ISSN 2451-7100

S-MINIMAL VALUE SET POLYNOMIALS AND AN IDENTITY OF LENSTRA

By

Ricardo Toledano

IMAL PREPRINT # 2014-0026

Publication date: December 29, 2014

Editorial: Instituto de Matemática Aplicada del Litoral
IMAL (CCT CONICET Santa Fe – UNL)
http://www.imal.santafe-conicet.gov.ar

Publications Director: Dr. Rubén Spies
E-mail: rspies@santafe-conicet.gov.ar

ISSN 2451-7100
IMAL PREPRINT # 2014-0026 Publication date: December 29, 2014

S-MINIMAL VALUE SET POLYNOMIALS AND AN IDENTITY OF LENSTRA

R. TOLEDANO

Abstract. In this paper we prove a new identity satisfied by a family of polynomials defined by Garcia, Stichtenoth and Thomas in their work on good recursive tame towers. We also generalize the notion of minimal value set polynomials and we prove that this family of polynomials is an example of this generalization.

1. Introduction

Garcia, Stichtenoth and Thomas studied in [2] a class of tame towers over a finite field $\mathbb{F}_q$ with $q \equiv 1 \mod m$ recursively defined by an equation of the form

$$y^m = x^d f(x)\,, \tag{1}$$

where $f(x)$ is a polynomial of degree $m-d$ such that $f(0) \neq 0$, $\gcd(d,m)=1$ and its leading coefficient is an mth-power in $\mathbb{F}_q$. The authors showed that these towers always have positive splitting rate and assuming the existence of a finite subset S of an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ such that $0 \in S$ and

$$\{\alpha \in \overline{\mathbb{F}}_q \,:\, \alpha^d f(\alpha) = \beta^m\} \subset S\,,$$

for any $\beta \in S$, the good asymptotic behavior of such towers can be deduced together with a concrete non trivial lower bound for their limit. Condition (2) imposes serious restrictions on the polynomial f in (1) and little is known on the nature of these restrictions. H. Lenstra Jr. showed in [3] that in the case of an equation of the form (1) over a prime field $\mathbb{F}_p$, there is not such a set $S \subset \overline{\mathbb{F}}_p$ satisfying (2). This situation suggest that it is an interesting problem to understand how the existence of such a set S shapes the structure of equation (1) and what kind of restrictions imposes on the roots and coefficients of f when the associated tower is asymptotically good.

In view of the above result of Garcia, Stichtenoth and Thomas it will be convenient to work with the following definitions. We shall say that a polynomial f of degree $m > 1$ over $\mathbb{F}_q$ is a *GST-polynomial* if it is of the form $f(x) = x^d h(x)$ where $h(0) \neq 0$ and $\gcd(d,m)=1$.

ISSN 2451-7100
IMAL PREPRINT # 2014-0026 Publication date: December 29, 2014

Let f be a polynomial over $\mathbb{F}_q$. We shall say that a finite set $S \subset \overline{\mathbb{F}}_q$ has the *root absorbent property* with respect to f if

$$\{\alpha \in \overline{\mathbb{F}}_q \,:\, f(\alpha) = \beta^m\} \subset S\,, \tag{2}$$

for any $\beta \in S$. The key property used by Lenstra in [3] is a polynomial identity which holds for GST-polynomials over $\mathbb{F}_q$ with $q \equiv 1 \mod m$ and for which there exists a finite set $S \subset \overline{\mathbb{F}}_q$ satisfying the root absorbent property with respect to f. More precisely let

$$V_{x^m}^S = \{\alpha^m \,:\, \alpha \in S\}\,,$$

be the value set of x^m restricted to S (if $S = \mathbb{F}_q$ it is customary to simply write V_{x^m}) and suppose that f is a GST-polynomial satisfying the root absorbent property (2) for some finite set $S \subset \overline{\mathbb{F}}_q$ such that $0 \in S$. Let us consider the polynomial

$$g(x) = \prod_{\gamma \in V_{x^m}^S} (x - \gamma)\,,$$

then the following identity

$$dx^{m-1} g(f(x)) = f'(x) g(x^m) \quad \text{(Lenstra's identity)} \tag{3}$$

holds as polynomials over some $\mathbb{F}_{q^r}$. The goal of this work is to prove that GST-polynomials for which there exists a finite set $S \subset \overline{\mathbb{F}}_q$ having the root absorbent property are minimal value set polynomials in some precise way defined in Section 3.

2. Another identity

We prove in this section a polynomial identity satisfied by a certain class of polynomials. This result will be used in our main result proven in the next section.

Proposition 1. *Let f be a GST-polynomial over $\mathbb{F}_q$ for which the root absorbent property (2) holds for some finite set $S \subset \overline{\mathbb{F}}_q$ with $0 \in S$. Consider the polynomials over $\mathbb{F}_q$*

$$g(x) = \prod_{\gamma \in V_{x^m}^S} (x - \gamma) \quad \textit{and} \quad H(x) = \prod_{\alpha \in S} (x - \alpha)\,.$$

Then there exists $\lambda \in \mathbb{F}_q$ such that the following identity holds

$$d\, g(f(x)) = m\lambda\, H(x) f'(x) \tag{4}$$

as polynomials over some $\mathbb{F}_{q^r}$.

ISSN 2451-7100
IMAL PREPRINT # 2014-0026 Publication date: December 29, 2014

Proof. Let $\gamma \in V_{x^m}^S$ and suppose that $\alpha^m = \gamma$ (in other words, suppose that $g(\alpha^m) = 0$). If $\alpha = 0$ then $\alpha \in S$. If $\alpha \neq 0$, by (3), we must have that $f(\alpha) = \delta$ for some $\delta \in V_{x^m}^S$. From the root absorbent property of S with respecto to f we conclude that $\alpha \in S$. Thus if $S' = \mathbb{F}_q \setminus S$ we see that

$$V_{x^m} = V_{x^m}^S \cup V_{x^m}^{S'} \quad \text{with} \quad V_{x^m}^S \cap V_{x^m}^{S'} = \emptyset\,. \tag{5}$$

Then

$$\prod_{\gamma \in V_{x^m}} (x^m - \gamma) = g(x^m) r(x^m)\,,$$

where

$$r(x) = \prod_{\gamma \in V_{x^m}^{S'}} (x - \gamma)\,,$$

Consider now the polynomial over $\mathbb{F}_q$

$$G(x) = \prod_{\alpha \in S'} (x - \alpha)\,.$$

Since $\mathbb{F}_q = S \cup S'$ and $S \cap S' = \emptyset$ then

$$x^q - x = H(x) G(x)\,.$$

It is well known that x^m is a minimal value set polynomial (MVSP) when $q \equiv 1 \mod m$. Then from Theorem 3.1 in [1] we have that there exists $\theta \in \mathbb{F}_q^*$ such that

$$\prod_{\gamma \in V_{x^m}} (x^m - \gamma) = m\theta (x^q - x) x^{m-1}\,.$$

Therefore

$$g(x^m) r(x^m) = m\theta H(x) G(x) x^{m-1}\,. \tag{6}$$

Suppose that $G(\alpha) = 0$. Then $\alpha \in S'$ and since $g(\alpha^m) \neq 0$ (otherwise $\alpha \in S$ as we have seen right before (5)) we must have that $r(\alpha^m) = 0$. Then $G(x)$ divides $r(x^m)$.

Suppose now that $r(\alpha^m) = 0$. Then there exists $\gamma \in V_{x^m}^{S'}$ such that $\alpha^m = \gamma$ and by (5) we see that $\alpha \notin S$. Therefore either $G(\alpha) = 0$ or $\alpha^{m-1} = 0$. The latter implies that $\alpha = 0$ and $0 \in S$ by definition and this is a contradiction. Thus $G(\alpha) = 0$ so that $r(x^m)$ divides $G(x)$. Therefore there exists $\eta \in \mathbb{F}_q^*$ such that

$$r(x^m) = \eta\, G(x)\,.$$

If we use this in (6) we see that there exists $\lambda \in \mathbb{F}_q^*$ such that

$$g(x^m) = m\lambda H(x) x^{m-1} \tag{7}$$

From the above identity and Lenstra's identity we have that (4) holds. □

ISSN 2451-7100
IMAL PREPRINT # 2014-0026 Publication date: December 29, 2014

3. S-Minimal value set polynomials

Let $\emptyset \neq S \subset \mathbb{F}_q$ and let $f \in \mathbb{F}_q[x]$ a polynomial of degree n. The S-value set of f is defined as

$$V_f^S = \{f(\alpha) \,:\, \alpha \in S\}\,.$$

When $S = \mathbb{F}_q$ it is customary to simply write V_f and this set is called the value set of f. Notice that

$$S = \cup_{\gamma \in V_f^S} (f^{-1}(\gamma) \cap S)$$

and this union is a disjoint union of sets. Then

$$|S| = \sum_{\gamma \in V_f^S} |f^{-1}(\gamma) \cap S| \leq n\, |V_f^S|$$

so that

$$|V_f^S| \geq \frac{|S|}{n}$$

We shall say that f is an *S-minimal value set polynomial* (S-MVSP) if the following equality holds:

$$|V_f^S| = \left\lceil \frac{|S|}{n} \right\rceil$$

When $S = \mathbb{F}_q$ an S-MVSP is clearly a MVSP.

Proposition 2. *Let S and Ω be non empty subsets of $\mathbb{F}_q$ and let us consider the polynomials over $\mathbb{F}_q$*

$$g(x) = \prod_{\gamma \in \Omega} (x - \gamma) \quad \textit{and} \quad H(x) = \prod_{\alpha \in S} (x - \alpha)\,.$$

If the polynomial identity

$$g(f(x)) = \theta\, H(x) f'(x)\,, \tag{8}$$

holds for some $\theta \in \mathbb{F}_q^*$ then f is an S-MVSP with $V_f^S = \Omega$.

Proof. We follow the same argument given in Theorem 3.1 of [1]. Let $\alpha \in S$. By (8) we have that $g(f(\alpha)) = 0$. Then there exists $\gamma \in \Omega$ such that $f(\alpha) = \gamma$. Thus $V_f^S \subset \Omega$ and so $|V_f^S| \leq |\Omega|$.

On the other hand $\deg g = n\, |\Omega|$ and

$$\deg H(x) f'(x) = |S| + \deg f'(x) \leq |S| + n - 1$$

Hence

$$n\, |\Omega| \leq |S| + n - 1$$

so that

$$|\Omega| - 1 \leq \frac{|S| - 1}{n}$$

ISSN 2451-7100
IMAL PREPRINT # 2014-0026 Publication date: December 29, 2014

Putting all together we have that

$$|V_f^S| \leq |\Omega| \leq \left\lfloor \frac{|S|-1}{n} \right\rfloor + 1 \leq \left\lceil \frac{|S|}{n} \right\rceil \leq |V_f^S| \,.$$

Therefore

$$|V_f^S| = \left\lceil \frac{|S|}{n} \right\rceil = \Omega \,,$$

as desired. □

Now we can prove our main result.

Theorem 3. *Let f be a GST-polynomial over $\mathbb{F}_q$ for which the root absorbent property* (2) *holds for some finite set $S \subset \overline{\mathbb{F}}_q$ with $0 \in S$. Then f is an S-MVSP and $V_f^S = V_{x^m}^S$.*

Proof. By Proposition 1 we have that the identity (4) holds for some $\lambda \in \mathbb{F}_q^*$ and this can be rewritten as

$$g(f(x)) = \theta \, H(x) f'(x) \,,$$

with $\theta = m \, d^{-1} \lambda \in \mathbb{F}_q^*$. Now this is just (8) with $\Omega = V_{x^m}^S$ so that the conclusion follows inmediately from Proposition 2. □

Acknowledgment. The author would like to thank H. Borges for helpful discussions on this subject and for suggesting that the result stated in Theorem 3 should be true.

References

[1] H. Borges and R. Conceicão. On the characterization of minimal value set polynomials. *J. Number Theory*, 133(6), 2021–2035, 2013.

[2] A. Garcia, H. Stichtenoth, and M. Thomas. On towers and composita of towers of function fields over finite fields. *Finite Fields Appl.*, 3(3):257–274, 1997.

[3] H. W. Lenstra, Jr. On a problem of Garcia, Stichtenoth, and Thomas. *Finite Fields Appl.*, 8(2):166–170, 2002.

Instituto de Matemática Aplicada del Litoral, Colectora Ruta Nac. NÂř 168, Paraje El Pozo - 3000 Santa Fe - Argentina.Departamento de Matemática, Facultad de Ingeniería Química (UNL), Santiago del Estero 2829 (3000) Santa Fe, Argentina

E-mail address: rtoledano@santafe-conicet.gov.ar