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.

2. MOORE GRAPHS

We make Ω into an undirected graph by putting an edge between α^σ and δ^σ, for all $\delta \in \Delta$, $\sigma \in G$. These graphs have been studied for arbitrary permutation groups in [12]. In particular, it is known that if in our case the group is a Moore group of rank $k+1$ and valence d, then the resulting graph is of diameter k and degree d and has the maximum number of vertices subject to these conditions. Such graphs are called *Moore graphs.* The following theorems on Moore graphs imply the corresponding theorems on Moore groups.

THEOREM 1'. *For each odd diameter, there are only finitely many possible degrees for a Moore graph.*

THEOREM 2'. *For each positive integer* k, *the set of positive integers* d *that are not degrees of any Moore graph of diameter* k *contains an arithmetic progression.*

For each graph, we consider functions from the vertices to the complex numbers. We define the *adjacency map* A on this vector space by saying that at each vertex the value of $A\phi$ is the sum of the values of ϕ at the adjacent vertices. The map A is represented, with respect to the obvious basis, by the adjacency matrix of the graph.

A homogeneous weight function for a primitive permutation group is an integral-valued eigenvector of the A of the corresponding graph, and its eigenvalue is therefore rational. Conversely, each rational eigenvalue of A gives rise to such a ϕ, whose values may be taken to be integers. Theorem 3 will therefore follow from Theorem 3'.

THEOREM 3'. *For* $k \geq 5$, *there are only finitely many* d *for which a Moore graph of diameter* k *and degree* d *can have a rational eigenvalue other than* d.

The gap between our nonexistence results and known existence results is enormous. For each k, the $(2k+1)$-gon is a Moore graph of diameter k. For $k = 3$, there are no others. For $k = 2$, there is one of degree 3 (the Petersen graph), one of degree 7, and possibly one of degree 57, but there are no others (see [9]). If there is one of degree 57, it does not arise from a Moore group [1]. No other Moore graphs are known. Nonexistence results for many values of d and k are obtained, by entirely different methods, in [5].

Note that for each degree and each diameter, there are only finitely many Moore graphs; in no known case are there more than one.

3. THE GEOMETRY OF THE POLYNOMIAL OF MOORE GRAPHS

For each regular connected graph there is a monic polynomial f, with integer coefficients, such that f(A), applied to a vector (function) from the natural basis, is identically 1 (or, equivalently, such that f applied to the adjacency matrix gives the matrix all of whose entries are 1); the polynomial f of smallest degree with these properties is called the *polynomial of the graph* (see [8]). Its zeros are distinct, and they constitute the set of eigenvalues, other than the degree of the graph, of A. It is easy to see that for a Moore graph the polynomial depends only on d and k. If we let $f_k(x, y)$ denote the polynomial of a Moore graph of diameter k and degree $d = y + 1$, then the f_k satisfy the relations

$$f_1(x, y) = x + 1,$$

$$f_2(x, y) = x^2 + x - y,$$

$$f_{k+1}(x, y) = xf_k(x, y) - yf_{k-1}(x, y)$$

(for details, see [9]).

It follows immediately that f_k is monic in x, so that in each solution of the equation $f_k(x, y) = 0$ in which y is an integer, x is an algebraic integer; hence the only rational solutions in which y is integral are integral.

We construct the corresponding homogeneous polynomials $F_k = F_k(X, Y, Z)$, which satisfy the formulas

$$F_1 = X + Z, \quad F_2 = X^2 + XZ - YZ, \quad F_{k+1} = XF_k - YZF_{k-1}.$$

If we let $G_k = G_k(X, Y)$ and $H_k = H_k(X, Z)$ denote the polynomials by which the highest powers of Z and Y, respectively, are multiplied in F_k, then

$$G_1 = 1, \quad G_2 = X - Y, \quad G_{2k+1} = -YG_{2k-1}, \quad G_{2k+2} = XG_{2k+1} - YG_{2k},$$

$$H_1 = X + Z, \quad H_2 = -Z, \quad H_{2k+1} = XH_{2k} - ZH_{2k-1}, \quad H_{2k+2} = -ZH_{2k}.$$

From this it follows by a simple induction that

$$G_{2k+1} = (-)^k Y^k, \quad G_{2k} = (-)^{k-1}(kXY^{k-1} + Y^k),$$

$$H_{2k+1} = (-)^k((k+1)XZ^k + Z^{k+1}), \quad H_{2k} = (-)^k Z^k.$$

Geometrically, this means that if C_k is the curve in the projective plane determined by $F_k = 0$, then

(i) C_{2k+1} has a k-fold point at (0, 0, 1) with k-fold tangent $Y = 0$, and a (k + 1)-fold point at (0, 1, 0) with k-fold tangent $Z = 0$ and simple tangent $(k+1)X + Z = 0$,

(ii) C_{2k} has a k-fold point at (0, 0, 1) with (k - 1)-fold tangent $Y = 0$ and simple tangent $kX + Y = 0$, and a k-fold point at (0, 1, 0) with k-fold tangent $Z = 0$.

This is enough to show that the C_k are of genus zero, that is, can be parametrized. In fact, it gives us an explicit parametrization. The quadratic curves having tangent $Y = 0$ at (0, 0, 1) and $Z = 0$ at (0, 1, 0) form a pencil, which is given by the equation $\mu X^2 + \lambda YZ = 0$. Each has intersection multiplicities 2k at (0, 0, 1) and 2k + 1 at (0, 1, 0) with C_{2k+1}, and intersection multiplicities 2k - 1 at (0, 0, 1) and 2k at (0, 1, 0) with C_{2k}. Hence each has exactly one further intersection with each C_k. Conversely, each point of C_k (other than (0, 0, 1) and (0, 1, 0)) is contained in exactly one curve of the pencil.

4. PROOFS OF THE THEOREMS

Proof of Theorem 2'. The curves are, in particular, irreducible. Hence, by Hilbert's irreducibility criterion [7], the set S of integral y_0 for which $f_k(x, y_0)$ is irreducible in Q[X] is infinite; by results in [3] and [10], the set S even contains an arithmetic progression. But A. J. Hofmann and R. R. Singleton have shown [9] that for such y_0 there exists no Moore graph of degree $d = y + 1$ and diameter k. This completes the proof.

We return to the affine plane and derive explicit formulas for the parametrizations. Here our quadratic curves take the form $-tx^2 + y = 0$, and the remaining intersection with $f_k(x, y) = 0$ is solved for by substitution.

A simple recursion shows that

$$f_{k+1}(x, tx^2) = x^k e_k(t) + x^{k-1} e_{k-1}(t),$$

where

$$e_0(t) = e_1(t) = 1, \quad e_{k+1}(t) = e_k(t) - t e_{k-1}(t).$$

In particular, the degree of e_k is $[k/2]$. An argument of Sturm type shows that no two consecutive e_k have a common root, and that each e_k has distinct roots, all of which are real. The parametrization of the affine part c_k of C_k is given by the equations

$$x = -e_{k-1}(t)/e_k(t), \quad y = tx^2.$$

We denote the rational function of t describing y by $h(t)$. Note that it is of degree k in t.

Proof of Theorem 3'. For $k \geq 6$, x has three distinct poles; for $k = 5$, x has two and y has another one at $t = \infty$. Hence, by C. L. Siegel's theorem (see [11, pp. 242-245]), there are only finitely many integral points on c_k; hence, by an earlier remark, there are only finitely many integral values y_0 for which $f_k(x, y_0)$ has a rational root, in other words, such that the adjacency map of a Moore graph of diameter k and degree $d = y_0 + 1$ has a rational eigenvalue other than the degree.

Proof of Theorem 1'. Suppose that for some k there are infinitely many possible degrees for Moore graphs, hence, again by [9], infinitely many integral values y_0 of y for which $f_k(x, y_0)$ is reducible. If we let $x_1, x_2, \cdots, x_r$ denote the zeros of $f_k(x, y)$ in some algebraic closure of $Q(y)$, then for some $S \subset \{1, 2, \cdots, r\}$, the field

$$L = Q\Big(y, \xi_1 = \sum_{\alpha \in S} x_\alpha, \xi_2 = \sum_{\substack{\alpha,\beta \in S \\ \alpha \neq \beta}} x_\alpha x_\beta, \cdots, \xi_s = \prod_{\alpha \in S} x_\alpha\Big)$$

has infinitely many places that take y and the ξ_i to rational integers. By Siegel's theorem, L is of genus zero, and we can choose a uniformizing parameter z such that $L = Q(z)$; since the ring of integers has only finitely many units, Siegel's theorem further tells us that z can be chosen so that y and the ξ_i are polynomials in z with rational coefficients, say $y = g(z)$. Hence $f_k(x, g(z))$ is reducible as a polynomial in $Q(z)[x]$.

This implies that $[Q(x, z) : Q(z)] = [Q(t, z) : Q(z)]$ is less than $[Q(x, y) : Q(y)]$. Hence $h(t) - g(t)$ is reducible.

Now, by Proposition 2 of [4], this implies that there are rational functions h_1 and h_2 and polynomials g_1 and g_2 such that

(i) $\deg(h_1) > 1$, $\deg(g_1) > 1$,

(ii) $h_1(h_2(t)) = h(t)$, $g_1(g_2(z)) = g(z)$,

(iii) the splitting fields of $h_1(t) - y$ and $g_1(z) - y$ (in a fixed algebraic closure of $Q(y)$) coincide (we denote this field by M),

(iv) $h_1(t) - g_1(z)$ is reducible.

Now consider a place of M taking y to ∞. We compute its ramification over $Q(y)$ in two different ways.

If we adjoin a root t_0 of the equation $h(t) - y = 0$ to $Q(y)$, then each place extending $y = \infty$ has ramification degree 1 or 2, since the poles of h(t) are of degree 1 or 2. Hence the same holds for roots of the equation $h_1(t) - y = 0$. Since the ramification is tame, it follows that if we adjoin all the roots we still get ramification 1 or 2.

Now if we adjoin a root of the equation $g_1(z) - y = 0$ to $Q(y)$, the ramification degree of each extension of the place $y = \infty$ is the degree of g_1. Hence, since the ramification is tame, it follows that if we adjoin all the roots, the ramification degree is still the degree of g_1. We conclude that the degree of g_1 is 2 and $[M : Q(y)] = 2$. Hence the degree of h_1 is 2, and the degree k of h is even.

Remark 1. It seems reasonable to investigate the properties of the Galois group G of the splitting fields of $h(t) - y$ over $Q(y)$. For example, one could prove Theorem 1' for even diameter k if it could be shown that G, acting on the roots of this polynomial, has no system of imprimitivity of order k/2.

Remark 2. Recent work of A. Baker and J. Coates [2] has lead to effective bounds on the integral points of curves such as those considered here; in some cases, the effective bound yields a practical bound. This could be used to determine all Moore graphs of a prescribed diameter admitting a homogeneous weight function; however, the calculations might still be unfeasible at the graph-theoretic level.

5. ELEMENTARY ANALYSIS OF THE INTEGRAL POINTS

We can use the parametrizations above to get some information on the integral points of c_k. For such points, $t = y/x^2$ is rational, say $t = u/v$, where u and v are relatively prime integers. In the expressions for x and y, multiply numerator and denominator by a high enough power of v to make them polynomials in u and v. Then our recursion formula for the polynomials e_k shows that if x and y are integers, then no prime can divide the bottom of the expression for x. For even k, this is also sufficient; but for odd k, there must, in addition, be no prime dividing v. Hence we have the following result.

PROPOSITION. *The integral points on* c_k *are given by*

(i) *integer solutions* t *of the equation* $e_k(t) = \pm 1$, *if* k *is odd*,

(ii) *integer solutions* u, v *with* $(u, v) = 1$ *of the equation* $v^{k/2} e_k(u/v) = \pm 1$, *if* k *is even.*

(For odd k, this gives Theorem 3' without the use of Siegel's theorem.)

In particular, for $k = 3$ the only integral points are seen to be (0, 0) and (1, 0) (as is shown in [9]). The only integral points for $k = 5$ are (0, 0) and (1, 0), and for $k = 7$, they are (0, 0), (-1, 0), and (-1, 1). Except for the last (which corresponds to the regular 15-gon) these points do not arise from Moore graphs.

However, for $k = 4$ there are infinitely many solutions of the equation $v^2 - 3uv + u^2 = \pm 1$. We obtain them by taking $(v - 3u/2) + \sqrt{5}u/2$ to be a unit in $Q(\sqrt{5})$, that is, a power of $(1 - \sqrt{5})/2$. It is not known whether any of the solutions come from Moore graphs. The values $t = 2, 2\frac{1}{2}$, and 3, for example, would correspond to degrees 18, 64, and 75, respectively, quite beyond the range of elementary calculation.

REFERENCES

1. M. Aschbacher, *The nonexistence of rank three permutation groups of degree* 3250 *and subdegree* 57. J. Algebra 19 (1971), 538-540.

2. A. Baker and J. Coates, *Integer points on curves of genus* 1. Proc. Cambridge Philos. Soc. 67 (1970), 595-602.

3. M. Fried, *Arithmetical properties of value sets of polynomials.* Acta Arith. 15 (1969), 91-115.

4. ———, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables.* Illinois J. Math. (to appear).

5. H. D. Friedman, *On the impossibility of certain Moore graphs.* J. Combinatorial Theory Ser. B 10 (1971), 245-252.

6. D. G. Higman, *Finite permutation groups of rank* 3. Math. Z. 86 (1964), 145-156.

7. D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten.* J. Reine Angew. Math. 110 (1892), 104-129; Ges. Abh., Vol. 2, pp. 264-286, Springer-Verlag, Berlin, 1933.

8. A. J. Hoffman, *On the polynomial of a graph.* Amer. Math. Monthly 70 (1963), 30-36.

9. A. J. Hoffman and R. R. Singleton, *On Moore graphs with diameters* 2 *and* 3. IBM J. Res. Develop. 4 (1960), 497-504.

10. A. Schinzel, *On Hilbert's irreducibility theorem.* Ann. Polon. Math. 16 (1965), 333-340.

11. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. (1929), No. 1, 70 pp.; Ges. Abh., Vol. 1, pp. 209-266, Springer-Verlag, Berlin, 1966.

12. C. C. Sims, *Graphs and finite permutation groups.* Math. Z. 95 (1967), 76-86.

13. H. Wielandt, *Finite permutation groups.* Academic Press, New York, 1964.

State University of New York
Stony Brook, New York 11790
and
Boston College
Chestnut Hill, Massachusetts 02167