( F \) over \( L \), respectively.

Applying a well-known transitivity property of the trace functions, and according to the fact that the powers of \( \beta \) belong to \( L \), it follows that

\[
\text{tr}(\alpha \beta^i) = T(c \beta^i) \quad \text{with} \quad c = \tau(\alpha). \tag{9}
\]

Now if \( w_c \) is the weight of the word \( \mu(c) \) as described in (1), then \( n_a = w_c \).

From (7), (8), (9), and Proposition 1 we obtain

\[
N = 2^{s-k} \sum_{a \in F} (2^{k-1} - dw_c)^s \quad \text{with} \quad c = \tau(\alpha). \tag{10}
\]

Obviously, for every \( c \) in \( L \) the number of \( a \) in \( F \) such that \( c = \tau(\alpha) \) is \((2^v)^{k/v - 1} = 2^{k-v}\). On the other hand, \( \mu \) is one-to-one and therefore the number \( A_i \) of words in \( C = C(\beta) \) of weight \( i \) is also the number of \( c \) in \( L \) such that \( w_c = i \). Finally (10) becomes

\[
N = 2^{s-k} \sum_{i=0}^{n} 2^{k-v} A_i (2^{k-1} - di)^s = 2^{s-v} \sum_{i=0}^{n} A_i (2^{k-1} - di)^s.
\]

Summarizing we have proved the following theorem:

**Theorem 2.** Let \( k, d, n \) be non-negative integers such that \( nd = 2^k - 1 \), \( F = GF(2^k) \), and let \( v \) be the multiplicative order of 2 modulo \( n \). Let \( C \) be a cyclic code of length \( n \) over \( GF(2) \) generated by \((x^n - 1)/m(x)\) where \( m(x) \) is a primitive irreducible divisor of \( x^n - 1 \) over \( GF(2) \). For \( i = 0, 1, \ldots, n \), let \( A_i \) be the number of words in \( C \) of weight \( i \).

If \( N \) is the number of solutions \((x_1, x_2, \ldots, x_n)\) in \( F^n \) of the equation \( x_1^i + x_2^i + \cdots + x_n^i = 0 \) then

\[
N = 2^{s-v} \sum_{i=0}^{n} A_i (2^{k-1} - di)^s. \tag{11}
\]

**Examples.** In order to apply the above theorem, the reader will find in [11] numerical results giving all the non-zero \( A_i \)'s for all non-degenerate irreducible cyclic codes such that \( 6 \leq v \leq 27 \).

For instance, if \( k = 6 \), \( d = 7 \), then \( n = 9 \) and \( v = 6 \). We find in [11], \( A_0 = 1, A_2 = 9, A_4 = 27, A_6 = 27 \), and \( A_i = 0 \) if \( i \neq 0, 2, 4, 6 \). We obtain the number of solutions in \((GF(64))^n\) of the equation \( x_1^i + x_2^i + \cdots + x_9^i = 0 \) as

\[
N = 2^{2s-6} [(16)^i + 9(9)^i + 27(2)^i + 27(-5)^i].
\]

**Remark.** By expanding \((2^{k-1} - di)^s\) the equality \(11\) becomes \( N = 2^{s-v} \sum_{j=0}^{s} (-1)^j \binom{s}{j} (2^{k-1})^{s-j} d^j \sum_{i=0}^{n} A_i i^j \) where \( \binom{s}{j} \) is the classical
Using the power moment identities given by Pless in [13], it is possible to write \( \sum_{i=0}^{n} A_i i^j = F_j(k, v, B_0, B_1, \ldots, B_{i-1}) \) where \( B_j \) denotes the number of words of weight \( i \) in the orthogonal code of \( C \). The number \( B_j \) is also the number of words of weight \( i \) in the cyclic code generated by \( m_p(x) \) as defined in 4.1. This gives rise to another, but more complicated, expression of \( N \) involving \( B_0, B_1, \ldots, B_5 \).

5. CONGRUENCES ON THE NUMBER OF SOLUTIONS

The previous Theorem 2 implies now the next result:

**Corollary 6.** Let \( k, d \) be non-zero natural integers such that \( d \) divides \( 2^k - 1 \) and \( F = GF(2^k) \). If \( N \) is the number of solutions \( (x_1, x_2, \ldots, x_s) \) in \( F^s \) of the equation \( x_1^d + x_2^d + \cdots + x_s^d = 0 \) then:

\[
\begin{align*}
(a) \quad N \equiv 0 \pmod{2^{k\lfloor s/d \rfloor}} \\
(b) \quad N/2^{k\lfloor s/d \rfloor} \equiv 1 \pmod{((2^k - 1)/d))},
\end{align*}
\]

where \( \lfloor s/d \rfloor \) is the integer part of \( s/d \).

**Proof.** The numbers \( k, d, n, v, A_i \) are defined as in Theorem 2.

Part (a) is a direct consequence of the well-known theorem of Ax in [1]. Now let \( a \) and \( a_1 \) be non-zero elements of \( F \) and \( \mu(a), \mu(a_1) \) the corresponding words in \( C(\beta) \) as defined in (6). If \( a \) and \( a_1 \) are congruent modulo the multiplicative sub-group of order \( n \) in \( F^* \) then \( \mu(a_1) \) is obtained by permuting the components of \( \mu(a) \). Consequently \( \mu(a) \) and \( \mu(a_1) \) have the same weight. This implies, for \( i \) non-zero, that \( A_i \) is a multiple of \( n \). From (6) we find

\[ 2^v N \equiv 2^{ks} \pmod{n}. \]

Because of the definitions of \( n \) and \( v \) we know that \( 2^v \) and \( 2^k \) are both equal to 1 modulo \( n \) and so \( N \equiv 1 \pmod{n} \). On the other hand, \( n \) and \( 2^{k\lfloor s/d \rfloor} \) are relatively prime. It follows from the above and (a) that \( N - 2^{k\lfloor s/d \rfloor} \equiv 0 \pmod{2^{k\lfloor s/d \rfloor}((2^k - 1)/d))} \), and this implies (b).

**Acknowledgment**

The author expresses his gratitude to A. Skorobogatov for a fruitful discussion motivating this paper.
REFERENCES