DISTINCT VALUES OF A POLYNOMIAL IN SUBSETS OF A FINITE FIELD

KENNETH S. WILLIAMS

1. Introduction. If A is a set with only a finite number of elements, we write $|A|$ for the number of elements in A. Let p be a large prime and let m be a positive integer fixed independently of p. We write $[p^m]$ for the finite field with p^m elements and $[p^m]'$ for $[p^m] - \{0\}$. We consider in this paper only subsets H of $[p^m]$ for which $|H| = h$ satisfies

$$\lim_{p\to\infty} \frac{p^{m/2}}{h} = 0. \tag{1.1}$$

If $f(x) \in [p^m, x]$ we let $N(f; H)$ denote the number of distinct values of y in H for which at least one of the roots of $f(x) = y$ is in $[p^m]$. We write d $(d \geqq 1)$ for the degree of f and suppose throughout that d is fixed and that $p \geqq p_0(d)$, for some prime p_0, depending only on d, which is greater than d. We call $f(x)$ primary if the coefficient of x^d is 1 and $f(0) = 0$. There are $p^{m(d-1)}$ primary polynomials of degree d over $[p^m]$. Uchiyama (**3**, p. 199) has proved that

$$\sum_{\deg f=d} N(f; [p^m]) = k_d p^{md} + O_d(p^{m(d-1)}), \tag{1.2}$$

where the summation is over all primary polynomials f defined over $[p^m]$ of degree d,

$$k_d = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + \frac{(-1)^{d-1}}{d!}, \tag{1.3}$$

and the subscript means that the O-symbol depends only on d, that is not on m or p. Our aim in this paper is to generalize (1.2). In § 3 we prove the following theorem.

THEOREM. *If H is any subset of $[p^m]$, satisfying* (1.1), *then*

$$\sum_{\deg f=d} N(f;H) = k_d h p^{m(d-1)} + O_d(p^{m(d-1/2)}). \tag{1.4}$$

This is a genuine asymptotic formula for large p as the term $O_d(p^{m(d-1/2)})$ is certainly $o(hp^{m(d-1)})$, as $p \to \infty$, in view of (1.1). We have thus generalized (1.2) but at the cost of weakening the error term.The error term in (1.4) can be improved when $d = 1$ or 2 to $O_d(p^{m(d-1)})$.

It turns out that the estimation of $\sum_{deg\ f=d} N(f; H)$ depends on that of the number of $(x_1, \ldots, x_d) \in [p^m]' \times \ldots \times [p^m]'$, $x_i \neq x_j$ $(i \neq j)$ for which

Received August 14, 1968. This research was supported in part by NRC Grant A-7233.

$(-1)^{d-1}x_1 \ldots x_d$ is in H. This number is denoted by $N(p, m, d, H)$. It is precisely in the estimation of $N(p, m, d, H)$ that the error term can be improved when $d = 1$ or 2 (or when $H = [p^m]$). We devote § 2 to the estimation of $N(p, m, d, H)$ and it will be shown there that

$$N(p, m, d, H) = hp^{m(d-1)} + O_d(p^{m(d-1/2)}). \tag{1.5}$$

2. Estimation of $N(p, m, d, H)$**.** We denote the trace of α from $[p^m]$ to $[p]$ by $t(\alpha)$, so that

$$t(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{m-1}} \in [p], \tag{2.1}$$

and hence can be considered as an integer (mod p). Clearly,

$$t(\alpha + \beta) = t(\alpha) + t(\beta) \tag{2.2}$$

and

$$t(\lambda\alpha) = \lambda t(\alpha), \tag{2.3}$$

for all $\alpha, \beta \in [p^m]$, $\lambda \in [p]$. Now let

$$e(\alpha) = \exp\{2\pi i t(\alpha)/p\}; \tag{2.4}$$

thus from (2.2) we have

$$e(\alpha + \beta) = e(\alpha)e(\beta). \tag{2.5}$$

It is well known that for $x \in [p^m]$, we have

$$\sum_{y \in [p^m]} e(xy) = \begin{cases} p^m & \text{if } x = 0, \\ 0 & \text{if } x \neq 0. \end{cases} \tag{2.6}$$

We define for any integer $k \geqq 1$,

$$S(k) = \{(x_1, \ldots, x_k) \mid x_i \in [p^m]', 1 \leqq i \leqq k\}.$$

Then, if $0 \neq a \in [p^m]$, we have on summing over x_d, by (2.6),

$$\sum_{S(d)} e(ax_1 \ldots x_d) = \sum_{S(d-1)} (-1) = -(p^m - 1)^{d-1}. \tag{2.7}$$

It is also well known (**1**, p. 39, display (12)) that for $0 \neq b \in [p^m]$ and $p > k \geqq 1$, we have:

$$\left| \sum_{y \in [p^m]} e(by^k) \right| \leqq (k-1)p^{m/2}. \tag{2.8}$$

For any l ($\geqq 1$) positive integers $i_1, \ldots, i_l$ we define

$$T(l) = \{x_{i_1}, \ldots, x_{i_l}) \mid x_{i_j} \in [p^m]', \quad 1 \leqq j \leqq l\}.$$

Thus for any positive integers $r, i_1, \ldots, i_r, a_1, \ldots, a_r$ satisfying

$$1 \leqq r \leqq d-1, \quad 1 \leqq i_1 < i_2 < \ldots < i_r \leqq d, \quad a_1 + a_2 + \ldots + a_r = d, \tag{2.9}$$

we have, by (2.8), as $p > d$,

$$\left| \sum_{T(r)} e(ax_{i_1}{}^{a_1} \ldots x_{i_r}{}^{a_r}) \right| \leqq \sum_{T(r-1)} \left| \sum_{x_{i_r} \in [p^m]'} e\{(ax_{i_1}{}^{a_1} \ldots x_{i_{r-1}}{}^{a_{r-1}}) x_{i_r}{}^{a_r}\} \right|$$

$$\leqq \sum_{T(r-1)} \{(a_r - 1)p^{m/2} + 1\} \leqq a_r p^{m/2} \cdot (p^m)^{r-1},$$

and thus as $r \leqq d - 1$, $a_r \leqq d$ we have:

$$\left| \sum_{T(r)} e(ax_{i_1}{}^{a_1} \ldots x_{i_r}{}^{a_r}) \right| \leqq dp^{m(d-3/2)}. \tag{2.10}$$

From (2.7) and (2.10) we have:

$$\sum_{S(d)}^{*} e(ax_1 \ldots x_d) = -(p^m - 1)^{d-1} + O_d(p^{m(d-3/2)}), \tag{2.11}$$

where the asterisk means that the summation is only taken over those $(x_1, \ldots, x_d) \in [p^m]' \times \ldots \times [p^m]'$ for which $x_i \neq x_j$ $(i \neq j)$, since any sum

$$\sum_{S(d)} e(ax_1 \ldots x_d) \quad (x_i = x_j \text{ for at least one pair } (i, j) \ (i \neq j)), \tag{2.12}$$

is of the form (2.10) for some $r, i_1, \ldots, i_r, a_1, \ldots, a_r$ satisfying (2.9). There are $O_d(1)$ such sums (2.12).

Now $N(p, m, d, H)$ is just the number of

$$(x_1, \ldots, x_d, y) \in [p^m]' \times \ldots \times [p^m]' \times H, \qquad x_i \neq x_j \ (i \neq j),$$

for which $(-1)^{d-1}x_1 \ldots x_d - y = 0$. Hence by (2.6) we have:

$$N(p, m, d, H) = \frac{1}{p^m} \sum_{S(d)}^{*} \sum_{y \in H} \sum_{t \in [p^m]} e\{t((-1)^{d-1}x_1 \ldots x_d - y)\}. \tag{2.13}$$

The terms with $t = 0$ in (2.13) contribute

$$\frac{1}{p^m} \sum_{S(d)}^{*} \sum_{y \in H} 1 = \frac{h}{p^m} (p^m - 1)(p^m - 2) \ldots (p^m - d).$$

The terms with $t \neq 0$ yield:

$$\frac{1}{p^m} \sum_{y \in H} \sum_{t \in [p^m]'} e(-ty) \sum_{S(d)}^{*} e((-1)^{d-1}tx_1 \ldots x_d)$$

$$= \frac{1}{p^m} \sum_{y \in H} \sum_{t \in [p^m]'} e(-ty)\{-(p^m - 1)^{d-1} + O_d(p^{m(d-3/2)})\}$$

$$= -\frac{(p^m - 1)^{d-1}}{p^m} \sum_{y \in H} \sum_{t \in [p^m]'} e(-ty) + O_d(p^{m(d-1/2)})$$

$$= -\frac{(p^m - 1)^{d-1}}{p^m} \{p^m \delta(H) - h\} + O_d(p^{m(d-1/2)}),$$

where

$$\delta(H) = \begin{cases} 1 & \text{if } 0 \in H, \\ 0 & \text{if } 0 \notin H. \end{cases} \tag{2.14}$$

Clearly

$$-\frac{(p^m - 1)^{d-1}}{p^m}\{p^m\delta(H) - h\} = O(p^{m(d-1)});$$

thus (2.13) becomes

$$N(p, m, d, H) = hp^{m(d-1)} + O_d(p^{m(d-1/2)}),$$

as required.

3. Proof of the Theorem. Let $g_0, g_1, \ldots, g_{p^m-1}$ be the p^m elements of $[p^m]$, with $g_0 = 0$. We let

(3.1) $\quad M \equiv M(p, m, d, H, x)$

$$= \{f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x - y \mid a_i \in [p^m], y \in H\}$$

so that $|M| = hp^{m(d-1)}$. For $i = 0, 1, \ldots, p^m - 1$ we define

(3.2) $\quad M_i \equiv M_i(p, m, d, H, g_i, x) = \{f \in M \mid f \text{ a multiple of } x - g_i\}.$

Now for

$$0 \leqq i_1 < i_2 < \ldots < i_r \leqq p^m - 1,\ 1 \leqq r \leqq d - 1\ (\leqq p - 2 \leqq p^m - 2)$$

we have:

$|M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_r}|$

$$= \text{number of } f \in M \text{ which are multiples of } \prod_{j=1}^{r}(x - g_{i_j})$$

$$= \text{number of } b_{d-r-1}, \ldots, b_0 \in [p^m] \text{ such that}$$

$$\prod_{j=1}^{r}(x - g_{i_j})(x^{d-r} + b_{d-r-1}x^{d-r-1} + \ldots + b_1 x + b_0) \in M$$

$$= p^{m(d-r-1)} \cdot \begin{cases} p^m & \text{if } i_1 = 0, 0 \in H, \\ 0 & \text{if } i_1 = 0, 0 \notin H, \\ h & \text{if } i_1 \neq 0, \end{cases}$$

as $(-1)^{r-1}g_{i_1} \ldots g_{i_r}$ has an inverse in $[p^m]$ if and only if $i_1 \neq 0$. Thus from (2.14) we have:

$$|M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_r}| = \begin{cases} p^{m(d-r)}\,\delta(H) & \text{if } i_1 = 0, \\ p^{m(d-r-1)}h & \text{if } i_1 \neq 0. \end{cases}$$

Hence, writing $U(k, l) = \{(i_1, \ldots, i_k) \mid l \leqq i_1 < i_2 < \ldots < i_k \leqq p^m - 1\}$, we have for $1 \leqq r \leqq d - 1$ $(\leqq p^m - 2)$:

$$\sum_{U(r,0)} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_r}|$$
$$= \sum_{U(r,0)-U(r,1)} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_r}| + \sum_{U(r,1)} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_r}|$$
$$= \binom{p^m - 1}{r - 1} p^{m(d-r)} \delta(H) + \binom{p^m - 1}{r} p^{m(d-r-1)} h$$
$$= hp^{m(d-r-1)} \left\{ \frac{p^{mr}}{r!} + O_r(p^{m(r-1)}) \right\} + \delta(H) p^{m(d-r)} O_r(p^{m(r-1)})$$
$$= \frac{hp^{m(d-1)}}{r!} + O_r(p^{m(d-1)}), \quad \text{as } h \leqq p^m.$$

We next estimate

$$|M_{i_1} \cap \ldots \cap M_{i_d}| = \text{number of } f = \prod_{j=1}^{d} (x - g_{i_j}) \in M$$
$$= \begin{cases} 1 & \text{if } (-1)^{d-1} g_{i_1} \ldots g_{i_d} \in H, \\ 0 & \text{otherwise,} \end{cases}$$

hence

$$\sum_{U(d,0)} |M_{i_1} \cap \ldots \cap M_{i_d}| = \sum_{U(d,0)}^{\dagger} 1,$$

where the dagger (†) denotes that only those $(i_1, \ldots, i_d)$ are counted for which $(-1)^{d-1} g_{i_1} \ldots g_{i_d} \in H$. Thus on picking out the terms with $i_1 = 0$ we have:

$$\sum_{U(d,0)}^{\dagger} 1 = \binom{p^m - 1}{d - 1} \delta(H) + \sum_{U(d,1)}^{\dagger} 1.$$

Now

$$d! \sum_{U(d,1)}^{\dagger} 1 = \sum_{(-1)^{d-1} x_1 \ldots x_d \in H}^{*} 1 = N(p, m, d, H)$$
$$= hp^{m(d-1)} + O_d(p^{m(d-1/2)}), \quad \text{by (1.5).}$$

Hence

$$\sum_{U(d,0)} |M_{i_1} \cap \ldots \cap M_{i_d}| = \frac{hp^{m(d-1)}}{d!} + O_d(p^{m(d-1/2)}).$$

Now

$$\sum_{\deg f = d} N(f; H) = |M_0 \cup M_1 \cup \ldots \cup M_{p^m - 1}|$$
$$= \sum_{r=1}^{d} (-1)^{r-1} \sum_{U(r,0)} |M_{i_1} \cap \ldots \cap M_{i_r}|$$
$$= \sum_{r=1}^{d-1} (-1)^{r-1} \left\{ \frac{hp^{m(d-1)}}{r!} + O_r(p^{m(d-1)}) \right\} + (-1)^{d-1} \left\{ \frac{hp^{m(d-1)}}{d!} + O_d(p^{m(d-1/2)}) \right\}$$
$$= hp^{m(d-1)} \sum_{r=1}^{d} \frac{(-1)^{r-1}}{r!} + O_d(p^{m(d-1/2)}),$$

as required.

https://doi.org/10.4153/CJM-1969-162-0 Published online by Cambridge University Press

4. Conclusion. The Theorem shows that for any given subset H of $[p^m]$ we have:

$$N(f; H) = k_d h + O_d(p^{m/2}) \tag{4.1}$$

on the average. Carlitz and Uchiyama (**1**, p. 40, display (17)) have also shown that

$$\sum_{\deg f=d} N^2(f; [p^m]) = k_d^{\,2} p^{m(d+1)} + O_d(p^{md}). \tag{4.2}$$

It would be interesting to find an analogous asymptotic formula for

$$\sum_{\deg f=d} N^2(f; H). \tag{4.3}$$

It seems reasonable to conjecture that the main term of any such asymptotic formula for (4.3), when it exists, would be

$$k_d^{\,2} h^2 p^{m(d-1)}. \tag{4.4}$$

This is certainly true when $d = 1$. It can also be verified in special cases when $d = 2$, 3 or 4. For example (see **2**, p. 79, Theorem 2) when $d = 4$ (so that $k_d = 5/8$), $m = 1$, $p > 3$ and H an arithmetic progression of h $(\leqq p)$ distinct terms in $[p]$, it was shown that

$$N(f; H) = (5/8)h + O(p^{1/2} \log p) \quad \text{if and only if } a_3{}^3 - 4a_2a_3 + 8a_1 \neq 0. \tag{4.5}$$

Hence

$$\begin{aligned} \sum_{\deg f=4} N^2(f; H) &= (p^3 - p^2)((5/8)h + O(p^{1/2} \log p))^2 + p^2 O(h^2) \\ &= (25/64)h^2 p^3 + O(p^{9/2} \log p), \quad \text{if} \lim_{p\to\infty} \frac{p^{3/4}\sqrt{\log p}}{h} = 0. \end{aligned}$$

References

1. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. *24* (1957), 37–41.
2. K. McCann and K. S. Williams, *The distribution of the residues of a quartic polynomial*, Glasgow Math. J. *8* (1967), 67–88.
3. S. Uchiyama, *Note on the mean value of V(f)*, Proc. Japan Acad. *31* (1955), 199–201.

Queen's University,
Kingston, Ontario;
Carleton University,
Ottawa, Ontario

https://doi.org/10.4153/CJM-1969-162-0 Published online by Cambridge University Press