THE VALUES OF A POLYNOMIAL OVER A FINITE FIELD

by S. D. COHEN

(Received 13 June, 1972)

1. The object of this paper is to derive, using a version of the large sieve for function fields due to J. Johnsen [**6**], explicit lower bounds for the average number of distinct values taken by a polynomial over a finite field.

Let k be the finite field with q elements, where q is a positive power of some prime p. For a polynomial $f(x)$ in $k[x]$, define $V(f)$ to be the number of distinct values $f(\alpha)$ as α varies in k. For our purpose it is sufficient to consider only monic polynomials with zero constant coefficient. Therefore, take $f(x)$ to be the monic polynomial of degree n given by

$$f(x) = x^n + \sum_{i=1}^{n-1} \alpha_i x^i \qquad (\alpha_i \in k). \tag{1}$$

When q is large, Birch and Swinnerton-Dyer [**1**, Theorem 2] have shown that $V(f)$ depends on a certain Galois group associated with f in a manner made explicit by the author in [**4**, Theorem 2]. However, if some of the coefficients α_i are allowed to vary in k, then the author has also shown that, for large q, the average value of $V(f)$ depends only on n. Specifically, if the integer t satisfies $0 \leqq t \leqq n-2$ and the t coefficients $\alpha_{n-1}, \ldots, \alpha_{n-t}$ in (1) are given, define $v(n, t)(= v(n, t; \alpha_{n-1}, \ldots, \alpha_{n-t}))$ by

$$v(n,t) = \sum_{\alpha_1, \ldots, \alpha_{n-t-1} \in k} V(f)/q^{n-t-1}.$$

(Thus $v(n, t)$ is the average value of $V(f)$ over all monic polynomials (1) whose first $t+1$ coefficients are fixed.) Then Theorem 3 of [**5**] (see also (1.3) of [**5**]) implies that, if $p > n$ or, with a few exceptions, if $2 < p \leqq n$, then, for fixed n,

$$v(n,t) = \mu_n q + O(q^{1/2}), \tag{2}$$

where

$$\mu_n = 1-(1/2!)+\ldots+(-1)^{n-1}/n!. \tag{3}$$

Previously, S. Uchiyama [**7**] had shown that, if $p > n$, then $v(n, 0)$ is given explicitly by

$$v(n,0) = b(q,n)q, \tag{4}$$

where $b(q,n) = \sum_{r=1}^{n} \binom{q}{r} (-1)^{r-1} q^{-r}$. In §2 below we provide a proof of (4) valid for all n and q. Note that, if μ_n is given by (3), then, for fixed n, we have

$$b(q,n) = \mu_n + O(q^{-1}) \qquad (q \to \infty). \tag{5}$$

(In fact, Uchiyama [**8**] also proved that, for fixed $n < p$ and $t \geqq 1$,

$$v(n,t) = b(q,n)q + O(q^{t+1-(n/t)}) \qquad (1 \leqq t \leqq n-1),$$

https://doi.org/10.1017/S0017089500001981 Published online by Cambridge University Press

an estimate which is nontrivial if $t^2 < n$ and, in view of (5), better than (2) if $t(t+\frac{1}{2}) < n$.) Further, if $n \geqq q$, then obviously

$$b(q,n) = 1-(1-q^{-1})^q \qquad (n \geqq q). \tag{6}$$

It is evident that, as n and q both increase, $b(q, n)$ converges extremely rapidly to $1-e^{-1} = 0{\cdot}632\ldots$. Since $f(x) \equiv g(x)(\text{mod } x^q - x)$ implies $V(f) = V(g)$, it is not hard to see that, when $n-t \geqq q$, we can supplement (4) with

$$v(n,t;\alpha_{n-1},\ldots,\alpha_{n-t}) = v(n,0) = b(q,n)q \qquad (n-t \geqq q), \tag{7}$$

where, since $n \geqq q$, $b(q, n)$ is given by (6).

In general, we therefore expect $v(n, t)$ to be approximately $b(q, n)q$. For large q, this is confirmed by (2) and (5). On the other hand, a lower bound for $v(n, t)$ close to this expected value for all n and q would seem to be of some interest. In this direction, L. Carlitz **[3]** proved that, if $p > n > 1$, then $v(n, n-2) \geqq q^2/(2q-1) > \frac{1}{2}q$, so that $v(n, t) \geqq q^2/(2q-1)$ for all $t \leqq n-2$. Our purpose here is to prove the following theorem, which strengthens this result for $0 \leqq t < n-2$.

THEOREM 1. *If* $0 \leqq t \leqq n-2$ *and* $m = [\frac{1}{2}(n-t)]$ (*in integral part notation*), *then*

$$v(n,t;\alpha_{n-1},\ldots,\alpha_{n-t}) \geqq c(q,m)q, \tag{8}$$

where

$$c(q,m) = 1 - \left\{\sum_{r=0}^{m}\binom{q}{r}(q-1)^{-r}\right\}^{-1}. \tag{9}$$

Note that, since, for $m \geqq q$, we have $c(q, m) = 1-(1-q^{-1})^q$, then (7) implies that, for $n-t \geqq 2q$, we actually have equality in (8). Further, for fixed m,

$$c(q,m) \to 1 - \{1+(1/2!)+\ldots+(1/m!)\}^{-1}, \quad \text{as} \quad q \to \infty.$$

Hence, for increasing m and q, $c(q, m)$ also converges rapidly to $1-e^{-1}$. When $t = n-2$, (8) is the inequality of Carlitz. For the next few even values of $n-t$, (8) yields

$$\begin{aligned}
&v(n,n-4) \geqq 3q^2/(5q-2) > (3/5)q && (n \geqq 4),\\
&v(n,n-6) \geqq q(10q^2-11q)/(16q^2-23q+6) > (5/8)q && (n \geqq 6, q \geqq 3),\\
&v(n,n-8) > (41/65)q = (0{\cdot}631\ldots)q && (n \geqq 8, q \geqq 4).
\end{aligned}$$

In what follows we shall denote the degree of a polynomial A by $d(A)$ and put $|A| = q^{d(A)}$.

2. For completeness we include a proof of (4) valid for all n and q. It is sufficient to evaluate $j(n)$, the number of monic polynomials of degree n in $k[x]$ not divisible by a linear factor, because evidently $j(n) = q^n - v(n, 0)q^{n-1}$. For a full description of the simple zeta function technique that we employ, see **[2]**.

For any non-zero A in $k[x]$, let $\theta(A) = 1$ if A has no linear factor; otherwise let $\theta(A) = 0$. If $s(>1)$ is real, then the zeta function

$$\zeta(s) = \sum_A |A|^{-s}\left(= \sum_{n=0}^{\infty} q^{n(1-s)}\right) = \prod_P (1-|P|^{-s})^{-1} \tag{10}$$

(where the sum and product in (10) are over all monic A in $k[x]$ and all monic irreducibles P in $k[x]$, respectively) converges (to $(1-q^{1-s})^{-1}$) and hence so does

$$\sum_A \theta(A)/|A|^s = \sum_{n=0}^{\infty} j(n)q^{-ns} = \prod_{\substack{P\\ d(P)>1}} (1-|P|^{-s})^{-1}.$$

It follows that

$$\sum_{n=0}^{\infty} j(n)q^{-ns} = \zeta(s) \prod_{\substack{P\\ d(P)=1}} (1-|P|^{-s}) = \zeta(s)(1-q^{-s})^q \qquad (s>1). \tag{11}$$

On equating coefficients of q^{-ns} in (11), we obtain

$$j(n) = \sum_{r=0}^{n} (-1)^r \binom{q}{r} q^{n-r}$$

from which (4) follows at once.

3. We now cite a particular case of the large sieve inequality contained in the Corollary to Theorem 5 of [**6**]. Let $\mathscr{S}$ be a set consisting of Z distinct polynomials of degree $\leqq N$ in $k[x]$, so that $Z \leqq q^{N+1}$. Let W be a set of *monic* square-free polynomials of degree not exceeding $X = [\frac{1}{2}(N+1)]$ with the property that, to every monic irreducible P dividing a member of W, there exists a set of $w(P)\ (>0)$ residue classes (mod P) such that all members of $\mathscr{S}$ belong to one of these residue classes (mod P).

THEOREM 2 (Johnsen). *Let* $S = \sum_{F\in W}\prod_{P|F}(|P|-w(P))/w(P)$, *where the product is over all monic irreducibles dividing F. Then*

$$Z \leqq S^{-1}q^{N+1}.$$

4. Let n be a given positive integer and A, D, H be given polynomials in $k[x]$, with $d(H) < n$. Define $J(n, A, D, H)$ to be the number of polynomials F with $d(F) \leqq n$ such that $F+A \equiv D \pmod H$ and such that $F+A$ has *no* linear factor in $k[x]$. We apply Theorem 2 to give an upper bound for $J(n, A, D, H)$ from which we deduce Theorem 1.

THEOREM 3. *Suppose that* $d(H) = h$ *and that H has precisely l distinct linear factors in* $k[x]$. *Then*

$$J(n, A, D, H) \leqq \left\{ \sum_{r=0}^{M} \binom{q-l}{r} (q-1)^{-r} \right\}^{-1} q^{n-h+1},$$

where $M = [\frac{1}{2}(n-h+1)]$.

Proof. If D_1 is the unique polynomial such that $D_1 = 0$ or $d(D_1) < h$ and such that $D_1 \equiv D - A \pmod H$, then clearly $J(n, A, D, H) = J(n, 0, D_1, H)$. Hence we may assume that $A=0$ and that $D=0$ or $d(D)<h$. Further, since the result is trivial if D and H have a common linear factor, we may also assume that this, in fact, is not the case. Let k' be the set of $q-l$ elements β of k such that $(x-\beta)\nmid H$. Then

$$J(n,0,D,H)\leqq J_1=\left|\{F\in k[x]:\ d(F)\leqq n,\ F\equiv D\,(\mathrm{mod}\ H) \text{ and } F(\beta)\neq 0\,\forall\,\beta\in k'\}\right|.$$

Now to every F counted in J_1, there exists a unique G in $k[x]$ with $d(G)\leqq n-h$ such that $F=D+GH$. Hence

$$\begin{aligned} J_1 &\leqq \left|\{G: d(G)\leqq n-h,\ D+GH\not\equiv 0\,(\mathrm{mod}\ x-\beta)\,\forall\,\beta\in k'\}\right| \\ &= \left|\{G: d(G)\leqq n-h,\ G(x)\not\equiv -(D(\beta)/H(\beta))\,(\mathrm{mod}\ x-\beta)\,\forall\,\beta\in k'\}\right|. \end{aligned} \tag{12}$$

We now apply Theorem 2 to the set of G counted by (12). Put $N=n-h$ and let W be the set of all square-free monic polynomials that are the products of not more than $[\frac{1}{2}(n-h+1)]=M$ (distinct) linear factors prime to H, so that $w(x-\beta)=q-1$ for all $\beta\in k'$. Obviously the number of polynomials in W of degree r $(\leqq M)$ is $\binom{q-l}{r}$. Thus Theorem 2 yields $J_1\leqq S^{-1}q^{n-h+1}$, where

$$S=\sum_{F\in W}\prod_{(x-\beta)\mid F}(q-1)^{-1}=\sum_{r=0}^{M}\binom{q-l}{r}(q-1)^{-r},$$

and the theorem is proved.

Proof of Theorem 1. In the situation of Theorem 1, let $A(x)=x^n+\sum_{i=n-t}^{n-1}\alpha_i x^i$. Then clearly

$$v(n,t;\alpha_{n-1},\ldots,\alpha_{n-t})q^{n-t-1}=q^{n-t}-J(n-t-1,A,0,1)\geqq q^{n-t}\left\{1-\left[\sum_{r=0}^{m}\binom{q}{r}(q-1)^{-r}\right]^{-1}\right\},$$

by Theorem 3, where $m=[\frac{1}{2}(n-t)]$, and the theorem follows.

We remark finally that, by using different choices of A, D and H in Theorem 3, one could derive similar expressions for the average value of $V(f)$ over other sets of polynomials (e.g., those with the first $t+1$ and last u (nonconstant) coefficients fixed).

REFERENCES

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

2. L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54** (1932), 39–50.

3. L. Carlitz, On the number of distinct values of a polynomial with coefficients in a finite field, *Proc. Japan. Acad.* **31** (1955), 119–120.

4. S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271.

5. S. D. Cohen, Uniform distribution of polynomials over finite fields, *J. London Math. Soc.* (2) **6** (1972), 93–102.

6. J. Johnsen, On the large sieve method in *GF* [q, x], *Mathematika* **18** (1971), 172–184.

7. S. Uchiyama, Note on the mean value of $V(f)$, *Proc. Japan. Acad.* **31** (1955), 199–201.

8. S. Uchiyama, Note on the mean value of $V(f)$, II, *Proc. Japan. Acad.* **31** (1955), 321–323.

University of Glasgow
Glasgow G12 8QQ