

POLYNOMIALS WITH MINIMAL VALUE SET OVER GALOIS RINGS

MARIA T. ACOSTA-DE-OROZCO

Department of Mathematics
Penn State University
Beaver Campus
Monaca, Pennsylvania 15061

and

JAVIER GOMEZ-CALDERON

Department of Mathematics
Penn State University
New Kensington Campus
New Kensington, Pennsylvania 15068

(Received September 12, 1989)

ABSTRACT. Let $GR(p^n, m)$ denote the Galois ring of order p^{nm} , where p is a prime. In this paper we define and characterize minimal value set polynomials over $GR(p^n, m)$.

KEY WORDS AND PHRASES. Minimal polynomials, Galois rings, special value set polynomials over Galois ring.

1985 REVISED AMS SUBJECT CLASSIFICATION CODE. Primary 11T06.

1. **INTRODUCTION.** Let $GF(q)$ denote the finite field of order q where q is a prime power. If $f(x)$ is a polynomial of positive degree d over $GF(q)$, let $V(f) = \{f(x) : x \in GF(q)\}$ denote the image or value set of $f(x)$ and let $|V(f)|$ denote the cardinality of $V(f)$. Since a polynomial of degree d cannot assume a given value more than d times over any field, it is clear that

$$[(q-1)/d] + 1 \leq |V(f)| \tag{1.1}$$

where $[x]$ denotes the greatest integer $\leq x$.

A polynomial for which equality is achieved in (1.1) is called a minimal value set polynomial. Minimal value set polynomials over finite fields have been studied in Carlitz, Lewis, Mills and Straus [1], and Mills [4]. Among their results, they proved that if $|V(f)| \geq 3$ and $2 < d < p$, p the characteristic of $GF(q)$, then d divides $q-1$ and $f(x)$ is of the form

$$f(x) = a(x-b)^d + c, \quad a \neq 0.$$

Conversely, if d divides $q - 1$ and $f(x)$ is of this form, then

$$|V(f)| = [(q - 1)/d] + 1.$$

In the present paper we define and study polynomials with minimal value set over Galois rings which are finite extensions of the ring Z_p^n of integers modulo p^n where p is a prime and $n \geq 1$. In particular, $GR(p^n, m)$ will denote the Galois ring of order p^{nm} which can be obtained as a Galois extension of Z_p^n of degree m . Thus, $GR(p^n, 1) = Z_p^n$ and $GR(p, m) = GF(p^m)$, the finite field of order p^m . The reader can find further details concerning Galois rings in the reference [3].

We start obtaining a lower bound for the cardinality of value set polynomials over the Galois ring $GR(p^n, m)$. As it could be expected, our lower bound reduces to $[(q - 1)/d] + 1$ when $n = 1$. More precisely, we have the following

2. MAIN RESULTS

LEMMA 2.1. Let $f(x)$ be a monic polynomial of degree d over the Galois ring $GR(p^n, m)$, $n \geq 2$. Let $V(f) = \{f(x) : x \in GR(p^n, m)\}$ denote the value set of $f(x)$ and let $|V(f)|$ denote the cardinality of $V(f)$. Let $q = p^m$. Assume $2 < d < \min\{p, 3\sqrt{2q}\}$. Then

$$[(q - 1)/d]q^{n-1} + 1 \leq |V(f)| \tag{2.1}$$

where $[x]$ denotes the greatest integer $\leq x$.

The proof uses the following Lemma that is a generalization of a well known result about lifting solutions over Z_p^n .

LEMMA 2.2. Let $f(x)$ be a monic polynomial with coefficients in $GR(p^n, m)$. Assume $n \geq 2$ and let T be a solution of the equation $f(x) = 0$ in the Galois ring $GR(p^{n-1}, m)$.

(a) Assume $f'(T) \neq 0$ over the field $GR(p, m)$. Then T can be lifted in a unique way from $GR(p^{n-1}, m)$ to $GR(p^n, m)$.

(b) Assume $f'(T) = 0$ over the field $GR(p, m)$. Then we have two possibilities:

(b.1) If $f(T) = 0$ over $GR(p^n, m)$, T can be lifted from $GR(p^{n-1}, m)$ to $GR(p^n, m)$ in p^m distinct ways.

(b.2) If $f(T) \neq 0$ over $GR(p^n, m)$, T cannot be lifted from $GR(p^{n-1}, m)$ to $GR(p^n, m)$.

PROOF. Let T be a solution of the equation $f(x) = 0$ in the ring $GR(p^{n-1}, m)$. Let Q be an element of $GR(p, m)$. Then, by Taylor's formula

$$f(T + Qp^{n-1}) = f(T) + f'(T)Qp^{n-1}$$

over the ring $GR(p^n, m)$. Further, since $f(T) = 0$ over $GR(p^{n-1}, m)$,

$$f(T + Qp^{n-1}) = [k + f'(T)Q]p^{n-1}$$

for some k in $GR(p, m)$. Therefore, $f(T + Qp^{n-1}) = 0$ over $GR(p^n, m)$ if and only if

$$k + f'(T)Q = 0 \tag{*}$$

over the field $GR(p, m)$. Now, if $f'(T) \neq 0$ then the linear equation (*) has a unique solution Q in

$GR(p, m)$. On the other hand, if $f'(T) = 0$, $(*)$ has no solutions when $k \neq 0$, and p^m solutions when $k = 0$.

This completes the proof of the lemma.

PROOF OF LEMMA 2.1. Let $V(f)$ denote the value set of $f(x)$ over $GR(p^n, m)$. Let $\bar{f}(x)$ denote the reduction of $f(x)$ modulo p . Let $V(\bar{f})$ denote the value set of $\bar{f}(x)$ over the field $GR(p, m)$. For $\bar{b} \in V(\bar{f})$, let $L(\bar{b})$ denote the set of elements in $V(f)$ that reduce to \bar{b} modulo p , i.e.

$$L(\bar{b}) = \{b \in V(f) : b \equiv \bar{b} \pmod{p}\}.$$

So, it is clear that

$$1 \leq |L(\bar{b})| \leq q^{n-1}$$

Now, if $\bar{f}(x) - \bar{b}$ has at least one simple root \bar{r} over the field $GR(p, m) = GF(q)$, then, by Lemma 2.2, \bar{r} can be lifted from $GR(p, m)$ to $GR(p^n, m)$ for all b in $GR(p^n, m)$, $b \equiv \bar{r} \pmod{p}$. Hence,

$$|L(\bar{b})| = (p^{n-1})^m = q^{n-1}.$$

Conversely, if $|L(\bar{b})| < q^{n-1}$ then $\bar{f}(x) - \bar{b}$ has no simple roots over the field $GF(q)$. We also observe that the number of images \bar{b} such that $|L(\bar{b})| < q^{n-1}$ is at most $d - 1$. Therefore,

$$(|V(\bar{f})| - N)q^{n-1} + N \leq |V(f)| \leq |V(\bar{f})|q^{n-1}$$

where N denotes the number of images \bar{b} such that $\bar{f}(x) - \bar{b}$ has no simple roots over the field $GF(q)$. So, $0 \leq N \leq d - 1$.

Now, if $N \neq 1$, $\bar{f}(x)$ is not a minimal value set polynomial. Hence, according to [2], the value set of $\bar{f}(x)$ satisfies the inequality

$$[(q-1)/d] + 2(q-1)/d^2 \leq |V(\bar{f})|.$$

Therefore,

$$[(q-1)/d] + 2(q-1)/d^2 - (d-1)q^{n-1} + (d-1) \leq |V(f)|$$

for all N , $N \neq 1$.

On the other hand, for $N = 1$ we have

$$[(q-1)/d]q^{n-1} + 1 \leq |V(f)|.$$

Now, it is easy to see that $d < 3\sqrt{2q}$ implies

$$[(q-1)/d]q^{n-1} + 1 < ([(q-1)/d] + 2(q-1)/d^2 - (d-1))q^{n-1} + (d-1).$$

This completes the proof of Lemma 2.1.

DEFINITION. Let $f(x)$ be a monic polynomial of degree d over the Galois ring $GR(p^n, m)$,

$n \geq 2$. Let $q = p^m$. Assume $2 < d < \min\{p, 3\sqrt{2q}\}$. Then $f(x)$ is called minimal value set polynomial if

$$[(q-1)/d]q^{n-1} + 1 = |V(f)|.$$

We are ready for the main result of the paper.

THEOREM 1. Let $f(x)$ be a monic polynomial of degree d over the Galois ring $GR(p^n, m)$, $n \geq 2$. Let $q = p^m$. Assume $2 < d < \min\{p, 3\sqrt{2q}\}$. If $f(x)$ is a minimal value set polynomial, then $d \geq n$, d divides $p-1$ and $f(x)$ is of the form

$$f(x) = b_0 + \left(\sum_{i=1}^{n-1} p^{n-i} b_i (x-a)^i \right) + p \left(\sum_{i=n}^{d-1} b_i (x-a)^i \right) + (x-a)^d. \quad (2.2)$$

Conversely, if $d \geq n$, d divides $p-1$ and $f(x)$ is of this form, then $f(x)$ is a minimal value set polynomial over $GR(p^n, m)$.

PROOF. With notation as in Lemma 2.1, it is easy to see that $f(x)$ is a minimal value set polynomial over $GR(p^n, m)$ if and only if the following two conditions hold.

- (i) $\bar{f}(x)$ is a minimal polynomial over the field $GR(p, m) = GF(q)$.
- (ii) $N = 1$ and for this unique image \bar{b} we have $L(\bar{b}) = \{b\}$.

First, suppose $f(x)$ is a minimal value set polynomial over $GR(p^n, m)$. Let \bar{r} be an element of $GR(p, m)$ so that $\bar{f}(\bar{r}) = \bar{b}$. Then, by (ii), $f(\bar{r} + rp) = b$ for all r in $GR(p^n, m)$. Thus, by Taylor's polynomial formula,

$$f^{(i)}(\bar{r}) = 0$$

over $GR(p^{n-i}, m)$ for $i = 1, \dots, n-1$. Hence, since $f(x)$ is monic, $d \geq n$ and $f(x)$ has the form given in (3). We also obtain, from (i), that d divides $p-1$.

Now suppose $d \geq n$, d divides $p-1$ and $f(x)$ is of the form given in (2.2). Then $f^{(i)}(a) = 0$ over $GR(p^{n-i}, m)$ for $i = 1, \dots, n-1$. Thus, $f(a + px) = 0$ for all x in $GR(p^n, m)$, from which condition (ii) follows. Finally, we obtain condition (i) by a straightforward application of [1].

This completes the proof of the theorem.

COROLLARY. With notation as in Theorem 1, if $f(x)$ is a minimal value set polynomial over $GR(p^n, m)$, then $f(x)$ is a minimal value set polynomial over $GR(p^i, m)$ for $i = 1, 2, \dots, n-1$.

REFERENCES

1. CARLITZ, L., LEWIS, D.J., MILLS, W.H. and STRAUS, E.G., Polynomials over finite fields with minimal value sets, *Mathematika* **8** (1961), 121-130.
2. GOMEZ-CALDERON, J., A note on polynomials with minimal value set over finite fields, *Mathematika* **35** (1988), 144-148.
3. MCDONALD, B.R., "Finite Rings with Identity", Marcel Dekker, New York, 1974.
4. MILLS, W.H., Polynomials with minimal value sets, *Pacific J. Math.* **14** (1964), 225-241.

Special Issue on Singular Boundary Value Problems for Ordinary Differential Equations

Call for Papers

The purpose of this special issue is to study singular boundary value problems arising in differential equations and dynamical systems. Survey articles dealing with interactions between different fields, applications, and approaches of boundary value problems and singular problems are welcome.

This Special Issue will focus on any type of singularities that appear in the study of boundary value problems. It includes:

- Theory and methods
- Mathematical Models
- Engineering applications
- Biological applications
- Medical Applications
- Finance applications
- Numerical and simulation applications

Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://www.hindawi.com/journals/bvp/guidelines.html>. Authors should follow the Boundary Value Problems manuscript format described at the journal site <http://www.hindawi.com/journals/bvp/>. Articles published in this Special Issue shall be subject to a reduced Article Processing Charge of €200 per article. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at <http://mts.hindawi.com/> according to the following timetable:

Manuscript Due	May 1, 2009
First Round of Reviews	August 1, 2009
Publication Date	November 1, 2009

Lead Guest Editor

Juan J. Nieto, Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad de Santiago de

Compostela, Santiago de Compostela 15782, Spain;
juanjose.nieto.roig@usc.es

Guest Editor

Donal O'Regan, Department of Mathematics, National University of Ireland, Galway, Ireland;
donal.oregan@nuigalway.ie