A GEOMETRIC APPROACH TO PERMUTATION POLYNOMIALS OVER A FINITE FIELD

By D. R. Hayes

1. Introduction. In 1897, Dickson [2], [3] classified the permutation polynomials of degrees less than 7 over a finite field. (A permutation polynomial is one for which the associated polynomial function is a one-to-one mapping of the finite field onto itself.) His results are quite remarkable in a number of ways. For example, he found that except for a few "accidents" over fields of low order, the permutation polynomials of a given degree fall into a finite number of well-defined categories. Further, his results show that, except for "accidents", there are no permutation polynomials of degrees 2, 4, and 6 except when the characteristic of the field is 2. In a recent address before the Mathematical Association of America, Professor L. Carlitz suggested that this behavior is perhaps characteristic. That is, Carlitz suggested the following conjecture:

Given an even positive integer $2n$, there is a constant K_{2n} such that if k is a finite field of odd order q with $q > K_{2n}$, then there are no permutation polynomials of degree $2n$ over k.

In this paper, a method for introducing some geometric ideas into the study of permutation polynomials is discussed. The principal advantage in looking at permutation polynomials from this point of view is that one is able to make use of a powerful theorem of Lang-Weil [4] which estimates the number of rational points on an absolutely irreducible curve defined over a finite field. We are able to verify the Carlitz conjecture when $2n$ is 8 and 10 respectively and to show generally that the conjecture is valid when the characteristic of the field does not divide $2n$. However, the principal aim of the paper is to present an organized introduction to the method in the hope of laying the foundation for a systematic theory, if such can be constructed along these lines.

This geometric approach is not altogether new. In fact, Davenport and Lewis in [1], although interested in a different problem, essentially establish the Carlitz conjecture when the characteristic of the field does not divide $2n$. Their method is basically the same as the one used in this paper for that purpose, although we have obtained a somewhat more general result (Theorem 3.4).

2. The Lang-Weil Theorem. Let k be a finite field of q elements, and let Ω be an algebraic closure of k. In the "plane" $\Omega \times \Omega$ we consider algebraic curves defined over k, i.e., subsets of $\Omega \times \Omega$ of the form

$$\mathbf{C}_P = \{(\alpha, \beta) \in \Omega \times \Omega \mid P(\alpha, \beta) = 0\},$$

Received May 13, 1966.