[11] R. Sedgewick, *Data movement in odd-even merging*, SIAM J. Comput. 7 (1978), 239–272.
[12] K. B. Stolarsky, *Power and exponential sums related to binomial digit parity*, SIAM J. Appl. Math. 32 (1977), 717–730.
[13] R. F. Tichy and G. Turnwald, *On the discrepancy of some special sequences*, J. Number Theory 26 (1987), 68–78.
[14] –, – *Gleichmässige Diskrepanzabschätzung für Ziffernsummen*, Anz. Österr. Akad. Wiss. (1986), 17–21.

MATHEMATISCHES INSTITUT
DER UNIVERSITÄT SALZBURG
Hellbrunner Strasse 34
A-5020 Salzburg, Austria

ABTEILUNG FÜR TECHNISCHE MATHEMATIK
TU WIEN
Wiedner Hauptstrasse 8–10
A-1040 Wien, Austria

Received on 14.8.1987 (1744)

ACTA ARITHMETICA
LII (1989)

On the number of values taken by a polynomial over a finite field

by

J. F. Voloch (Rio de Janeiro)

Let F_q be the finite field with q elements and $f(x) \in F_q[x]$ a polynomial of degree n. Let $r(f) = \#f(F_q)$, considering f as a function $f\colon F_q \to F_q$. A classical problem, raised by Chowla [3] (see [4] for other references), is to estimate $r(f)$ an terms of n and q. One has the trivial bounds $q/n \leqslant r(f) \leqslant q$. The lower bound is essentially best possible and a characterization of the cases with equality when q is prime was obtained in [2].

On the other hand, if f is a "general" polynomial (in a sense that can be made precise, see below) Uchiyama [6] proved that $r(f) \geqslant q/2 + O(q^{1/2})$ and Birch and Swinnerton-Dyer [1] found the precise result

$$r(f) = q\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i!}\right) + O(q^{1/2}).$$

They proved this when the Galois group of $f(x) = y$ over $\bar{F}_q(y)$ is the full symmetric group. Of course these results are interesting only when q is large compared to n. The purpose of this paper is to give lower bounds for $r(f)$, valid for f "general", which improves on the above bounds in several cases.

Uchiyama's condition is that the polynomial

$$f^*(u, v) = (f(u) - f(v))/(u - v)$$

is absolutely irreducible. When this is the case he could apply Weil's estimate ([7]) on the number of points of $f^*(u, v) = 0$ over F_q to get his result.

To relate the number of solutions of $f^*(u, v) = 0$ in F_q^2 with $r(f)$, Uchiyama [6] proved the following:

LEMMA 1. *Let N be the number of solutions of $f^*(u, v) = 0$ in F_q^2 and n_0 the number of solutions of $f'(x) = 0$ in F_q. Then*

$$r(f) \geqslant q^2/(N + q - n_0).$$

Proof. First notice that $f^*(u, v) = 0$ and $u \neq v$ if and only if $f(u) = f(v)$ and that $f^*(u, u) = f'(u)$. Let $\{a_1, \ldots, a_r\} = f(F_q)$, $r = r(f)$ and n_i

$= \#f^{-1}(a_i)$, $i = 1, \ldots, r$. Then $\sum_{i=1}^{r} n_i = q$ and

$$N = \sum_{i=1}^{r} n_i(n_i - 1) + n_0.$$

Hence, $\sum_{i=1}^{r} n_i^2 = N + q - n_0$. By the Cauchy–Schwarz inequality

$$\sum_{i=1}^{r} n_i^2 \geqslant \frac{1}{r}(\sum n_i)^2 = \frac{q^2}{r}$$

and the result follows.

Using the trivial bound $N \leqslant (n-1)q$ (since f^* has degree $n-1$) one gets $r(f) \geqslant q/n$. If f^* is absolutely irreducible (i.e. irreducible over $\bar{F}_q$), Weil's estimate $N \leqslant q + (n-3)(n-2)(q^{1/2}+1)$ gives

$$r(f) \geqslant \frac{q}{2} - \frac{(n-3)(n-2)(q^{1/2}+1)}{4}.$$

We shall now give upper bounds for N which follow from the results of [5] and improve on the above bounds on several instances.

THEOREM. *Let X be an absolutely irreducible plane curve of degree d defined over F_q with N rational points, then*

(i) *If q is prime and $q^{1/4} < d < q$ then $N \leqslant 4d^{4/3}q^{2/3}$.*

(ii) *If $h(x, y) = 0$ is an affine equation for X and $d^2y/dx^2 \neq 0$, then $N \leqslant \frac{1}{2}d(d+q-1)$.*

Proof. (i) Let X be an absolutely irreducible curve of degree D contained in P^n, not contained in a hyperplane. If p is the characteristic of F_q and $D \leqslant p$, it follows from [5], Theorem 2.13 and Corollary 2.7, that the number of rational points, M say, of a non-singular model of X satisfies

$$M \leqslant (n-1)(g-1) + D(q+n)/n$$

where g is the genus of X.

Returning to the situation of the theorem, let x, y be affine coordinates in the plane. If $m < d$, we can embed X in P^n, $n = \binom{m+2}{2} - 1$ by $(x, y) \mapsto (x, y, x^2, xy, y^2, \ldots, x^m, \ldots, y^m)$ in affine coordinates. In this case $D = md$, and this embedding is not contained in a hyperplane, so we can apply the above bound if $D \leqslant p$. Now the number of singular points of X is bounded by $(d-1)(d-2)/2 - g$, hence for $m < d$ and $D \leqslant p$ we get

$$N \leqslant (n-1)\frac{d(d-3)}{2} + \frac{D(q+n)}{n}$$

with $n = \binom{m+2}{2} - 1$, $D = md$.

If we take now $m = [(q/d)^{1/3}]$, the conditions $m < d$ and $D \leqslant p$ follow from the hypotheses $q^{1/4} < d < q$ and $q = p$, and the result stated follows immediately.

(ii) is just Theorem 0.1 of [5].

Applying item (i) of the theorem to $f^*(u, v) = 0$ when it is absolutely irreducible, it follows that $r(f) \geqslant \frac{1}{4}\left(\frac{q}{n-1}\right)^{4/3}$, if q is prime and $q^{1/4} < n-1 < q$. In this range this bound is better than those mentioned above.

Whenever (ii) applies, it gives

$$r(f) \geqslant \frac{2q^2}{(n+1)q + (n-1)(n-2)}$$

which improves on Uchiyama's bound for $n > q^{1/2}/2$.

We shall now study when the conditions $f^*(u, v)$ absolutely irreducible and $d^2v/du^2 \neq 0$ on $f^*(u, v) = 0$, hold. Consider the following condition on f:

(*) *f' has $n-1$ distinct roots* and f is injective on the roots of f'.

This condition already appears in [1]. There they prove that (*) is sufficient for the Galois group of $f(x) = y$ over $\bar{F}_q(y)$ to be the full symmetric group ([1], Lemma 3). They also remark that (*) is equivalent to the non-vanishing of the discriminant in y of the discriminant in x of $f(x) - y$. The aforementioned discriminant is a function on the coefficients of f, which does not vanish identically if $p \neq 2$ and $p \nmid n$, where p is the characteristic of F_q. Hence (*) is a generic condition.

Concerning condition (*) we shall prove

PROPOSITION. *Suppose that the characteristic of F_q is not 2 and let $f(x) \in F_q[x]$ be of degree $n \geqslant 2$.*

(i) *$f^*(u, v) = 0$ is non-singular if and only if f satisfies (*).*

(ii) *If f satisfies (*) then, on $f^*(u, v) = 0$, $d^2v/du^2 \neq 0$.*

Proof. (i) Let p be the characteristic of F_q. If $p \nmid n$ it is easy to see that $f^*(u, v) = 0$ has $n-1$ points at infinity, hence they are all non-singular points. If $p \mid n$ it is also easy to see that the point at infinity on the line $u = v$ is a singular point of $f^*(u, v) = 0$. Also condition (*) implies that $p \nmid n$, for otherwise f' would have degree at most $n-2$. This takes care of the points at infinity.

For the affine points, we have:

$$\frac{\partial f^*}{\partial u} = \frac{(u-v)f'(u)-(f(u)-f(v))}{(u-v)^2},$$

$$\frac{\partial f^*}{\partial v} = \frac{-(u-v)f'(v)+f(u)-f(v)}{(u-v)^2}.$$

A point (u_0, v_0) with $u_0 \neq v_0$ is in $f^*(u, v) = 0$ if and only if $f(u_0) = f(v_0)$ and is a singular point if and only if $f'(u_0) = f'(v_0) = 0$, in which case f is not injective on the set of zeros of $f'(x) = 0$.

Let now (u_0, u_0) be a point of $f^*(u, v) = 0$. Changing variables, x to $x+u_0$, u to $u+u_0$, v to $v+u_0$, we may assume that $u_0 = 0$ and $f'(0) = 0$. If $f(x) = \sum_{i=0}^{n} \alpha_i x^i$, then $\alpha_1 = 0$ and

$$f^*(u, v) = \alpha_2(u+v)+\alpha_3(u^2+uv+v^2)+ \ldots$$

Hence $(0, 0)$ is a singular point of $f^* = 0$ if and only if $\alpha_2 = 0$, which is equivalent to $x = 0$ be a double root of $f'(x) = 0$. This proves part (i) of the proposition.

(ii) On $f^*(u, v) = 0$ we have $f(u) = f(v)$, hence $f'(u) = f'(v)\,dv/du$ and

$$f''(u) = f''(v)(dv/du)^2+f'(v)\,d^2v/du^2.$$

If $d^2v/du^2 = 0$ we conclude that $f''(u)\cdot f'(v)^2 = f''(v)f'(u)^2$, whenever $f(u) = f(v)$. Suppose f satisfies (*). Let α be a root of $f'(x) = 0$. Since (*) holds there exists $\beta \neq \alpha$ with $f(\beta) = f(\alpha)$. Then

$$f''(\alpha)f'(\beta)^2 = f''(\beta)f'(\alpha)^2 = 0.$$

If $f''(\alpha) = 0$, α is a double root of $f'(x) = 0$, contradicting (*). If $f'(\beta) = 0$ then f is not injective on the roots of $f'(x) = 0$, again contradicting (*). This completes the proof of the proposition.

Remarks. 1. A non-singular plane curve is necessarily absolutely irreducible, since two irreducible components would necessarily meet at a singular point. Hence $f^* = 0$ is absolutely irreducible when (*) holds.

2. It follows from item (ii) of the proposition that item (ii) of the theorem holds for f^* whenever (*) holds for f and, in this case, we have the corresponding bound on $r(f)$.

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, D. J. Lewis, W. H. Mills and E. G. Straus, *Polynomials over finite fields with minimum value sets*, Mathematika 8 (1961), 121–130.

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

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[5] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52 (1986), 1–19.

[6] S. Uchiyama, *Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini*, Proc. Japan Acad. 30 (1955), 930–933.

[7] A. Weil, *Sur les courbes algébriques et variétés qui s'en déduisent*, Hermann, Paris 1948.

IMPA
Estrada Dona Castorina 110
22460 – Rio de Janeiro, RJ
Brazil

Received on 5.11.1987 (1765)