BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 2, March 1977

FUNCTIONS AND CORRESPONDENCES IN A FINITE FIELD

BY L. CARLITZ[1]

1. Introduction. It is well known that any function from a finite field into itself can be represented by a polynomial with coefficients in the field. More precisely, if the field is of order q, then the function is represented by a *unique* polynomial of degree less than q. Conversely, any field with the property that any function from the field into itself can be represented by a polynomial with coefficients in the field, is necessarily finite **[14]**. It has been proved recently **[1]**, **[16]** that if a ring R with identity has the property that any function from R into itself can be represented by a *generalized* polynomial, then R is isomorphic to the matric ring $(\mathrm{GF}(q))_n$, for some prime power q and some $n \geqslant 1$. As customary, we denote by $\mathrm{GF}(q)$ the finite field of order q. By a generalized polynomial is meant a sum of multinomials of the form

$$a_0 x^{e_1} a_1 x^{e_2} \cdots a_{k-1} x^{e_k} a_k,$$

where $a_i \in R$, $e_i > 0$ and k is arbitrary.

With every function f from $F_q = GF(q)$ into itself we may associate a set of numbers $a_1, a_2, \ldots, a_k \in F_q$ and a partition **[5]–[8]**, **[13]**

$$F_q = A_1 \cup A_2 \cup \cdots \cup A_k, \tag{1.1}$$

where

$$A_i \cap A_j = \varnothing \qquad (i \neq j), \tag{1.2}$$

the sets A_i are nonvacuous and

$$f(b_i) = a_i \qquad (b_i \in A_i;\ i = 1, 2, \ldots, k). \tag{1.3}$$

For example, for the function $f(x) = x^{q-1}$, we have $k = 2$, $a_1 = 0$, $a_2 = 1$, $A_1 = \{0\}$, $A_2 = \{a \mid a \in F_q,\ a \neq 0\}$. On the other hand, for the function $f(x) = x^{q-2}$, $k = q$ and each A_i consists of a single element. Thus x^{q-2} is a *permutation function*. Clearly, for any permutation function, the number of sets A_i in the partition (1.1) is equal to q.

We can generalize the above in the following way. Let

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k \tag{1.4}$$

denote partitions of F_q. It is assumed that each of the sets

$$A_1, \ldots, A_k, \quad B_1, \ldots, B_k \tag{1.5}$$

is nonvacuous; however A_0, B_0 are unrestricted. Then (by the Lagrange interpolation formula for several variables) there exists a polynomial **[9]** $f(x, y) \in F_q[x, y]$ such that

An address delivered to the American Mathematical Society in Tallahassee, Florida, March 4, 1976; received by the editors April 22, 1976.

AMS (MOS) subject classifications (1970). Primary 12C05.

Key words and phrases. Finite fields, functions, correspondences.

[1]Supported in part by NSF grant GP-37924X.