1993

The Proportion of Fixed-Point-Free Elements of a Transitive Permutation Group

Nigel Boston
University of Illinois at Urbana-Champaign, boston@math.uiuc.edu

Walter Dabrowski
University of Illinois at Urbana-Champaign

Tuval Foguel
University of Illinois at Urbana-Champaign, TFOGUEL@ADELPHI.EDU

Paul J. Gies
University of Illinois at Urbana-Champaign, paulgies@maine.edu

Judy Leavitt Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

See next page for additional authors

Published in Communications in Algebra, 21:9 (1993), pp 3259-3275.
doi 10.1080/00927879308824728

.

THE PROPORTION OF FIXED-POINT-FREE ELEMENTS OF A TRANSITIVE PERMUTATION GROUP

Nigel Boston, Walter Dabrowski, Tuval Foguel, Paul J. Gies, Judy Leavitt, and David T. Ose

Department of Mathematics
University of Illinois
Urbana, IL 61801

David A. Jackson

Department of Science and Mathematics
Parks College of Saint Louis University
Cahokia, IL 62206

1. Introduction

In 1990 Hendrik W. Lenstra, Jr. asked the following question: if G is a transitive permutation group of degree n and A is the set of elements of G that move every letter, then can one find a lower bound (in terms of n) for $f(G) = |A|/|G|$? Shortly thereafter, Arjeh Cohen showed that $\frac{1}{n}$ is such a bound.

Lenstra's problem arose from his work on the number field sieve [2]. A simple example of how $f(G)$ arises in number theory is the following: if h is an irreducible polynomial over the integers, consider the proportion:

$$\frac{|\{primes \leq x \mid h \text{ has no zeroes mod } p\}|}{|\{primes \leq x\}|}$$

As $x \longrightarrow \infty$, this ratio approaches $f(G)$, where G is the Galois group of h considered as a permutation group on its roots.

Our results in this paper include explicit calculations of $f(G)$ for groups G in several families. We also obtain results useful for computing $f(G)$ when G is a

wreath product or a direct product of permutation groups. Using this we show that $\{f(G) \mid G \text{ is transitive}\}$ is dense in $[0,1]$. The corresponding conclusion is true if we restrict G to primitive groups.

2. Examples and basic facts

Let G be a permutation group of degree n. Let X denote the set of n letters acted on by G. Let $Stab_G(x)$ denote the stabilizer of $x \in X$ and for any subset $Y = \{y_1, y_2, \ldots, y_m\}$ of X, let $Stab_G(y_1, y_2, \ldots, y_m)$ be the pointwise stabilizer of Y. Given any $g \in G$, define the permutation character, $Ch_G(g)$, of g to be the number of letters fixed by g. We will omit the subscript when the group is clear from context. Let A be the set of elements of G fixing no letters, and $f(G) = |A|/|G|$. Recall [4, 10.1.5] that $\sum_{g\in G} Ch(g) = k|G|$, where k is the number of orbits in X. In particular, if G acts transitively, this sum is just $|G|$.

Example 2.1. Consider D_4, the dihedral group on four letters, of order 8. The three nontrivial rotations and the two reflections about the midpoints of parallel sides are the only elements which have no fixed points. Thus $f(D_4) = \frac{5}{8}$.

More generally, let D_n be the dihedral group on n letters. Here the value of $f(D_n)$ depends upon the parity of n. If n is even, there are $\frac{n}{2}$ reflections about axes through a pair of antipodal vertices. These reflections fix the pair of vertices. The $\frac{n}{2}$ reflections about the midpoints of parallel sides and the $n-1$ nontrivial rotations have no fixed points. It follows that $|A| = n-1+\frac{n}{2}$ and that $f(D_n) = \frac{3n-2}{4n}$. If n is odd, each of the n reflections fixes a vertex and only the $n-1$ nontrivial rotations are without fixed points. From this, $f(D_n) = \frac{n-1}{2n}$.

Example 2.2. Let G be the group of rotations of the n-gon or let G be any group of order n acting regularly on its elements. In a regular action, every nontrivial element acts without fixed points, so $f(G) = \frac{n-1}{n}$. There is no group G with $f(G) = 1$ since the identity always fixes every letter, but this example shows that for each $\epsilon \geq 0$, there are infinitely many groups G with $f(G) \geq 1 - \epsilon$.

For many groups, the following instance of the inclusion-exclusion principle is useful when calculating $|A|$. We observe first that $A = G - \cup_{x\in X} Stab(x)$. For subsets Y_1 and Y_2 of X, note that $Stab(Y_1) \cap Stab(Y_2) = Stab(Y_1 \cup Y_2)$ Then accounting for the overlap between stabilizers, we express the inclusion-exclusion principle as

$$|A| = |G| + \sum_{i=1}^{n} (-1)^i \sum_{\substack{|Y|=i \\ Y\subseteq X}} |Stab(Y)|$$

.

Theorem 2.3. *Let G act sharply k-transitively on a set X with n elements. Then*

$$f(G,X) = \sum_{j=0}^{k-1} \frac{(-1)^j}{j!} + \sum_{j=k}^{n} \frac{(-1)^j \binom{n}{j}}{|G|}.$$

Proof. It is known that a sharply k-transitive group of degree n has order $\frac{n!}{(n-k)!}$. When G acts sharply k-transitively on a set X with n elements, we obtain,

$$|Stab_G(Y)| = \begin{cases} \dfrac{(n-|Y|)!}{(n-k)!} & \text{if } |Y| < k \\ 1 & \text{if } |Y| \geq k, \end{cases}$$

Using the inclusion-exclusion principle, we have

$$\begin{aligned}|A(G,X)| &= |G| + \sum_{j=1}^{n}(-1)^j \sum_{|Y|=j, Y\subseteq X} |Stab(Y)| \\ &= |G| + \sum_{j=1}^{k-1}(-1)^j \binom{n}{j}\frac{(n-j)!}{(n-k)!} + \sum_{j=k}^{n}(-1)^j\binom{n}{j} \\ &= |G| + \sum_{j=1}^{k-1}(-1)^j \frac{n!}{j!(n-k)!} + \sum_{j=k}^{n}(-1)^j\binom{n}{j}.\end{aligned}$$

The result follows when we divide by $|G|$. ■

We will make further use of the special cases of Theorem 2.3 where k is $2, 3, n-2$, or n. The case where $k = 1$ and G acts regularly on X, seen in Example 2.2, could also be obtained as a corollary of Theorem 2.3.

Corollary 2.4. *If G acts sharply 2-transitively on a set X with n elements, then $f(G) = \frac{1}{n}$.*

Proof. With $k = 2$, the first sum in the conclusion of Theorem 2.3 vanishes. We apply the binomial theorem to $(1-1)^n$ to rewrite the second sum as $\frac{1}{|G|}(-1+n)$. Since $|G| = n(n-1)$ for a sharply 2-transitive group, the result follows. ■

The proof of Corollary 2.5 is similar and we omit it.

Corollary 2.5. *If G acts sharply 3-transitively on a set X with n elements, then $f(G) = \frac{1}{2} - \frac{1}{2n}$.* ■

Corollary 2.6. *Assume $n \geq 3$. Then*

$$f(S_n) = \sum_{j=0}^{n}\frac{(-1)^j}{j!} \text{ for the symmetric group } S_n, \text{ and}$$

$$f(A_n) = \sum_{j=0}^{n-2}\frac{(-1)^j}{j!} + \frac{(-1)^{n-1}2(n-1)}{n!} \text{ for the alternating group } A_n. \blacksquare$$

¿From Corollary 2.6, $f(S_n) - f(A_n) = (-1)^n\frac{n-1}{n!}$ so that $f(S_n) < f(A_n)$ if n is odd, and $f(A_n) < f(S_n)$ if n is even. It is also clear that both $f(S_n)$ and $f(A_n)$ closely approximate e^{-1} except for very small values of n.

Example 2.7. Suppose that q is a prime power and write $GF(q)$ for the field having q elements. We will use F_q to denote the 1-dimensional affine general linear group over $GF(q)$. That is, F_q acts on $GF(q)$ as the group of functions $x \mapsto ax + b$ where $a, b \in GF(q), a \neq 0$. The groups F_q are sharply 2-transitive Frobenius groups. It follows from Corollary 2.4 that $f(F_q) = \frac{1}{q}$.

Lemma 2.8. *If q is an odd prime power, then $f(PSL(2,q)) = \frac{q-1}{2(q+1)}$. If q is a power of 2, then $f(PSL(2,q)) = \frac{q}{2(q+1)}$.*

Proof. We prove the result when q is odd. The proof when q is even is similar.

With q odd, the order of $PSL(2,q)$ is $\frac{1}{2}q(q-1)(q+1)$. Since $PSL(2,q)$ is 2-transitive of degree $q+1$, the order of $Stab(x_1)$ is $\frac{1}{2}q(q-1)$ and the order of $Stab(x_1,x_2)$ is $\frac{1}{2}(q-1)$. By the Fundamental Theorem of Projective Geometry, no nontrivial element of $PSL(2,q)$ can fix three or more points, so $|Stab(Y)|=1$ if Y is a subset of X with 3 or more elements. We use the inclusion-exclusion principle to write $|A|$

$$= |PSL(2,q)| - \binom{q+1}{1}|Stab(x_1)| + \binom{q+1}{2}|Stab(x_1,x_2)| + \sum_{j=3}^{q+1}(-1)^j\binom{q+1}{j}$$

$$= \frac{1}{2}q(q+1)(q-1) - (q+1)\frac{q(q-1)}{2} + \frac{(q+1)q}{2}\frac{q-1}{2} + \sum_{j=3}^{q+1}(-1)^j\binom{q+1}{j}$$

We use the binomial theorem on $(1-1)^{q+1}$ to rewrite the final summand as $-\frac{q(q-1)}{2}$ and divide by $|PSL(2,q)|$ to obtain the result. ■

In the following table we list the lowest f-values for primitive groups having degree at most 50. The table was constructed using the CAYLEY library of primitive groups. We omit from the table degrees which are a power of a prime, since the lowest f-values in degrees which are a prime power are described in Theorem 3.1 and the remarks following it. We also omit those degrees n for which the group with minimal f-value is S_n (n odd) or A_n (n even).

We use $P^n(q)$ to denote the projective n dimensional space over the field of q elements. If q is a power of the prime p, then $PZL(n,q)$ denotes the semidirect product of $PSL(n,q)$ with $\mathrm{Gal}(GF(q)/GF(p))$.

Degree	Minimal f-value	Primitive group
6	$\frac{1}{3}(.3333)$	$PSL(2,5)$ on $P^1(5)$
10	$\frac{13}{40}(.325)$	S_6 on the cosets of an F_9
15	$\frac{13}{45}$ (.2889)	$PSL(4,2)$ on $P^3(2)$
21	$\frac{2}{7}$ (.2857)	$PSL(3,4)$ on $P^2(4)$
28	$\frac{1}{7}$ (.1429)	$PZL(2,8)$ on cosets of $N_G(Sylow(G,3))$
33	$\frac{4}{11}$ (.3636)	$PZL(2,32)$ on $P^1(32)$
36	$\frac{3355}{10368}$ (.3236)	$PSp(6,2)$ on the cosets of an S_8
40	$\frac{201}{640}$ (.3141)	$PGL(4,3)$ on $P^3(3)$
45	$\frac{14}{45}(.3111)$	Mathieu group M_{10} on cosets of a Sylow-2-subgroup

3. Some Lower Bounds

We begin this section with a simple proof of Cohen's result mentioned in the introduction.

Theorem 3.1. *Suppose G acts transitively and $n>1$. Then $f(G)\geq\frac{1}{n}$. Equality holds if and only if G acts sharply 2-transitively on X.*

Proof. Recall equation (1) $|G| = \sum_{g\in G} Ch_G(g)$.

For any $x \in X$, we have equation

$$\frac{k|G|}{n} = k|Stab(x)| = \sum_{g \in Stab(x)} Ch_{Stab(x)}(g) \quad (2)$$

where k is the number of orbits of $Stab(x)$ on $X - \{x\}$.

Subtracting equation (2) from equation (1) and separating G into the three subsets A, $Stab(x)$, and the remainder:

$$|G| - \frac{k|G|}{n} = \sum_{g \in A} Ch_G(g) + \sum_{g \in G - A - Stab(x)} Ch_G(g) + \sum_{g \in Stab(x)} 1 \geq \sum_{g \in G - A} 1 = |G| - |A|.$$

So $\frac{|A|}{|G|} \geq \frac{k}{n} \geq \frac{1}{n}$.

If there is equality, then first $k = 1$ and so G is 2-transitive. Second, if $g \in G$ has $Ch_G(g) \geq 2$, then $g \in Stab(x)$. However, x is arbitrary and so $g = 1$, implying that G is sharply 2-transitive.

The converse was already proven in Corollary 2.4. ■

The lower bound $\frac{1}{n}$ for $f(G)$ is achieved only in degrees which are a prime power. By [10, Chapter 9], the sharply 2-transitive groups have degree the power of a prime. The groups F_q of Example 2.7 show that this lower bound is always achieved in degrees which are a power of a prime.

Theorem 3.2. *If p is a prime number $\neq 3, 5$ such that $2p$ is not of the form $r^m + 1$ with r prime and $m > 1$, then the group G of degree $2p$ with smallest $f(G)$ is A_{2p}.*

Proof. Note first of all that since $2p$ is even, $f(A_{2p}) < f(S_{2p})$ and $f(A_{2p})$ is just a little less than e^{-1}. Consider now the imprimitive groups G of degree $2p$. Then G either has 2 blocks each of length p or p blocks each of length 2.

In the first case, G has a cyclic quotient of order 2 and half the elements of G swap the blocks. These elements are in A and so $f(G) \geq \frac{1}{2}$.

In the second case, if i and j belong to the same block, then $Stab(i) = Stab(j)$. Thus $\cup Stab(i)$ is a union of p subgroups each of order $|G|/2p$, so $A = G - \cup Stab(i)$ has order at least $|G|/2$, whence $f(G) \geq \frac{1}{2}$.

Next consider the primitive groups G of degree $2p$. From the classification of finite simple groups, it is known [8] that if G is not 2-transitive, then $p = 5$ and $G = A_5$ or S_5. Thus G is 2-transitive.

The 2-transitive groups have been classified. Excluding the alternating and symmetric groups, they occur in families of degree

$$r^m, \quad \frac{r^m - 1}{r - 1}(m > 1), \quad 2^{2m-1} \pm 2^{m-1}(m > 2), \quad r^3 + 1, \quad 2^{2(2m+1)} + 1,$$

together with isolated examples of degree $11, 12, 15, 22, 23, 24, 176, 276$, where r is a prime power and m a positive integer. The only degrees in this list that can have the form $2p$ are $4, 22$, and $r + 1$. We already know that $F_4 = A_4$ has minimal f-value for degree 4 groups. The only groups of degree 22 to be considered are M_{22} and Aut M_{22}, that have f-values 0.3902 and 0.3904 respectively and so do not beat out A_{22}.

As for degree $r + 1$, if r is prime, then the only groups to be considered are $PSL(2, r)$ and $PGL(2, r)$. These have f-values $\frac{(r-1)}{2(r+1)}$ and $\frac{r}{2(r+1)}$ by Lemma 2.8

and Corollary 2.5 respectively. Excluding the cases $p = 2, 3$, $(r = 3, 5)$, these are always greater than e^{-1}. ■

There is a group $G = PZL(2, 81)$ of degree 82 containing $PSL(2, 81)$ with index 4 such that $f(G) \approx 0.3470$. This shows that the theorem does not extend to cases where $2p = r^4 + 1$ (r prime). It seems likely that it will extend to cases where $2p = r^2 + 1$ (r prime).

If we consider only primitive permutation groups, then we have the following suggestive result.

Theorem 3.3. *For a set of positive integers n of density 1, the minimum $f(G)$ for G a primitive permutation group of degree n is greater than $e^{-1} - \frac{1}{(n-1)!}$.*

Proof. By [5], for a set of n of density 1, the only primitive groups of degree n are S_n and A_n.

By Corollary 2.6, $f(S_n) = e^{-1} + \frac{(-1)^n}{(n+1)!}(1 - \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} - ...)$ and $f(A_n) = e^{-1} + \frac{(-1)^{n-1}}{(n-1)!}(1 - \frac{1}{n} - \frac{1}{n(n+1)} + \frac{1}{n(n+1)(n+2)} - ...)$, both of which exceed $e^{-1} - \frac{1}{(n-1)!}$. ■

We can obtain nice bounds for at least one other kind of transitive group immediately.

Theorem 3.4. *If G is a nilpotent transitive permutation group, then $f(G) \geq \frac{1}{2}$.*

Proof. Since G is transitive, its stabilizers are all conjugate. Call one of them H. Then $A = G - \cup_{x \in G} H^x$. Pick a maximal subgroup M with $H \leq M$. Since G is nilpotent, M is normal and so $\cup H^x \subseteq M$, whence $G - M \subseteq A$. Since $[G : M] \geq 2, |A|/|G| \geq \frac{1}{2}$. ■

Note that if G is a transitive p-group, then similarly $f(G) \geq \frac{p-1}{p}$. See Section 7 for more comments on how $f(G)$ is restricted if G is nilpotent.

4. Density of transitive groups

The wreath product of two groups turns out to be an important tool in further examination of $f(G)$ for transitive G. We note that the wreath product of transitive groups is transitive and we calculate its f-value in Theorem 4.3. (See [9, p.32] for a definition of the usual action of the wreath product.)

Definition. If G is any permutation group, let $m_i(G) = |\{g \in G \mid Ch(g) = i\}|$, denoted m_i if G is understood. Define the polynomial

$$p_G(t) = \frac{1}{|G|} \sum_{i=0}^{deg(G)} m_i t^i$$

Example 4.1. If G is any group of order n with its regular representation (so acting on a set of n letters), then the identity fixes all letters, while the remaining $n - 1$ elements fix nothing. Hence $p_G(t) = \frac{1}{n}(t^n + (n - 1))$.

Example 4.2. If $G = D_4$, the dihedral group of order 8, with its usual action on 4 letters, then the identity fixes all letters, two elements fix two letters and the remainder fix nothing. Thus $p_G(t) = \frac{1}{8}(t^4 + 2t^2 + 5)$.

Theorem 4.3. $f(H \wr K) = p_K(f(H))$.

Proof. Write a typical element of $G = H \wr K$ as $g = (h_1, h_2, ...h_n, k)$, so that K has degree n. We note that $g \in A(G) \iff h_i \in A(H)$ for every i fixed by k. Thus $|A(G)| = m_0(K)|H|^n + m_1(K)|A(H)||H|^{n-1} + ... + m_n(K)|A(H)|^n$, where $m_i(K)$ is the number of elements of K fixing exactly i letters. Dividing by $|G| = |H|^n|K|$ yields the result. ■

Example 4.4. For the Frobenius groups F_q of Example 2.7, there are $q-1$ elements of the form $x \mapsto x + b$ with $b \neq 0$, which have no fixed points. For an element $a \neq 1, a \neq 0$ of $GF(q)$, the mapping $x \mapsto ax + b$ fixes only the element $\frac{b}{1-a}$ of $GF(q)$. There are $q(q-2)$ of these. The only remaining element is the identity. It follows that the polynomial p for F_q is given by $p(t) = \frac{1}{q(q-1)}(q-1+q(q-2)t+t^q)$.

Example 4.5. The group of degree n giving minimal f-value need not be primitive. The wreath product allows us to conveniently constuct examples to illustrate this. In degree 35, we have found from the CAYLEY library files of primitive groups, that the lowest f-value for a primitive group of degree 35 is approximately e^{-1} for the symmetric group S_{35}. By the preceding theorem we can calculate that $f(F_7 \wr F_5) \approx 0.3071$, where, for q a prime power, F_q is the sharply 2-transitive group of degree q defined in Example 2.7. $F_7 \wr F_5$ is imprimitive.

The basic properties of the polynomial are as follows.

Theorem 4.6. *(1) $p_G(t)$ has degree $n = deg(G)$, and its coefficients are rational, with denominators dividing $|G|$.*

(2) $p_G(t)$ and its first $n-1$ derivatives are strictly increasing functions of t for $t \geq 0$.

(3) $p_G(0) = f(G), p_G(1) = 1$, and for any $x \in X$, $p'_G(1)$ is the number of orbits of $Stab(x)$ on $X - \{x\}$.

(4) If G is transitive and $H = Stab(x)$, acting on $X - \{x\}$, then $p_H(t) = p'_G(t)$.

(5) The action of G on X is k-transitive if and only if $p_G^{(k)}(1) = 1$.

(6) If H acts on X and K acts on Y then taking the usual action of $H \times K$ on $X \coprod Y$ yields $p_{H\times K}(t) = p_H(t)p_K(t)$.

(7) If we instead let $H \times K$ act on $X \times Y, p_{H\times K}(t) = p_H(t) * p_K(t)$, where the operation $*$ is defined by $(\sum a_i t^i) * (\sum b_j t^j) = \sum a_i b_j t^{ij}$.

(8) $p_{H\wr K}(t) = p_K(p_H(t))$.

Proof. (1) is immediate from the definition. Note that only the identity fixes n or $n-1$ letters.

(2) $p_G(t)$ has nonnegative coefficients, and so its first $n-1$ derivatives are sums of strictly increasing functions for t positive.

(3) follows from (respectively) the definition of f and the formulae $\sum_{g\in G} 1 = |G|$ and $\sum_{g\in G} Ch(g) = k|G|$ where k is the number of orbits of G.

(4) $g \in H$ fixes exactly $i-1$ letters in $X-\{x\}$ if and only if g fixes exactly i letters in X, one of which is x. Hence $p'_G(t) = \frac{1}{|G|}(nt^{n-1} + ... + rm_r(G)t^r + ... + m_1(G))$

$= \frac{n}{|G|}(t^{n-1} + ... + m_{r-1}(H)t^{r-1} + ... + m_0(H))$

$= p_H(t)$ since, if G is transitive, $|G| = n|H|$.

(5) For $1 \leq j \leq n$, let $X^{[j]}$ be the set of j-tuples from X with all coordinates distinct. Then G acts naturally on $X^{[j]}$ coordinate-wise and it is easy to see that the action of G on X is k-tranisitive if and only if the action of G on $X^{[k]}$ is transitive.

Note that the degree of $(G, X^{[k]})$ as a permutation group is $N = \frac{n!}{(n-k)!}$. For the action of G on X, let $p(t) = \sum_{i=0}^{n} m_i t^i$ be the corresponding polynomial, and for the action of G on $X^{[k]}$, write $\tilde{p}(t) = \sum_{j=0}^{N} \widetilde{m}_j t^j$.

Suppose $g \in G$ fixes exactly i symbols of X. Then g fixes $i(i-1)\dots(i-(k-1))$ symbols of $X^{[k]}$. It will be useful to write this number as

$$\begin{cases} 0 & \text{if } i < k \\ \dfrac{i!}{(i-k)!} & \text{otherwise} \end{cases}$$

So $\widetilde{m}_j = \sum m_i$, where the sum is over all those i such that $i(i-1)\dots(i-(k-1)) = j$. Then $\widetilde{m}_0 = m_0 + \dots m_{k-1}$ and for all other $j, \widetilde{m}_j = m_i$ for a unique i or $\widetilde{m}_j = 0$.

Then $\tilde{p}'(1) = \sum_{j=1}^{N} j\widetilde{m}_j = \sum_{i=k}^{n} \frac{i!}{(i-k)!} m_i = p^{(k)}(1)$. Hence, $p^{(k)}(1) = 1 \Leftrightarrow \tilde{p}'(1) = 1 \Leftrightarrow G$ is transitive on $X^{[k]} \Leftrightarrow G$ is k-transitive on X.

(6) $(h, k) \in H \times K$ fixes exactly i letters in $X \coprod Y$ if and only if h fixes exactly j letters in X and k fixes exactly $i - j$ letters in Y for some j. Summing over $0 \le j \le i$, $m_i(H \times K) = \sum_j m_j(H) m_{i-j}(K)$. But this is exactly what happens to polynomial coefficients when they are multiplied.

(7) With this action, $Ch_{H\times K}(h, k) = Ch_H(h) Ch_K(k)$ for $h \in H, k \in K$. The result follows since we can also write $p_G(t) = \frac{1}{|G|}(\sum_{g\in G} t^{Ch(g)})$.

(8) Note that $(G \wr H) \wr K \cong G \wr (H \wr K)$. Thus $p_{H\wr K}(f(G)) = f((G \wr H) \wr K) = p_K(f(G \wr H)) = p_K(p_H(f(G)))$. The result follows by noting that there are infinitely many values of $f(G)$–so the two polynomials being compared, $p_{H\wr K}$ and $p_H(p_K)$, must be the same. ■

Theorem 4.6 allows new proofs of the following two known results.

Notation. Let $k(G)$ denote the number of orbits of G.

Corollary 4.7. *If H acts on X, K on Y, then, taking the usual action of $H \times K$ on $X \coprod Y$, we have $k(H \times K) = k(H) + k(K)$.*

Proof. $k(H \times K) = p'_{H\times K}(1) = (p_H p_K)'(1) = p'_H(1)p_K(1) + p'_K(1)p_H(1)$ (by the product rule) $= k(H) + k(K)$. ■

Corollary 4.8. $k(H \wr K) = k(H)k(K)$.

Proof. $k(H \wr K) = p'_{H\wr K}(1) = (p_K \circ p_H)'(1) = p'_K(p_H(1))p'_H(1) = p'_K(1) \cdot p'_H(1) = k(H)k(K)$■

Example 4.9. The polynomial defined above can easily be computed for groups which act sharply k-transitively. If (G, X) is a permutation group of degree n which acts sharply k-transitively and $x \in X$, then $H = Stab_G(x)$ acts sharply $(k-1)$-transitively on the set $X - \{x\}$. For $j < k$, the pointwise stabilizer of j letters of X, denoted $Stab_G(x_1, \dots, x_j)$, acts sharply $(k-j)$-transitively on the remaining $n - j$ letters of X.

Let (G, X) be a sharply k-transitive permutation group with corresponding polynomial

$$p_G(t) = \frac{1}{|G|} \sum_{i=0}^{n} m_i t^i.$$

Then

$$m_0 = |\{g \in G : Ch(g) = 0\}| = |A(G)|$$
$$m_1 = |\{g \in G : Ch(g) = 1\}| = n|\{h \in Stab_G(x) : Ch(h) = 0\}| = n|A(Stab_G(x))|$$

and in general for $j < k$,

$$m_j = \binom{n}{j}|\{h \in Stab_G(x_1, \ldots, x_j) : Ch(h) = 0\}| = \binom{n}{j}|A(Stab_G(x_1, \ldots, x_j))|$$

Further, since no nonidentity element of a sharply k-transitive group can fix k or more letters, $m_i = 0$ for $k \leq i \leq n-1$ and $m_n = 1$.

Remarks. A natural question to ask is how "forgetful" p_G is: If H and K have the same polynomial, what other properties do they have in common? They need not be isomorphic as groups, since if H and K are any two groups of order n embedded in S_n by their regular representations, then they both have polynomial $\frac{1}{n}(t^n + n - 1)$. However, by Theorem 4.6(1), they must have the same degree and order and by Theorem 4.6(3), the same f-value. Also by Theorem 4.6(3), if one is transitive, then the other must be. A question that we have not answered is: If one is primitive, must the other be also?

Example 4.10. Of basic importance in the theory of transitive groups is the question of transitive extensions, i.e., given a permutation group (H, X) of degree n, does there exist a permutation group $(G, X \cup \{x\})$ of degree $n+1$ such that $Stab_G(x) = H$ with its given action on X? In terms of polynomials, this translates into a question involving integration.

For example, let us show that there is no transitive extension of the dihedral group H of order 8 acting on 4 letters. Suppose, for the sake of contradiction, that G is one such. Then $p'_G(t) = p_H(t)$ and $p_G(1) = 1$ together imply that $p_G(t) = \frac{t^5}{40} + \frac{t^3}{12} + \frac{5t}{8} + \frac{4}{15}$. The order of G must be 40 and so $40p_G(t) \in \mathbf{Z}[t]$, which patently does not hold.

For the rest of this section, $G = (G, X)$ will denote a transitive permutation group of degree n.

Lemma 4.11. *If $t \in [0, 1)$, then $p_G(t) > t$.*

Proof. The derivative of $p_G(t) - t$ is $p_{Stab(x)}(t) - 1 < 0$. Thus $p_G(t) - t$ is strictly decreasing in $[0, 1)$. Evaluated at $t = 1$, it is 0. ■

Lemma 4.12. *Define $G_1 = G$ and $G_k = G_{k-1} \wr G$. Then as $k \to \infty$, $f(G_k) \to 1$.*

Proof. Let $f(G_k) = c_k$. Then $c_k = p_G(c_{k-1})$. By Lemma 4.11, the sequence (c_k) is increasing and bounded above. It therefore must approach a limit, which is a solution of $p_G(t) = t$. Again, by Lemma 4.11 and Theorem 4.6(2), the only solution is $t = 1$. ■

Theorem 4.13. *The set $\{f(G) \mid G$ is transitive$\}$ is dense in [0,1].*

Proof. Given $\epsilon > 0$, by Corollary 2.4 there exists a transitive G such that $f(G) < \epsilon$. With the notation of Lemma 4.12, for $k \geq 2$ (setting $c_0 = 0$) $c_k - c_{k-1} = p_G(c_{k-1}) - p_G(c_{k-2}) = p'_G(\zeta)(c_{k-1} - c_{k-2})$ for some $\zeta \in [0, 1)$, by the Mean Value Theorem. Since $p'_G(\zeta) = p_{Stab(x)}(\zeta) < 1$, we have, by induction, on k $c_k - c_{k-1} < \epsilon$. Thus the set of $f(G)$ is ϵ-dense. ■

Remark. The proof of this theorem actually gives that the set of f-values of transitive imprimitive groups is dense in [0,1]. Compare with Theorem 5.11.

5. Density of primitive groups

In Section 4, we used the action of the wreath product $H \wr K$ on $X \times Y$ to show that $\{f(G) \mid G \text{ is transitive}\}$ is dense in $[0,1]$. With only trivial exceptions, $H \wr K$ acts imprimitively on $X \times Y$. In this section, we use methods analogous to those in Section 4 to show that $\{f(G) \mid G \text{ is primitive}\}$ is also dense in $[0,1]$.

The wreath product $H \wr K$ has a natural action on X^Y given by $(x_y)\cdot(h_y;k^{-1}) = (x_{y\cdot k}\cdot h_y)$. This action provides us with a rich collection of examples of primitive permutation groups: we will make use of the following known result [7].

Lemma 5.1. *Suppose that (H,X) is a primitive permutation group which is not just a cyclic group of prime order acting regularly on its elements, and that (K,Y) is any transitive permutation group. Then $H \wr K$ acts primitively on X^Y.* ■

A second useful tool will be a polynomial q_K, analogous to the polynomial p_K of Section 4, for which $f(H \wr K, X^Y) = q_K(f(H))$.

For notational convenience, we will write n for the degree of K, $(\mathbf{h};k)$ for an element $((h_y);k)$ of $H \wr K$ and $\mathbf{x}$ for an element (x_y) of X^Y. For $1 \le j \le n$, define $\lambda_j = \lambda(K,Y,j) = card\{k \in K \mid k \text{ is a product of } j \text{ disjoint cycles on } Y, \text{ including cycles of length } 1\}$. Define the polynomial $r = r_K$ by $r(t) = \frac{1}{|K|}\sum_{j=1}^{n}\lambda_j t^j$ and define the polynomial $q = q_K$ by $q(t) = 1 - r(1-t)$.

Example 5.2. For the symmetric group S_3 acting on $\{1,2,3\}$, we have $\lambda_1 = 2,\ \lambda_2 = 3,\ \lambda_3 = 1,\ r(t) = \frac{1}{6}(2t + 3t^2 + t^3)$ and $q(t) = \frac{1}{6}(11t - 6t^2 + t^3)$.

Example 5.3. For the regular action of the cyclic group C_6, it is easy to see that $\lambda_1 = \lambda_2 = 2,\ \lambda_3 = \lambda_6 = 1,\ \lambda_4 = \lambda_5 = 0,\ r(t) = \frac{1}{6}(2t + 2t^2 + t^3 + t^6)$ and $q(t) = \frac{1}{6}(15t - 20t^2 + 21t^3 - 15t^4 + 6t^5 - t^6)$.

Theorem 5.4.

(1) $|A(H \wr K, X^Y)| = |H \wr K| - \sum_{j=1}^{n}\lambda_j(|H| - |A(H,X)|)^j|H|^{n-j}$.
(2) $f(H \wr K, X^Y) = 1 - r_K(1 - f(H)) = q_K(f(H))$.

Proof. Since $|H \wr K| = |H|^n|K|$, statement (2) follows immediately from (1).

For $k \in K$, let $B_k = \{(\mathbf{h};k) \in H \wr K \mid (\mathbf{h};k) \text{ fixes at least one element of } X^Y\}$. Then the sets B_k are clearly disjoint from each other and from $A(H \wr K, X^Y)$ and $H \wr K$ is the disjoint union $A(H \wr K, X^Y) \bigcup (\bigcup_{k\in K} B_k)$. It will suffice to show that $|B_k| = (|H| - |A(H,X)|)^j|H|^{n-j}$ if k is a product of j disjoint cycles on Y.

Suppose that $(\mathbf{h};k) \in B_k$ and that θ^{-1} (here θ^{-1} rather than θ for purely notational reasons) of length $l = l_\theta \ge 1$ is one of the j disjoint cycles of k on Y. Then there is an element $\mathbf{x}$ of X^Y which is fixed by $(\mathbf{h};k)$: thus, $x_{y\cdot k^{-1}}\cdot h_y = x_y$ for every $y \in Y$ and, in particular, $x_{y\cdot\theta}\cdot h_y = x_y$ for the l distinct values of y which occur in the cycle θ. Arbitrarily choose one value $u = u_\theta$ of y which does occur in θ. Then the set of values of Y which occur in θ (or in θ^{-1}) is precisely $\{u\cdot\theta^t \mid 0 \le t < l\}$. We have, for $0 \le t < l-1$, that $x_{u\cdot\theta^t} = x_{u\cdot\theta^{t+1}}\cdot h_{u\cdot\theta^t}$, and, with $t = l-1$, that $x_{u\cdot\theta^{l-1}} = x_{u\cdot\theta^l}\cdot h_{u\cdot\theta^{l-1}} = x_u\cdot h_{u\cdot\theta^{l-1}}$. It follows that

$$x_u = x_{u\cdot\theta}\cdot h_u = x_{u\cdot\theta^2}\cdot h_{u\cdot\theta}h_u = \cdots = x_u\cdot h_{u\cdot\theta^{l-1}}\ldots h_{u\cdot\theta}h_u.$$

Hence $\mathbf{h}$ must satisfy the constraint that for each cycle θ^{-1} of length l in k, there is a product $h_{u\cdot\theta^{l-1}}\ldots h_{u\cdot\theta}h_u$ of elements which is in $H - A_H$.

Conversely, suppose that we have k and j as above and that for each cycle θ^{-1} of k of length $l = l_\theta$, we have chosen some fixed element $u = u_\theta$ of Y which occurs in θ. For each θ, we choose elements $g_1, g_2, \ldots, g_{l-1}$ arbitrarily from H, and one element g_l restricted to $H - A_H$, but arbitrarily from that set. Let x_u be an element of X which is fixed by g_l and define elements $x_{u\cdot\theta^t} \in X$ by $x_{u\cdot\theta^t} = x_u \cdot g_t^{-1}$ for $1 \le t < l$. Having done this for every θ^{-1} in k, we have defined an element $\mathbf{x}$ of X^Y. Similarly, define elements $h_{u\cdot\theta^t} \in H$ by $h_u = g_1$ and $h_{u\cdot\theta^t} = g_{t+1}g_t^{-1}$ for $1 \le t < l$. Having done this for every θ, we have defined an element $(\mathbf{h}; k)$ of $H \wr K$. We wish to verify that $\mathbf{x} \cdot (\mathbf{h}; k) = \mathbf{x}$ and hence $(\mathbf{h}; k) \in B_k$. It will suffice to show that, for each cycle θ^{-1} of k and for each t with $0 \le t < l_\theta$, that $x_{u\cdot\theta^{t+1}} \cdot h_{u\cdot\theta^t} = x_{u\cdot\theta^t}$. For $t = 0$, $x_{u\cdot\theta} \cdot h_u = (x_u \cdot g_1^{-1})g_1 = x_u$. For $0 < t < l-1$, $x_{u\cdot\theta^{t+1}} \cdot h_{u\cdot\theta^t} = (x_u \cdot g_{t+1}^{-1})(g_{t+1}g_t^{-1}) = x_u \cdot g_t^{-1} = x_{u\cdot\theta^t}$. Finally, for $t = l-1$, $x_{u\cdot\theta^l} \cdot h_{u\cdot\theta^{l-1}} = x_{u\cdot\theta^l} \cdot (g_l g_{l-1}^{-1})$. Then observe that $u \cdot \theta^l = u$ and that x_u was chosen to be fixed by g_l, so that $x_{u\cdot\theta^l} \cdot h_{u\cdot\theta^{l-1}} = x_u \cdot g_{l-1}^{-1} = x_{u\cdot\theta^{l-1}}$.

It is easy to see that different choices for $\mathbf{g}$ will lead to different values for $\mathbf{h}$ and that given $(\mathbf{h}; k) \in B_k$, we can, for each θ, set $g_t = h_{u\cdot\theta^{t-1}} \ldots h_{u\cdot\theta} h_u$ and thus obtain $\mathbf{h}$ by the process above. ■

Corollary 5.5. *If $(H_1, X_1), (H_2, X_2)$ and (K, Y) are transitive permutation groups with $f(H_1, X_1) \le f(H_2, X_2)$ then $f(H_1 \wr K, X_1^Y) \le f(H_2 \wr K, X_2^Y)$.*

Proof. We need to show that q_K is an increasing function on $[0, 1]$. The function r_K is increasing on $[0, 1]$, hence is a decreasing function in $1 - t$ on $[0, 1]$. ■

We remark that $f(H \wr K, X^Y)$ is monotonic only in $f(H)$, not in $f(K)$. See Example 5.8 below.

In the next two lemmas, we need Euler's totient function ϕ, where $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

Lemma 5.6. *If (C_n, X) is the cyclic group of order n acting as a regular permutation group on its own elements, then $r(t) = \frac{1}{n}\sum_{d|n} \phi(\frac{n}{d})t^d$. As a special case, when n is a prime p, $r(t) = \frac{1}{p}(t^p + (p-1)t)$ and $q(t) = \frac{1}{p}(1 + (p-1)t - (1-t)^p)$.*

Proof. Write $X = \{1, 2, \ldots, n\}$ and $C_n = \langle a \mid a^n = 1\rangle$ where for $1 \le m \le n$ the action of a^m on X is given by

$$i \cdot a^m = \begin{cases} i + m & \text{if} \quad i \le n - m \\ i + m - n & \text{if} \quad i > n - m \end{cases}$$

Let $d = (m, n)$ and observe that a^m is a product of d disjoint cycles of length $\frac{n}{d}$, which correspond to the congruence classes modulo d. Thus λ_d is nonzero only when d is a divisor of n. When d divides n, $\lambda_d = |\{\ m \mid 1 \le m \le n,\ (m, n) = d\}| = |\{\ m = jd \mid 1 \le j \le \frac{n}{d},\ (j, \frac{n}{d}) = 1\}| = \phi(\frac{n}{d})$. ■

Lemma 5.7. *If $Q = p^m$, p a prime and F_Q is the Frobenius group of Example 2.7, then*

$$r(t) = \frac{1}{Q(Q-1)}\left[t^Q + (Q-1)t^{\frac{Q}{p}} + Q\sum_{\substack{1 \le j \le Q-2 \\ j \mid Q-1}} \phi(\frac{Q-1}{j})t^{j+1}\right].$$

Proof. For $a, b \in GF(Q)$, $a \neq 0$, define the transformation $\theta_{a,b}$ on $GF(Q)$ by $x\theta_{a,b} = ax + b$. Choose an element c of $GF(Q)$ which is a generator of the cyclic, multiplicative group $GF(Q)$. We note that F_Q has Frobenius kernel $M = \{\ \theta_{1,b}\}$ and that the cyclic group H generated by $\theta_{c,0}$ is a Frobenius complement of M. Since every nontrivial element of F_Q lies either in M or else in exactly one of the Q distinct conjugates of H in F_Q, we can complete the proof by adequately describing the permutation action of elements of M and of H.

We show that every nontrivial element of M is a product of $\frac{Q}{p} = p^{m-1}$ cycles of length p. Let $\theta_{1,b}$ be such a nontrivial element. Regard $GF(Q)$ as an m-dimensional vector space V over $GF(p)$ and choose a basis $\{v_1, v_2, \ldots, v_m\}$ for V with $v_1 = b$. If $m = 1$, it is clear that $\theta_{1,b}$ acts as the single cycle $(0, b, 2b, \ldots, (p-1)b)$ of length p. If $m > 1$, then each of the $\frac{Q}{p}$ elements of the form $x = \sum_{j=2}^{m} k_j v_j,\ k_j \in GF(Q)$ occurs in a different cycle $(x, x+b, \ldots, x+(p-1)b)$ of length p.

We consider elements of the cyclic group $H = \langle\theta_{c,0}\rangle$. All powers of $\theta_{c,0}$ fix 0. Arguing as in Lemma 5.6, H contains, for any divisor $j < Q-1$ of $Q-1$, $\phi(\frac{Q-1}{j})$ elements which are a product of j nontrivial cycles of length $\frac{Q-1}{j}$ and one cycle of length 1. ■

The expression for $r(t)$ in Lemma 5.7 is slightly misleading when $m = 2$, since the term t^p occurs in two places.

Example 5.8. For the Frobenius group F_5, we have that $q_{F_5}(t) = \frac{1}{20}(44t - 35t^2 + 15t^3 - 5t^4 + t^5)$, while for the cyclic group C_5, we have $q_{C_5}(t) = \frac{1}{5}(1 + 4t - (1-t)^5)$. It follows that $f(C_2 \wr F_5, 2^5) = q_{F_5}(\frac{1}{2}) = \frac{95}{128}$ while $f(C_2 \wr C_5, 2^5) = q_{C_5}(\frac{1}{2}) = \frac{76}{128}$. Note that this shows that it is possible to have $f(H \wr K_1) < f(H \wr K_2)$, even when $f(K_1) > f(K_2)$.

Lemma 5.9. *If (K, Y) is a nontrivial transitive permutation group and $t \in (0, 1)$, then $r_K(t) < t < q_K(t)$.*

Proof. For $t \in (0, 1)$, $\lambda_j t^j \leq \lambda_j t$ with equality only for $j = 1$. Since $\sum \lambda_j = |K|$, it follows that $t = \frac{1}{|K|}\sum \lambda_j t > \frac{1}{|K|}\sum \lambda_j t^j = r_K(t)$. Replace t by $1 - t$ to obtain $1 - t > r_K(1-t)$ and $t < 1 - r_K(1-t) = q_K(t)$. ■

Lemma 5.10. *Let (G_0, X_0) and (K, Y) be transitive permutation groups. Inductively define (G_{k+1}, X_{k+1}) to be $(G_k \wr K, (X_k)^Y)$. Then $\lim_{k\to\infty} f(G_k, X_k) = 1$.*

Proof. We use the same proof as in Lemma 4.11. ■

Theorem 5.11. *The set $\{f(G, X) \mid (G, X)$ is primitive$\}$ is dense in $[0, 1]$.*

Proof. Let $\epsilon > 0$ be given. We construct a sequence $\{(G_k, X_k)\}_{k\geq 0}$ of primitive permutation groups with $f(G_0, X_0) < \epsilon$, $f(G_{k+1}, X_{k+1}) - f(G_k, X_k) < \epsilon$ and $\lim_{k\to\infty} f(G_k, X_k) = 1$. Let Q be a prime power with $\frac{1}{Q} < \epsilon$ and let (G_0, X_0) be the Frobenius group $(F_Q, GF(Q))$. Then (G_0, X_0) is primitive and $f(G_0, X_0) < \epsilon$. Use l'Hôpital's Rule to verify that $\lim_{t\to\infty}(\frac{1}{t})^{\frac{1}{t-1}} = 1$. Choose a prime p sufficiently large that

$$1 - \left(\frac{1}{p}\right)^{\frac{1}{p-1}} < \frac{1}{Q} \text{ and } \frac{1}{p} < \epsilon$$

It can be shown that the second requirement is redundant. We define (G_k, X_k) inductively by $(G_{k+1}, X_{k+1}) = (G_k \wr C_p, (X_k)^p)$. Write q for q_{C_p} and c_k for $f(G_k, X_k)$.

By Theorem 5.4, $c_{k+1} = q(c_k)$. By Lemma 5.1, (G_k, X_k) is primitive for $k \geq 1$. By Lemma 5.10, $\lim_{k\to\infty} f(G_k, X_k) = 1$. We may assume that p is odd. By Lemma 5.6, $q(t) = \frac{1}{p}(1 + (p-1)t + (t-1)^p)$, hence $q\prime(t) = \frac{1}{p}(p - 1 + p(t-1)^{p-1})$. It is easy to see that $q\prime(t)$ is a strictly decreasing function on $[0, 1]$ and that $q\prime(t) = 1$ when $t = 1 - (\frac{1}{p})^{\frac{1}{p-1}}$. Our requirement on the choice of p above is to insure that $q\prime(t) < 1$ on $[\frac{1}{Q}, 1]$. We need to verify that $c_{k+1} - c_k < \epsilon$ for $k \geq 0$. As in Theorem 4.13, we use induction on k and the Mean Value Theorem. For $k = 0$, a routine calculation shows that $c_1 - c_0 = q(\frac{1}{Q}) - \frac{1}{Q} = \frac{1}{p}(1 - \frac{1}{Q})(1 - (1 - \frac{1}{Q})^{p-1}) < \frac{1}{p} < \epsilon$. For $k > 0$, we assume inductively that $c_k - c_{k-1} < \epsilon$ and apply the Mean Value Theorem to q on $[c_{k-1}, c_k]$ to obtain ξ_k in $[c_{k-1}, c_k]$ with $c_{k+1} - c_k = q(c_k) - q(c_{k-1}) = q\prime(\xi_k)(c_k - c_{k-1}) < c_k - c_{k-1} < \epsilon$. ■

Remark We have even shown that given any prime p the solvable primitive groups of degree a power of p have f-values dense in $[0, 1]$.

The remaining results in this section are peripheral; we won't make further use of them. We use $s(n, k)$ to denote the Stirling number of the first kind. We make use of well-known properties of $s(n, k)$ which can be found in standard texts on combinatorics [1].

Proposition 5.12. *For the symmetric group S_n acting on a set of n elements we have,*

(1)
$$r(t) = \frac{1}{n!}\sum_{j=1}^{n} |s(n, j)|t^j$$

(2)
$$r(t) = \frac{1}{n!}\prod_{j=0}^{n-1}(t + j)$$

(3)
$$q(t) = 1 - \frac{1}{n!}\prod_{j=1}^{n}(j - t) = 1 - \prod_{j=1}^{n}(1 - \frac{t}{j})$$

(4)
$$q(t) = \frac{(-1)^{n+1}}{n!}\sum_{j=1}^{n} s(n + 1, j + 1)t^j$$

Proof. (1) This is essentially an exercise [1,Chapter 2,Section 3,Exercise 18]. We need to show that $\lambda(S_n, j)$ satisfies the known recursion $|s(n, j)| = |s(n - 1, j - 1)| + (n-1)|s(n-1, j)|$. Observe that for an element α of S_{n-1}, which is a product of $j - 1$ cycles in S_{n-1}, we may regard α as a product of j cycles in S_n. For any element β of S_{n-1} which is a product of j cycles, we may obtain $n - 1$ elements of S_n by inserting n into β in $n - 1$ different positions.

(2) This follows from (1) and known properties of $|s(n, j)|$.

(3) This follows from (2) and the definition of q.

(4) We show that (4) follows from (3). Observe that

$$\prod_{j=1}^{n}(j-t) = (-1)^n \prod_{j=1}^{n}(t-j) = (-1)^n \frac{1}{t}\prod_{j=0}^{n}(t-j) =$$

$$(-1)^n \frac{1}{t}\sum_{k=1}^{n+1} s(n+1,k)t^k = (-1)^n \left[s(n+1,1) + \sum_{k=2}^{n+1} s(n+1,k)t^{k-1} \right] =$$

$$(-1)^n \left[(-1)^n n! + \sum_{j=1}^{n} s(n+1,j+1)t^j \right] = n! - (-1)^{n+1}\sum_{j=1}^{n} s(n+1,j+1)t^j \blacksquare$$

.

Proposition 5.13. *For the alternating group A_n acting transitively on a set of n elements,*

$$r(t) = \begin{cases} \displaystyle\sum_{j=1}^{m} s(n,2j)t^{2j} & \text{if } n = 2m \text{ is even} \\ \displaystyle\sum_{j=0}^{m} s(n,2j+1)t^{2j+1} & \text{if } n = 2m+1 \text{ is odd} \end{cases}$$

Moreover, if (K, Y) is a permutation group of degree n, then $K \subseteq A_n$ if and only if r_K is an even polynomial or an odd polynomial, according as n is even or odd.

Proof. We have a natural inclusion of A_n or of K in S_n as a permutation group. We assume that n is even: the case when n is odd is similar. It will suffice to show that an element θ of S_n is contained in A_n if and only if θ is a product of an even number of disjoint cycles. Suppose that θ is a product of j disjoint cycles of which a have even length and b have odd length. Write $\theta = \theta_1\theta_2$ where θ_1 is a product of a disjoint cycles of even length and θ_2 is a product of b cycles of odd length. Since every one of the n letters of Y is contained in some cycle and n is even, we must have that b is even. It follows that θ_2 is contained in A_n and that θ_1 and hence θ is contained in A_n if and only if a is even. ■

6. An Alternative Proof

In this section we give an alternative proof of Theorem 4.13 that the set $\{f(G) \mid G$ is transitive$\}$ is dense in $[0, 1]$.

Proof. Let $\epsilon > 0$ be given. Choose a prime or a prime power q such that $\frac{1}{q} < \epsilon$. Write G_i for the ith direct power of the Frobenius group F_q acting on the ith power of $GF(q)$; that is $G_i = ((F_q)^i, (GF(q))^i)$. It follows from Lemma 6.2 below that $f(G_i) = 1 - (1 - \frac{1}{q})^i$. It is clear that $f(G_1) = \frac{1}{q} < \epsilon$ and that $\lim_{i\to\infty} f(G_i) = 1$. We need only show that $f(G_{i+1}) - f(G_i) < \epsilon$ for every i. This is easy since $f(G_{i+1}) - f(G_i) = (1 - (1 - \frac{1}{q})^{i+1}) - (1 - (1 - \frac{1}{q})^i) = \frac{1}{q}(1 - \frac{1}{q})^i < \frac{1}{q} < \epsilon$. ■

Remark The groups G_i are solvable and have degree a prime power q^i.

Lemma 6.1. *If H acts on X and K acts on Y, then for the action $(x,y)(h,k) = (xh, yk)$ of $H \times K$ on $X \times Y$,*

$$1 - f(H \times K, X \times Y) = (1 - f(H,X))(1 - f(K,Y))$$

Proof. An element (x,y) of $X \times Y$ is fixed by (h,k) in $H \times K$ if and only if h fixes x and k fixes y. ■

Lemma 6.2. *If H acts on X, then $f(H^m, X^m) = 1 - (1 - f(H,X))^m$ for the coordinate-wise action of H^m on X^m.*

Proof. This follows from Lemma 6.1 by induction on m. ■

Lemma 6.3. *If H is transitive on X and K is transitive on Y, then $H \times K$ is transitive on $X \times Y$ and H^m is transitive on X^m.*

Proof. Given (x_1, y_1) and (x_2, y_2) in $X \times Y$, there is an $h \in H$ with $x_1 h = x_2$ and a $k \in K$ with $y_1 k = y_2$. Then $(x_1, y_1)(h,k) = (x_2, y_2)$. The second statement follows by induction. ■

7. Conclusion

There are still many interesting questions that remain to be answered. Some of them are:

1. Do $p_K(t)$ and $q_K(t)$ determine primitivity of the group K?

2. What is the lower bound for $\{f(G) \mid G$ simple$\}$?
There is empirical evidence to suggest that the bound is $\frac{2}{7}$. If so, the bound is sharp, for it is achieved by both $PSL(3,2)$ of degree 7 and $PSL(3,4)$ of degree 21.

3. Is there a limiting value for $f(PSL(n,2))$ as $n \to \infty$?
Examples suggest that the limit would be $\prod_{n=1}^{\infty}(1 - \frac{1}{2^n})$, or approximately .288788. Computations in CAYLEY show that for $2 \le n \le 6$,

$$f(PSL(n,2)) = \sum_{j=0}^{n}(-1)^j \frac{1}{\prod_{i=1}^{j}(2^i - 1)}$$

We suspect that the obvious replacement of 2 by a prime power q calculates $f(GL(n,q))$ rather than $f(PSL(n,q))$.

4. Define
$$c_n = min\{f(G) \mid G \text{ of degree } n\}$$
$$p_n = min\{f(G) \mid G \text{ primitive of degree } n\}.$$
Are there better bounds for c_n and p_n? What forms do the minimal groups have?

5. What are the accumulation points of $\{f(G) \mid G$ is nilpotent$\}$?
Extending the method of Theorem 3.4, one shows that if G is a nilpotent transitive group and $f(G) > \frac{1}{2}$, then $f(G) \ge \frac{5}{8}$. Thus $\frac{1}{2}$ is isolated. The results of [4] produce sequences of p-groups with accumulation points $\frac{p}{p+1}$.

6. For a given n, is there a limit of $f(PSL(n,q))$ as $q \to \infty$?

We have seen in Lemma 2.8 that $f(PSL(2,q)) \to \frac{1}{2}$ as $q \to \infty$ and we have numerical evidence that $f(PSL(3,q)) \to \frac{1}{3}$ as $q \to \infty$, but the obvious conjecture seems to be false for $n \geq 4$.

7. What constraints must be satisfied by the coefficients m_i of p_G for a transitive group G?

We have the following constraint (note that $f(G) = \frac{m_0}{|G|}$ and $f(H) = \frac{m_1 n}{|G|}$).

Proposition 7.1. *Let G be transitive with one-point stabilizer H. Then $2f(G) + f(H) \geq 1$.*

Proof. $f(G) = \int_0^1 (1 - p_H(t))dt$. The function $1 - p_H(t)$ is strictly decreasing and convex in $[0,1]$, so the integral is at least the area of the right-angled triangle with sides of length $1 - f(H)$ and 1. ■

8. Is every rational number in $(0,1)$ equal to $f(G)$ for some transitive (primitive) group G ?

In the transitive case, by Lemma 6.1, it is enough to show that the semigroup generated by $\{\frac{q-d}{q} \mid q \text{ is a prime power } , d \mid q-1 \}$ consists of all rational numbers in $(0,1)$. Alternatively, also by Lemma 6.1, it is enough to show that , for all n, $\frac{1}{n}$ is the f-value of a transitive group or to show that, whenever b is a prime power, $\frac{a}{b}$ is the f-value of a transitive group.

Acknowledgements

This paper was begun in a class on the computational software package CAYLEY led by the first author. The authors wish to thank Matthew Pestle and Elliot Weinberg for their contributions to the class. The first author was partially supported by NSF grant DMS 90-14522. He thanks God for leading him to results.

References

1. Kenneth P. Bogart, *Introductory Combinatorics*, Pitman Publishing Inc., Marshfield, Massachusetts, 1983.
2. J.P. Buhler, H.W. Lenstra, Jr., and Carl Pomerance, *Factoring integers with the number field sieve*, in preparation.
3. P.J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.
4. Peter J. Cameron, L.G. Kovács, M.F. Newman and Cheryl E. Praeger, *Fixed-point-free permutations in transitive permutation groups of prime-power order*, Quart. J. Math. Oxford (2) **36** (1985), 273–278.
5. P.J. Cameron, P.M. Neumann, and D.N. Teague, *On the degrees of primitive permutation groups*, Math. Zeit. **180** (1982), 141–149.
6. J.J. Cannon, *An introduction to the group theory language Cayley*, in Computational Group Theory (M.D.Atkinson, ed.), (Proceedings of the LMS Symposium on Computational Group Theory, Durham, July 30 – August 9, 1982), Academic Press, London, 1984, pp. 143–182.
7. Lev Arkadjevič Kalužnin, Platon Michajlovič Beleckij, and Valerij Zalmanovič Fejnberg, *Kranzprodukte*, Teubner-Texte zur Mathematik, Band 101, Leipzig, 1987.
8. Martin W. Liebeck and Jan Saxl, *Primitive permutation groups containing an element of large prime order*, J.London Math. Soc. (2) **31** (1985), 237–249.
9. D.J.S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, 1982.
10. Joseph J. Rotman, *The Theory of Groups, An Introduction*, 3rd ed, Allyn and Bacon, Inc., Boston, 1984.
11. W. R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs N. J., reprinted by Dover Publications, Inc., Mineola, N.Y., (1987).