PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 31, No. 2, February 1972

THE DISTRIBUTION OF ABSOLUTELY IRREDUCIBLE POLYNOMIALS IN SEVERAL INDETERMINATES

M. L. FREDMAN

ABSTRACT. Asymptotic formulas are derived for the distribution of absolutely irreducible polynomials in two indeterminates over finite fields. A pair of inversion formulas is presented which yield exact formulas relating the distributions of irreducible and absolutely irreducible polynomials.

1. **Introduction.** An absolutely irreducible polynomial over a field F is a polynomial that has no proper factorization in any extension field of F. The only absolutely irreducible polynomials in one indeterminate are first degree polynomials. In this paper we examine the distribution of absolutely irreducible polynomials in two indeterminates with coefficients in $GF(q)$. L. Carlitz has derived ([**1**] and [**2**]) estimates for the number of irreducible polynomials in two indeterminates with coefficients in $GF(q)$. We use his estimates to derive some of the results presented here.

Let $f_j(m, n)$ denote the number of normalized polynomials in x and y with coefficients in $GF(q^j)$, where m is the degree in x and n is the degree in y. Let $\psi_j(m, n)$ denote the number of normalized irreducible polynomials. Finally, let $\tau_j(m, n)$ denote the number of normalized absolutely irreducible polynomials with coefficients contained in $GF(q^j)$ but not contained in any proper subfield of $GF(q^j)$ that contains $GF(q)$. We prove

$$(1) \qquad \tau_j(m, n) = \psi_j(m, n) + O(q^{j(m+2)(n+2)/2}), \qquad m, n > 0.$$

Combining this with the result in [**2**], we have

$$(2) \qquad \tau_j(m, n) \sim (1 - q^{-jm}) f_j(m, n) \qquad (n \to \infty)$$

for fixed m.

We remark that $\tau_1(m, n)$ is the number of normalized absolutely irreducible polynomials with coefficients in $GF(q)$.

2. **The relation between $\tau_j(m, n)$ and $\psi_j(m, n)$.** We begin by presenting the following formula.

Received by the editors June 29, 1970.

AMS 1970 *subject classifications.* Primary 12C05; Secondary 10A20.

Key words and phrases. Irreducible polynomial, absolutely irreducible, several indeterminates, finite fields, inversion formulas, distributions.

THEOREM 1.

$$\psi_j(m, n) = \sum_{d|m;d|n} (1/d) \sum_{e|j;(e,d)=1} \tau_{jd/e}(m/d, n/d). \tag{3}$$

PROOF. Let $p(x, y)$ be an irreducible polynomial with coefficients in $GF(q^j)$ of degrees m and n in x and y. Assume $p(x, y)=t_1(x, y)t_2(x, y) \cdots t_d(x, y)$ when factored into absolute irreducibles. It is not difficult to show

(A) The coefficients of each polynomial, $t_1(x, y), \cdots, t_d(x, y)$, are contained in $GF(q^{jd})$ but in no smaller field containing $GF(q^j)$.

(B) $t_1(x, y), \cdots, t_d(x, y)$ are distinct and they form the complete set of automorphic images of $t_1(x, y)$ with respect to the automorphisms of $GF(q^{jd})$ that fix $GF(q^j)$.

Conversely, if $t_1(x, y), \cdots, t_d(x, y)$ satisfy (A) and (B), then $t_1(x, y)t_2(x, y) \cdots t_d(x, y)$ is irreducible in $GF(q^j)$. Hence,

$$\psi_j(m, n) = \sum_{d|m;d|n} (1/d)H_{j,d}(m/d, n/d) \tag{4}$$

where $H_{j,d}(m, n)$ denotes the number of normalized absolutely irreducible polynomials with coefficients contained in $GF(q^{jd})$ but in no smaller field containing $GF(q^j)$. Clearly,

$$H_{j,d}(m, n) = \sum_{r:\mathrm{lcm}(r,j)=dj} \tau_r(m, n) = \sum_{e|j;(e,d)=1} \tau_{jd/e}(m, n). \tag{5}$$

Equations (4) and (5) imply (3), and this proves the theorem.

It is convenient to rewrite equation (3) as follows:

$$\psi_j(m, n) - S_j(m, n) = \sum_{e|j} \tau_e(m, n) \tag{6}$$

where

$$S_j(m, n) = \sum_{e|j} \sum_{d|m;d|n;d\neq 1;(d,e)=1} (1/d)\tau_{jd/e}(m/d, n/d). \tag{6.1}$$

Using (6) and (6.1), $\tau_j(m, n)$ can be computed recursively in terms of $\psi_j(m, n)$. When $(m, n)=1$, we clearly have $S_j(m, n)=0$. Inverting (6), we obtain $\tau_j(m, n)=\sum_{d|j} \mu(j/d)\psi_d(m, n)$ when $(m, n)=1$. Now assume $\tau_j(a, b)$ has been computed when $(a, b)<k$, and assume $(m, n)=k$. Then we have enough information to compute $S_j(m, n)$ using (6.1); and by inverting (6) we can compute $\tau_j(m, n)$.

3. Estimates for $\tau_j(m, n)$.

We are now ready to prove (1).

THEOREM 2. $\tau_j(m, n)=\psi_j(m, n)+O(q^{j(m+2)(n+2)/2})$, $m, n>0$.

PROOF. Referring to equations (6) and (6.1), we begin by showing that $S_j(m, n)=O(q^{j(m+2)(n+2)/2})$. Clearly $\tau_j(m, n)\leqq f_j(m, n)\leqq q^{j(m+1)(n+1)}$. Hence,

$$\tau_{jd/e}(m/d, n/d) = O(q^{(jd/e)(m/d+1)(n/d+1)}),$$

and

$$\sum_{d|m;d|n;d\neq 1} (1/d)\tau_{jd/e}(m/d, n/d) = O(q^{(j/e)(m+2)(n+2)/2}).$$

Finally,

$$S_j(m, n) = \sum_{e|j} O(q^{(j/e)(m+2)(n+2)/2}) = O(q^{j(m+2)(n+2)/2}).$$

Using this estimate for $S_j(m, n)$, we invert (6) to obtain

$$\tau_j(m, n) = \sum_{d|j} \mu(j/d)\psi_d(m, n) + \sum_{d|j} O(q^{d(m+2)(n+2)/2}).$$

Hence

$$\tau_j(m, n) = \sum_{d|j} \mu(d)\psi_{j/d}(m, n) + O(q^{j(m+2)(n+2)/2}). \tag{7}$$

Now

$$\sum_{d|j} \mu(j/d)\psi_d(m, n) = \psi_j(m, n) + \sum_{d|j;d\neq 1} \mu(d)\psi_{j/d}(m, n).$$

Using the fact that $\psi_{j/d}(m, n) \leqq f_{j/d}(m, n) = O(q^{(j/d)(m+1)(n+1)})$, we have

$$\sum_{d|j} \mu(d)\psi_{j/d}(m, n) = \psi_j(m, n) + O(q^{j(m+1)(n+1)/2}). \tag{8}$$

Theorem 2 is proved by combining equations (7) and (8).

THEOREM 3. $\tau_j(m, n) \sim (1 - q^{-jm})f_j(m, n)$ $(n \to \infty)$ *for fixed* m.

PROOF. It is easy to show that $f_j(m, n) > A_j q^{j(m+1)(n+1)}$ for some constant $A_j > 0$. From Theorem 2 it follows that $\tau_j(m, n) = \psi_j(m, n) + o(f_j(m, n))$ $(n \to \infty)$ for fixed $m > 0$. In [2], Carlitz proves that $\psi_j(m, n) \sim (1 - q^{-jm})f_j(m, n)$ $(n \to \infty)$ for fixed m. These considerations prove the theorem for the case where $m > 0$. When $m = 0$, $(1 - q^{-jm}) = 0$, and $\tau_j(m, n) = 0$ when $n > 1$. Hence, the theorem is obvious for this case.

We conclude this paper with some remarks about the single indeterminate analogue of equation (3):

$$\psi_j(m) = \sum_{d|m} (1/d) \sum_{e|j;(e,d)=1} \tau_{jd/e}(m/d). \tag{9}$$

It is an interesting exercise to derive the formula,

$$\psi_j(m) = (1/m) \sum_{d|m} \mu(d) q^{jm/d},$$

from considerations involving equation (9). First, it is clear that $\tau_j(m) = 0$ when $m > 1$. Recalling the definition of $\tau_j(m)$, it is easy to show that $q^j = \sum_{d|j} \tau_d(1)$. Hence, $\tau_j(1) = \sum_{d|j} \mu(d) q^{j/d}$. Substituting these expressions for $\tau_j(m)$ in equation (9), we obtain

$$\psi_j(m) = (1/m) \sum_{e|j;(e,m)=1} \sum_{d|jm/e} \mu(d) q^{jm/de}. \tag{10}$$

Now in equation (10), either $d=d_1d_2$ where $(d_1, m)=1$, $d_1 \mid j/e$, $d_2 \mid m$; or $\mu(d)=0$. Hence,

$$\psi_j(m) = (1/m) \sum_{e\mid j;(e,m)=1} \sum_{d_1\mid j/e;(d_1,m)=1} \mu(d_1) \sum_{d_2\mid m} \mu(d_2) q^{jm/(d_1d_2e)}$$
$$= (1/m) \sum_{r\mid j;(r,m)=1} \sum_{d_1e=r} \mu(d_1)\left(\sum_{d_2\mid m} \mu(d_2) q^{jm/rd_2}\right) = (1/m)\sum_{d\mid m} \mu(d) q^{jm/d}.$$

We can continue these arguments to obtain the following inversion formulas. Given functions $A(j, m)$ and $B(j, m)$ over positive integers j and m,

$$A(j, m) = \sum_{d\mid m} (1/d) \sum_{e\mid j;(e,d)=1} B(jd/e, m/d) \quad \text{if and only if}$$
$$(11) \qquad B(j, m) = \sum_{d\mid j} \sum_{e\mid m} \mu(d)\mu(e) \sum_{c\mid m/e} cA(je/d, c).$$

Given fixed u and v with $(u, v)=1$, if we choose $A(j, m)=\psi_j(mu, mv)$ and $B(j, m)=\tau_j(mu, mv)$, then (11) produces an exact solution to (3).

References

1. L. Carlitz, *The distribution of irreducible polynomials in several indeterminates*, Illinois J. Math. **7** (1963), 371–375. MR **27** #3627.

2. ———, *The distribution of irreducible polynomials in several indeterminates*. II, Canad. J. Math. **17** (1965), 261–266. MR **30** #3088.

3. Stephen D. Cohen, *The distribution of irreducible polynomials in several indeterminates over a finite field*, Proc. Edinburgh Math. Soc. (2) **16** (1968/69), 1–17. MR **38** #138.

Department of Computer Science, Stanford University, Stanford, California 94305