Canad. Math. Bull. Vol. 14 (3), 1971

NOTE ON THE NUMBER OF SOLUTIONS OF $f(x_1)=f(x_2)=\cdots=f(x_r)$ OVER A FINITE FIELD

BY
KENNETH S. WILLIAMS

Let $GF(q)$ denote the finite field with $q=p^n$ elements and let

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

where each $a_i \in GF(q)$ and $1<d<p$. For $r=2,3,\ldots,d$ we let n_r denote the number of solutions $(x_1,\ldots,x_r)$ over $GF(q)$ of

$$f(x_1)=f(x_2)=\cdots=f(x_r), \tag{2}$$

for which $x_1, x_2,\ldots,x_r$ are all different. Birch and Swinnerton-Dyer [1] have shown that

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

where each ν_r is a nonnegative integer depending on f and q and the constant implied by the O-symbol depends here, and throughout the paper, only on d. It is the purpose of this note to calculate ν_2 and conjecture the value of ν_3 in terms of the number of absolutely irreducible factors over $GF(q)$ of

$$f^*(x,y) = \frac{f(x)-f(y)}{x-y}. \tag{4}$$

In order to do this we introduce, for $x \in GF(q)$,

$$n(x) = \sum_{\substack{y\in GF(q)\\ f(x)=f(y)}} 1, \tag{5}$$

so that

$$n_r = \sum_{x\in GF(q)} \left\{\prod_{i=1}^{r-1} (n(x)-i)\right\}. \tag{6}$$

In particular

$$\begin{aligned} n_2 &= \sum_{x\in GF(q)} (n(x)-1) \\ &= \sum_{\substack{x,y\in GF(q)\\ f^*(x,y)=0}} 1+O(1) \\ &= aq+O(q^{1/2}), \end{aligned}$$

Received by the editors August 10, 1970.

https://doi.org/10.4153/CMB-1971-074-0 Published online by Cambridge University Press

appealing to a result based on the deep work of Lang and Weil (see [2, Lemma 8]), where a is the number of absolutely irreducible factors of $f^*(x, y)$ over $GF(q)$. Clearly $0 \le a \le d-1$. Hence we have proved:

THEOREM 1. *For $q \ge A_1(d)$, where $A_1(d)$ is a constant depending only on d,*

$$\nu_2 = a. \tag{7}$$

A similar result for ν_3 seems difficult to obtain and we prove only

THEOREM 2. *For $q \ge A_2(d)$, where $A_2(d)$ is a constant depending only on d,*

$$a^2-a \le \nu_3 \le (d-3)(a+1)+2. \tag{8}$$

We have from (6)

$$n_3 = \sum_{x \in GF(q)} (n(x)-1)(n(x)-2)$$

so that

$$\sum_{x \in GF(q)} \{n(x)\}^2 = n_3+(3a+1)q+O(q^{1/2}).$$

Now

$$\frac{1}{q}\left\{\sum_{x \in GF(q)} n(x)\right\}^2 \le \sum_{x \in GF(q)} \{n(x)\}^2 \le \max_{x \in GF(q)} n(x) \cdot \sum_{x \in GF(q)} n(x)$$

so that

$$\frac{1}{q}\{(a+1)q+O(q^{1/2})\}^2 \le n_3+(3a+1)q+O(q^{1/2}) \le d\{(a+1)q+O(q^{1/2})\}$$

giving

$$(a^2-a)q+O(q^{1/2}) \le n_3 \le ((d-3)(a+1)+2)q+O(q^{1/2}),$$

which gives the result.

Theorem 2 gives the exact value of ν_3 when

$$a^2-a = (d-3)(a+1)+2,$$

that is when

$$a = d-1,$$

in which case $f^*(x, y)$ factorizes completely into linear factors over $GF(q)$. Such a polynomial is extremal of index $d-1$ and has $\nu_3 = a^2-a$ (see [3]). More generally if $f(x)$ is extremal of index a $(0 \le a \le d-1)$, that is $f^*(x, y)$ in its unique decomposition into irreducible factors has a linear factors and no non-linear absolutely irreducible factors, then $\nu_3 = a^2-a$. If we write l for the number of linear factors of $f^*(x, y)$ over $GF(q)$ in the case of extremal polynomials we have $a = l$. Next let us examine some polynomials of small degree for which $a \neq l$. If $f(x)=x^3+cx(c\neq 0)$, $f^*(x, y)=x^2+xy+y^2+c$, which is absolutely irreducible over $GF(q)$ as $p>3$. In this case $a=1$, $l=0$, $\nu_3=1$. If $f(x)=x^4+cx^2(c\neq 0)$, $f^*(x, y)=(x+y)(x^2+y^2+c)$, so that $a=2$, $l=1$, $\nu_3=3$. Finally if $f(x)=x^4+cx^2+ex$ $(e\neq 0)$, $f^*(x, y)$ is absolutely irreducible over $GF(q)$ as $p>4$, and $a=1$, $l=0$, $\nu_3=1$. In all these examples we see that $\nu_3=a^2-l$ and so we make our first conjecture.

Conjecture 1. For $q \geq A_3(d)$, where $A_3(d)$ is a constant depending only on d,

$$\nu_3 = a^2-l. \tag{9}$$

It is easy to check that this conjecture is consistent with Theorem 2, we have only to prove that

$$a^2-l \leq (d-3)(a+1)+2.$$

As the sum of the degrees of the l linear factors and the $(a-l)$ nonlinear absolutely irreducible factors of f^* is at most the degree of f^* we have

$$1\cdot l+2(a-l) \leq d-1,$$

that is,

$$l \geq 2a-d+1,$$

so that

$$\begin{aligned} a^2-l &\leq a(a-2)+d-1 \\ &\leq a(d-3)+d-1, \quad \text{as } a \leq d-1, \\ &= (a+1)(d-3)+2, \end{aligned}$$

as claimed.

Conjecture 1 could be proved if we could prove

Conjecture 2. If $a(x, y)$, $a'(x, y)$ are nonlinear absolutely irreducible factors of $f^*(x, y)$ over $GF(q)$ (possibly $a=a'$) then the number of solutions (x, y, z) over $GF(q)$ of $a(x, y)=a'(x, z)=0$ with $x\neq y$, $y\neq z$, $z\neq x$ is $q+O(q^{1/2})$.

To see this we write (as f^* has no squared factors over $GF(q)$).

$$f^*(x, y) = \prod_{i=1}^{l} l_i(x, y) \prod_{j=1}^{a-l} a_j(x, y) \prod_{k=1}^{m} t_k(x, y), \tag{10}$$

where each l_i is linear, each a_j is nonlinear and absolutely irreducible over $GF(q)$, and each t_k is irreducible but not absolutely irreducible over $GF(q)$. Now the number of solutions (x, y, z) over $GF(q)$ with $x\neq y$, $y\neq z$, $z\neq x$ of

(i) $l_i(x, y)=l_j(x, z)=0$ is $q+O(1)$, if $i\neq j$; 0 if $i=j$ (see [3]),

(ii) $l_i(x, y)=a_j(x, z)=0$ or $a_j(x, y)=l_i(x, z)=0$ is $q+O(q^{1/2})$, as a_j is absolutely irreducible,

(iii) $a_i(x, y)=a_i(x, z)=0$ is $q+O(q^{1/2})$, by Conjecture 2,

(iv) $t_i(x, y) = a_j(x, z) = 0$ or $t_i(x, y) = l_j(x, z) = 0$ or $t_i(x, y) = t_j(x, z) = 0$ is $O(1)$ as t_i is irreducible but not absolutely irreducible (see [3]).

Hence n_3, which is just the number of solutions of $f^*(x, y) = f^*(x, z) = 0$ with $x \neq y$, $y \neq z$, $z \neq x$, is given by

$$(l^2 - l)(q + O(1)) + 2(a-l)l(q + O(q^{1/2})) + (a-l)^2(q + O(q^{1/2})) \\ + 2m(a+m)O(1) = (a^2 - l)q + O(q^{1/2}),$$

as conjectured.

References

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

2. J. H. H. Chalk and K. S. Williams, *The distribution of solutions of congruences*, Mathematika **12** (1965), 176–192.

3. K. S. Williams, *On extremal polynomials*, Canad. Math. Bull. **10** (1967), 585–594.

Carleton University,
Ottawa, Ontario