On the exact number of solutions of certain linearized equations

Ferruh Özbudak

Department of Mathematics and Institute of Applied Mathematics,
METU, Ankara, Turkey.

*joint work with Zülfükar Saygı

** This work is supported by TÜBİTAK TBAG–109T672 and TBAG–109T344.

18 April 2013

Outline

- Notations
- Motivation of the work
- Main Result
- Application
- Remarks

Notations

- p be an odd prime,
- n, k be positive integers,
- $\mathbb{F}_q$ be a finite field with q elements, where $q = p^k$,
- We set $e = \gcd(n, k)$, $n_1 = n/e$, $q_1 = p^e$ and $q_2 = p^{nk/e}$,
- Norm be the relative norm map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{q_1}$, where (that is, $\mathrm{Norm}(x) = x^{\frac{p^n-1}{q_1-1}}$ for any $x \in \mathbb{F}_{p^n}$).

Extensions of $\mathbb{F}_{q_1}$

We work on the following extensions of $\mathbb{F}_{q_1}$:

$$\begin{tikzcd}
 & F_{p^{\frac{nk}{e}}} = F_{q_2} \arrow[dl, dash] \arrow[dr, dash, "\frac{n}{e}"] & \\
F_{p^n} \arrow[dr, dash, "\frac{n}{e}"'] & & F_{p^k} = F_q \arrow[dl, dash] \\
 & F_{p^e} = F_{q_1} &
\end{tikzcd}$$

Motivation

Lemma (Trachtenberg)

Let r,s, and t be pairwise relatively prime. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$, $m \leq s$, *be a set of elements of* $\mathbb{F}_{p^{rs}}$ *which are linearly independent over* $\mathbb{F}_{p^r}$. *Then* $\sigma_1, \sigma_2, \ldots, \sigma_m$ *are linearly independent over* $\mathbb{F}_{p^{rt}}$.

Lemma

Let $\mathcal{B} \subseteq \mathbb{F}_{p^n}$ *be a non-empty set. If* $\mathcal{B}$ *is linearly independent over* $\mathbb{F}_{q_1}$, *then* $\mathcal{B}$ *is also linearly independent over* $\mathbb{F}_q$.

- Our lemma is a stronger version of the Trachtenberg's lemma.

Motivation

Lemma (Trachtenberg)

Let r,s, and t be pairwise relatively prime. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$*,* $m \leq s$*, be a set of elements of* $\mathbb{F}_{p^{rs}}$ *which are linearly independent over* $\mathbb{F}_{p^r}$*. Then* $\sigma_1, \sigma_2, \ldots, \sigma_m$ *are linearly independent over* $\mathbb{F}_{p^{rt}}$*.*

Lemma

Let $\mathcal{B} \subseteq \mathbb{F}_{p^n}$ *be a non-empty set. If* $\mathcal{B}$ *is linearly independent over* $\mathbb{F}_{q_1}$*, then* $\mathcal{B}$ *is also linearly independent over* $\mathbb{F}_q$*.*

- Our lemma is a stronger version of the Trachtenberg's lemma.

Motivation

- It is possible to decide the number of solutions of certain linearized equations using our lemma.
- But, it is not easy to find the exact number of solutions of that equation.
- In many cases we can easily find the exact number of solutions of linearized equations depending on the *coefficients of that equation*.

A Useful Result

Proposition

Let $\alpha \in \mathbb{F}_{p^n} \setminus \{0\}$ *and* $N(\alpha)$ *denote the number of* $z \in \mathbb{F}_{p^n}$ *such that*

$$z^q - \alpha z = 0.$$

Let ψ_α *be the map on* $\mathbb{F}_{p^n}$ *given by*

$$\begin{array}{rccc} \psi_\alpha : & \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ & x & \longmapsto & x^q - \alpha x. \end{array}$$

Then we have

$$N(\alpha) = \begin{cases} 1, & \textit{if} \quad \mathrm{Norm}(\alpha) \neq 1, \\ q_1, & \textit{if} \quad \mathrm{Norm}(\alpha) = 1. \end{cases}$$

A Useful Result

Proposition

Let $\alpha \in \mathbb{F}_{p^n} \setminus \{0\}$ *and* $N(\alpha)$ *denote the number of* $z \in \mathbb{F}_{p^n}$ *such that*

$$z^q - \alpha z = 0.$$

Let ψ_α *be the map on* $\mathbb{F}_{p^n}$ *given by*

$$\begin{array}{rccc} \psi_\alpha : & \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ & x & \longmapsto & x^q - \alpha x. \end{array}$$

Then we have

$$N(\alpha) = \begin{cases} 1, & \textit{if} \quad \mathrm{Norm}(\alpha) \neq 1, \\ q_1, & \textit{if} \quad \mathrm{Norm}(\alpha) = 1. \end{cases}$$

A Useful Result Cont.

Proposition continued

Let $A_\alpha(T) \in \mathbb{F}_{p^n}[T]$ *be the* $\mathbb{F}_{q_1}$*-linearized polynomial given by*

$$\begin{aligned} A_\alpha(T) \; = \; & T^{q_1^{n_1-1}} + \alpha^{q_1^{n_1-1}} T^{q_1^{n_1-2}} + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}} T^{q_1^{n_1-3}} \\ & + \cdots + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}+\cdots+q_1^2} T^{q_1} + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}+\cdots+q_1} T. \end{aligned} \quad (1)$$

If $\mathrm{Norm}(\alpha) = 1$*, then we also have the followings:*

1. $\mathrm{Ker}\psi_\alpha$ *is the roots of the polynomial* $T^{q_1} - \alpha T$ *over* $\mathbb{F}_{p^n}$*. This polynomial is separable and splits over* $\mathbb{F}_{p^n}$*.*
2. $\mathrm{Im}\psi_\alpha$ *is the roots of the polynomial* $A_\alpha(T)$*. This polynomial is separable and splits over* $\mathbb{F}_{p^n}$*.*

A Useful Result Cont.

Proposition continued

Let $A_\alpha(T) \in \mathbb{F}_{p^n}[T]$ *be the* $\mathbb{F}_{q_1}$*-linearized polynomial given by*

$$\begin{aligned} A_\alpha(T) &= T^{q_1^{n_1-1}} + \alpha^{q_1^{n_1-1}} T^{q_1^{n_1-2}} + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}} T^{q_1^{n_1-3}} \\ &\quad + \cdots + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}+\cdots+q_1^2} T^{q_1} + \alpha^{q_1^{n_1-1}+q_1^{n_1-2}+\cdots+q_1} T. \end{aligned} \tag{1}$$

If $\mathrm{Norm}(\alpha) = 1$*, then we also have the followings:*

1. $\mathrm{Ker}\psi_\alpha$ *is the roots of the polynomial* $T^{q_1} - \alpha T$ *over* $\mathbb{F}_{p^n}$*. This polynomial is separable and splits over* $\mathbb{F}_{p^n}$*.*
2. $\mathrm{Im}\psi_\alpha$ *is the roots of the polynomial* $A_\alpha(T)$*. This polynomial is separable and splits over* $\mathbb{F}_{p^n}$*.*

Main Result

Theorem

Let α, β be nonzero elements of $\mathbb{F}_{p^n}$. Let $N(\alpha,\beta)$ denote the number of $z \in \mathbb{F}_{p^n}$ such that

$$(z^q - \alpha z) \circ (z^q - \beta z) = z^{q^2} - (\alpha + \beta^q)\, z^q + \alpha\beta z = 0.$$

Let $C_{\alpha,\beta}$ denote the constant in $\mathbb{F}_{p^n}$ defined as

$$C_{\alpha,\beta} = \frac{1}{\beta} + \frac{\alpha}{\beta^{q_1+1}} + \frac{\alpha^{q_1+1}}{\beta^{q_1^2+q_1+1}} + \cdots + \frac{\alpha^{q_1^{n_1-3}+\cdots+q_1+1}}{\beta^{q_1^{n_1-2}+\cdots+q_1+1}} + \alpha^{q_1^{n_1-2}+\cdots+q_1+1}.$$

Then $N(\alpha,\beta) \in \{1, q_1, q_1^2\}$. Moreover we have the followings:

1. $N(\alpha,\beta) = 1$ *if and only if* $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
2. $N(\alpha,\beta) = q_1$ *if and only if one of the followings hold:*
    1. $\mathrm{Norm}(\alpha) = 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
    2. $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) = 1$.
    3. $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} \neq 0$.
3. $N(\alpha,\beta) = q_1^2$ *if and only if* $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} = 0$.

Main Result

Theorem

Let α, β *be nonzero elements of* $\mathbb{F}_{p^n}$. *Let* $N(\alpha,\beta)$ *denote the number of* $z \in \mathbb{F}_{p^n}$ *such that*

$$(z^q - \alpha z) \circ (z^q - \beta z) = z^{q^2} - (\alpha + \beta^q)\, z^q + \alpha\beta z = 0.$$

Let $C_{\alpha,\beta}$ *denote the constant in* $\mathbb{F}_{p^n}$ *defined as*

$$C_{\alpha,\beta} = \frac{1}{\beta} + \frac{\alpha}{\beta^{q_1+1}} + \frac{\alpha^{q_1+1}}{\beta^{q_1^2+q_1+1}} + \cdots + \frac{\alpha^{q_1^{n_1-3}+\cdots+q_1+1}}{\beta^{q_1^{n_1-2}+\cdots+q_1+1}} + \alpha^{q_1^{n_1-2}+\cdots+q_1+1}.$$

Then $N(\alpha,\beta) \in \{1, q_1, q_1^2\}$. *Moreover we have the followings:*

1. $N(\alpha,\beta) = 1$ *if and only if* $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
2. $N(\alpha,\beta) = q_1$ *if and only if one of the followings hold:*
    1. $\mathrm{Norm}(\alpha) = 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
    2. $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) = 1$.
    3. $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} \neq 0$.
3. $N(\alpha,\beta) = q_1^2$ *if and only if* $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} = 0$.

Main Result

Theorem

Let α, β be nonzero elements of $\mathbb{F}_{p^n}$. Let $N(\alpha, \beta)$ denote the number of $z \in \mathbb{F}_{p^n}$ such that

$$(z^q - \alpha z) \circ (z^q - \beta z) = z^{q^2} - (\alpha + \beta^q) z^q + \alpha\beta z = 0.$$

Let $C_{\alpha,\beta}$ denote the constant in $\mathbb{F}_{p^n}$ defined as

$$C_{\alpha,\beta} = \frac{1}{\beta} + \frac{\alpha}{\beta^{q_1+1}} + \frac{\alpha^{q_1+1}}{\beta^{q_1^2+q_1+1}} + \cdots + \frac{\alpha^{q_1^{n_1-3}+\cdots+q_1+1}}{\beta^{q_1^{n_1-2}+\cdots+q_1+1}} + \alpha^{q_1^{n_1-2}+\cdots+q_1+1}.$$

Then $N(\alpha, \beta) \in \{1, q_1, q_1^2\}$. Moreover we have the followings:

1. *$N(\alpha, \beta) = 1$ if and only if $\mathrm{Norm}(\alpha) \neq 1$ and $\mathrm{Norm}(\beta) \neq 1$.*
2. *$N(\alpha, \beta) = q_1$ if and only if one of the followings hold:*
   1. *$\mathrm{Norm}(\alpha) = 1$ and $\mathrm{Norm}(\beta) \neq 1$.*
   2. *$\mathrm{Norm}(\alpha) \neq 1$ and $\mathrm{Norm}(\beta) = 1$.*
   3. *$\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ and $C_{\alpha,\beta} \neq 0$.*
3. *$N(\alpha, \beta) = q_1^2$ if and only if $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ and $C_{\alpha,\beta} = 0$.*

Main Result

Theorem

Let α, β be nonzero elements of $\mathbb{F}_{p^n}$. Let $N(\alpha,\beta)$ denote the number of $z \in \mathbb{F}_{p^n}$ such that

$$(z^q - \alpha z) \circ (z^q - \beta z) = z^{q^2} - (\alpha + \beta^q)\, z^q + \alpha\beta z = 0.$$

Let $C_{\alpha,\beta}$ denote the constant in $\mathbb{F}_{p^n}$ defined as

$$C_{\alpha,\beta} = \frac{1}{\beta} + \frac{\alpha}{\beta^{q_1+1}} + \frac{\alpha^{q_1+1}}{\beta^{q_1^2+q_1+1}} + \cdots + \frac{\alpha^{q_1^{n_1-3}+\cdots+q_1+1}}{\beta^{q_1^{n_1-2}+\cdots+q_1+1}} + \alpha^{q_1^{n_1-2}+\cdots+q_1+1}.$$

Then $N(\alpha,\beta) \in \{1, q_1, q_1^2\}$. Moreover we have the followings:

1. $N(\alpha,\beta) = 1$ *if and only if* $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
2. $N(\alpha,\beta) = q_1$ *if and only if one of the followings hold:*
    1. $\mathrm{Norm}(\alpha) = 1$ *and* $\mathrm{Norm}(\beta) \neq 1$.
    2. $\mathrm{Norm}(\alpha) \neq 1$ *and* $\mathrm{Norm}(\beta) = 1$.
    3. $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} \neq 0$.
3. $N(\alpha,\beta) = q_1^2$ *if and only if* $\mathrm{Norm}(\alpha) = \mathrm{Norm}(\beta) = 1$ *and* $C_{\alpha,\beta} = 0$.

More results

Proposition

Let $m \geq 2$ be an integer. Let

$$A(T) = T^{q^m} + A_{m-1}T^{q^{m-1}} + \cdots + A_1 T^q + A_0 T \in \mathbb{F}_{p^n}[T]$$

be an $\mathbb{F}_q$-linearized polynomial with $A_0 \neq 0$.
If there exists $\eta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that $A(\eta) = 0$, then there exist $\beta \in \mathbb{F}_{p^n} \setminus \{0\}$ and $\mathbb{F}_q$-linearized monic and separable polynomial $B(T) \in \mathbb{F}_{p^n}[T]$ such that

$$A(T) = B(T) \circ (T^q - \beta T).$$

- This result is well known if $k \mid n$.
- It is a slight extension, including the case $k \nmid n$ as well.

A Remark

Let $a, b \in \mathbb{F}_{p^n} \setminus \{0\}$. Let N denote the number of $z \in \mathbb{F}_{p^n}$ s.t.

$$z^{q^2} + az^q + bz = 0.$$

- The main problem is to compute N explicitly.
- This problem is now reduced to a "factorization" problem in the following sense:
  - If there exist $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that

    $$z^{q^2} + az^q + bz = (z^q - \alpha z) \circ (z^q - \beta z), \qquad (2)$$

    then N is computed explicitly using our Theorem as $N = N(\alpha, \beta)$.
  - If there is no $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that (2) holds, then $N = 1$ by our Proposition.

A Remark

Let $a, b \in \mathbb{F}_{p^n} \setminus \{0\}$. Let N denote the number of $z \in \mathbb{F}_{p^n}$ s.t.

$$z^{q^2} + az^q + bz = 0.$$

- The main problem is to compute N explicitly.
- This problem is now reduced to a "factorization" problem in the following sense:
  - If there exist $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that

    $$z^{q^2} + az^q + bz = (z^q - \alpha z) \circ (z^q - \beta z), \tag{2}$$

    then N is computed explicitly using our Theorem as $N = N(\alpha, \beta)$.
  - If there is no $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that (2) holds, then $N = 1$ by our Proposition.

A Remark

Let $a, b \in \mathbb{F}_{p^n} \setminus \{0\}$. Let N denote the number of $z \in \mathbb{F}_{p^n}$ s.t.

$$z^{q^2} + az^q + bz = 0.$$

- The main problem is to compute N explicitly.
- This problem is now reduced to a "factorization" problem in the following sense:
    - If there exist $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that

      $$z^{q^2} + az^q + bz = (z^q - \alpha z) \circ (z^q - \beta z), \tag{2}$$

      then N is computed explicitly using our Theorem as $N = N(\alpha, \beta)$.
    - If there is no $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that (2) holds, then $N = 1$ by our Proposition.

An example

Example

Let $p = 3$, $n = 3$, $k = 1$ and
γ be a primitive element in $\mathbb{F}_{3^3}$, s.t.$\gamma^3 + 2\gamma + 1 = 0$.
Then by computer search we see that

$$z^9 + \gamma^7 z^3 + z$$

can not be written of the form $\left(z^3 - \alpha z\right) \circ \left(z^3 - \beta z\right)$ for all $\alpha, \beta \in \mathbb{F}_{3^3} \setminus \{0\}$.

A connection of the factorization problem above with a result of Bluher

- We want to find $\alpha, \beta \in \mathbb{F}_{p^n} \setminus \{0\}$ such that

$$\begin{aligned} z^{q^2} + az^q + bz &= (z^q - \alpha z) \circ (z^q - \beta z) \\ &= z^{q^2} - (\alpha + \beta^q)\, z^q + \alpha\beta z, \end{aligned}$$

which means that

$$a = \alpha + \beta^q \text{ and } b = \alpha\beta.$$

- Then by substituting $\alpha = b/\beta$ in the first equality

$$a = \frac{b}{\beta} + \beta^q.$$

- That is, β is a solution of the equation

$$0 = x^{q+1} - ax + b \in \mathbb{F}_{p^n}[x].$$

A result of Trachtenberg

Proposition (Trachtenberg)

Let γ be a nonzero element of $\mathbb{F}_{p^n}$ where p is prime and n is odd. Then the equation

$$z^{p^{4m}} - (2\gamma)^{p^{2m}} z^{p^{2m}} + z = 0 \quad (3)$$

has exactly 1, p^e, or p^{2e} roots in $\mathbb{F}_{p^n}$, where $e = gcd(m, n)$.

- Remark that using our Theorem and Proposition it possible to find the exact number of roots of (3) depending on γ. Note that $k = 2m$ in our notation.

More equations

Now, it is possible to find the exact number of solutions of the following linearized equations depending on the coefficients of that equation.

$$z^{q^3} + az^{q^2} + bz^q + cz = 0. \tag{4}$$

- The problem of finding the exact number of solutions of (4) can be reduced to a "factorization" problem.
- Note that using Trachtenberg's Lemma the number of solutions of (4) is in the set $\{1, q_1, q_1^2, q_1^3\}$.
- But in many cases depending on the coefficients of the equations, the number of solutions of (4) will not take all the values in the set $\{1, q_1, q_1^2, q_1^3\}$.

A result of Trachtenberg

Proposition

Let γ be a nonzero element of $\mathbb{F}_{p^n}$ where p is an odd prime and n is odd. Then the equation

$$z^{p^{6m}} - \gamma^{p^{3m}} z^{p^{4m}} - \gamma^{p^{2m}} z^{p^{2m}} + z = 0 \tag{5}$$

has exactly 1, p^e, or p^{2e} roots in $\mathbb{F}_{p^n}$, where $e = \gcd(m, n)$.

- The proof of the proposition is suggested by L. Welch.
- The equation (5) is of the form
  $0 = z^{q^3} + b^{p^{(k/2)}} z^{q^2} + bz^q + z \in \mathbb{F}_{p^n}[z] \quad (k = 2m)$.

Remarks on the last result

$$z^{p^{6m}} - \gamma^{p^{3m}} z^{p^{4m}} - \gamma^{p^{2m}} z^{p^{2m}} + z = 0 \tag{6}$$

- If the equation (6) has a nonzero root then

  $$z^{q^3} + b^{p^{(k/2)}} z^{q^2} + bz^q + z = (z^q - \alpha_1 z) \circ (z^q - \alpha_2 z) \circ (z^q - \alpha_3 z)$$

  for some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{p^n}$.
- Using this observation it is proved that the equation (6) can not have q_1^3 solutions in $\mathbb{F}_{p^n}$.
- Furthermore, using similar techniques as in our Theorem it is possible to make further improvements depending on the values of α_1, α_2 and α_3.

Thank you for your attention...