Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
FINITE FIELDS AND THEIR APPLICATIONS
Finite Fields and Their Applications ••• (••••) •••–•••
http://www.elsevier.com/locate/ffa

On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p

Francis N. Castro [a,*,1], Ivelisse Rubio [b,2], Puhua Guan [a,1], Raúl Figueroa [a,1]

[a] *Department of Mathematics, University of Puerto Rico, Box 23355, S.J. PR 00931-3355, Puerto Rico*
[b] *Department of Mathematics, University of Puerto Rico, Humacao PR 00791, Puerto Rico*

Received 19 March 2007; revised 24 September 2007

Communicated by Gary L. Mullen

Abstract

One of the most important questions in number theory is to find properties on a system of equations that guarantee solutions over a field. A well-known problem is Waring's problem that is to find the minimum number of variables such that the equation $x_1^d + \cdots + x_n^d = \beta$ has solution for any natural number β. In this note we consider a generalization of Waring's problem over finite fields: To find the minimum number $\delta(k, d, p^f)$ of variables such that a system

$$x_1^k + \cdots + x_n^k = \beta_1,$$
$$x_1^d + \cdots + x_n^d = \beta_2$$

has solution over $\mathbb{F}_{p^f}$ for any $(\beta_1, \beta_2) \in \mathbb{F}_{p^f}^2$. We prove that, for $p > 3$, $\delta(1, p^i + 1, p^f) = 3$ if and only if $f \neq 2i$. We also give an example that proves that, for $p = 3$, $\delta(1, 3^i + 1, 3^f) \geqslant 4$.

Keywords: System of diagonal equations; Waring number

* Corresponding author.
E-mail addresses: franciscastr@gmail.com (F.N. Castro), iverubio@uprrp.edu (I. Rubio), pguan@cnnet.upr.edu (P. Guan), rffigueroa@uprrp.edu (R. Figueroa).
[1] Fax: +1 787 281 0651.
[2] Fax: +1 787 773 1717.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.09.008

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

1. Introduction

One of the most important questions in number theory is to find properties on a system of equations that guarantee solutions over a field. This type of question is called of the *Chevalley type* and there are many results related to this [3,9,~~19~~]. A well-known problem is Waring's problem that is to find the minimum number of variables such that the equation $x_1^d + \cdots + x_n^d = \beta$ has solution for any natural number β. This minimum number is called the *Waring number* associated to d. For finite fields there are many bounds for Waring numbers [10,20]. For an excellent survey of work related to Waring's problem see [17,19].

In this note we consider a generalization of Waring's problem over finite fields: To find the minimum number of variables such that a system

$$\begin{aligned} x_1^k + \cdots + x_n^k &= \beta_1, \\ x_1^d + \cdots + x_n^d &= \beta_2 \end{aligned} \tag{1}$$

has solution over $\mathbb{F}_{p^f}$ for any $(\beta_1, \beta_2) \in \mathbb{F}_{p^f}^2$. We denote this number by $\delta(k, d, p^f)$.

The cases $\delta(1, d, 2^f)$ have been studied intensively because of their application to the computation of the covering radius of certain cyclic codes. The following are some examples of the known cases. It is known that $\delta(1, 2^i + 1, 2^f) = 3$ if $(i, f) = 1$ and this is called Gold's case [5,12,15]. Also, $\delta(1, 2^i + 1, 2^f) = 3$ if $\mathrm{ord}_2(l + 1) < f/2$, and $l = (2^f - 1, 2^i - 1)$ [12]. In particular, $\delta(1, 2^i + 1, 2^f) = 3$ whenever $l \equiv 1 \bmod 4$. It is also known that $\delta(1, 2^{2i} - 2^i + 1, 2^f) = 3$ and this is called Kasami's case [6,8,13]. Recently, the case $\delta(1, 2^i + 3, 2^{2i+1}) = 3$ was proved by Canteaut et al. [2] and it is called the Welch's case. In [1] it was proved that $\delta(1, 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1, 2^{5i}) \leqslant 4$.

For the case where $p > 3$, it has been known for a long time that $\delta(1, 2, p^f) = 3$ (see [4,7,18]). When $p = 3$ it was proved in [4] that $\delta(1, 2, 3^f) = 4$.

In Section 3 we prove that, for $p > 3$, $\delta(1, p^i + 1, p^f) = 3$ if and only if $f \neq 2i$. We also give an example that proves that, for $p = 3$, $\delta(1, 3^i + 1, 3^f) \geqslant 4$. In Section 2 we compute the splitting field of a polynomial that it is used in the proof of $\delta(1, p^i + 1, p^f) = 3$ for $p > 3$. In the last section we find conditions on the coefficients of a system of diagonal equations so that the system has solutions for any value of the constant terms.

2. Splitting field

In this section we compute the splitting field of a polynomial of the form $ax^{q+1} + bx^q + bx + d \in \mathbb{F}_q[x]$.

Theorem 1. *Let $q = p^f$ and $f(x) = ax^{q+1} + bx^q + bx + d \in \mathbb{F}_q[x]$, where $a \neq 0$. Then $f(x)$ factors into linear factors over $\mathbb{F}_{q^2}[x]$.*

Proof. We have

$$\begin{aligned} f(x) &= ax^{q+1} + bx^q + bx + d \\ &= x^q(ax + b) + bx + d \end{aligned}$$

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

$$= ax^q\left(x+\frac{b}{a}\right)+b\left(x+\frac{b}{a}\right)+d-\frac{b^2}{a}$$
$$= \left(x+\frac{b}{a}\right)\left(ax^q+b\right)+d-\frac{b^2}{a}$$
$$= a\left(x+\frac{b}{a}\right)\left(x+\frac{b}{a}\right)^q+d-\frac{b^2}{a}.$$

Then

$$f(x)=a\left(x+\frac{b}{a}\right)^{q+1}-\left(\frac{b^2}{a}-d\right). \tag{2}$$

If $b^2=ad$, then $f(x)=a(x+\frac{b}{a})^{q+1}$ and $f(x)$ factors completely over $\mathbb{F}_q$. Now suppose that $b^2\neq ad$. If we let $d'=\frac{1}{a}(\frac{b^2}{a}-d)$, we obtain

$$f(x)=a\left(\left(x+\frac{b}{a}\right)^{q+1}-d'\right).$$

Note that, since $d'\in\mathbb{F}_q$, there exists $D\in\mathbb{F}_{q^2}$ such that $D^{q+1}=d'$. Therefore

$$f(x)=a\left(\left(x+\frac{b}{a}\right)^{q+1}-D^{q+1}\right)=aD^{q+1}\left(\left(\frac{x}{D}+\frac{b}{aD}\right)^{q+1}-1\right)$$
$$=aD^{q+1}\left(y^{q+1}-1\right),$$

for $y=\frac{x}{D}+\frac{b}{aD}$. Since

$$\prod_{0\neq\alpha\in\mathbb{F}_{q^2}}(y-\alpha)=y^{q^2-1}-1=\left(y^{q+1}-1\right)\left(\sum_{i=0}^{q-2}\left(y^{q+1}\right)^i\right),$$

one has that $f(x)$ factors into linear factors over $\mathbb{F}_{q^2}$. □

The next corollary will be needed to prove that $\delta(1,p^i+1,p^f)=3$ for $p>3$, if and only if $f\neq 2i$ (Theorem 7).

Corollary 2. *Let $p>2$ and suppose that $\frac{b}{a}\in\mathbb{F}_{p^l}$. The number of different roots of $f(x)$ over $\mathbb{F}_{p^l}$ is even if and only if $b^2\neq ad$.*

Proof. Suppose that $b^2\neq ad$ and $x=s\in\mathbb{F}_{p^l}$ is a root of $f(x)$. Then, for $y=\frac{s}{D}+\frac{b}{aD}$, one has that $f(s)=aD^{q+1}(y^{q+1}-1)=0=aD^{q+1}((-y)^{q+1}-1)$. This implies that $-s-\frac{2b}{a}\in\mathbb{F}_{p^l}$ is also a solution of $f(x)=0$.

To see that the number of different roots is even, we first see that $s\neq -s-\frac{2b}{a}$. If $s=-s-\frac{2b}{a}$, then $s=\frac{-b}{a}$. But $f(\frac{-b}{a})=0$ implies that $b^2=ad$ and we are assuming that this is not true. Hence, if s is a root of $f(x)$, we have that $-s-\frac{2b}{a}$ is a different root of $f(x)$ and we have sets of roots $\{s_i, -s_i - \frac{2b}{a}\}$ with two elements. These sets are either equal or disjoint because (1) $s_i = s_j$ if and only if $-s_i - \frac{2b}{a} = -s_j - \frac{2b}{a}$, and (2) $s_i = -s_j - \frac{2b}{a}$ if and only if $s_j = -s_i - \frac{2b}{a}$. This implies that the number of roots of $f(x)$ is even.

Suppose now that $b^2 = ad$. Then, from the proof of Theorem 1 we can see that $x = -\frac{b}{a} \in \mathbb{F}_{p^l}$ is the only root of $f(x)$ and hence the number of different roots is odd. $\square$

Consider the polynomial $x^3 + 1 = (x+1)(x^2+x+1) \in \mathbb{F}_2[x]$. This polynomial has the form $f(x) = ax^{q+1} + bx^q + bx + d$ with $a = d = 1$ and $b = c = 0$. The polynomial has only one solution over $\mathbb{F}_{2^{2i+1}}$ but $0 = b^2 \neq ad = 1$. This implies that the previous corollary is not true for $p = 2$.

The next are some results on the reducibility and type of roots of polynomials similar to the one in Theorem 1.

Proposition 3. *The polynomial $g(x) = ax^{q+1} + bx^q + cx + d \in \mathbb{F}_q[x]$ has a root over $\mathbb{F}_q$ if and only if $ax^2 + (b+c)x + d$ is reducible over $\mathbb{F}_q$.*

Corollary 4. *The polynomial $g(x)$ has at most two different roots over $\mathbb{F}_q$.*

Corollary 5. *Let $q = p^f$, $p > 2$ and $f(x) = ax^{p+1} + bx^p + bx + d \in \mathbb{F}_p[x]$, where $a \neq 0$. If $b^2 \neq ad$ and $(f, 2) = 1$, we have that*

1. *$f(x) = (x - \alpha_1)(x - \alpha_2)p_1(x) \cdots p_{\frac{p-1}{2}}(x)$ over $\mathbb{F}_{p^f}$ whenever $ax^2 + 2bx + d$ is reducible over $\mathbb{F}_{p^f}$, where the $p_i(x)$'s are irreducible polynomials of degree 2, and α_1, α_2 are zeros of $ax^2 + 2bx + d$ over $\mathbb{F}_p$.*
2. *$f(x) = p_1(x) \cdots p_{\frac{p+1}{2}}(x)$ over $\mathbb{F}_{p^f}$ whenever $ax^2 + 2bx + d$ is irreducible over $\mathbb{F}_{p^f}$, where the $p_i(x)$'s are irreducible polynomials of degree 2.*
3. *$f(x)$ is always reducible over $\mathbb{F}_{p^f}$.*

Proof. By Theorem 1,

$$f(x) = p_0(x)p_1(x) \cdots p_{\frac{p-1}{2}}(x),$$

where $p_i(x) \in \mathbb{F}_p[x]$ have degree 2 for $i = 0, \ldots, \frac{p-1}{2}$. Suppose that $\alpha \in \mathbb{F}_{p^f}$ and $p_0(\alpha) = 0$. Then α is a root of degree at most 2 over $\mathbb{F}_p$. This implies that $\alpha \in \mathbb{F}_{p^2} \cap \mathbb{F}_{p^f}$, and since f is odd, we have $\alpha \in \mathbb{F}_p$. Therefore $0 = f(\alpha) = a\alpha^2 + (b+c)\alpha + d$. Note that any other root of $f(x)$ will also be a root of $ax^2 + (b+c)x + d$. This implies that $f(x)$ has exactly two roots in $\mathbb{F}_p$ and $p_i(x)$ is irreducible over $\mathbb{F}_{p^f}$ for $i = 1, \ldots, \frac{p-1}{2}$. $\square$

Proposition 6. *Let $g(x) = ax^{q+1} + bx^q + cx + d$. If $b \neq c$ and $bc = ad$, then $g(x)$ has exactly two distinct roots.*

Proof. Just note that

$$g(x) = ax^{q+1} + bx^q + cx + d = \left(x + \frac{b}{a}\right)(ax^q + c) = \left(x + \frac{b}{a}\right)(ax + c)^q. \qquad \square$$

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

3. Calculation of $\delta(1, p^i + 1, p^f)$

As we mentioned in the introduction, $\delta(1, d, 2^f)$ has been studied intensively because of the applications to the computation of the covering radius of certain cyclic codes. In particular, $\delta(1, 2^i + 1, 2^f) = 3$ under certain conditions, although the necessary conditions for this are still not known.

In this section we find the necessary and sufficient conditions for $\delta(1, p^i + 1, p^f) = 3$ for any field of characteristic greater than 3. The proof that we present here is elementary and uses a technique introduced in [12].

Theorem 7. *Let $p > 3$. Then the system of polynomial equations*

$$\begin{aligned} x_1 + x_2 + x_3 &= \beta, \\ x_1^{p^i+1} + x_2^{p^i+1} + x_3^{p^i+1} &= \gamma, \end{aligned} \tag{3}$$

has solutions for every $\beta, \gamma \in \mathbb{F}_{p^f}$, if and only if $f \neq 2i$.

Proof. Consider the system

$$\begin{aligned} x_1 + x_2 + x_3 &= \beta_0 x_4, \\ x_1^{p^i+1} + x_2^{p^i+1} + x_3^{p^i+1} &= \gamma_0 x_4^{p^i+1}. \end{aligned} \tag{4}$$

Note that (a, b, c, d), $d \neq 0$, is a solution to system (4) if and only if $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ is a solution to system (3) with $\beta = \beta_0$, $\gamma = \gamma_0$. To prove that system (3) has solutions we will see that system (4) has solutions with $x_4 \neq 0$. For this, consider the system

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1^{p^i+1} + x_2^{p^i+1} + x_3^{p^i+1} &= 0. \end{aligned} \tag{5}$$

The number of solutions of (5) is the number of solutions of $x_1^{p^i+1} + x_2^{p^i+1} + (x_1 + x_2)^{p^i+1} = 0$.

If $x_2 = 0$ then $2x_1^{p^i+1} = 0$, and $x_1 = 0$. Suppose that $x_2 = b \neq 0$. Then $x_1^{p^i+1} + b^{p^i+1} + (x_1 + b)^{p^i+1} = x_1^{p^i+1} + b^{p^i+1} + (x_1 + b)^{p^i}(x_1 + b) = 2x_1^{p^i+1} + bx_1^{p^i} + b^{p^i}x_1 + 2b^{p^i+1} = 0$. This equation is equivalent to $2(\frac{x_1}{b})^{p^i+1} + (\frac{x_1}{b})^{p^i} + (\frac{x_1}{b}) + 2 = 0$ and has the same number of solutions as

$$2z^{p^i+1} + z^{p^i} + z + 2 = 0. \tag{6}$$

Note that the polynomial in this equation is of the type considered in Theorem 1 and therefore it has all its solutions in $\mathbb{F}_{p^{2i}}$. Suppose that N is the number of different solutions of (6) over $\mathbb{F}_{p^f}$. Then the number of solutions of system (5) is $N(p^f - 1) + 1 = Np^f - (N - 1)$. By Moreno–Moreno's theorem (see [14]), we have that $p^{\lceil f/2 \rceil}$ divides the number of solutions of (4).

If $N = 0$, then $(0, 0, 0)$ is the only solution to system (5) and therefore there is only one solution to system (4) with $x_4 = 0$. Since $p^{\lceil f/2 \rceil}$ divides the number of solutions of (4), we must

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

have that this system has solutions with $x_4 \neq 0$, and system (3) has solutions. Suppose that $N = 1$. Then, since $\frac{b}{a} = \frac{1}{2} \in \mathbb{F}_p$, Corollary 2 implies that $b^2 = ad$. Therefore $p = 3$ and this is a contradiction.

For $N > 1$, if we prove that $\operatorname{ord}_p(N-1) < \lceil \frac{f}{2} \rceil$ then the number of solutions of system (4) is not equal to the number of solutions of system (5). This means that system (4) has solutions with $x_4 \neq 0$ and we obtain the desired result.

Since $p > 3$ and the degree of (6) is $p^i + 1$, one has that $\operatorname{ord}_p(N-1) \leqslant i$. Now, if $i < \lceil \frac{f}{2} \rceil$, then $\operatorname{ord}_p(N-1) < \lceil \frac{f}{2} \rceil$ and we are done. We now have to prove that this is also true when $i \geqslant \lceil \frac{f}{2} \rceil$. Suppose that $2i > f$. Without loss of generality, we can assume that $p^i \leqslant p^f - 2$. Hence $i < f < 2i$. Note that all the solutions of (6) over $\mathbb{F}_{p^f}$ are in $\mathbb{F}_{p^k} = \mathbb{F}_{p^f} \cap \mathbb{F}_{p^{2i}}$, where $k = (2i, f)$. Hence, $N \leqslant p^k$. Since $k | f$, we must have that $k \leqslant \frac{f}{2}$ or $k = f$.

If $k \leqslant \frac{f}{2}$, then $N - 1 < p^k \leqslant p^{\lceil f/2 \rceil}$ and we are done. If $k = f$, then $f | 2i$ and one has that $fr = 2i$ for some $r \in \mathbb{Z}$. Since $i < f$, then $ir < fr = 2i$ and hence $r = 1$. This implies that $f = 2i$, which is a contradiction. Hence, for $f \neq 2i$ system (3) has solutions for every $\beta, \gamma \in \mathbb{F}_{p^{2i}}$.

If $f = 2i$, then system (3) does not have solutions for all $\beta, \gamma \in \mathbb{F}_{p^{2i}}$. For example, consider $\gamma \in \mathbb{F}_{p^{2i}} \setminus \mathbb{F}_{p^i}$. Since $(\alpha^{p^i+1})^{p^i-1} = 1$ for $\alpha \in \mathbb{F}^*_{p^{2i}}$, one has that $\alpha^{p^i+1} \in \mathbb{F}_{p^i}$ and $x_1^{p^i+1} + x_2^{p^i+1} + x_3^{p^i+1} = \gamma$ does not have solutions. $\square$

Corollary 8. *Let p be any prime. Then $\delta(1, p^i + 1, p^{2i})$ does not exist.*

Proof. Note that the last argument of the proof of Theorem 7 applies to a similar system with any number of variables. $\square$

Theorem 9. *Suppose that $p > 3$. Then $\delta(1, p^i + 1, p^f) = 3$ if and only if $f \neq 2i$.*

Proof. Consider the system

$$\begin{aligned} x_1 + x_2 &= 0, \\ x_1^{p^i+1} + x_2^{p^i+1} &= \beta. \end{aligned} \tag{7}$$

A solution to this system has to satisfy $x_1^{p^i+1} = \frac{\beta}{2}$, and this does not have a solution for each β. This implies that $\delta(1, p^i + 1, p^f) \geqslant 3$. By the previous theorem $\delta(1, p^i + 1, p^f) = 3$ if and only if $f \neq 2i$. $\square$

For $p = 3$ system (3) does not have a solution for each $\beta, \gamma \in \mathbb{F}_{3^f}$. For example, consider

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1^{3^i+1} + x_2^{3^i+1} + x_3^{3^i+1} &= \beta. \end{aligned} \tag{8}$$

Note that a solution to (8) has to satisfy $\beta = (x_2 + x_3)^{3^i+1} + x_2^{3^i+1} + x_3^{3^i+1} = 2(x_2 + 2x_3)^{3^i+1}$, and this equation does not have a solution for each β.

Proposition 10. $\delta(1, 3^i + 1, 3^f) > 3$.

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

4. Generalizations

One of the possible generalizations of Theorem 7 is to consider a system of two equations with coefficients different from 1 and find conditions on the coefficients so that the system has solutions over $\mathbb{F}_{p^f}$. This is, to find conditions on $a_1, a_2, a_3, b_1, b_2, b_3$ so that

$$\begin{aligned} b_1x_1 + b_2x_2 + b_3x_3 &= \beta, \\ a_1x_1^{p^i+1} + a_2x_2^{p^i+1} + a_3x_3^{p^i+1} &= \gamma, \end{aligned} \tag{9}$$

have solutions over $\mathbb{F}_{p^f}$ for every $\beta, \gamma \in \mathbb{F}_{p^f}$. It is important to note that the results here work for any $\mathbb{F}_{p^f}$ with $p \neq 2$.

Theorem 11. *Suppose that $a_1a_2a_3b_1b_2b_3 \neq 0$, $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_{p^f}$, and $f \neq 2i$. Then, system* (9) *has solutions for every $\beta, \gamma \in \mathbb{F}_{p^f}$ if one of the following conditions hold*:

1. (a) $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_{p^i}$;
   (b) $a_1b_1^{-2}b_2^2 + a_2 = 0$ *and* $a_1b_1^{-2}b_3^2 + a_3 \neq 0$.
2. (a) $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_{p^i}$;
   (b) $a_1b_1^{-2}b_2^2 + a_2 \neq 0$ *and* $a_1b_1^{-2}b_3^2 + a_3 = 0$.
3. $a_1b_1^{-(p^i+1)}b_2^{p^i+1} + a_2 = 0$ *and* $a_1b_1^{-(p^i+1)}b_3^{p^i+1} + a_3 = 0$.
4. (a) $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_{p^i}$;
   (b) $a_1b_1^{-2}b_2^2 + a_2 \neq 0$ *and* $a_1b_1^{-2}b_3^2 + a_3 \neq 0$;
   (c) $a_1b_1^{-2}b_2^2a_3 + a_2a_1b_1^{-2}b_3^2 + a_2a_3 \neq 0$.

Proof. We are going to use the same technique used in the proof of Theorem 7. Consider the system (9) with $\beta = \gamma = 0$.

Then, $x_1 = -b_1^{-1}b_2x_2 - b_1^{-1}b_3x_3$, and we want to compute the number of solutions of

$$\begin{aligned} &a_1\left(b_1^{-1}b_2x_2 + b_1^{-1}b_3x_3\right)^{p^i+1} + a_2x_2^{p^i+1} + a_3x_3^{p^i+1} \\ &\quad = \left(a_1b_1^{-(p^i+1)}b_2^{p^i+1} + a_2\right)x_2^{p^i+1} + a_1b_1^{-(p^i+1)}b_2^{p^i}b_3x_3x_2^{p^i} \\ &\qquad + a_1b_1^{-(p^i+1)}b_2b_3^{p^i}x_3^{p^i}x_2 + \left(a_1b_1^{-(p^i+1)}b_3^{p^i+1} + a_3\right)x_3^{p^i+1} \\ &\quad = 0. \end{aligned} \tag{10}$$

(a) For coefficients satisfying Theorem 4, part (1), we obtain

$$a_1b_1^{-2}b_2b_3x_3x_2^{p^i} + a_1b_1^{-2}b_2b_3x_3^{p^i}x_2 + \left(a_1b_1^{-2}b_3^2 + a_3\right)x_3^{p^i+1} = 0.$$

If $x_2 = 0$, then $x_3 = 0$. If $x_2 = \alpha$, then

$$a_1b_1^{-2}b_2b_3z + a_1b_1^{-2}b_2b_3z^{p^i} + \left(a_1b_1^{-2}b_3^2 + a_3\right)z^{p^i+1} = 0,$$

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

where $z = \frac{x_3}{\alpha}$. The polynomial here has the form $ax^{q+1} + bx^q + bx + d$, the polynomial considered in Theorem 1. Here $\frac{b}{a} \in \mathbb{F}_{p^f}$ and $b^2 = (a_1 b_1^{-2} b_2 b_3)^2 \neq 0 = ad$. Corollary 2 implies that the number of roots of the polynomial is even and the rest of the proof follows the arguments in the proof of Theorem 7.

Q1 (b) The case (2) in Theorem 4 is similar to case (1) of this theorem.

(c) For case (3), we obtain

$$\begin{aligned} &a_1 b_1^{-(p^i+1)} b_2^{p^i} b_3 x_3 x_2^{p^i} + a_1 b_1^{-(p^i+1)} b_2 b_3^{p^i} x_3^{p^i} x_2 \\ &\quad = x_2 x_3 a_1 b_1^{-(p^i+1)} b_2 b_3 \big(b_2^{p^i-1} x_2^{p^i-1} + b_3^{p^i-1} x_3^{p^i-1}\big) \\ &\quad = 0 \end{aligned} \tag{11}$$

So, either $x_2 = 0, x_3 = 0$, or $b_2^{p^i-1} x_2^{p^i-1} + b_3^{p^i-1} x_3^{p^i-1} = 0$. Suppose that $x_2 = a \neq 0$. Then, the number of solutions of $b_2^{p^i-1} x_2^{p^i-1} + b_3^{p^i-1} x_3^{p^i-1} = 0$ with $x_2 \neq 0$ is the number of roots of the polynomial $1 + z^{p^i-1}$ over $\mathbb{F}_{p^f}$, where $z = \frac{b_3 x_3}{a b_2}$, which is 0 or $d = (p^f - 1, p^i - 1) \geqslant 2$. Hence, any solution to (11) will have the form $(0,0), (0,a), (a,0), (a,c)$, where $a \neq 0$ and c is a solution to $1 + z^{p^i-1} = 0$. Therefore, the number of solutions of (11) is either $2p^f - 1$ or $2p^f + dp^f - (d+1)$. Note that any root of $1 + z^{p^i-1}$ over $\mathbb{F}_{p^f}$ is also a root of $z^{p^{2i}-1} - 1$ and therefore is an element in $\mathbb{F}_{p^{2i}} \cap \mathbb{F}_{p^f}$. Divisibility arguments similar to the ones in Theorem 7 imply the desired result.

(d) For case (4), if $x_2 = 0$, then $x_3 = 0$. If $x_2 = \alpha$, then $(a_1 b_1^{-2} b_2^2 + a_2)\alpha^{p^i+1} + a_1 b_1^{-2} b_2 b_3 \times \alpha^{p^i+1} z + a_1 b_1^{-2} b_2 b_3 \alpha^{p^i+1} z^{p^i} + (a_1 b_1^{-2} b_3^2 + a_3)\alpha^{p^i+1} z^{p^i+1} = 0$, where $z = \frac{x_3}{\alpha}$. We divide both sides by α^{p^i+1} to obtain again a polynomial $p(x)$ of the form $ax^{q+1} + bx^q + bx + d$, the polynomial considered in Theorem 1. Since $ad = (a_1 b_1^{-2} b_2 b_3)^2 + a_1 b_1^{-2} b_2^2 a_3 + a_2 a_1 b_1^{-2} b_3^2 + a_2 a_3$ and $a_1 b_1^{-2} b_2^2 a_3 + a_2 a_1 b_1^{-2} b_3^2 + a_2 a_3 \neq 0$, we have that $ad \neq (a_1 b_1^{-2} b_2 b_3)^2 = b^2$. Again, by Corollary 2, the number of roots of the polynomial $p(x)$ is even, and the rest of the proof follow the arguments of the proof of Theorem 7. □

Q2 **Example 1.** Using part (1) of Theorem 4, we obtain that the system

$$\begin{aligned} x_1 + x_2 + x_3 &= \beta, \\ a_1 x_1^{p^i+1} - a_1 x_2^{p^i+1} + a_3 x_3^{p^i+1} &= \gamma, \end{aligned} \tag{12}$$

has at least one solution for every $\beta, \gamma \in \mathbb{F}_{p^f}$, whenever $f \neq 2i$, $a_1, a_2, a_3 \in \mathbb{F}_{p^i}$, and $a_3 \neq -a_1$.

Theorem 12. *Suppose that $a_1, a_2, a_3, b_1, b_2 \in \mathbb{F}_{p^f} \cap \mathbb{F}_{p^i}$ and $f \neq 2i$. Then, the system of polynomial equations*

$$\begin{aligned} b_1 x_1 + b_2 x_2 &= \beta, \\ a_1 x_1^{p^i+1} + a_2 x_2^{p^i+1} + a_3 x_3^{p^i+1} &= \gamma, \end{aligned} \tag{13}$$

has at least one solution for every $\gamma, \beta \in \mathbb{F}_{p^f}$ if $a_1(-b_2 b_1^{-1})^2 + a_2 \neq 0$ and $a_3 \neq 0$.

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008

Proof. Again, we will use the same technique used in the proof of Theorem 7. Consider the system (13) with $\beta = \gamma = 0$. Then $x_1 = -b_2 b_1^{-1} x_2$ and we want to compute the number of solutions of

$$\left(a_1\left(-b_2 b_1^{-1}\right)^2 + a_2\right)x_2^{p^i+1} + a_3 x_3^{p^i+1} = 0.$$

Suppose that $a_1(-b_2 b_1^{-1})^2 + a_2 \neq 0$. If $x_2 = 0$, then $x_3 = 0$. If $x_2 = \alpha \neq 0$, then we need to compute the number of solutions of $d + a_3 x_3^{p^i+1} = 0$, where $d = (a_1(-b_2 b_1^{-1})^2 + a_2)\alpha^{p^i+1} \neq 0$. The polynomial here has the form $ax^{q+1} + bx^q + bx + d$, the polynomial considered in Theorem 1. Here $\frac{b}{a} = 0 \in \mathbb{F}_{p^f}$ and $b^2 = 0 \neq a_3 d = ad$. Corollary 2 implies that the number of roots is even and the rest of the proof follow the arguments in the proof of Theorem 7. □

Uncited references

Q3

[11] [16]

Acknowledgments

The authors appreciate the careful review, corrections and helpful suggestions to this paper made by Dr. Arne Winterhof and the referees. The work of I. Rubio was partially supported by the National Security Agency, Grant Number H98230-04-C-0486.

References

[1] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 1 (1998) 125–156.
[2] A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, IEEE Trans. Inform. Theory 46 (2000) 4–8.
[3] L. Carlitz, Some applications of a theorem of Chevalley, Duke Math. J. 18 (1951) 811–819.
[4] E. Cohen, Simultaneous pairs of linear and quadratic equations in Galois field, Canad. J. Math. 9 (1957) 74–78.
[5] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inform. Theory 14 (1968) 154–156.
[6] H. Janwa, R.M. Wilson, Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in characteristic 2 and some applications to cyclic codes, in: G. Cohen, T. Mora, O. Moreno (Eds.), Proc. AAECC-10, in: Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 180–194.
[7] B.Zh. Kamaletdinov, The number of solutions of a system of linear quadratic equations in Galois fields of characteristic 2, Mat. Zametki 3 (1986) 325–330.
[8] T. Kasami, The weight enumerators for several classes of subcodes of second order binary Reed–Muller codes, IEEE Trans. Inform. Theory 18 (1971) 369–394.
[9] M.P. Knapp, Systems of diagonal equations over p-adic fields, J. London Math. Soc. 63 (2001) 257–267.
[10] S.V. Konyagin, Estimates for Gaussian sums and Waring's problem modulo a prime, Tr. Mat. Inst. Steklova 198 (1992) 111–124 (in Russian); English transl.: Proc. Steklov Inst. Math. 1 (1994) 105–117.
[11] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, Reading, MA, 1984.
[12] O. Moreno, F.N. Castro, Divisibility properties for covering radius of certain cyclic codes, IEEE Trans. Inform. Theory 49 (2003) 3299–3303.
[13] O. Moreno, F.N. Castro, On the covering radius of certain cyclic codes, in: Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Springer, Berlin, 2003, pp. 129–138.
[14] O. Moreno, C.J. Moreno, Improvements of the Chevalley–Warning and the Ax–Katz theorems, Amer. J. Math. 117 (1995) 241–244.
[15] K. Nyberg, Differentially uniform mappings for cryptography, in: T. Helleseth (Ed.), Advances in Cryptology—EUROCRYPT'93, in: Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55–64.

[16] S.H. Schanuel, An extension of Chevalley's theorem to congruence modulo prime powers, J. Number Theory 6 (1974) 284–290.
[17] C. Small, Waring's problem mod n, Amer. Math. Monthly 84 (1977) 12–25.
[18] A. Tietäväinen, On systems of linear and quadratic equations in finite fields, Ann. Acad. Sci. Fenn. Ser. A 382 (1965).
Q4 [19] R.C. Vaughan, T.D. Wooley, Waring's problem: A survey, in: Number Theory for the Millennium III, A K Peters, Wellesley, MA, 2002.
[20] A. Winterhof, On Waring's problem in finite fields, Acta Arith. 87 (2) (1998) 171–177.

Please cite this article in press as: F.N. Castro et al., On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.09.008