Finite Fields and Their Applications **6**, 302–308 (2000)
doi.10.1006/ffta.2000.0278, available online at http://www.idealibrary.com on IDEAL®

On Polynomials over Prime Fields Taking Only Two Values on the Multiplicative Group

András Biró

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda u. 13-15, 1053 Budapest, Hungary
E-mail: biroand@math-inst.hu

Communicated by Gerhard Turnwald

Received February 26, 1999; revised November 8, 1999; published online August 19, 2000

Let $p > 2$ be a prime, denote by F_p the field with $|F_p| = p$, and let $F_p^* = F_p \setminus \{0\}$. We prove that if $f \in F_p[x]$ and f takes only two values on F_p^*, then (excluding some exceptional cases) the degree of f is at least $\frac{3}{4}(p-1)$. © 2000 Academic Press

1. INTRODUCTION

The problem of examining the possible degrees of polynomials $f \in F_p[X]$ taking only two values on F_p^* was raised by András Gács. He was led to this problem in connection with the problem of determining the possible number of difference quotients of polynomials (see [G]).

It is obvious that the smallest possible value of $\delta = \deg f/(p-1)$ is 1/2, and it is attained by the Legendre symbol, i.e., $f(X) = X^{(p-1)/2}$. More generally, if $d > 1$ is a divisor of $p - 1$, then the polynomial

$$f(X) = \sum_{j=1}^{d-1} X^{j(p-1)/d}$$

also takes only two values on F_p^*, so the numbers 1/2, 2/3, 3/4, 4/5, ... are possible values of δ.

We show here that the smallest three values of δ are 1/2, 2/3, and 3/4. More precisely, we prove the following theorem.

1071-5797/00 $35.00

THEOREM. *Let* $f \in F_p[X]$, $\deg f < p-1$, *and assume that* $|f(F_p^*)| = 2$. *Then one of the following three assertions is true*:

(i) $f(X) = a + bX^{(p-1)/2}$, $a \in F_p$, $b \in F_p^*$;

(ii) $p \equiv 1 \pmod 3$ *and* f *is a polynomial of* $X^{(p-1)/3}$;

(iii) $\deg f \geq \frac{3}{4}(p-1)$.

The main point (as we will see) is the constant 3/4 in (iii) (which is best possible there in view of the above remarks); it would be easier to prove the theorem with a slightly smaller constant (which is greater than 2/3).

One could think that the next value of δ is 4/5 (and a related theorem of T. Szőnyi (see [Sz]) also could suggest it). But this is not the case; we will show by a numerical example (with $p = 29$) that $3/4 < \delta < 4/5$ is possible. So the most interesting problem here is to determine the quantities

$$I = \inf_p M_{p,3/4} \text{ and } L = \liminf_p M_{p,3/4},$$

where we denote by $M_{p,3/4}$ the minimum of $\delta = \deg f/(p-1)$ taken over polynomials $f \in F_p[X]$ satisfying $|f(F_p^*)| = 2$ and $\delta > 3/4$. It is not sure that $I = L$ (in particular, our example does not show that $L < 4/5$, just that $I < 4/5$), but I guess that $I = L = 3/4$ (though there is no evidence for this).

It would be also interesting to describe the polynomials with $\delta = 3/4$.

Remark that it is easy to determine explicitly the possible polynomials in (ii); these are

$$a + b(X^{(p-1)/3} + X^{2(p-1)/3}) \text{ and } a + b((1+\varepsilon)X^{(p-1)/3} - X^{2(p-1)/3}),$$

where $a \in F_p$, $b, \varepsilon \in F_p^*$, and $\varepsilon^3 = 1$, $\varepsilon \neq 1$.

Remark finally that the polynomials investigated in this paper are two-valued on F_p^*, but they are in fact three-valued on F_p; i.e., $V(f) = 3$ (using the usual notation $V(f) = |f(F_p)|$), and one of the values occurs exactly once. Classical references concerning the estimation of $V(f)$ are [C] and [B-SD]. It is known (see [GC-M]) that "usually" $f \in F_q(X)$ has at least $2q/d$ values provided that $d = \deg f$ is small compared with q. Upper bounds for $V(f)$ are proved in [G-W] by applying group-theoretic methods.

2. PROOF OF THE THEOREM

We may assume that $F_p^* = A \cup B$, $f(A) = \{0\}$, $f(B) = \{1\}$, $1 \leq |B| \leq (p-1)/2$. We have

$$\sum_{x \in B} x^k = 0 \text{ for } 1 \leq k < p - 1 - \deg f, \tag{1}$$

because $\sum_{x \in B} x^k = \sum_{x \in F_p^*} f(x)x^k$, and $\sum_{x \in F_p^*} x^l = 0$, if $1 \leq l < p-1$.

We shall need the following well-known statement.

LEMMA 1. *If* $H_1, H_2 \subseteq F_p^*$, $|H_1| = |H_2| = n$, *and*

$$\sum_{x \in H_1} x^k = \sum_{x \in H_2} x^k$$

for $1 \leq k \leq n$, *then* $H_1 = H_2$.

Proof. It is an easy consequence of the Newton–Girard formulas that the equality of the first n power sums implies the equality of the elementary symmetric polynomials ($n \leq p-1$), and then the lemma follows. ■

The next lemma is basic in our proof.

LEMMA 2. *If* $r \in F_p^*$, *then either* $rB = B$, *or*

$$|B| - |B \cap rB| \geq p - 1 - \deg f.$$

Proof. For $r \in F_p^*$ and $1 \leq k < p - 1 - \deg f$ we have

$$\sum_{x \in B} x^k = 0 = \sum_{x \in rB} x^k,$$

so, omitting the common terms,

$$\sum_{x \in H_1} x^k = \sum_{x \in H_2} x^k$$

with $H_1 = B \backslash (B \cap rB)$, $H_2 = rB \backslash (B \cap rB)$. Since $H_1 \cap H_2 = \emptyset$, the lemma follows by Lemma 1. ■

Let $G = \{r \in F_p^* : rB = B\}$. It is clear that G is a multiplicative subgroup of F_p^*, and B is a union of G-cosets. Observe that G is not equal to F_p^*, since $1 \leq |B| \leq (p-1)/2$.

Introduce the notations

$$\beta = \frac{|B|}{p-1}, \quad \gamma = \frac{|G|}{p-1}, \quad \delta = \frac{\deg f}{p-1}.$$

We would like to prove that either $\delta \geq 3/4$ or f is a polynomial of $X^{(p-1)/2}$ or $X^{(p-1)/3}$.

We use Lemma 2 and an averaging argument to prove the following inequality.

LEMMA 3. *One has the inequality*

$$\delta \geq 1 + \frac{\beta^2 - \beta}{1 - \gamma}. \tag{2}$$

If equality holds in (2), *then there is an integer M such that*

$$|B \cap rB| = M$$

for every $r \in F_p^* \setminus G$.

Proof. Let $\bar{B}$ and $\bar{1}$ be the image of B and 1 in F_p^*/G, respectively. Then, computing in two different ways the number of ordered pairs of different elements of B, we get

$$\sum_{\bar{r} \in F_p^*/G, \bar{r} \neq \bar{1}} |\bar{B} \cap \bar{r}\bar{B}| = |\bar{B}|(|\bar{B}| - 1).$$

The sum on the left-hand side has $(p-1)/|G| - 1$ terms, so, since $|B| = |\bar{B}||G|$, we obtain that

$$\max_{\bar{r} \in F_p^*/G, \bar{r} \neq \bar{1}} |\bar{B} \cap \bar{r}\bar{B}| \geq |B| \frac{|\bar{B}| - 1}{p - 1 - |G|},$$

and multiplying by $|G|$,

$$\max_{r \in F_p^* \setminus G} |B \cap rB| \geq |B| \frac{\beta - \gamma}{1 - \gamma}. \tag{3}$$

If equality holds in (3) then $|B \cap rB| = |B|(\beta - \gamma)/(1 - \gamma)$ for every $r \in F_p^* \setminus G$. By this remark, (3), and Lemma 2 (choosing r to maximize $|B \cap rB|$ there), we get the assertions of the lemma. ■

Since G is a subgroup of F_p^*, we have

$$\gamma = \frac{1}{t}$$

with an integer $t > 1$. The quotient β/γ is also an integer, since B is a union of G-cosets.

If $r \in G$, then $f(X) = f(rX)$ (we have $f(x) = f(rx)$ for $x \in F_p^*$ by the definition of G, and since $\deg f < p - 1$, this implies that $f(X) = f(rX)$ as polynomials), and G is a cyclic group (because F_p^* is cyclic), so the order of r may be $|G|$, consequently f is a polynomial of $X^{|G|}$. In particular, $|G|$ divides $\deg f$, so δ/γ is also an integer.

We may assume that $\delta < 3/4$, and we may also assume that $\gamma < 1/2$ (using the preceding paragraph). The inequality (2) can be written in the form

$$\delta \geq \frac{3}{4} + \frac{(\beta - 1/2)^2}{1-\gamma} - \frac{\gamma}{4(1-\gamma)} \geq \frac{3}{4} - \frac{\gamma}{4(1-\gamma)}. \tag{4}$$

We get by (4) and our assumptions that

$$\frac{3}{4} - \frac{\gamma}{2} < \delta < \frac{3}{4};$$

i.e.,

$$3t - 2 < 4\frac{\delta}{\gamma} < 3t.$$

Since δ/γ and t are integers, we obtain that $4\delta/\gamma = 3t - 1$, which means that $t \equiv 3 \pmod 4$ and

$$\delta = \frac{3}{4} - \frac{\gamma}{4}. \tag{5}$$

Inserting this into (4), using also $\beta \leq 1/2$, we get

$$\frac{1}{2} - \frac{\gamma}{2} \leq \beta \leq \frac{1}{2};$$

i.e.,

$$t - 1 \leq 2\frac{\beta}{\gamma} \leq t.$$

Since β/γ is an integer and t is an odd integer, we obtain $2\beta/\gamma = t - 1$, or

$$\beta = \frac{1}{2} - \frac{\gamma}{2}. \tag{6}$$

Using (5) and (6) in (2), we see that (2) hold with equality.

The equality in (2) means by Lemma 3 that $|B \cap rB| = M$ for every $r \in F_p^* \setminus G$ with an integer M, and of course $|B \cap rB| = |B|$ for $r \in G$. We combine these facts with (1), writing $k = |G|$ there. This is possible if $|G| < p - 1 - \deg f$, or what is the same, if $\gamma < 1 - \delta$. This is true by (5) if $\gamma < 1/3$, and we may assume that this is the case, because f is a polynomial of $X^{(p-1)/3}$ for $\gamma = 1/3$. So we can use (1) with $k = |G|$, and this gives

$$\left(\sum_{x \in B} x^{|G|}\right)\left(\sum_{y \in B} y^{-|G|}\right) = 0,$$

since the first factor is 0. Then

$$\sum_{r \in F_p^*} |B \cap rB| r^{|G|} = 0,$$

$$0 = |B| \sum_{r \in G} r^{|G|} + M \sum_{r \in F_p^* \setminus G} r^{|G|} = (|B| - M) \sum_{r \in G} r^{|G|} = (|B| - M)|G|,$$

where we used $1 \leq |G| < p - 1$. These inequalities and the fact that p divides $(|B| - M)|G|$ imply that $M = |B|$ (as integers). But then $B = rB$ for all $r \in F_p^*$, which is impossible. So $\delta < 3/4$ and $\gamma < 1/3$ cannot hold simultaneously, which proves the theorem. ■

3. AN EXAMPLE

Let $p = 29$, and assume that $B \subseteq F_{29}^*$ satisfies $-B = B$, $1 \leq |B| \leq 14$, and

$$\sum_{x \in B^2} x = \sum_{x \in B^2} x^2 = 0, \tag{7}$$

where

$$B^2 = \{x \in F_{29}^* : x = y^2 \text{ for some } y \in B\}.$$

The condition $-B = B$ implies that each odd power sum of the elements of B is 0, so the first five power sums of B vanish by (7). Let $f \in F_{29}[X]$ be the unique polynomial with $\deg f \leq 27$ and with the property that f and the characteristic function of B are equal as functions on F_{29}^* (we get f by Lagrange interpolation). The vanishing of the power sums implies that in fact $\deg f \leq 22$. If $\deg f < 22$, then $\deg f \leq 20$ (since $\deg f$ is even by $-B = B$), so $\deg f < 3/4(p-1) = 21$. Hence $f(X) = a + bX^{14}$ by our theorem, and then $|B| = 14$, because f vanishes on $F_{29}^* \setminus B$, so it has at least $28 - |B|$ distinct roots, and $1 \leq |B| \leq 14$.

Summing up: if $1 \leq |B| < 14$, $-B = B$, and (7) is true, then $\deg f = 22$, and

$$\frac{3}{4} < \delta = \frac{\deg f}{p-1} = \frac{11}{14} < \frac{4}{5}.$$

We now give the set explicitly. Let

$$B = \{\pm 1,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 7,\ \pm 11\}.$$

Then $|B| = 12$, and

$$B^2 = \{1, 5, 7, 9, 16, 20\}.$$

It is easy to verify that (7) is valid, so each condition is satisfied.

Remark (just to determine all quantities occurring in the above proof) that one has $G = \{\pm 1\}$, since $|G|$ divides both $p - 1 = 28$ and $\deg f = 22$, so

$$\beta = 3/7, \quad \gamma = 1/14, \quad \delta = 11/14$$

in this special case.

REFERENCES

[B-SD] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arithm.* **5** (1959), 417–423.

[C] S. Chowla, The Riemann zeta and allied functions, *Bull. Amer. Math. Soc.* **58** (1952), 287–305.

[G] A. Gács, On the size of the smallest non-classical blocking set in $PG(2, p)$, *J. Combin. Theory Ser. A*, to appear.

[GC-M] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* **28** (1988), 167–188.

[G-W] R. Guralnick, D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* **101** (1997), 255–287.

[Sz] Szőnyi, T. Combinatorial problems for Abelian groups arising from geometry, *in* "Proc. of the Second International Mathematical Miniconference, Part II, Budapest, 1988," Period. Polytech. Transportation Engrg. **19** No. 1–2 (1991), 91–100.