# A NOTE ON PERMUTATION FUNCTIONS OVER A FINITE FIELD

By L. Carlitz

1. Let $F$ denote the finite field $GF(q)$ of order $q$. It is familiar that every function $f(x)$ over $F$ with values in $F$ can be represented by a polynomial with coefficients in $F$. Indeed by the Lagrange interpolation formula we have

$$f(x) = -\sum_{a \varepsilon F} \frac{x^q - x}{x - a} f(a). \tag{1}$$

The values $f(a)$ are arbitrary elements of $F$. In particular if the $f(a)$ are distinct, then $f(x)$ is a *permutation polynomial.*

For many purposes it is convenient to adjoin a symbol $\infty$ to $F$. We assume that $\infty = 1/0, 0 = 1/\infty$, $\infty + a = \infty$ $(a \varepsilon F)$, $a \cdot \infty = \infty$ $(a \neq 0)$. For brevity we let $F^*$ denote the enlarged system. A function $f(x)$ over $F^*$ will have the obvious meaning, namely $f(a) \varepsilon F^*$ for all a $\varepsilon F^*$. In particular if the quantities $f(a)$ are distinct for all $a \varepsilon F^*$, then $f(x)$ is called a *permutation function* over $F^*$.

Suppose now that $f(x)$ is a permutation function over $F^*$. If, in the first place, $f(\infty) = \infty$ then the numbers $f(a)$, where $a \varepsilon F$, are a permutation of the numbers of $F$. Thus we may identify $f(x)$ with the permutation polynomial $\bar{f}(x)$ defined by

$$\bar{f}(x) = -\sum_{a \varepsilon F} \frac{x^q - x}{x - a} f(a).$$

Because of the hypothesis concerning $f(x)$ it is clear that deg $\bar{f}(x) \geq 1$, so that $\bar{f}(\infty) = \infty$.

In the next place suppose that $f(\infty) \neq \infty$. Let $f(k) = \infty$, where $k \varepsilon F$, and put

$$g(x) = f\left(k + \frac{1}{x - k}\right) \qquad (x \neq a). \tag{2}$$

Then clearly $g(\infty) = f(k) = \infty$. Moreover for $x \varepsilon F$, $x \neq k$, the numbers

$$k + \frac{1}{x - k}$$

are distinct and different from $k$; thus the numbers

$$k, k + \frac{1}{x - k} \qquad (x \varepsilon F, x \neq k) \tag{3}$$

run through the numbers of $F$. By the present hypothesis it follows that the numbers

$$f(\infty), \qquad f\left(k + \frac{1}{x - k}\right) \tag{4}$$

Received June 21, 1961. Supported in part by National Science Foundation grant G16485.