81. On the Cardinality of Value Set of Polynomials with Coefficients in a Finite Field

By Javier GOMEZ-CALDERON

The Pennsylvania State University

(Communicated by Shokichi, IYANAGA, M. J. A., Dec. 14, 1992)

1. Introduction. Let F_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 F_q, let $V_f = \{f(x) : x \in F_q\}$ denote the image or value set of $f(x)$ and $|V_f|$ denote the cardinality of V_f. Since $f(x)$ cannot assume a given value more than d times, it is clear that

$$\left[\frac{q-1}{d}\right] + 1 \leq |V_f| \leq q,$$

where $[x]$ denotes the greatest integer $\leq x$. Uchiyama [3] has proved that if F_q is of sufficiently large characteristic and

$$\frac{f(x) - f(y)}{x - y}$$

is absolutely irreducible, then $|V_f| > \frac{q}{2}$ for all $d \geq 4$. Carlitz [1] has also proved that $|V_f| > \frac{q}{2}$ "on the average." More precisely, Carlitz proved that

$$\sum_{a_1 \in F_q} |V_f| \geq \frac{q^2}{2},$$

where the summation is over the coefficients of the first degree term in $f(x)$.

In this note we determine a lower bound for $|V_f|$ when $(d, q) = 1$, $d^4 < q$ and the multiplicative order of q modulo $p_i^{a_i}$ is $p_i^{a_i} - p_i^{a_i - 1}$ for all prime power $p_i^{a_i} \| d$. We prove that

$$|V_f| \geq \frac{q}{1 + \sum_{D|d} \emptyset(D)/\mathrm{lcm}(\emptyset(p_1^{b_1}), \ldots, \emptyset(p_r^{b_r}))},$$

where $D = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ and $\emptyset(D)$ denotes the Euler Phi Function.

2. Theorem and proof. We will need the following two lemmas.

Lemma 1. *Let $f(x)$ be a monic polynomial over F_q of degree $d < q$. Let $\# f^*(x, y)$ denote the number of solutions (x, y) in $F_q \times F_q$ of the equation $f^*(x, y) = f(x) - f(y) = 0$. Assume*

$$\# f^*(x, y) \leq c\, q$$

for some constant c, $1 < c < d$. Then

$$\frac{q}{c} \leq |V_f|.$$

Proof. Let R_i denote the number of images of $f(x)$ that occur exactly i times as x ranges over F_q, not counting multiplicities. Then

$$\sum_{i=1}^{d} i R_i = q, \quad |V_f| = \sum_{i=1}^{d} R_i, \text{ and } \# f^*(x, y) = \sum_{i=1}^{d} i^2 R_i.$$

Hence, we can apply Cauchy-Schwarz inequality to obtain

$$\begin{aligned} q^2 &= \left(\sum_{i=1}^{d} i R_i\right)^2 \\ &\le \left(\sum_{i=1}^{d} i^2 R_i\right)\left(\sum_{i=1}^{d} R_i\right) \\ &\le \# f^*(x, y) \mid V_f \mid. \end{aligned}$$

Therefore, $|V_f| \ge \dfrac{q^2}{\# f^*(x, y)} \ge \dfrac{q^2}{cq} \ge \dfrac{q}{c}.$

Lemma 2. *Let $d > 1$ denote an integer with prime factorization given by*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

For $(t, s) = 1$, let $\mathrm{ord}_t(s)$ denote the multiplicative order of s modulo t. Assume $\mathrm{ord}_{p_i^{a_i}}(q) = \emptyset(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1}$ for $i = 1,2,\ldots, r$. Let D denote a divisor of d and write

$$D = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r},$$

where $0 \le b_i \le a_i$ for $i = 1,2,\ldots, r$. Then

$$\mathrm{ord}_D(q) = \mathrm{lcm}(\emptyset(p_1^{b_1}), \emptyset(p_2^{b_2}), \ldots, \emptyset(p_r^{b_r})).$$

Proof. Assume $\mathrm{ord}_{p_i^{b_i}}(q) = e < \emptyset(p_i^{b_i})$ with $1 \le b_i < a_i$. So $q^e \equiv 1 \bmod p_i^{b_i}$ and then $1 + q^e + q^{2e} + \cdots + q^{(p_i-1)e} \equiv 0 \bmod p_i$. Therefore,

$$\begin{aligned} q^{p_i e} - 1 &= (q^e - 1)(1 + q^e + \cdots + q^{(p_i-1)e}) \\ &\equiv 0 \text{ and } p_i^{b_i+1}, \end{aligned}$$

where $p_i e < p_i \emptyset(p_i^{b_i}) = p_i(p_i^{b_i} - p_i^{b_i-1}) = \emptyset(p_i^{b_i+1})$. Thus, an induction argument gives

$$q^c \equiv 1 \bmod p_i^{a_i}$$

for some positive integer c such that $c < \emptyset(p_i^{a_i})$, a contradiction to the fact that $\mathrm{ord}_{p_i^{a_i}}(q) = \emptyset(p_i^{a_i})$. Therefore, $\mathrm{ord}_{p_i^{b_i}}(q) = \emptyset(p_i^{b_i})$ for $1 \le b_i \le a_i$ and $i = 1,2,\ldots, r$. So,

$$\mathrm{ord}_D(q) = \mathrm{lcm}(\emptyset(p_1^{b_1}), \emptyset(p_2^{b_2}), \ldots, \emptyset(p_r^{b_r}))$$

We are ready for the theorem:

Theorem 3. *Let $f(x)$ be a monic polynomial over F_q of degree d. Assume $(d, q) = 1$ and $d^4 < q$. Let the prime factorization of d be given by*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Assume $\mathrm{ord}_{p_i^{a_i}}(q) = \emptyset(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1}$ for $i = 1,2,\ldots, r$. Then

$$|V_f| \ge \frac{q}{1 + \sum_{D|d} \emptyset(D)/\mathrm{lcm}(\emptyset(p_1^{b_1}), \ldots, \emptyset(p_r^{b_r}))},$$

where $D = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$.

Proof. Let the factorization of $f^*(x, y) = f(x) - f(y)$ into irreducibles over F_q be given by

$$f^*(x, y) = \prod_{i=1}^{s} f_i(x, y).$$

Let

$$f_i(x, y) = \prod_{j=0}^{n_i} h_{ij}(x, y)$$

be the homogeneous decomposition of $f_i(x, y)$ so that $h_{ij}(x, y)$ is homogenous of degree j. So, it is clear that

$$x^d - y^d = \prod_{i=1}^{s} h_{in_i}.$$

We also have, since $(d, q) = 1$, that $x^d - y^d$ is a product of $\emptyset(d)$ polynomials,

$$x^d - y^d = \prod_{D|d} \Phi_D(x, y)$$

where $\Phi_D(x, y)$ factors into $\emptyset(D)/\mathrm{ord}_D(q)$ distinct irreducibles polynomials in $F_q[x, y]$ of the same degree $\mathrm{ord}_D(q)$. Therefore

$$s \leq \sum_{D|d} \frac{\emptyset(D)}{\mathrm{ord}_D(q)}.$$

Now, if $f_i(x, y)$ is absolutely irreducible over the field F_q, then

$$\# f_i(x, y) \leq (d_i - 1)(d_i - 2)\sqrt{q} + d_i^2 + q \quad [2, \text{pp.}330\text{-}331]$$

where $d_i = \deg(f_i(x, y))$.

For $f_i(x, y)$ not absolutely irreducible, the situation is simpler and we estimate

$$\# f_i(x, y) \leq d_i^2.$$

Therefore, if $d < \sqrt[4]{q}$ we obtain:

$$\begin{aligned} \# f^*(x, y) &\leq \sum_{i=1}^{s} \# f_i(x, y) \\ &\leq \left\{ \sum_{i=1}^{s} (d_i - 1)(d_i - 2)\sqrt{q} + d_i^2 \right\} + sq \\ &\leq \sum_{i=1}^{s} d_i^2 \sqrt{q} + sq \\ &\leq (1 + s)q. \end{aligned}$$

Hence, combining with Lemmas 1 and 2 we obtain:

$$\begin{aligned} |V_f| &\geq \frac{q}{1+s} \\ &= \frac{q}{1 + \sum_{D|d} \emptyset(D)/\mathrm{lcm}(\emptyset(p_1^{b_1}), \ldots, \emptyset(p_r^{b_r}))}, \end{aligned}$$

where $D = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$.

Corollary 4. With notation and assumptions as in Theorem 3, if $r = a_1 = 1$, then

$$|V_f| \geq \frac{q}{3}.$$

References

[1] L. Carlitz: On the numbers of distinct values of a polynomial with coefficients in a finite field. Proc. Japan Acad., **31**, 119–120 (1955).

[2] R. Lidl and H. Niederreiter: Finite Fields. Encyclo. Math. and Appls., vol. 20, Addison-Wesley, Reading, Mass. (1983) (Now distributed by Cambridge Univ. Press).

[3] S. Uchiyama: Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini. Proc. Japan Acad., **30**, 930–933 (1954).