FURTHER ARITHMETICAL FUNCTIONS IN FINITE FIELDS

by STEPHEN D. COHEN

(Received 12th December 1968)

1. Introduction

In this paper, the author continues his investigation, initiated in (4) and (5), into the nature of certain " arithmetical " functions associated with the factorisation of normalised non-zero polynomials in the ring $GF[q, X_1, ..., X_k]$, where $k \geqq 1$, $GF(q)$ is the finite field of order q and $X_1, ..., X_k$ are indeterminates. By normalised polynomials we mean that exactly one polynomial has been selected from equivalence classes with respect to multiplication by non-zero elements of $GF(q)$. With this normalisation $GF[q, X_1, ..., X_k]$ becomes a unique factorisation domain. The constant polynomial will be denoted by 1. By the degree of a polynomial A in $GF[q, X_1, ..., X_k]$, we shall mean the ordered set $(m_1, ..., m_k)$, where m_i is the degree of A in X_i, $1 \leqq i \leqq k$. We shall assume that $A(\neq 1)$, a typical polynomial in $GF[q, X_1, ..., X_k]$, has prime factorisation

$$A = P_1^{\alpha_1}...P_t^{\alpha_t}, \tag{1.1}$$

where $P_1, ..., P_r$ are distinct irreducible polynomials (i.e. primes).

We now define the following real functions of $GF[q, X_1, ..., X_k]$.

Let

$$\omega(A) = \begin{cases} 0, A = 1, \\ t, A \neq 1; \end{cases} \tag{1.2}$$

$$\Omega(A) = \begin{cases} 0, A = 1, \\ \alpha_1 + ... + \alpha_t, A \neq 1; \end{cases} \tag{1.3}$$

$$\beta_r(A) = \begin{cases} 1, \alpha_1 + ... + \alpha_t = r, \\ 0, \text{otherwise}; \end{cases} \tag{1.4}$$

and

$$\gamma_r(A) = \begin{cases} 1, t = r, \alpha_1 = ... = \alpha_r = 1, \\ 0, \text{otherwise}, \end{cases} \tag{1.5}$$

where in (1.4) and (1.5), r is an integer $\geqq 1$. It follows from (1.2) and (1.3) that $\omega(A)$ and $\Omega(A)$ are the number of distinct prime factors of A and prime factors of A, respectively. We are interested in the average values of $\omega(A)$ and $\Omega(A)$ over all polynomials of the same degree. Accordingly, we consider the functions $w(m_1, ..., m_k) = \Sigma\omega(A)$, and $W(m_1, ..., m_k) = \Sigma\Omega(A)$, the sum in each case being over all polynomials of degree $(m_1, ..., m_k)$. Similarly, we put, for $r \geqq 1$, $\tau_r(m_1, ..., m_k) = \Sigma\beta_r(A)$ and $\pi_r(m_1, ..., m_k) = \Sigma\gamma_r(A)$, where Σ

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

has the same meaning as before. Thus $\tau_r(m_1, \ldots, m_k)$ is the number of polynomials of degree $(m_1, \ldots, m_k)$ which are the product of exactly r prime factors, while $\pi_r(m_1, \ldots, m_k)$ is the number of such polynomials which are square-free, i.e., which are the product of r distinct primes. In particular, we have

$$\pi_1(m_1, \ldots, m_k) = \tau_1(m_1, \ldots, m_k) = \pi(m_1, \ldots, m_k), \tag{1.6}$$

where $\pi(m_1, \ldots, m_k)$ is the number of irreducibles of degree $(m_1, \ldots, m_k)$.

We derive relations involving the functions w, W, τ_r and π_r and the functions π and N, where $N(m_1, \ldots, m_k)$ is the total number of polynomials of degree $(m_1, \ldots, m_k)$. Now, if $k = 1$, then $N(m) = q^m$ and $\pi(m)$ is given explicitly by

$$\pi(m) = m^{-1} \sum_{st = m} \mu(s)q^t, \tag{1.7}$$

$$\sim m^{-1}N(m),\ m \to \infty. \tag{1.8}$$

On the other hand, if $k \geqq 2$, although the value of $N(m_1, \ldots, m_k)$ is known explicitly (see (4), Lemma 2), it is, in general, a cumbersome function to manipulate. Moreover, no explicit value of $\pi(m_1, \ldots, m_k)$ is known, although it has been shown in (3) and (5) that, if $m_1, \ldots, m_{k-1}$ are not all zero, then

$$\pi(m_1, \ldots, m_k) \sim (1-q^{1-n})N(m_1, \ldots, m_k),\ m_k \to \infty, \tag{1.9}$$

where, if $k \geqq 2$,

$$n = (m_1+1)\ldots(m_{k-1}+1). \tag{1.10}$$

As a consequence of the above remarks, when $k = 1$ we can find explicit formulae for $w(m)$ and $W(m)$. When we allow m to tend to infinity, these yield

$$w(m) \sim W(m) \sim (\log m)N(m),\ m \to \infty. \tag{1.11}$$

However, if $k \geqq 2$, it is not possible to evaluate w and W exactly, although we prove that

$$w(m_1, \ldots, m_k) \sim \left(1+\log\left\{\prod_{s=1}^{\infty} (1-q^{1-sn})^{-\mu(s)/s}\right\}\right) N(m_1, \ldots, m_k),\ m_k \to \infty, \tag{1.12}$$

where n is given by (1.10). In the corresponding expression for $W(m_1, \ldots, m_k)$, $\mu(s)$ in (1.12) is replaced by $\phi(s)$.

When we attempt to compute $\tau_r(m_1, \ldots, m_k)$ and $\pi_r(m_1, \ldots, m_k)$, we find that even in the case $k = 1$, it is difficult to produce exact results. We prove that, if $r \geqq 0$,

$$\Pi_{r+1}(m) \sim \tau_{r+1}(m) \sim \frac{(\log m)^r}{r!m} N(m), \quad m \to \infty. \tag{1.13}$$

Because of the uselessness of (1.13) for small m, when $k \geqq 2$, we can prove only that

$$\sigma_{r+1}(m_1, \ldots, m_k) \sim S_\sigma(r)N(m_1, \ldots, m_k),\ r \geqq 0,\ m_k \to \infty, \tag{1.14}$$

where σ denotes τ or π and $S_\sigma(r)$ is independent of m_k. Certainly we have $0 < S_\sigma(r) \leqq q^{(1-n)r}$.

We note that formulae (1.8), (1.11) and (1.13) (where $k = 1$) are of an

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

entirely different nature from (1.9), (1.12) and (1.14) (where $k \geqq 2$). We note also that (1.11) and (1.13) appear to be new, whereas most of our single indeterminate evaluations in (5) were not. Moreover in Section 5, we indicate how it is possible to extend these two results to cover the case of " factorable " polynomials in k indeterminates.

It is convenient in what follows to abbreviate, where possible, any function $\theta(m_1, \ldots, m_k)$ to $\theta(m_i)$. Similarly the degree of a polynomial $(m_1, \ldots, m_k)$ will be written (m_i). The sum $\sum_{s_1=0}^{m_1} \ldots \sum_{s_k=0}^{m_k}$ and the product $\prod_{s_1=0}^{m_1} \ldots \prod_{s_k=0}^{m_k}$ will be denoted simply by $\sum_{s_i}$ and $\prod_{s_i}$, respectively. No confusion should arise as k, as well as q, is to be considered fixed. We shall use $\sum_{\deg A = (m_i)}$ and $\sum_{C \mid A}$ to denote a sum over all polynomials A of degree (m_i) and a sum over all divisors C of A, respectively, and a similar rotation for products. Moreover, we shall reserve the letter P in such a sum or product (e.g. $\sum_{\deg P = (m_i)}$, $\sum_{P \mid A}$) to signify that such a sum or product is restricted to irreducible polynomials P.

2. Relations involving the functions

We find relations involving $w(m_i)$ and $W(m_i)$ directly from their definitions. We assume that $\pi(0, \ldots, 0) = 0$.

Theorem 1. *If $k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$w(m_i) = \sum_{s_i} \pi(s_i) N(m_i - s_i).$$

Proof. It follows from (1.2) that

$$w(m_i) = \sum_{\deg A = (m_i)} \omega(A) = \sum_{\deg A = (m_i)} \sum_{P \mid A} 1,$$

$$= \sum_{s_i} \sum_{\deg C = (m_i - s_i)} \sum_{\deg P = (s_i)} 1. \tag{2.0}$$

The result is immediate from (2.0) and the theorem is proved.

Incidentally, we can derive an expression for $\pi(m_i)$ from Theorem 1, using a formula proved in (5). Let $\mu(A)$ be the Möbius function in $GF[q, X_1, \ldots, X_k]$ and put

$$M(m_i) = \sum_{\deg A = (m_i)} \mu(A). \tag{2.1}$$

By the formula mentioned (5, Theorem 2), we can " invert " the assertion of Theorem 1 to yield

$$\pi(m_i) = \sum_{s_i} w(s_i) M(m_i - s_i).$$

Before stating the theorem for $W(m_i)$ corresponding to Theorem 1 for $w(m_i)$, we introduce the function $\rho(m_i)$ defined for all non-negative integers $m_1, \ldots, m_k$, not all zero, by

$$\rho(m_i) = \sum_{e \mid (m_1, \ldots, m_k)} \pi(m_i / e). \tag{2.2}$$

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

(In (2.2) and wherever the context demands it, $(m_1, \ldots, m_k)$ means the greatest common divisor of $m_1, \ldots, m_k$). We set $\rho(0, \ldots, 0) = 0$.

Theorem 2. *If $k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$W(m_i) = \sum_{s_i} \rho(s_i)N(m_i - s_i).$$

Proof. By the definition of $\Omega(A)$ we have

$$\Omega(A) = \sum_{P^e \mid A} 1. \tag{2.3}$$

Let $h = h(m_i, s_i)$ be the greatest integer such that $hs_i \leqq m_i$, $i = 1, \ldots, k$. It follows from (1.3) and (2.3) that

$$\begin{aligned} W(m_i) &= \sum_{\deg A = (m_i)} \sum_{P^e \mid A} 1 \\ &= \sum_{s_i} \sum_{e=1}^{h} \sum_{\deg C = (m_i - es_i)} \sum_{\deg P = (s_i)} 1 \\ &= \sum_{s_i} \sum_{e=1}^{h} \pi(s_i)N(m_i - es_i) \\ &= \sum_{u_i} \Big\{ \sum_{e \mid (u_1, \ldots, u_k)} \pi(u_i/e) \Big\} N(m_i - u_i), \end{aligned} \tag{2.4}$$

putting $u_i = es_i$, $i = 1, \ldots, k$. By (2.4) and (2.2) the theorem is proved.

In dealing with the functions π_r and τ_r it is convenient to extend their definitions ((1.4) and (1.5)) slightly. First if $r \geqq 1$ and $m_1, \ldots, m_k$ are integers, not all non-negative, let $\tau_r(m_i) = \pi_r(m_i) = 0$. Again, for all integers $m_1, \ldots, m_k$ (positive, negative, or zero), put

$$\pi_0(m_i) = \tau_0(m_i) = \begin{cases} 1, & m_1 = \ldots = m_k = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{2.5}$$

By an r-polynomial ($r \geqq 0$), will be meant a polynomial which is the product of exactly r prime factors, i.e., one for which $\beta_r(A) = 1$. 1 is the only 0-polynomial. We note here for future reference that

$$\tau_r(m_i) = \pi_r(m_i) = 0 \tag{2.6}$$

whenever $m_1 + \ldots + m_k < r$.

We now prove two recurrence relations with respect to r for each of τ_r and π_r. We use a similar approach to that of Lemma 1 of (4).

Theorem 3. *If $r, k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$m_1\tau_r(m_i) = \sum_{s_i} \sum_{e=1}^{r} s_1\tau_{r-e}(m_i - es_i)\pi(s_i), \tag{2.7}$$

and

$$r\tau_r(m_i) = \sum_{s_i} \sum_{e=1}^{r} \tau_{r-e}(m_i - es_i)\pi(s_i). \tag{2.8}$$

Proof. Let $F(m_i)$ be the product of all the $\tau_r(m_i)$ r-polynomials of degree

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

(m_i). For any irreducible P let $\Phi_r(m_i;\, P)$ denote the number of r-polynomials of degree (m_i) relatively prime to P. Extend the definition of $\Phi_r(m_i;\, P)$ to all integers $m_1, \ldots, m_k$ and to $r = 0$ in the same manner in which we extended $\tau_r(m_i)$. Now, for any irreducible P of degree (s_i), any r-polynomial of degree (m_i) possesses a unique expression of the form P^eA where $0 \leqq e \leqq r$ and A is an $(r-e)$-polynomial of degree $(m_i - es_i)$, with $(A, P) = 1$. In particular, if $r = e$ then $m_i = rs_i$, $i = 1, \ldots, k$ and $A = 1$. Hence, by our conventions, including (2.5),

$$F(m_i) = \prod_{s_i} \prod_{\deg P = (s_i)} \prod_{e=1}^{r} P^{e\Phi_{r-e}(m_i - es_i;\, P)} \tag{2.9}$$

holds for all non-negative $(m_1, \ldots, m_k)$ and $r \geqq 1$. Now we can evaluate $\Phi_r(m_i;\, P)$ in terms of τ_r. Since the set of all r-polynomials of degree (m_i) is the disjoint union of the set of all r-polynomials of degree (m_i), which are prime to P and the set of all r-polynomials of the form PA, where A is an arbitrary $(r-1)$-polynomial, of degree $(m_i - s_i)$ where $\deg P = (s_i)$, we have

$$\Phi_r(m_i;\, P) = \tau_r(m_i) - \tau_{r-1}(m_i - s_i). \tag{2.10}$$

Note that, by (2.5), (2.10) holds even if $r = 1$. Hence

$$\sum_{e=1}^{r} e\Phi_{r-e}(m_i - es_i;\, P) = \sum_{e=1}^{r} \tau_{r-e}(m_i - es_i), \tag{2.11}$$

since $\Phi_0(m_i - es_i) = \tau_0(m_i - es_i)$. Now, if we equate the degree in X_1 on either side of (2.9), we obtain

$$\begin{aligned} m_1\tau_r(m_i) &= \sum_{s_i} \sum_{\deg P = (s_i)} s_1 \sum_{e=1}^{r} e\Phi_{r-e}(m_i - es_i;\, P) \\ &= \sum_{s_i} \sum_{e=1}^{r} s_1\pi(s_i)\tau_{r-e}(m_i - es_i), \end{aligned}$$

by (2.11). This proves (2.7). If instead we equate the number of prime factors on either side of (2.9), we obtain

$$r\tau_r(m_i) = \sum_{s_i} \sum_{\deg P = (s_i)} \sum_{e=1}^{r} e\Phi_{r-e}(m_i - es_i;\, P). \tag{2.12}$$

(2.12) leads to (2.8) by way of (2.11). The proof is complete.

Theorem 4. *If $r, k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$m_1\pi_r(m_i) = \sum_{s_i} \sum_{e=1}^{r} (-1)^{e-1} s_1 \pi_{r-e}(m_i - es_i)\pi(s_i) \tag{2.13}$$

and

$$r\pi_r(m_i) = \sum_{s_i} \sum_{e=1}^{r} (-1)^{e-1} \pi_{r-e}(m_i - es_i)\pi(s_i). \tag{2.14}$$

Proof. Let $G(m_i)$ be the product of all square-free r-polynomials of degree (m_i). A similar argument to that used in Theorem 3 yields

$$G(m_i) = \prod_{s_i} \prod_{\deg P = (s_i)} P^{\Phi_{r-1}(m_i - s_i;\, P)}, \tag{2.15}$$

where $\Phi_r(m_i; P)$ is the number of square free r-polynomials of degree (m_i), prime to P, and obeys the usual conventions. Now, every square free r-polynomial of degree (m_i) is either prime to a given irreducible P of degree (s_i) or has the form PA where A is a square-free $(r-1)$-polynomial of degree (m_i-s_i) ,which is relatively prime to P. It follows that

$$\pi_r(m_i) = \Phi_r(m_i;\ P)+\Phi_{r-1}(m_i-s_i;\ P)$$

holds for all $r \geqq 1$ and hence that

$$\Phi_{r-1}(m_i-s_i;\ P) = \sum_{e=1}^{r}(-1)^{e-1}\pi_{r-e}(m_i-es_i). \tag{2.16}$$

Equating degree in X_1 on either side of (2.15) and substituting (2.16) leads to (2.13). Similarly (2.14) is obtained by equating the number of prime factors on either side of (2.15). This completes the proof.

In succeeding work, we employ the expressions (2.7) and (2.13) in preference to (2.8) and (2.14). For instance, we can use (2.13) to derive a relation (proved by another method in (5)) involving $M(m_i)$ defined by (2.1). It is evident from the definitions of $\pi_r(m_i)$ and $M(m_i)$ that

$$M(m_i) = \sum_{r=0}^{b}(-1)^r\pi_r(m_i), \tag{2.17}$$

where $b = m_1+\ldots+m_k$. Hence by (2.13) and (2.17) we have

$$m_1M(m_i) = \sum_{r=0}^{b}\sum_{s_i}\sum_{e=1}^{r}(-1)^{r+e-1}s_1\pi_{r-e}(m_i-es_i)\pi(s_i). \tag{2.18}$$

Putting $r-e = t$ in (2.18) yields

$$\begin{aligned} m_1M(m_i) &= \sum_{t=0}^{b-1}\sum_{s_i}\sum_{e=1}^{b-t}(-1)^{t-1}s_1\pi_t(m_i-es_i)\pi(s_i) \\ &= -\sum_{s_i}\sum_{e=1}^{b}s_1\left\{\sum_{t=0}^{b-e}(-1)^t\pi_t(m_i-es_i)\right\}\pi(s_i) \\ &= -\sum_{s_i}\sum_{e=1}^{b}s_1M(m_i-es_i)\pi(s_i), \end{aligned} \tag{2.19}$$

by (2.17) and (2.6), since we can assume that $s_1 \geqq 1$ and hence that

$$b-e = \sum_{i=1}^{k}m_i-e \geqq \sum_{i=1}^{k}(m_i-es_i).$$

From (2.19), we immediately deduce the relation

$$m_1M(m_i) = -\sum_{s_i}s_1\{\sum_{e\,|\,(s_1,\ldots,s_k)}1/e\,.\,\pi(s_i/e)\}M(m_i-s_i),$$

which is contained in Theorem 1 of (5).

3. Case of one indeterminate

In order to evaluate the functions we have defined, it is necessary to treat the case $k = 1$ separately.

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

It is convenient to discuss the functions w and W together. We make some remarks about $\rho(m)$ defined by (2.2) with $k = 1$. By the well known identity

$$X^{q^m} - X = \prod_{\deg P \mid m} P, \quad m \geqq 1,$$

we see that $\rho(m)$ is the number of prime factors of the polynomial $X^{q^m} - X$. In fact, we can express $\rho(m)$ in a form resembling that of $\pi(m)$ (see (1.7)) where Euler's function $\phi(s)$ plays the role of $\mu(s)$.

Lemma 1. *If $m \geqq 1$, we have*

$$\rho(m) = m^{-1} \sum_{st = m} \phi(s) q^t.$$

Proof. It follows from (2.2) and (1.7) that

$$\begin{aligned} \rho(m) &= \sum_{u \mid m} u^{-1} \sum_{st = u} \mu(s) q^t \\ &= \sum_{t \mid m} q^t/t \sum_{s \mid mt^{-1}} \mu(s)/s \\ &= \sum_{t \mid m} q^t/t \,.\, (t/m \,.\, \phi(m/t)) \end{aligned}$$

and the lemma is proved.

We now proceed to evaluate $w(m)$ and $W(m)$.

Theorem 5. *We have*

$$w(m) \sim W(m) \sim (\log m) q^m, \; m \to \infty.$$

More precisely,

$$q^{-m} w(m) = \sum_{u=1}^{m} \sum_{st = u} u^{-1} \mu(t) q^{-s(t-1)} = \log m + \gamma + E_1 + o(1), \; m \to \infty, \quad (3.1)$$

and

$$q^{-m} W(m) = \sum_{u=1}^{m} \sum_{st = u} u^{-1} \phi(t) q^{-s(t-1)} = \log m + \gamma + E_2 + o(1), \; m \to \infty, \quad (3.2)$$

where γ is Euler's constant and E_1 and E_2 are small constants.

Proof. Since $N(m) = q^m$, we have by Theorem 2 and Lemma 1

$$\begin{aligned} W(m) &= \sum_{u=1}^{m} \{ \sum_{st = u} u^{-1} \phi(t) q^s \} q^{m-u} \\ &= \left\{ \sum_{u=1}^{m} \sum_{st = u} u^{-1} \phi(t) q^{-s(t-1)} \right\} q^m \\ &= \left\{ \sum_{u=1}^{m} u^{-1} + E_2(m) \right\} q^m, \end{aligned} \quad (3.3)$$

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

where $E_2(1) = 0$ and, if $m \geqq 2$,

$$\begin{aligned} E_2(m) &= \sum_{u=2}^{m} \sum_{\substack{st=u \\ t \geqq 2}} \phi(t)/u \,.\, q^{-s(t-1)} \\ &\leqq \sum_{u=2}^{m} u^{-1} q^{-u/2} \Big(\sum_{\substack{t \mid u \\ t \geqq 2}} \phi(t) \Big) \\ &= \sum_{u=2}^{m} (1-u^{-1}) q^{-u/2} \\ &\leqq (1-m^{-1})(1-q^{-(m-1)/2}) q^{-1} (1-q^{-\frac{1}{2}})^{-1} \\ &< q^{-\frac{1}{2}}(q^{\frac{1}{2}}-1)^{-1}. \end{aligned} \tag{3.4}$$

Since $E_2(m)$ is increasing, it is evident from (3.4) that $E_2(m) \to E_2$ as $m \to \infty$, where

$$1/2q < E_2 = \sum_{u=2}^{\infty} \sum_{\substack{st=u \\ t \geqq 2}} u^{-1}\phi(t) q^{-(u-s)} < q^{-\frac{1}{2}}(q^{\frac{1}{2}}-1)^{-1} < 1{\cdot}71, \tag{3.5}$$

since $q \geqq 2$. Statement (3.1) now follows from (3.3) and (3.5) by allowing m to tend to infinity.

By using Theorem 1 and (1.7) we arrive at a similar result for $w(m)$. In this case, we have

$$E_1 = \sum_{u=2}^{\infty} \sum_{\substack{st=u \\ t \geqq 2}} u^{-1}\mu(t) q^{-(u-s)}$$

and hence

$$| E_1 + (\tfrac{1}{2}q) | < \tfrac{1}{4} q^{-1}(q-1)^{-1} + q^{-2}(1-q^{-\frac{2}{3}})^{-1}. \tag{3.6}$$

Moreover,

$$| E_1 | < E_2 < 1.71.$$

This completes the proof of the theorem.

The bounds (3.4) and (3.6) for E_1 and E_2 are sufficient to show that these constants are very small in general. Thus if $q = 2^6 = 64$, we have

$$| E_1 + 1/128 | < 0.0001 \text{ and } \tfrac{1}{128} < E_2 < \tfrac{1}{56}.$$

By comparison, γ (= 0.5772...) is large.

We now discuss the functions τ_r and π_r with $k = 1$. Exact formulae proved by induction on r from Theorems 3 and 4 would be vastly complicated for $r \geqq 2$. Hence, we prove only an estimate.

Theorem 6. *For fixed $r \geqq 0$ and large m, we have*

$$\sigma_{r+1}(m) = \frac{(\log m)^r}{r!m} q^m + O((\log m)^{r-1} m^{-1} q^m), \tag{3.7}$$

where σ_r denotes either τ_r or π_r.

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

Proof. The proof is by induction on r. By (1.6) and (1.7)

$$\begin{aligned}\sigma_1(m) &= m^{-1}q^m + O(m^{-1}q^{m/2})\\ &= m^{-1}q^m + O((\log m)^{-1}m^{-1}q^m),\end{aligned}$$

for large m. Thus (3.7) holds when $r = 0$. Assume, therefore, that $r \geqq 1$ and that (3.7) is valid for all integers less than r. Consider relations (2.7) and (2.13) with $k = 1$, and r replaced by $r+1$. We separate out the terms for which $e = 1$ and estimate the remaining terms using the induction hypothesis. Using also (2.6), (2.5) and (1.8), we obtain for large m

$$m\sigma_{r+1}(m) = \sum_{s=1}^{m-r} s\sigma_r(m-s)\pi(s) + O\left(\sum_{s=1}^{m} (\log m)^{r-2}q^{m-s}\right) + O(q^{m/(r+1)}), \tag{3.8}$$

where the first error term occurs only if $r \geqq 2$ and the second only if $e = r+1$ and $(r+1) \mid m$. Now use the induction hypothesis and (1.7) on the σ_r terms of (3.8) to yield

$$m\sigma_{r+1}(m) = \sum_{s=1}^{m-r} \sum_{d \mid s} (1+O((\log(m-s))^{-1})) \frac{[\log(m-s)]^{r-1}}{(m-s)(r-1)!} q^{m-s+(s/d)} + O((\log m)^{r-1}q^m) \tag{3.9}$$

Indeed, if $r = 1$, then by (1.7) the $O((\log(m-s))^{-1})$ appearing in (3.9) may be replaced by $O(q^{-(m-s)/2})$. Now for large m, we have

$$\begin{aligned}\sum_{s=1}^{m-r} \sum_{\substack{d \mid s\\ d>s}} \frac{[\log(m-s)]^{r-1}}{m-s} q^{-s(1-(1/d))} &= O\left((\log m)^{r-1} \sum_{s=1}^{m} sq^{-s/2}\right)\\ &= O((\log m)^{r-1}).\end{aligned} \tag{3.10}$$

Again, if $r \geqq 1$,

$$\sum_{s=1}^{m-r} \frac{[\log(m-s)]^{r-1}}{m-s} = \sum_{s=1}^{m-1} \frac{(\log s)^{r-1}}{s} + O(1). \tag{3.11}$$

Now if $1 \leqq s \leqq m-1$, $(\log s)^{r-1}/s$ is increasing if $\log s \leqq r-1$ and decreasing if $\log s \geqq r-1$. It follows that, if $\log m > r \geqq 1$, then

$$\left| \sum_{s=1}^{m-1} \frac{(\log s)^{r-1}}{s} - \int_1^m \frac{(\log x)^{r-1}}{x} dx \right| \leqq \int_c^{c+1} \frac{(\log x)^{r-1}}{x} dx = O(1), \tag{3.12}$$

where $c = [e^{r-1}]$. But

$$\int_1^m \frac{(\log x)^{r-1}}{x} dx = \int_0^{\log m} y^{r-1} dy = \frac{(\log m)^r}{r}, \; r \geqq 1. \tag{3.13}$$

If $r \geqq 2$, the result now follows from (3.9), (3.10), (3.11), (3.12) and (3.13). Finally, since, when $r = 1$, by (3.12) and (3.13) we have

$$\begin{aligned}\sum_{s=1}^{m-1} (1+O(q^{-(m-s)/2}))(m-s)^{-1} &= \log m + \sum_{s=1}^{m-1} sq^{-s/2} + O(1)\\ &= \log m + O(1),\end{aligned} \tag{3.14}$$

the induction hypothesis for $r = 1$ follows from (3.9) and (3.14). The theorem is thus proved by induction.

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

4. Case of several indeterminates

In this section we assume that $k \geqq 2$ and estimate the functions we have defined as $m_k \to \infty$. In order to deal with polynomials in which at least two indeterminates actually appear we shall assume wherever necessary and without loss of generality that $m_1, \ldots, m_k$ are non-negative integers ordered so that

$$m_{k-1} = \max_{1 \leqq i \leqq k-1} m_i \geqq 1 \tag{4.1}$$

Define the integer $R(\geqq 1$, if (4.1) holds) by

$$R = nm_{k-1}(m_{k-1}+1)^{-1}, \tag{4.2}$$

where n is given by (1.10). We recall the following estimates of $N(m_i)$ and $\pi(m_i)$ from (**4**).

Lemma 2. *If $m_1, \ldots, m_k$ are non-negative integers satisfying* (4.1), *then*

$$(q-1)N(m_i) = (q^n-1)q^{nm_k} + O(q^{Rm_k}), \tag{4.3}$$

where the implied constant is independent of m_k. Moreover,

$$\pi(m_i) = (1-q^{1-n})N(m_i) + O(m_k q^{Rm_k}). \tag{4.4}$$

To assist in our computations, we state another lemma from (**4**).

Lemma 3. *Suppose that $k \geqq 2$ and that $m_1, \ldots, m_k$ are non-negative integers satisfying* (4.1). *Suppose also that $s_1, \ldots, s_k$ are integers, not all zero, satisfying $0 \leqq s_i \leqq m_i$, $i = 1, \ldots, k$, and $s_i \neq m_i$ for at least one i, $1 \leqq i \leqq k-1$. Then*

$$N(s_i)N(m_i - s_i) = O(q^{Rm_k}),$$

where the implied constant is independent of m_k.

We first estimate $w(m_i)$.

Theorem 7. *If $k \geqq 2$ and $m_1, \ldots, m_k$ are non-negative integers such that* (4.1) *holds, then*

$$w(m_i) = \left(1 + \log\left\{\prod_{s=1}^{\infty} (1-q^{1-sn})^{-\mu(s)/s}\right\}\right) N(m_i) + O(m_k q^{Rm_k}), \tag{4.5}$$

where the implied constant is independent of m_k and n and r are given by (1.10) *and* (4.2), *respectively.*

Proof. It will be shown during the course of the proof that the infinite product on the right hand side of (4.5) is convergent.

Since $\pi(s_i) \leqq N(s_i)$ it follows from Theorem 1, using Lemma 3, that, for large m_k, we have

$$\begin{aligned} w(m_i) &= \sum_{s_k=0}^{m_k} \pi(m_1, \ldots, m_{k-1}, s_k)N(0, \ldots, 0, m_k - s_k) \\ &\quad + \sum_{s_k=1}^{m_k} \pi(0, \ldots, 0, s_k)N(m_1, \ldots, m_{k-1}, m_k - s_k) + O(m_k q^{Rm_k}), \\ &= S_1 + S_2 + O(m_k q^{Rm_k}), \end{aligned} \tag{4.6}$$

say. In (4.6), S_1 is given by

$$\begin{aligned} S_1 = \pi(m_1, \ldots, m_{k-1}, 0)N(0, \ldots, 0, m_k) & \\ + \sum_{s=1}^{m_k} \pi(m_1, \ldots, m_{k-1}, s)N(0, \ldots, 0, m_k - s) & \\ = O(q^{m_k}) + (q-1)^{-1}(1-q^{1-n})(q^n-1)q^{m_k} \sum_{s=1}^{m_k} q^{(1-n)s} & \\ + O(m_k q^{Rm_k}), & \qquad (4.7) \end{aligned}$$

using Lemma 2. Simplifying (4.7) we obtain

$$\begin{aligned} S_1 &= (q-1)^{-1}(q^n-1)q^{nm_k} + O(m_k q^{Rm_k}) \\ &= N(m_i) + O(m_k q^{Rm_k}) \qquad (4.8) \end{aligned}$$

by (4.3) again. The sum S_2 in (4.5) is more complicated. We have, by (1.7) and Lemma 2,

$$\begin{aligned} S_2 &= \sum_{s=1}^{m_k} \pi(0, \ldots, 0, s)N(m_1, \ldots, m_{k-1}, m_k - s) \\ &= (q-1)^{-1}(q^n-1)q^{nm_k} \left\{ \sum_{s=1}^{m_k} \sum_{t \mid s} s^{-1}\mu(t)q^{-(n-(1/t))s} \right\} + O(m_k q^{Rm_k}) \qquad (4.9) \\ &= \left\{ \sum_{t=1}^{m_k} \mu(t)/t \sum_{u=1}^{[m_k/t]} u^{-1}q^{-(nt-1)u} \right\} N(m_i) + O(m_k q^{Rm_k}), \qquad (4.10) \end{aligned}$$

by (4.3) and putting $u = s/t$. Let $B(m_k)$ denote the quantity in braces in (4.9) and (4.10). Using the form in (4.9) we have $B(m_k) = \sum_{s=1}^{m_k} b_s$, where since $| \mu(t) | \leqq t$

$$| b_s | \leqq \sum_{t \mid s} s^{-1}tq^{-(n-(1/t))s} \leqq sq^{(1-n)s}.$$

Since the series $\sum_{s=1}^{m} sq^{(1-n)s}$ is convergent as $m \to \infty$ provided $q^{1-n} < 1$, it follows, by the comparison test, that $B(m_k)$ tends to a finite limit, B, as $m_k \to \infty$. Consider now (4.10). If $1 \leqq t \leqq m_k$ we have

$$\begin{aligned} \sum_{u=1}^{[m_k/t]} u^{-1}q^{-(nt-1)u} &= -\log(1-q^{1-tn}) + O\left(tm_k^{-1} \sum_{u=[m_k/t]+1} q^{-(n-1)tu} \right) \\ &= -\log(1-q^{1-tn}) + O(tm_k^{-1}q^{(1-n)m_k}). \qquad (4.11) \end{aligned}$$

It is now a consequence of (4.9) and (4.11) that

$$B(m_k) = -\sum_{t=1}^{m_k} (\mu(t)/t) . \log(1-q^{1-tn}) + O(m_k q^{(1-n)m_k}). \qquad (4.12)$$

Statement (4.5) follows from (4.12) by allowing m_k to tend to infinity since $B = \lim_{m_k \to \infty} B(m_k)$ exists. The proof of the theorem is complete.

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

Theorem 8. *If $k \geqq 2$, and $m_1, \ldots, m_k$ are non-negative integers satisfying* (4.1), *then*

$$W(m_i) = \left(1+\log\left\{\prod_{s=1}^{\infty}(1-q^{(1-sn)})^{-\phi(s)/s}\right\}\right)N(m_i)+O(m_kq^{Rm_k}),$$

where the implied constant is independent of m_k.

Proof. The proof is identical with that of Theorem 7 except that we use Theorem 2 and Lemma 1 in place of Theorem 1 and (1.7), i.e., $\rho(m_i)$ and $\phi(s)$ replace $\pi(m_i)$ and $\mu(s)$. Now it is clear from (2.2) that for large m_k

$$\begin{aligned}\rho(m_i) &= \pi(m_i)+O(q^{nm_k/2})\\ &= \pi(m_i)+O(q^{Rm_k}),\end{aligned} \tag{4.13}$$

provided $m_{k-1} \geqq 1$. It follows from (4.13) and (4.4) that

$$\rho(m_i) = (1-q^{1-n})N(m_i)+O(m_kq^{Rm_k}). \tag{4.14}$$

Moreover, the only property of $\mu(s)$ used in Theorem 7 was the trivial fact that $|\mu(s)| \leqq s$. Accordingly, since (4.14) holds and $\phi(s) \leqq s$, this theorem is proved by the argument used for the proof of Theorem 7. The proof is complete.

We remark that a more detailed analysis of the above arguments would indicate that we could improve the results of Theorems 7 and 8 slightly except when $k = 2$ and $m_1 = 1$ or 2 or $k = 3$ and $m_1 = m_2 = 1$. The improvements are obtained by replacing $O(m_kq^{Rm_k})$ by $O(q^{Rm_k})$ in their statements. We note also the following behaviour of $w(m_i)$ and $W(m_i)$ as m_k *and* m_{k-1} tend to infinity. From (1.9), such behaviour is almost inevitable.

Corollary 9. *We have*

$$\lim_{m_{k-1},\, m_k\to\infty} w(m_i)/N(m_i) = \lim_{m_{k-1},\, m_k} W(m_i)/N(m_i) = 1.$$

Proof. The right hand side of Theorem 8 may be written (without error term)

$$(1+\lim_{m_k\to\infty} B(m_k))N(m_i), \tag{4.15}$$

where $B(m_k)$ appears in (4.10). Hence

$$\begin{aligned}\left|\lim_{m_{k-1},\, m_k\to\infty} B(m_k)\right| &\leqq \lim_{m_{k-1},\, m_k\to\infty}\sum_{u=1}^{m_k} uq^{(1-n)u}\\ &= \lim_{m_k\to\infty}\sum_{u=1}^{m_k} u\lim_{n\to\infty} q^{(1-n)u}\\ &= 0.\end{aligned} \tag{4.16}$$

The proof for $W(m_i)$ is immediate from (4.15) and (4.16). But

$$1 \leqq w(m_i)/N(m_i) \leqq W(m_i)/N(m_i),$$

and hence the proof is complete.

We turn now to the functions τ_r and π_r. We will show that, if $r \geqq 2$, then in order to find $\lim\limits_{m_k \to \infty} \tau_r(m_i)/N(m_i)$, say, when $k \geqq 2$, it would be necessary to know the exact value of $\tau_r(m)$ ($k = 1$) for small m ($\geqq r$). We do not possess this knowledge. However, we can prove the less precise type of relation (1.14) by evaluating $\tau_r(r)$ and $\pi_r(r)$. In the following lemma, an empty product, is as usual, taken to be 1.

Lemma 4. *If $k = 1$ and $r \geqq 0$, we have*

$$\tau_r(r) = \left\{\prod_{i=0}^{r-1} (1+(i/q)\right\}/r\,!\,.\,q^r \tag{4.17}$$

and

$$\pi_r(r) = \left\{\prod_{i=0}^{r-1} (1-(i/q)\right\}/r\,!\,.\,q^r \tag{4.18}$$

Proof. By (2.5), we can assume $r \geqq 1$. Now, if a polynomial in $GF[q, X]$ has degree r and r prime factors, they must all be linear. Thus if $q<r$, then clearly $\pi_r(r) = 0$ and (4.18) holds. If $q \geqq r$, it is evident that $\pi_r(r) = \binom{q}{r}$, which may be written in the form (4.18). This proves (4.18). Again $\tau_r(r)$ is the number of terms of total degree r in the expression

$$\prod_{j=1}^{q} (1+t_j+t_j^2+\ldots) \tag{4.19}$$

in the q real variables $t_1, \ldots, t_q$, where each t_j is associated with a unique element of $GF(q)$. The product (4.19) exists when $|\,t_j\,|<1, j = 1, \ldots, q$. Hence $\tau_r(r)$ is the coefficient of t^r in $(1+t+t^2+\ldots)^q = (1-t)^{-q}$, $|\,t\,|<1$. Accordingly

$$\tau_r(r) = (q+r-1)!/[(q-1)!r!]$$

which is the same as (4.17). This completes the proof.

Theorem 10. *If $k \geqq 2, r \geqq 0$ and $m_1, \ldots, m_{k-1}$ are non-negative integers such that* (4.1) *holds then if σ_r denotes τ_r or π_r we have, for large m_k,*

$$\sigma_{r+1}(m_i) = S_\sigma(r)N(m_i)+O(m_k q^{Rm_k}), \tag{4.20}$$

where $S_\sigma(r)$ is positive and satisfies

$$(1-q^{1-n})\left\{\prod_{i=0}^{r-1} (1\pm(i/q))\right\}/r! \leqq S_\sigma(r)q^{rn} \leqq q^r, \tag{4.21}$$

the + and − signs in (4.21) *being taken according as $\sigma = \tau$ or π respectively.*

Proof. By (1.6) and (4.4), when $r = 0$, (4.20) holds with $S_\sigma(0) = 1$. Therefore assume that $r \geqq 1$. Consider the expressions (2.7) and (2.13). It is evident that $\sigma_r(m_i) \leqq N(m_i)$. Suppose $s_1, \ldots, s_k$ satisfy the conditions of Lemma 3. Then, if $1 \leqq e \leqq r+1$,

$$\sigma_{r+1-e}(m_i-es_i)\pi(s_i) \leqq \sigma_{r+1-e}(m_i-s_i)\pi(s_i) = O(q^{Rm_k}) \tag{4.22}$$

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

holds for large m_k, by that Lemma and (4.4). In fact, even if $s_i = m_i$, $i = 1, \ldots, k-1$ and $e \geqq 2$, then

$$\sigma_{r+1-e}(m_i - es_i)\pi(s_i) = 0 \tag{4.23}$$

holds trivially by (2.5) and (2.6) since $r \geqq 1$. Since we can assume $s_1 \geqq 1$ in (2.7) and (2.13), it is a consequence of these equations together with (4.22) and (4.23) that

$$\begin{aligned}\sigma_{r+1}(m_i) &= \sum_{s=0}^{m_k} \sigma_r(0, \ldots, 0, s)\pi(m_1, \ldots, m_{k-1}, m_k - s) + O(m_k q^{Rm_K}) \\ &= (1-q^{1-n})\left\{\sum_{s=0}^{m_k} \sigma_r(s)q^{-ns}\right\} N(m_i) + O(m_k q^{Rm_k}).\end{aligned} \tag{4.24}$$

It follows from (4.24) that (4.20) is true where $S_\sigma(r)$ satisfies

$$(1-q^{1-n})^{-1}S_\sigma(r) = \sum_{s=0}^{\infty} \sigma_r(s)q^{-ns} = \sum_{s=r}^{\infty} \sigma_r(s)q^{-ns}, \tag{4.25}$$

by (2.6). We see from (4.25), using the fact that $\sigma_r(s) < q^s$, that

$$(1-q^{1-n})\sigma_r(r)q^{-rn} \leqq S_\sigma(r) \leqq \sum_{s=r}^{\infty} q^{(1-n)s}.(1-q^{(1-n)}) = q^{(1-n)r}. \tag{4.26}$$

We deduce immediately from (4.26) and Lemma 4 that $S_\sigma(r)$ satisfies (4.21). Now (4.21) indicates that $S_\sigma(r)$ is positive except possibly if $r > q$. However even if $r > q$, it is clear that there exists a positive integer s_0, independent of m_k, which is the least integer such that $\sigma_r(s_0) \geqq 1$. Thus $S_\sigma(r) \geqq (1-q^{1-n})q^{-s_0 n}$ and the theorem is proved.

5. Factorable polynomials

It has been shown (see, for example, (1), (2) and (6)) that the most natural extensions of results concerning polynomials in $GF[q, X]$ to polynomials in $GF[q, X_1, \ldots, X_k]$ (where $k \geqq 1$) are obtained by considering only normalised *factorable* polynomials in k indeterminates, i.e., polynomials which split into linear factors in some finite extension of $GF(q)$. The number of such factors is the degree of such a polynomial. If we further restrict our attention to factorable polynomials in which X_k^m actually appears (m being the degree of the polynomial) we effect the most exact correspondence. For example, in an obvious notation, Carlitz (1) has proved that

$$N(m;\ k) = q^{km} \tag{5.1}$$

and that

$$\pi(m;\ k) = m^{-1} \sum_{st=m} \mu(s)q^{kt}. \tag{5.2}$$

Moreover, examination of the proofs of Theorems 1-4 reveals that these theorems for $k = 1$ remain valid if we generalise the functions occurring in the relations of the theorems by the corresponding functions over factorable polynomials in k indeterminates and in which X_k^m actually appears. We see

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press

from these relations that the values of $w(m;\ k)$, $W(m;\ k)$, $\tau_r(m;\ k)$ and $\pi_r(m;\ k)$ depend only on (5.1) and (5.2). Thus we can generalise Theorems 5 and 6 to cover the case of factorable polynomials in k indeterminates by substituting q^k for q in the statement of these theorems. Finally, we observe that the various relations proved in (5) for $k = 1$ generalise in the same way. However, the exact values of functions which are the factorable polynomial generalisation of those discussed in that paper have already been obtained in (1) and (2).

REFERENCES

(1) L. Carlitz, On factorable polynomials in several indeterminates, *Duke Math. J.* **2**(1936), 660-670.

(2) L. Carlitz, Some formulas for factorable polynomials in several indeterminates, *Bull. Amer. Math. Soc.* **43** (1937), 299-304.

(3) L. Carlitz, The distribution of irreducible polynomials in several indeterminates II, *Canadian J. Math.*, **17** (1965), 261-266.

(4) S. D. Cohen, The distribution of irreducible polynomials in several indeterminates over a finite field, *Proc. Edinburgh Math. Soc.* **16** (1968), 1-17.

(5) S. D. Cohen, Some arithmetical functions in finite fields, *Glasgow Math. J.*, **11** (1969), to appear.

(6) A. F. Long, Some theorems on factorable irreducible polynomials, *Duke Math. J.* **34** (1967), 281-291.

The University
Glasgow, W.2

https://doi.org/10.1017/S0013091500013031 Published online by Cambridge University Press