

ON GENERAL POLYNOMIALS

Kenneth S. Williams

(received April 9, 1967)

Let d denote a fixed integer > 1 and let $\text{GF}(q)$ denote the finite field of $q = p^n$ elements. We consider q fixed $\geq A(d)$, where $A(d)$ is a (large) constant depending only on d . Let

$$(1) \quad f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x,$$

where each $a_i \in \text{GF}(q)$. Let n_r ($r = 2, 3, \dots, d$) denote the number of solutions in $\text{GF}(q)$ of

$$f(x_1) = f(x_2) = \dots = f(x_r)$$

for which x_1, x_2, \dots, x_r are all different. Birch and Swinnerton-Dyer [1] have shown, as a consequence of Weil's work, that

$$(2) \quad n_r = \nu_r q + O(q^{1/2}), \quad r = 2, 3, \dots, d,$$

where each ν_r is a positive integer depending on f and the constant implied by the O -symbol depends only on d — throughout this note all constants implied by O -symbols depend only on d unless otherwise stated. They deduce from (2) that the number $V(f)$ of distinct values of $f(x)$, $x \in \text{GF}(q)$ satisfies

$$V(f) = \lambda(f)q + O(q^{1/2}),$$

where

$$\lambda(f) = 1 - \frac{\nu_2}{2!} + \frac{\nu_3}{3!} - \dots + (-1)^{d-1} \frac{\nu_d}{d!}.$$

The polynomial f is called a general polynomial if

$$\lambda(f) = 1 - \frac{1}{2!} + \frac{1}{3!} - \dots + (-1)^{d-1} \frac{1}{d!}.$$

It is the purpose of this note to prove that the number N of general polynomials of the form (1) is given by

$$N = q^{d-1} + O(q^{d-2}).$$

Since the number of polynomials of the form (1) is exactly q^{d-1} this shows that for a fixed d almost all polynomials are general.

As the number of solutions x_i of

$$f(x_1) = f(x_i), \quad i = 2, 3, \dots, r,$$

for a given x_1 , is $\leq d$ we have for $r = 2, 3, \dots, d$

$$n_r \leq d^{r-1} q$$

and so for q sufficiently large

$$0 \leq v_r \leq d^{r-1}.$$

Hence $\lambda(f)$ takes a finite number $\ell \equiv \ell(d)$ of rational values between (and possibly including) 0 and 1. Let $\lambda_1, \dots, \lambda_\ell$ denote the ℓ λ -values in ascending order of magnitude, with $1 - \frac{1}{2!} + \dots + \frac{(-1)^{d-1}}{d!}$ as the k^{th} one ($1 \leq k \leq \ell$). We note that each λ_i depends only on d . Let \mathcal{C}_i be the class of polynomials f having $\lambda(f) = \lambda_i$. For $f \in \mathcal{C}_i$ ($1 \leq i \leq k-1$)

$$\begin{aligned} \lambda_k q - V(f) &= (\lambda_k - \lambda_i)q + O(q^{1/2}) \\ &\geq \frac{1}{2}(\lambda_k - \lambda_{k-1})q, \end{aligned}$$

for q sufficiently large. For $f \in \mathcal{C}_i$ ($k+1 \leq i \leq \ell$)

$$\begin{aligned} V(f) - \lambda_k q &= (\lambda_i - \lambda_k)q + O(q^{1/2}) \\ &\geq \frac{1}{2}(\lambda_{k+1} - \lambda_k)q, \end{aligned}$$

for q sufficiently large. Set

$$2\mu^{1/2} = \min(\lambda_k - \lambda_{k-1}, \lambda_{k+1} - \lambda_k)$$

so that for $f \in \mathcal{C}_i$ ($i \neq k$)

$$\{V(f) - \lambda_k q\}^2 \geq \mu q^2,$$

where μ depends only on d . Hence

$$\begin{aligned} \sum_f \{V(f) - \lambda_k q\}^2 &= \sum_{i=1}^{\ell} \sum_{f \in \mathcal{C}_i} \{V(f) - \lambda_k q\}^2 \\ &\geq \sum_{\substack{i=1 \\ i \neq k}}^{\ell} \sum_{f \in \mathcal{C}_i} \{V(f) - \lambda_k q\}^2 \\ &\geq \sum_{\substack{i=1 \\ i \neq k}}^{\ell} \sum_{f \in \mathcal{C}_i} \mu q^2 \\ &= \mu q^2 N^*, \end{aligned}$$

where N^* denotes the number of f with $\lambda(f) \neq \lambda_k$. Now Uchiyama [2] has shown that

$$\sum_f \{V(f) - \lambda_k q\}^2 = O(q^d)$$

so

$$N^* = O(q^{d-2}).$$

But $N + N^* = q^{d-1}$ so we have

$$N = q^{d-1} + O(q^{d-2})$$

as required.

If $d = 2, 3$ or 4 we can determine N exactly. When $d = 2$, so that $f(x) = x^2 + a_1 x$ ($p \neq 2$), we have

$$V(f) = \frac{q+1}{2},$$

giving

$$N = q.$$

When $d = 3$, so that $f(x) = x^3 + a_2 x^2 + a_1 x$ ($p \neq 2, 3$), we have

$$V(f) = \frac{2}{3} q + O(1)$$

if and only if

$$a_2^2 - 3a_1 \neq 0;$$

hence

$$N = q(q-1) = q^2 - q.$$

When $d = 4$, so that $f(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x$ ($p \neq 2, 3$), we have

$$V(f) = \frac{5}{8} q + O(q^{1/2})$$

if and only if

$$a_3^3 - 4a_2 a_3 + 8a_1 \neq 0;$$

hence

$$N = q^2(q-1) = q^3 - q^2.$$

Finally we note that our result shows that

$$\sum_f |V(f) - \lambda_k q|^n = O(q^{n+d-2}), \quad (n \geq 2)$$

where the constant implied by the O -symbol depends only on d and n .

REFERENCES

1. B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arithmetica* 5 (1959), 417-423.
2. S. Uchiyama, Note on the mean value of $V(f)$ III. *Proc. Japan Acad.*, 32 (1956), 97-98.

Carleton University, Ottawa