PRIMITIVE GROUPS, MOORE GRAPHS, AND RATIONAL CURVES

Michael Fried and John H. Smith

0. INTRODUCTION

Roughly speaking, a Moore group is a primitive permutation group in which the orbits of the stabilizer of a point actually achieve a certain theoretical bound on their sizes. Such groups appear to be fairly rare; we prove some results limiting the possibile degrees that Moore groups of fixed rank may have. First, we use standard methods to reduce the problem to the study of certain graphs called Moore graphs. With each possible diameter for Moore graphs we associate a polynomial in two variables, one of which corresponds to the degree. (Note that the standard group-theoretic and graph-theoretic meanings of "degree" do not correspond here; the degree of a permutation group is not the degree of the corresponding graph. The terms are defined in Sections 1 and 2.) Theorems from Diophantine geometry then yield information about reducibility and integral roots of this polynomial, which in turn gives information about possible Moore graphs of the given diameter.

1. MOORE GROUPS

Let G denote a primitive permutation group of rank $k + 1$ on a finite set Ω, and for each element α of Ω, let G_α denote the stabilizer of α. If for some α we arrange the orbits of G_α in the order of increasing size, then the rate of growth of these orbits is subject to some restrictions (see [13, Section 17] and [12, Proposition 4.5]). In particular, if the order d of Δ, the smallest nontrivial orbit, is strictly smaller than the other orders, then the latter are bounded by $d(d - 1)$, $d(d - 1)^2$, $\cdots$, $d(d - 1)^{k-1}$. If these bounds are actually attained, we call the group a *Moore group of valence* d. Moore groups of rank 3 are classified in [1] and [6]. A partial classification follows from graph-theoretic results in [9].

THEOREM 1. *For each even rank, there are only finitely many possible valences (hence only finitely many possible degrees) for a Moore group.*

THEOREM 2. *For each rank* $k + 1$, *the set of integers that are not possible valences for a Moore group of rank* $k + 1$ *contains an arithmetic progression.*

Definition. A function f from Ω to the integers is called a *homogeneous weight function* if $\sum_{\delta\in\Delta} f(\delta^\sigma)/f(\alpha^\sigma)$ is independent of $\sigma \in G$.

THEOREM 3. *For each* $k \geq 5$, *there are only finitely many* d *for which there exists a Moore group of rank* $k + 1$ *and valence* d *with a nonconstant homogeneous weight function.*

The proofs will be given in the following sections.

Received January 8, 1972.

Michigan Math. J. 19 (1972).