REPRESENTATION OF ARITHMETIC FUNCTIONS IN $GF[p^n, x]$ WITH VALUES IN AN ARBITRARY FIELD

By Joseph A. Silva

1. Let $GF[p^n, x]$ denote the set of polynomials in an indeterminate x with coefficients from a finite field $GF(p^n)$. By an arithmetic function f will be meant a single-valued function defined over $GF[p^n, x]$ with values $f(A)$ in a field $\mathfrak{F}$. The sum of two functions $h = f + g$ is defined by $h(A) = f(A) + g(A)$. Instead of the ordinary product we use one of the Cauchy products called C_3 multiplication [4]. Let r be a fixed positive integer. Then for two functions f and g the C_3 product is defined by

$$h(M) = \sum_{A+B=M} f(A)g(B) \qquad (\deg M < r),$$

where the sum extends over all polynomials A and B (including 0) of degree $< r$ such that $A + B = M$. For convenience we sometimes write this product as $h = f \cdot g$; when the dot is omitted, the ordinary product is understood. We define two functions f and g as equivalent (written $f \sim g$) if $f(A) = g(A)$ for all A for which $\deg A < r$; we shall usually replace the symbol $\sim$ by $=$. It is evident that the set of functions with addition, multiplication, and equivalence defined as above form a commutative ring $\mathfrak{R} = \mathfrak{R}^r$ with unit element; the unit element is given by $\iota(0) = 1$, $\iota(A) = 0$ for $A \neq 0$.

It has been shown [2] that if $\mathfrak{F}$ is of characteristic zero and contains the p-th roots of unity, then there exists a set of p^{nr} orthogonal (hence linearly independent) functions ϵ_{GH} such that an arbitrary function f in $\mathfrak{R}$ may be represented uniquely by

$$f = \sum{}^{*} \alpha_{GH}\epsilon_{GH} ,$$

where the α_{GH} are numbers of $\mathfrak{F}$ and the asterisk indicates a summation over the p^{nr} orthogonal functions ϵ_{GH}.

The ϵ_{GH} are defined in the following manner. If $\alpha \in GF(p^n)$, we put $\alpha = a_1\theta^{n-1} + \cdots + a_n$, where $a_i \in GF(p)$ and θ generates the $GF(p^n)$; we put $a_1 = t(\alpha)$. If H is a primary polynomial of degree h in $GF[p^n, x]$ and $A \equiv \alpha_1 x^{h-1} + \cdots + \alpha_h \pmod{H}$ we put

$$\epsilon(A, H) = e^{2\pi i t(\alpha_1)/p}.$$

Now let $(G, H) = 1$, then we define

$$\epsilon_{GH}(A) = \epsilon(GA, H).$$

It follows that $\mathfrak{R}$ is a direct sum of p^{nr} fields $\mathfrak{F}$. Thus $\mathfrak{R}$ contains no nilpotent elements, and every element of $\mathfrak{R}$ which is not a divisor of zero has a unique inverse in $\mathfrak{R}$.

Received May 30, 1951.