ARITHMETIC FUNCTIONS OF POLYNOMIALS

ECKFORD COHEN

1. **Introduction.** Let $D = GF[p^n, x]$ represent the domain of polynomials over the Galois field $GF(p^n)$ in the indeterminate x. Let K be a field of characteristic 0 containing the pth roots of unity and R a primary polynomial of D of degree r. We say that a single-valued function f defined for all elements of D and assuming values in K is (R, K) arithmetic or simply arithmetic if $f(A) = f(A')$ for $A \equiv A' \pmod{R}$. Two arithmetic functions f and g are said to be equivalent if $f(A) = g(A)$ for all $A \in D$, or what is the same, for all A of degree less than r. We define the Cauchy product of two arithmetic functions f, g to be the function $h = f \cdot g$, defined by

$$h(F) = f \cdot g = \sum_{F=A+B} f(A)g(B) \tag{1}$$

where the summation is over all polynomials A, B of degree less than r such that $F = A + B$, F being a polynomial of degree less than r. The sum $f + g$ has the usual significance; note that the set of all (R, K) functions forms a ring.

In [3] Carlitz discussed arithmetic functions over D and their Cauchy products. He introduced two basic sets of functions, the ω_U and the ϵ^*_{GH} functions, which were of importance in his study. It is the aim of this paper to introduce still another such set of arithmetic functions over D and to deduce certain of their applications. Although these functions are equivalent in the above sense to the ϵ^*_{GH} and ω functions of Carlitz, they seem to be particularly advantageous in the treatment of purely modular problems. In addition, they present features which easily carry over to the rational case. These questions will be discussed more fully in a later paper.

In §2, the functions in question, denoted by ϵ_Z, will be defined and the fundamental theorem, which states that every arithmetic function can be represented in the form $f(A) = \sum_Z a_Z \epsilon_Z(A)$, $a_Z \in K$, deg $Z < r$, will be proved. Although this result follows from [3, Theorem 1], using the equivalence of the ω_U and the ϵ_Z, an independent discussion is given, showing the essential simplicity of the ϵ_Z. In §3 two applications of this theorem will be made to the question of representations of polynomials by linear sums. One of these results will in turn be applied in §4 to obtain the number of representations of a polynomial F in the form

Presented to the Society, September 6, 1951; received by the editors August 24, 1951.

$$F = P_1X_1Y_1 + \cdots + P_sX_sY_s, \tag{2}$$

where the P_i are primary irreducibles in D (not all equal) and certain conditions on degree are satisfied. The result obtained represents an advance over previous results [6, Corollary, §4] in that nontrivial coefficients P_i are now introduced in every term of (2). The previous results applied only when at least one coefficient was trivial, that is, an element of $GF(p^n)$.

2. **The fundamental theorem.** Let H be a primary polynomial of D of degree h and let A be a polynomial such that $A \pmod{H} = \alpha_1X^{h-1} + \cdots + \alpha_h$ ($\alpha_i \in GF(p^n)$). Then following [2, §2] we define $\epsilon(A, H)$ to be $e^{2\pi i a_1/p}$, where a_1 is defined to be the integer $(\text{mod } p)$ which occurs as the initial coefficient in the expression $\alpha_1 = a_1\theta^{n-1} + \cdots + a_n$, θ being a generator of $GF(p^n)$ relative to $GF(p)$. We have immediately:

$$\epsilon(A + B, H) = \epsilon(A, H)\epsilon(B, H), \qquad \epsilon(H'A, HH') = \epsilon(A, H), \tag{3}$$

where H, H' are primary. We also list the following useful result proved in [2]:

$$\sum_{U \,(\text{mod } H)} \epsilon(AU, H) = \begin{cases} p^{nh} & \text{if } H \mid A, \\ 0 & \text{if } H \nmid A, \end{cases} \tag{4}$$

the summation being over a complete set of residues (mod H).

Now choose a primary polynomial R of degree r, and define

$$\epsilon_Z(A) = \epsilon(ZA, R). \tag{5}$$

One deduces immediately that $\epsilon_Z(A) = \epsilon_A(Z)$, $\epsilon_Z(A+B) = \epsilon_Z(A)\epsilon_Z(B)$ and the dual relation $\epsilon_{Z+Z'}(A) = \epsilon_Z(A)\epsilon_{Z'}(A)$. It also follows that

$$\epsilon_Z = \epsilon_{Z'} \rightleftarrows Z \equiv Z' \pmod{R}. \tag{6}$$

Furthermore, application of (4) gives

$$\sum_{A \,(\text{mod } R)} \epsilon_Z(A) = \begin{cases} p^{nr} & \text{if } Z \equiv 0 \pmod{R}, \\ 0 & \text{if } Z \not\equiv 0 \pmod{R}, \end{cases} \tag{7}$$

and the dual of (7) is obtained by interchanging Z and A. We also have the following lemma:

LEMMA 1. *For any F of degree less than r,*

$$\epsilon_Z \cdot \epsilon_{Z'} = \sum_{F=A+B} \epsilon_Z(A)\epsilon_{Z'}(B) = \begin{cases} p^{nr}\epsilon_Z(F), & Z \equiv Z' \pmod{R}, \\ 0, & Z \not\equiv Z' \pmod{R}. \end{cases} \tag{8}$$

PROOF. We can rewrite the sum in (8) as

$$\epsilon_Z \cdot \epsilon_{Z'} = \sum_{\deg A<r} \epsilon_Z(A)\epsilon_{Z'}(F-A) = \epsilon_{Z'}(F)\sum_A \epsilon_{Z-Z'}(A)$$

which by (7) yields the desired result.

Lemma 2. *The functions* ϵ_Z(deg $Z<r$) *are linearly independent over* K.

Proof. Suppose we have a relation $g=\sum_{\deg Z<r} a_Z\epsilon_Z=0$ $(a_Z\in K)$. Then by Lemma 1, the Cauchy product $g\cdot\epsilon_Z=a_Z\epsilon_Z\cdot\epsilon_Z=a_Zp^{nr}\epsilon_Z=0$ which implies that $a_Z=0$.

Now we prove the fundamental result:

Theorem 1. *Any* (R, K) *arithmetic function* f *can be represented uniquely in the form*

$$(9)\quad f(A) = \sum_{\deg Z<r} a_Z\epsilon_Z(A), \qquad a_Z = p^{-nr}\sum_{\deg U<r} f(U)\epsilon_Z(-U).$$

Proof. If we apply (7), the sum in (9) reduces to $f(A)$. The uniqueness follows from the linear independence established in Lemma 2.

Finally, as the Cauchy product $f\cdot g$ of two functions $f(A)=\sum a_Z\epsilon_Z$, $g(B)=\sum b_Z\epsilon_Z$, we have

$$(10)\qquad f\cdot g = \sum_{F=A+B} f(A)g(B) = p^{-nr}\sum_{\deg Z<r} a_Zb_Z\epsilon_Z = h(F).$$

The result in (10) can be extended to products of any number of functions.

3. **Representations by linear sums.**

In this section we prove first a theorem which generalizes an earlier result [4, Lemma, §2].

Theorem 2. *If* $s>1$ *and* $A_1, \cdots, A_s$ *are primary polynomials of* D *of degree* $a_1, \cdots, a_s$ *respectively,* $(A_1, \cdots, A_s)=1$, *then the number of solutions* $N_s(F)$ *of*

$$(11)\qquad F = \alpha_1A_1X_1 + \cdots + \alpha_sA_sX_s \qquad (F\in D)$$

where deg $F<r=a_1+\cdots+a_s+\lambda$ $(\lambda\geqq 0)$ *and the* α_i *are nonzero elements of* $GF(p^n)$, *such that* deg $A_iX_i<r$ *for all* i, *is given by* $N_s(F)=p^{n\{\lambda+r(s-2)\}}$.

Proof. Choose Λ to be primary of degree λ. With $R=A_1\cdots A_s\Lambda$ (deg $R=r$), we see from Theorem 1 that the number f_i of X_i such that $B_i=\alpha_iA_iX_i$ (deg $B_i<r$) is given by

$$f_i = p^{-nr}\sum_{\deg Z<r}\epsilon_Z(B_i)\sigma_i \qquad \left(\sigma_i = \sum_{\deg A_iX_i<r}\epsilon_Z(\alpha_iA_iX_i)\right)$$

and by compounding the functions $f_1, f_2, \cdots, f_s$ in the manner of

(10), we get

$$N_s(F) = f_1 \cdot f_2 \cdot \cdots \cdot f_s = p^{-nr} \sum_{\deg Z<r} \epsilon_Z(F) \prod_{i=1}^{s} \sigma_i. \tag{12}$$

Applying (4) we get

$$\sigma_i = \sum_{X_i} \epsilon(\alpha_i Z X_i,\ R A_i^{-1}) = \begin{cases} p^{n(r-a_i)} & \text{if } A_i^{-1} R \mid Z, \\ 0 & \text{if } A_i^{-1} R \nmid Z. \end{cases} \tag{13}$$

Let Q be an irreducible dividing some A_i. There exists then another A, say A_k, such that $(Q, A_k)=1$. If we take $i=k$ in (13), then it follows that, for Z to contribute to $N_s(F)$ in (12), $A_k^{-1}R$ must divide Z. This shows that $Q^t \mid Z$ where t is the highest power to which Q appears in R. Since Λ must also divide Z by the same argument, it follows that $R \mid Z$. Hence the only value of Z contributing to $N_s(F)$ is $Z=0$, and from (12) we get

$$N_s(F) = p^{-nr} \prod_{i=1}^{s} p^{n(r-a_i)} = p^{n\{\lambda+r(s-2)\}}.$$

A second application of Theorem 1 to linear sums is given by the following theorem.

THEOREM 3. *If F and P are polynomials of D, P irreducible of degree π,* $\deg F<\pi\lambda$ $(\lambda>0)$, *and if $\alpha_1, \cdots, \alpha_s$ are nonzero elements of $GF(p^n)$, then the number of solutions $\nu_s(F)$ of $F=\alpha_1 X_1 + \cdots + \alpha_s X_s$ in polynomials $X_1, \cdots, X_s$ of degree less than $\pi\lambda$ and such that each X_i is prime to P is given by*

$$\nu_s(F) = p^{n\pi\{\lambda(s-1)-s\}}\{(p^{n\pi}-1)^s + \mu_s \xi(F)\}$$

where $\mu_s=+1$ or -1 according as s is even or odd and $\xi(F)=p^{n\pi}-1$ or -1 according as $P \mid F$ or $P \nmid F$.

PROOF. Using Theorem 1 and (10) as in the proof of Theorem 2 and with $R=P^\lambda$, $r=\pi\lambda$, we see that

$$\nu_s(F) = p^{-n\pi\lambda} \sum_{Z \pmod{P_\lambda}} \epsilon_Z(F) \prod_{i=1}^{s} \sum_{(P,X_i)=1} \epsilon_Z(\alpha_i X_i), \tag{14}$$

the second summation being over all X_i of degree less than $\pi\lambda$ and prime to P. One may write

$$\nu_s(F) = p^{-n\pi\lambda}\left\{(\phi(P^\lambda))^s + \sum_{0 \leqq \deg Z<\pi\lambda} \epsilon_Z(F) \prod_{i=1}^{s} \eta(\alpha_i Z,\ P^\lambda)\right\} \tag{15}$$

where ϕ represents the Euler ϕ-function in D, η replacing the inner sum of (14). We know that

$$\phi(P^\lambda) = p^{n\pi\lambda} - p^{n\pi(\lambda-1)}, \tag{16}$$

and by [2, §4], for the Z occurring in (15),

$$\eta(\alpha_i Z, P^\lambda) = \begin{cases} -p^{n\pi(\lambda-1)} & \text{if } P^{\lambda-1} \mid Z, \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

By (17) we see that for Z to contribute to $\nu_s(F)$, it must be of the form $Z=Z'P^{\lambda-1}$ $(0\leqq\deg Z'<\pi)$. Thus from (15), (16), (17) we get

$$\nu_s(F) = p^{-n\pi\lambda}\left\{(p^{n\pi\lambda} - p^{n\pi(\lambda-1)})^s + \sum_{0\leqq \deg Z'<\pi} \epsilon_{Z'P^{\lambda-1}}(F)\left\{-p^{n\pi(\lambda-1)}\right\}^s\right\},$$

but the Z' sum is equal to $\xi(F)$ by (4), and the theorem follows on simplification.

4. **Bilinear sums.** In this section we show how Theorem 2 can be applied to sums of products of the type given by (2). We first prove the following simple extension of [1, Lemma 1]:

LEMMA. *The number of relatively prime sets ψ of primary polynomials $[A_1, \cdots, A_s]$ of degree $a_1, \cdots, a_s$ respectively is given (in case all $a_i>0$) by*

$$\psi(a_1, \cdots, a_s) = p^{n(a_1+\cdots+a_s)}(1 - p^{n(1-s)}).$$

PROOF. Let a be the minimum of $a_1, \cdots, a_s$. Then

$$\begin{aligned} p^{n(a_1+\cdots+a_s)} &= \sum_{u=0}^{a} p^{nu}\psi(a_1 - u, \cdots, a_s - u) \\ &= \sum_{u=1}^{a} p^{nu}\psi(a_1 - u, \cdots, a_s - u) + \psi(a_1, \cdots, a_s) \\ &= p^n\sum_{u=0}^{a-1} p^{nu}\psi(a_1 - u - 1, \cdots, a_s - u - 1) \\ &\quad + \psi(a_1, \cdots, a_s) \end{aligned} \tag{18}$$

which gives, on applying (18),

$$p^{n(a_1+\cdots+a_s)} = p^n\cdot p^{n(a_1+\cdots+a_s-s)} + \psi(a_1, \cdots, a_s)$$

and the lemma follows. We now prove the following theorem.

THEOREM 4. *Let m, s, t, k be integers, $m=t+k$, $s>1$, $t>k\geqq 0$, and F, $P_1, \cdots, P_s$ polynomials of D, deg $F<ms$, $P_1, \cdots, P_s$ all primary*

and irreducible of degree t and not all equal. Then the number of solutions $\sigma(F, s)$ of

$$F = \alpha_1 P_1 X_1 Y_1 + \cdots + \alpha_s P_s X_s Y_s \qquad (\alpha_i \in GF(p^n),\ \alpha_i \neq 0) \tag{19}$$

in primary polynomials X_i of degree k and arbitrary polynomials Y_i of degree less than $m(s-1)$, $i=1, \cdots, s$, is given by

$$\sigma(F, s) = p^{ns\{k+m(s-2)\}} \sum_{z=0}^{k} \gamma_z(F) p^{-nz(s-1)}$$

where $\gamma_z(F) = \delta_z(F) - \delta_{z-1}(F)$, $\delta_z(F)$ being the number of primary divisors of F of degree z.

PROOF. If (19) has a solution (X_i, Y_i) where $Z = (X_1, \cdots, X_s)$, then we may write $J_i = Z^{-1}X_i$ so that $(J_1, \cdots, J_s) = 1$. We have

$$\begin{aligned} Z^{-1}F &= (\alpha_1 Z^{-1} P_1 X_1) Y_1 + \cdots + (\alpha_s Z^{-1} P_s X_s) Y_s \\ &= \alpha_1 A_1 Y_1 + \cdots + \alpha_s A_s Y_s \ (A_i = P_i J_i, \deg J_i = j = k - z). \end{aligned} \tag{20}$$

Since the P_i are irreducible and not all equal, $(P_1, \cdots, P_s) = 1$, and since $\deg P_i = t > j$, it follows that $(A_1, \cdots, A_s) = 1$, $\deg A_i = m - z$, $z = \deg Z \leqq k$ $(i = 1, \cdots, s)$. With $r = ms - z$, $\lambda = z(s-1)$ we see that Theorem 2 applies to (20). If we let the J_i range over all permissible values, meaning all primary J_i with $(J_1, \cdots, J_s) = 1$, $\deg J_i = k - z$ ($z \leqq k$ being the degree of polynomials Z such that $Z \mid F$), then we get

$$\sigma(F, s) = \sum_{Z \mid F} \psi(k - z, \cdots, k - z) \cdot N_s(Z^{-1}F) \qquad (Z \text{ primary}), \tag{21}$$

and applying the above lemma and Theorem 2 to (21), one obtains

$$\begin{aligned} \sigma(F, s) &= \sum_{z=0}^{k-1} \delta_z(F) \cdot p^{ns(k-z)}(1 - p^{n(1-s)}) p^{n\{z+ms(s-2)\}} \\ &\quad + \delta_k(F) p^{m\{k+ms(s-2)\}} \\ &= c\left\{(1 - p^{n(1-s)}) \sum_{z=0}^{k-1} \delta_z(F) p^{-nz(s-1)} + p^{nk(1-s)} \delta_k(F)\right\}, \end{aligned}$$

where $c = p^{ns\{k+m(s-2)\}}$. Simplification of the expression in braces (see [4, §3]) leads to the theorem.

Comparison of this result with the main result of [6] for the case $s = 1$ of that paper shows that nontrivial coefficients can be introduced in each term in the sum of the products (19) with quite simple results. It should be pointed out, however, that certain new restrictions have been placed on the degree of the Y_i. Although the method of this paper can be applied to higher sums, $\sum P_i^e X_i^e Y_i$ as in [6], no essentially new points arise and the result can be expressed in terms of divisor functions which generalize the functions δ_z and γ_z[5, §4].

In the above proof, (19) is assumed to possess a solution of the type required by the theorem. That this assumption is valid can be seen by assigning to the X_i any relatively prime set of primary polynomials of degree k and applying Theorem 2. Thus (19) is solvable for all values of s permitted by the theorem, including the minimal value $s=2$. This fact can be restated as the following Waring type result for sums of products:

COROLLARY. *If P_1, P_2 are irreducible primary polynomials of D of degree t ($P_1 \neq P_2$) and α_1, α_2 are nonzero elements of $GF(p^n)$, then every polynomial $F \in D$ of degree less than $2m$, $m=t+k$ ($t>k\geqq 0$) can be expressed as a sum of two products,*

$$F = \alpha_1 P_1 X_1 Y_1 + \alpha_2 P_2 X_2 Y_2$$

where X_1, X_2 are primary polynomials of degree k and Y_1, Y_2 are arbitrary polynomials of degree less than m.

BIBLIOGRAPHY

1. L. Carlitz, *On the representation of a polynomial in a Galois field as the sum of an even number of squares*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 397–410.

2. ———, *The singular series for sums of squares of polynomials*, Duke Math. J. vol. 14 (1947) pp. 1015–1120.

3. ———, *Representations of arithmetic functions in $GF[p^n, x]$*, Duke Math. J. vol. 14 (1947) pp. 1121–1137.

4. Eckford Cohen, *Sums of an even number of squares in $GF[p^n, x]$*, Duke Math. J. vol. 14 (1947) pp. 251–267.

5. ———, *An extension of Ramanujan's sum*, Duke Math. J. vol. 15 (1949) pp. 85–90.

6. ———, *Sums of products of polynomials in a Galois field*, Duke Math. J. vol. 18 (1951) pp. 425–430.

INSTITUTE FOR ADVANCED STUDY