POLYNOMIALS WITH IRREDUCIBLE FACTORS OF SPECIFIED DEGREE

Kenneth S. Williams

Let d be a positive integer and let p be a prime $> d$. Set $q = p^m$, where $m \geq 1$, and let $I(q, d)$ denote the number of distinct primary irreducible polynomials of degree d over $GF(q)$. It is a simple deduction from the well-known expression for $I(q, d)$ that

$$(1) \qquad \left| I(q, d) - \frac{1}{d} q^d \right| \leq \left(1 - \frac{1}{d}\right) q^{d^*},$$

where d^* is the largest positive integer $< d$ which divides d if $d > 1$, and d^* is 0 if $d = 1$. We can write (1) as an asymptotic formula, namely,

$$(2) \qquad I(q, d) = \frac{1}{d} q^d + O(q^{d^*}),$$

where the constant implied by the O-symbol depends here (and throughout this note) only on d. Our purpose in this note is to obtain a generalization of (2).

Let e and s be integers such that $1 \leq e \leq d$ and $1 \leq s \leq [d/e]$. We let $I(q, d, e, s)$ denote the number of distinct primary polynomials of degree d over $GF(q)$ having exactly s distinct primary irreducible factors of degree e over $GF(q)$. We prove that

$$(3) \qquad I(q, d, e, s) = \ell_{d,e,s} q^d + O(q^{d-e+e^*}),$$

where

$$(4) \qquad \ell_{d,e,s} = \sum_{i=0}^{[d/e]-s} \frac{(-1)^i}{i!\, s!\, e^{i+s}}.$$

This provides a generalization of (2), as $I(q, d, d, 1) \equiv I(q, d)$ and $\ell_{d,d,1} = 1/d$.

We begin by noting that $I(q, e) > [d/e]$, for from (1),

$$\begin{aligned} I(q, e) &\geq \frac{1}{e} q^{e} - (1 - \frac{1}{e}) q^{e^*} \\ &\geq \frac{1}{e} \{q^{e} - (e-1) q^{e-1}\}, \text{ as } e^* \leq e-1, \\ &\geq \frac{1}{e} \{e q^{\max(1, e-1)} - (e-1) q^{e-1}\}, \text{ as } q \geq e, \\ &\geq q/e \\ &> d/e . \end{aligned}$$

Thus the number of primary polynomials of degree d over $GF(q)$ which are divisible by i distinct primary irreducible polynomials of degree e over $GF(q)$ is q^{d-ie}, if $1 \leq i \leq [d/e]$, and 0, if $[d/e] < i \leq I(q, e)$. Hence, by the input-output formula, the number of such polynomials with with at least one primary irreducible factor of degree e is

$$(5) \qquad \sum_{i=1}^{[d/e]} (-1)^{i-1} \binom{I(q, e)}{i} q^{d-ie} .$$

From (2) we have

$$\binom{I(q, e)}{i} = \frac{q^{ie}}{i!\, e^{i}} + O\left(q^{ie-e+e^*}\right) ,$$

so (5) becomes

$$(6) \qquad \left\{ \sum_{i=1}^{[d/e]} \frac{(-1)^{i-1}}{i!\, e^{i}} \right\} q^{d} + O\left(q^{d-e+e^*}\right) .$$

Hence the number of primary polynomials of degree d over $GF(q)$ having no irreducible factor of degree e over $GF(q)$ is given by

$$(7) \qquad N(q, e, d) = \left\{ \sum_{i=0}^{[d/e]} \frac{(-1)^{i}}{i!\, e^{i}} \right\} q^{d} + O(q^{d-e+e^*}) .$$

Now

$$(8) \qquad I(q, d, e, s) = M(q, e, s)\, N(q, e, d - es) ,$$

where we understand $N(q, e, d - es)$ to mean q^{d-es} when $s = [d/e]$, and $M(q, e, s)$ denotes the number of distinct polynomials which are the product of s (not necessarily distinct) primary irreducible polynomials of degree e over $GF(q)$. $M(q, e, s)$ is just the number of distinct s-combinations with repetition of $I(q, e)$ distinct things and so is just

$$(9) \qquad \binom{I(q, e) + s - 1}{s} = \frac{q^{es}}{s!\, e^s} + O(q^{es - e + e^*}) .$$

Hence from (7), (8) and (9)

$$I(q, d, e, s) = \left\{ \frac{q^{es}}{s!\, e^s} + O(q^{es-e+e^*}) \right\} \left\{ \left(\sum_{i=0}^{[d/e]-s} \frac{(-1)^i}{i!\, e^i} \right) q^{d-es} + O(q^{d-es-e+e^*}) \right\}$$

$$= \ell_{d, e, s} q^d + O(q^{d-e+e^*}) ,$$

as required. We remark that (5) and (6) were obtained by Uchiyama (Note on the mean value of $V(f)$. II, Proc. Japan Acad. 31 (1955) 321-323) when $e = 1$, in his work on the distinct values of a polynomial over a finite field.

Summer Research Institute
Queen's University
Kingston

Carleton University
Ottawa