Fixed point polynomials of permutation groups

C. M. Harden D. B. Penman

Department of Mathematical Sciences
University of Essex
United Kingdom

cmhard@essex.ac.uk dbpenman@essex.ac.uk

Submitted: Dec 7, 2012; Accepted: Apr 30, 2013; Published: May 9, 2013
Mathematics Subject Classifications: 20B99

Abstract

In this paper we study, given a group G of permutations of a finite set, the so-called fixed point polynomial $\sum_{i=0}^{n} f_i x^i$, where f_i is the number of permutations in G which have exactly i fixed points. In particular, we investigate how root location relates to properties of the permutation group. We show that for a large family of such groups most roots are close to the unit circle and roughly uniformly distributed round it. We prove that many families of such polynomials have few real roots. We show that many of these polynomials are irreducible when the group acts transitively. We close by indicating some future directions of this research.

Keywords: group theory, finite permutation groups

1 Introduction and definition

In this paper we introduce the fixed-point polynomial of a permutation group, calculate it for various well-known families of groups, and give some results about irreducibility and the location of roots for such polynomials. One motivation will be the recent study of the chromatic polynomials of graphs and the links between their roots and the properties of the associated graphs—see e.g. [21, 29, 1]—though our results will be of different character.

Definition 1.1. *Let G be a group of permutations of a finite set Ω of order n, and f_i be the number of elements of G which fix* exactly *i points. The fixed-point polynomial, $P_{G,\Omega}$, is defined to be the polynomial $\sum_{i=0}^{n} f_i x^i$.*

Sometimes Ω is clear and in such cases we may just write P_G instead of $P_{G,\Omega}$. This polynomial was (effectively) introduced in [7]: the $p_G(t)$ in Section 4 there is $\frac{1}{|G|} P_{G,\Omega}(t)$. We will use the lower-case p form occasionally (see e.g. Lemma 1.2 below). [7] contains some observations on these polynomials, though its main concern is the proportion of elements which are derangements. $P_{G,\Omega}$ is also $|G|$ times the cycle index polynomial of the permutation group (see [9, p. 143] for definition), specialised to $s_1 \to x$, $s_i \to 1$ for all $i \geqslant 2$. It is also easy to check that $P_{G,\Omega}(x)$ is $|G|$ times the probability generating function of the number of fixed points of a uniformly at random selected element of G in its action on Ω. We note that $f_n = 1$ and $f_{n-1} = 0$.

Some properties of the group can obviously be recovered from this polynomial. For example, it is easy to see that the order of G is $P_{G,\Omega}(1)$ and the degree of G is equal to the degree of $P_{G,\Omega}$. The number of orbits is $P'_{G,\Omega}(1)$ divided by $|G|$. The rank, r, of G (i.e. the number of orbits on $\Omega \times \Omega$) is equal to $\frac{P''_{G,\Omega}(1)+P'_{G,\Omega}(1)}{P_{G,\Omega}(1)}$. The theory behind the latter comes about by viewing $\mathrm{fix}(g)$ as a character function on the vector space with basis set Ω. Taking the inner product of $\mathrm{fix}(g)$ with itself gives us $\sum_{i=0}^{n} \mathrm{fix}(g)^2 = r\,|G|$, and from this the result follows. The minimum degree is also easy to recover.

However this polynomial does not determine the group up to isomorphism. Indeed, any group acting on itself in the regular action where g acts on x by forming gx has $P_{G,G}(x) = x^{|G|} + (|G| - 1)$ so taking two non-isomorphic groups of the same order (the smallest examples are C_4 and V_4) we get the abstract groups non-isomorphic but the polynomials the same. One might hope for uniqueness if (say) the groups are both primitive, but the Mathieu group M_9 acting on 9 points and $\mathrm{AGL}_1(\mathbb{F}_9)$ both have fixed-point polynomial $x^9 + 63x + 8$. Further, GAP gives an example in degree 15 of two transitive permutation groups (G,Ω) and (H,Ω) - in GAP's notation, these are $A_6(15)$ and $3S_5(15)$ - for which $P_{G,\Omega}(x) = P_{H,\Omega}(x)$ but one of the two groups is primitive but the other not: this answers a question left open in [7]. We hope at some future date to address an observation [31] that these pairs of non-isomorphic groups with the same fixed point polynomials also arise naturally in the study of so-called Gassmann-Sunada triples.

We note here two properties of the polynomials: they are (effectively) from [7], Theorem 4.6 parts (6) and (8).

Lemma 1.2. *Suppose (G_1, Ω_1) and (G_2, Ω_2) are two permutation groups. Then*

1. *If $G_1 \times G_2$ acts on the disjoint union $\Omega_1 \coprod \Omega_2$ by $(g_1, g_2)\omega = g_1\omega$ if $\omega \in \Omega_1$ and $(g_1, g_2)\omega = g_2\omega$ otherwise, we have*

$$P_{G_1 \times G_2, \Omega_1 \coprod \Omega_2}(x) = P_{G_1,\Omega_1}(x) P_{G_2,\Omega_2}(x).$$

2. *In the imprimitive action of the wreath product $G_1 \wr G_2$ on $\Omega_1 \times \Omega_2$ we have*

$$p_{G_1 \wr G_2, \Omega_1 \times \Omega_2}(x) = p_{G_2,\Omega_2}(p_{G_1,\Omega_1}(x)).$$

We have observed empirically that for many families of fixed-point polynomials the fixed-point polynomials are very often (but not always) irreducible if the group is transitive, have few real roots (Theorem 2.9 will give some general insight on this, but in fact real roots seem to be rarer still) and that these roots tend to be concentrated near the unit circle unless the group is very large, when more interesting behaviours are possible. We amplify on some of these observations in what follows.

2 Roots and their properties

The first property we will look at are the location of the roots of P_G. We aim to give a few basic theorems which often tell us where most roots of P_G are, and add restrictions to the factors of P_G.

The following consequence of Rouché's theorem is proven in e.g. [35].

Theorem 2.1. *Let $p(x) = \sum_{i=0}^{n} f_i x^i$ be a complex polynomial. If there exists an integer k such that $|f_k| > \sum_{i \neq k} |f_i|$ then $p(x)$ has exactly k roots inside the unit circle, no roots on the unit circle, and $n-k$ roots outside the unit circle. In particular, if $f_0 > \frac{|G|}{2}$, all roots are outside the unit circle.*

The next theorem, from [20, Theorem 3] says that, when $f_0 \neq 0$, unless $\frac{|G|}{\sqrt{f_0}}$ is large, most roots are in a small annulus around the unit circle. Thus the typical behaviour of roots is unlikely to distinguish such groups.

Theorem 2.2 (Hughes and Nikeghbali)**.** *Let $P(z) = \sum_{i=0}^{n} f_i z^i$ be a polynomial over the complex numbers such that $f_0 f_n \neq 0$. Then, given $0 < \rho \leqslant 1$, we have that*

$$1 - \frac{\left|\{\alpha : P(\alpha) = 0, 1-\rho \leqslant |\alpha| \leqslant \frac{1}{1-\rho}\}\right|}{n} \leqslant \frac{2}{n\rho} L_n(P)$$

where

$$L_n(P) = \log\left(\sum_{i=0}^{n} |f_i|\right) - \frac{\log(|f_0|) + \log(|f_n|)}{2}.$$

In the case of fixed-point polynomials the above is satisfied if G contains a derangement, and the L_n function simplifies to $\log\left(\frac{|G|}{\sqrt{f_0}}\right)$. So if $\log\left(\frac{|G|}{\sqrt{f_0}}\right)$ is small compared to n, most roots will be in the annulus.

Corollary 2.3. *Let (G_n, Ω_n) be primitive permutation groups of degree n such that A_n is not contained in G_n. Then P_{G_n} has a proportion $1 - o(1)$ of its roots in the annulus $1 - \rho \leqslant |\alpha| \leqslant \frac{1}{1-\rho}$, for any $\rho > 0$, as $n \to \infty$.*

Proof. By (e.g.) Maróti [22], an upper bound on the cardinality of such a group is $50n^{\sqrt{n}}$. Thus $L_n(P) \leqslant \sqrt{n}\log(50n)$, which is $o(n)$ as required. (Those who want to avoid the use of the classification of finite simple groups in Maróti's proof can instead use results of Babai on primitive but not 2-transitive groups [4], and Pyber [27] for 2-transitive groups). □

If we have a sequence (G_n, Ω_n) of groups whose degree tends to infinity, and an absolute bound on the number of points any element in the family can fix, then we can make a stronger statement: for any $\epsilon > 0$ for all large enough n G_n has *all* its roots of modulus less than $1 + \epsilon$. We need a lemma:

Theorem 2.4 (Blichfeldt's Theorem). *Let G be a permutation group of degree n, and $L = \{\text{fix}(g) : g \in G \setminus \{e\}\}$. Then $|G|$ divides $\prod_{l \in L}(n - l)$.*

Theorem 2.5. *Let $G_1, G_2, \ldots$ be a family of permutation groups, and n_i be the degree of G_i. If*

- *The sequence $n_1, n_2, \ldots$ tends to infinity*
- *there exists a number k, such that for all i we have that $\text{fix}(g) \leqslant k$ for all non-identity elements in G_i*

then for any $\epsilon > 0$ there exists only finitely many i such that $P_{G_i}(z)$ has a root with modulus at least $1 + \epsilon$.

Proof. Firstly, note that there exists a subexponential function S (i.e. S satisfies

$$\lim_{x \to \infty} \frac{S(x)}{e^{cx}} = 0$$

for all $c > 0$) such that, for all i we have $|G_i| \leqslant S(n_i)$. By Blichfeldt's Theorem, $|G|$ divides $\prod_{l \in L}(n - l)$, and so $|G| \leqslant \prod_{l \in L}(n - l)$. Thus $S(n_i) = \prod_{j \in L}(n_i - j)$ is a subexponential function that satisfies our requirements.

Since there is no permutation that fixes more than k points, we have that $P_{G_i}(z) = z^{n_i} + f_k z^k + f_{k-1} z^{k-1} + \cdots + f_0$. Let α be a root of $P_{G_i}(z)$ such that $|\alpha| = 1 + \epsilon$ for some $\epsilon > 0$. Then $-(\alpha^{n_i}) = \sum_{i=0}^{k} f_i \alpha^i$. The triangle equality then gives us

$$|\alpha|^{n_i} = \left| \sum_{j=0}^{k} f_j \alpha^j \right| \leqslant \sum_{j=0}^{k} f_j \, |\alpha|^j .$$

Since $\sum_{j=0}^{k} f_j = |G_i| - 1 < |G_i|$ the right hand side is at most $|G_i| \, |\alpha|^k \leqslant S(n_i)(1 + \epsilon)^k$, and so we have

$$|\alpha|^{n_i} = (1 + \epsilon)^{n_i} \leqslant S(n_i)(1 + \epsilon)^k.$$

The left hand side is, however, an exponential function in n_i, whereas the right hand side is a subexponential function in n_i. Thus only a finite number of α's satisfying $|\alpha| > 1 + \epsilon$ can exist. □

Not only can we often get most of the roots around the unit circle, but the same condition gives that they are spaced roughly evenly around the circle. This was first proved by Erdős and Turán - again, see [20, Theorem 2].

Theorem 2.6 (Erdős and Turán). *Let $P(z) = \sum_{i=0}^{n} f_i z^i$ be a polynomial over the complex numbers such that $f_0 f_n \neq 0$. Then, with $L_n(P)$ as in Theorem 2.2, there is some constant C such that, given $0 < \theta < \phi < 2\pi$, we have*

$$\left| \frac{|\{\alpha : P(\alpha) = 0, \theta \leqslant \arg \alpha \leqslant \phi|}{n} - \frac{\phi - \theta}{2\pi} \right|^2 \leqslant \frac{C}{n} L_n(P).$$

This is saying that provided $L_n(P)/n$ tends to zero, the uniform distribution on the roots will weakly converge to normalised Lebesgue measure on the unit circle.

Though we often get many roots *close* to the unit circle, roots *on* the unit circle are a lot rarer. Note that S_2 has $P_{S_2}(x) = x^2 + 1$ so i is a root of a fixed-point polynomial (this is a lot easier than the apparently unsolved question "does there exist a graph whose chromatic polynomial has $\sqrt{-1}$ as a root"!). However, given some conditions, this is a rarity:

Lemma 2.7. *Let $P(x) = \sum_{i=0}^{n} f_i x^i$ be a monic irreducible polynomial $\in \mathbb{Z}[x]$ such that $P(1) \neq 0$ and P has a root α of modulus 1. Then P is a reciprocal polynomial (i.e one for which $f_i = f_{n-i}$ for all $0 \leqslant i \leqslant n$).*

Proof. Since α is a root, $\bar{\alpha} = \alpha^{-1}$ is also a root. Thus

$$\sum_{i=0}^{n} f_i \alpha^i = 0 \implies \sum_{i=0}^{n} f_i \alpha^{n-i} = 0 \implies \sum_{i=0}^{n} f_{n-i} \alpha^i = 0.$$

Since P is irreducible, P is the minimal polynomial of θ. Thus there exists a scalar k such that $\sum_{i=0}^{n} f_{n-i} x^i = kP(x)$. Substituting $x = 1$ we get $P(1) = kP(1)$, and so $k = 1$. Thus $f_i = f_{n-i}$ as required. □

We use the Rado notation $[n]$ to mean $\{1, 2, \ldots n\}$.

Corollary 2.8. *Let G be a group acting on Ω such that P_G is irreducible and transitive. Then, if P_G has a root of modulus 1, G is S_2 acting on $[2]$.*

Proof. We can assume G is non-trivial. By the above lemma, P_G must be reciprocal. Thus we get $f_0 = f_n = 1$ and $f_1 = f_{n-1} = 0$.

Now we use the Orbit-Counting Lemma. Since the one derangement has no fixed points, and every other element at least 2 fixed points,

$$\frac{1}{|G|}(0 + 2(|G| - 1)) \leqslant 1.$$

Manipulation yields $|G| \leqslant 2$: by transitivity and non-triviality, $G = S_2$. □

It seems to be the case that, for most transitive G, P_G is irreducible over $\mathbb{Q}$ (or equivalently over $\mathbb{Z}$), and so has neither repeated roots, nor rational roots. There are exceptions: if k is a positive integer such that $k^3 = 3m-1$ for an integer m, the cyclic group C_{k^3+1} acting regularly on $[k^3 + 1]$ has fixed-point polynomial $P_{C_{k^3+1}}(x) = x^{k^3+1} + k^3 = (x^m + k)(x^{2m} - kx^m + k^2)$, and there are other occasional factorisations for regular G. (Note, though, that most polynomials $x^n + (n-1)$ are irreducible: for if any prime divides $n - 1$ exactly, we can use that prime in Eisenstein's criterion to deduce irreducibility, so a necessary condition for reducibility is that $n - 1$ is powerful - i.e. for every prime p dividing $n - 1$, p^2 divides $n - 1$ - and Golomb [16] showed that only $\frac{\zeta(\frac{3}{2})}{\zeta(3)}\sqrt{x}(1 + o(1))$ of the positive integers $\leqslant x$ are powerful, where ζ denotes the Riemann zeta function).

Lemma 1.2 part 2 has the consequence that if some group has a reducible fixed point polynomial, then infinitely many further reducible examples can be constructed from it by taking wreath products. We have been informed [8] of an unpublished construction of, for each odd prime p, two imprimitive groups of degree p^2 (with orders p^{p-1} and p^p respectively) whose fixed-point polynomials are reducible: this construction uses coding theory. We know at present of no transitive groups with reducible fixed-point polynomial other than the possibilities implied by this and the previous paragraph. (It is easy to see that many intransitive permutation groups can have reducible polynomials. For example, if S_n acts on $[m]$ where $m > n$ by acting on the first n letters, then x^{m-n} is a factor of $P_{S_n,[m]}$).

We now turn to real roots. We can often get a crude upper bound with the following. Again, this is related to the ideas of Erdős and Turán, and we refer to [26] for the proof.

Theorem 2.9. *Let $P(z) = \sum_{i=0}^{n} f_i x^i$ be a polynomial with m real roots. If $f_0 f_n \neq 0$ then, again with $L_n(P)$ as in Theorem 2.2*

$$m^2 \leqslant 2nL_n(P).$$

Thus for fixed point polynomials, this inequality simplifies to

$$m^2 \leqslant 2n \log\left(\frac{|G|}{\sqrt{f_0}}\right).$$

For many groups, the number of real roots of its fixed-point polynomial seem to be smaller still than predicted by this bound. Indeed, of the examples we have done so far with irreducible polynomials, we have not got more than two real roots, for A_n with n even, or the group of invertible transforms $x \to ax + b$ acting on a finite field of order 2^n, with $n \geqslant 2$. (See below for more, and intransitive examples with many roots).

A toy observation in this direction is that no non-trivial fixed-point polynomial has all of its roots on the real axis. If it did, then by e.g. [24] the sequence (f_i) is a so-called PF_2 sequence (i.e. the infinite matrix $M = (f_{i-j})$ where $f_k = 0$ for any $k < 0$ or $> n$, has all its 1×1 or 2×2 minors having non-negative determinant). This implies (again see [24]) that it has no internal zeros (that is, if $0 \leqslant i < j < k \leqslant n$ and $f_i f_k > 0$, then $f_j > 0$). However, $f_n > 0$, $f_{n-1} = 0$, and $f_i > 0$ for some $i < n-1$, so there is an internal zero. (Even if one restricts to the non-zero f_is, these do not form a unimodal sequence, even for $P_{S_n}(x)$).

We may ask whether the complex roots are dense in the plane, which is known to be true for chromatic polynomials by a result of Sokal. The answer is no when G is transitive or has a bounded number of orbits.

Theorem 2.10. *The set of all roots of $P_G(x)$ for transitive groups G is not dense in the complex plane.*

Proof. Let α be a complex number such that $|\alpha| < 1$ and $|\alpha - 1| < 1$. We will show that there does not exist a transitive group G such that $P_G(\alpha) = 0$.

Assume that there exists a transitive group G such that $P_G(\alpha) = 0$ for some α. For all groups G we have $P_G(1) = |G|$. Thus, using the triangle inequality to note that $|1 + \alpha + \cdots + \alpha^{i-1}| \leqslant i$, we get

$$\begin{aligned}
&\implies \sum_{i=0}^{n} f_i(1-\alpha^i) = |G| \implies \sum_{i=0}^{n} f_i\,|1-\alpha|\,i \geqslant |G| \\
&\implies |1-\alpha| \sum_{i=0}^{n} i f_i \geqslant |G| \implies |1-\alpha| \geqslant 1
\end{aligned}$$

which is a contradiction. Thus α cannot be a root, as required. □

Corollary 2.11. *Let $k > 0$ be an integer. Then the set of all roots of $P_G(x)$ for groups G with k or less orbits is not dense in the complex plane.*

Proof. The proof is the same as Theorem 2.10, except that the zero-free zone is the intersection of the circles $|z| < 1$ and $|z - 1| < \frac{1}{k}$. This follows because

$$\sum_{i=0}^{n} i f_i = t\,|G|$$

where t is the number of orbits of G, which is bounded above by k. □

It appears also that the set $\{\alpha : |\alpha| < 1, \alpha \notin \mathbb{R}^-\}$ could potentially be a zero-free zone. Calculations with GAP[15] show that this is true for transitive groups of degree < 15.

In fact, there may well be larger zero-free regions. For example, if we know more about the proportion of derangements, results in [19] can sometimes be used to extend the zero-free region a bit. A result of Saff and Varga [28] shows that the region $y^2 \leqslant 4x$ contains no zeros $z = x+iy$ of the $(P_{S_n}(z))$: there may be similar results for other families.

Question. Are the roots of all fixed point polynomials (including intransitive ones) dense in the complex plane?

We have no very clear idea of the answer to this question.

3 Examples

Example 3.1 (The symmetric group on $\boldsymbol{n}$ letters)**.** We first need a lemma.

Lemma 3.1. *Let G be a group of degree n. Let F_k denote the number of orbits of G acting on k-tuples of distinct elements of Ω. Then*

$$\frac{P_G(x)}{|G|} = \sum_{k=0}^{n} F_k \frac{(x-1)^k}{k!}.$$

Proof. Combine [9, Theorem 6.12] with the fact that the left-hand side of that lemma is, by an earlier observation, $\frac{P_G(x)}{|G|}$. $\square$

Of course S_n acting on $[n]$ in the usual way has one orbit on distinct k-tuples for all $k \leqslant n$, and so the fixed-point polynomial can be easily seen from Lemma 3.1.

$$P_{S_n,[n]}(x) = n! \sum_{i=0}^{n} \frac{(x-1)^i}{i!}.$$

Thus $\frac{P_{S_n,[n]}}{n!}$ is the first n terms of the Maclaurin series for e^{x-1}.

Example 3.2 (The alternating group on $\boldsymbol{n}$ letters)**.** We first note the relation $f_i(A_n) = \binom{n}{i} f_0(A_{n-i})$ and that $f_0(A_n) = \frac{(f_0(S_n)-(-1)^n(n-1))}{2}$, see e.g. [11]. This allows us to calculate the fixed-point polynomial (see [18] for details)

$$P_{A_n}(x) = \frac{1}{2}\left(P_{S_n}(x) + (x-1)^n + n(x-1)^{n-1}\right).$$

Example 3.3 (Frobenius groups)**.** A transitive permutation group G acting on a finite set Ω is called Frobenius if $\mathrm{fix}(g) \leqslant 1$ for all non-identity elements of the group, and there exists an element of the group such that $\mathrm{fix}(g) = 1$.

The fixed point polynomial for a Frobenius group can be calculated easily:

$$P_{G,\Omega} = x^{|\Omega|} + (|G| - |\Omega|)x + |\Omega| - 1.$$

We investigate two families of Frobenius groups in more detail. The first is the dihedral group Dih_n of symmetries of a regular n-gon, in the case where n is odd. In this case, the fixed-point polynomial is

$$P_{\mathrm{Dih}_n}(x) = x^n + nx + n - 1.$$

The second contains the automorphism groups of Paley graphs of prime order. Recall these have vertex set the integers modulo p, for a prime p congruent to 1 modulo 4. Two vertices x and y are adjacent if $x - y \equiv a^2 \mod p$ for some a. It is well-known that the automorphism group consists of all functions $f(x) = ax + b$ with $a \neq 0$ a square in $\mathbb{F}_p$ and b any element of $\mathbb{F}_p$: (see e.g. [10]: the result has been rediscovered several times). Thus a non-identity automorphism is a derangement if and only if $a = 1$, otherwise it has the one fixed point $x = \frac{-b}{(a-1)}$. Thus

$$P_{\mathrm{Aut}\, P_p, V(P_p)}(x) = x^p + \frac{p(p-3)}{2}x + p - 1.$$

Example 3.4 (Mathieu groups)**.** Since there are only a few Mathieu groups, we can use [15] to calculate the relevant f_i's. (One could also approach the problem for at least some of the groups based on Lemma 3.1 and the fact the groups are sharply transitive).

$$\begin{aligned}
P_{M_9}(x) &= x^9 + 63x + 8\\
P_{M_{10}}(x) &= x^{10} + 315x^2 + 80x + 324\\
P_{M_{11}}(x) &= x^{11} + 1155x^3 + 440x^2 + 3564x + 2760\\
P_{M_{12}}(x) &= x^{12} + 3465x^4 + 1760x^3 + 21384x^2 + 33120x + 35310\\
P_{M_{21}}(x) &= x^{21} + 315x^5 + 2240x^3 + 11844x + 5760\\
P_{M_{22}}(x) &= x^{22} + 1155x^6 + 12320x^4 + 130284x^2 + 126720x + 173040\\
P_{M_{23}}(x) &= x^{23} + 3795x^7 + 56672x^5 + 998844x^3 + 1457280x^2 + 3979920x\\
&\quad + 3704448\\
P_{M_{24}}(x) &= x^{24} + 11385x^8 + 226688x^6 + 5993064x^4 + 11658240x^3\\
&\quad + 47759040x^2 + 88906752x + 90267870.
\end{aligned}$$

Example 3.5 (Hyperoctahedral groups)**.** Consider an n-dimensional hypercube, Q_n. Then the hyperoctahedral group H_n is the automorphism group of Q_n. We will follow the notation of [12] and represent the elements of H_n as signed permutations. That is, we will attach minus signs to certain elements of a permutation (for example, $(2, \bar{5}, \bar{3}, 1)$). The vertices will be seen as numbers in their binary form. The permutation will then permute the binary digits, and will negate any bits permuted by a number with an attached minus sign.

The sequence of f_i's was mentioned very briefly in [12, Corollary 2.4] as a means of calculating f_0. The relevant part of it is described below.

Theorem 3.2. *Let H_n be the hyperoctahedral group of order n, and $0 < i \leqslant n$. Then $f_{2^i} = 2^{n-i}c(n, i)$ where $c(n, i)$ is the unsigned Stirling number of the first kind. The only other non-zero f_j is f_0.*

Proof. A permutation fixes 2^i points if it has i cycles, and every cycle has an even number of minus signs attached to it. If a cycle is of length l, there are 2^{l-1} ways of attaching an even number of minus signs. Thus there is 2^{n-i} ways of attaching an even number of minus signs to a given permutation with i cycles. By definition, there are $c(n, i)$ permutations on $[n]$ with i cycles. The last sentence follows from [12, Proposition 2.5] ☐

We can then work out the number of permutations with fixed points, and subtract this from the order of H_n, which is well known to be $2^n n!$ - see again [12]. This gives (using a fact about Stirling numbers at the end of the proof of Corollary 2.4 in [12])

$$P_{H_n,V(Q_n)}(x) = 2^n n! - \frac{(2n)!}{2^n n!} + \sum_{i=1}^{n} 2^{n-i}c(n, i)x^{2^i}.$$

Example 3.6 (Projective planes)**.** Let $\mathbb{F}_p$ be the finite field of prime order p. Define the group $\mathrm{PG}_2(p)$ as the automorphism (collineation) group of a projective plane whose point set is equal to the 1-dimensional subspaces of $\mathbb{F}_p^3$ and line set is equal to the 2-dimensional subspaces of $\mathbb{F}_p^3$, with incidence defined by inclusion. By the Fundamental Theorem of Projective Geometry, $\mathrm{PG}_2(p) \cong \mathrm{PGL}_3(p)$, which has order $p^3(p^2+p+1)(p-1)^2(p+1)$.

The fixed-point polynomial for $\mathrm{PG}_2(p)$ has four non-zero coefficients f_0, f_1, f_{p+1} and $f_{p^2+p+1} = 1$, as any collineation which fixes two points fixes the whole line containing them, and any automorphism which fixes a line and a point not on the line in fact clearly fixes all points. It is known that the automorphism group is 2-transitive. This gives the equations

$$\begin{aligned}|G| &= 1 + f_{p+1} + f_1 + f_0 \\ &= (p^2+p+1) + (p+1)f_{p+1} + f_1 \\ &= p(p+1)(p^2+p+1) + p(p+1)f_{p+1}\end{aligned}$$

using the fact that if (G, Ω) is k-transitive, then $P_G^{(k)}(1) = |G|$ (see [7, Theorem 4.6. (v)]). Solving these equations gives

$$\begin{aligned}P_{\mathrm{PG}_2(p)}(x) = x^{p^2+p+1} &+ (p^2+p+1)(p^2-p-1)(p^2-p+1)x^{p+1} \\ &+ p(p^2+p+1)(p^5-2p^4+2p^2-p+1)x + p^4(p^3-p^2-1).\end{aligned}$$

Example 3.7 (Bipartite double cover of a stable graph)**.** Let $G = (V, E)$ be a graph. We can define the bipartite double cover of G, $\tilde{G}$, to be a graph with vertex set $V \times \{1, -1\}$: we refer to the two sets $V_1 = \{(v, 1) : v \in V\}$ and $V_{-1} = \{(v, -1) : v \in V\}$ as the vertex classes. Two vertices, (v, ϵ_v) and (w, ϵ_w), are adjacent in $\tilde{G}$ if and only if v and w are adjacent in G and $\epsilon_v \neq \epsilon_w$. An automorphism α of G induces an automorphism $\tilde{\alpha}$ of $\tilde{G}$ by $\tilde{\alpha}(v, \epsilon) = (\alpha(v), \epsilon)$. There is also a 'swapping' automorphism that interchanges the two vertex classes. If these are the only automorphisms of $\tilde{G}$ then G is called a stable graph.

If a graph is stable, every automorphism of $\tilde{G}$ which fixes (v, ϵ_v) will also fix $(v, -\epsilon_v)$, so every automorphism coming from G which fixes i points in G fixes $2i$ points in $\tilde{G}$. Also, any automorphism which swaps round V_1 and V_{-1} will be a derangement. Thus we get, for a stable graph,

$$P_{\mathrm{Aut}(\tilde{G}), V(\tilde{G})}(x) = P_{\mathrm{Aut}(G), V(G)}(x^2) + |\mathrm{Aut}(G)|\,.$$

Examples of stable graphs can be found via Surowski's theorem [30].

Theorem 3.3 (Surowski's Theorem)**.** *Any strongly regular graph (n, k, λ, μ) with $k > \mu \neq \lambda \geqslant 1$ is stable.*

Example 3.8. Suppose we consider, for a prime p, the Sylow p-subgroup of S_{p^k}. This is well-known to be the iterated wreath product of k copies of $\mathbb{Z}_p$. In particular, in the case $p = 2$, its fixed point polynomial will be the k-fold iteration of (x^2+1) with itself.

4 Irreducibility of the fixed-point polynomial

We return now to showing that various of the polynomials are irreducible. We start with S_n and A_n, using the following generalisation by Filaseta of a theorem of Schur (see [14]).

Lemma 4.1. *Any polynomial of the form*

$$\sum_{i=0}^{n} c_i \frac{X^i}{i!} = 1 + c_1 \frac{X^1}{1!} + c_2 \frac{X^2}{2!} + \cdots + c_{n-1} \frac{X^{n-1}}{(n-1)!} + c_n \frac{X^n}{n!}$$

where $c_0 = 1$, $0 < |c_i| < n$ for all $i \in [n]$, and all c_i are integers, is irreducible in $\mathbb{Q}[X]$, except possibly if $c_n = \pm 5$ and $n = 6$ or $c_n = \pm 7$ and $n = 10$.

Theorem 4.2. *Let G be a transitive group of degree $n \neq 6, 10$ with $0 < k < n$ orbits on n-tuples of distinct elements. Then $P_G(x)$ is irreducible.*

Proof. We have to show that the conditions of Lemma 4.1 apply to $P_G/|G|$. We know that $P_G(1) = |G|$. Using Lemma 3.1,

$$\frac{P_G(x)}{|G|} = \sum_{k=0}^{n} F_k \frac{(x-1)^k}{k!}.$$

and1we are told that $0 < F_i < n$. The right-hand side is irreducible as a polynomial in $u = x - 1$ by Filaseta's result, and so the left-hand side is irreducible as a polynomial in $\mathbb{Q}[x]$. $\square$

Corollary 4.3. *Suppose that $G = S_n$ acting on $\{1, 2, \ldots, n\}$ where $n \geqslant 2$, or A_n with $n \geqslant 3$. Then $P_G(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. The cases with $n = 6$ or $n = 10$ can be handled by calculating the expressions in Examples 3.1. and 3.2: one can then use e.g. MAPLE to check that these four fixed-point polynomials are indeed irreducible. In the other cases, note that S_n has just one orbit on distinct n-tuples, as there is a permutation taking any ordering of $\{1, 2, \ldots, n\}$ to any other. For A_n, there are two orbits on the n-tuples of distinct elements from $\{1, 2, \ldots, n\}$: indeed one orbit is all the even permutations of $\{1, 2, \ldots, n\}$ and the other orbit is the odd permutations. This finishes the proof by Theorem 4.2, as in each case n exceeds the number of orbits. $\square$

It is natural to try to prove irreducibility of the polynomials by considering reductions mod a suitable prime p, as if the reduction is irreducible so is the original polynomial. However, any fixed point polynomial is reducible modulo 2, as if f_0 is even, then x is a factor modulo 2, and if $|G|$ is even, then $(x - 1)$ is a factor mod 2: and at least one of $|G|$ and f_0 has to be even, e.g. considering the Handshake Lemma in the f_0-regular graph on vertex set G where $x \sim y$ if and only if xy^{-1} is a derangement. More generally, it will be reducible modulo any prime dividing $|G|\, f_0$. There does not seem to be any obvious choice of prime in general modulo which to look for irreducibility.

Another obvious tool is Eisenstein's criterion from Galois theory. Here are two examples of it in action.

Theorem 4.4. *Suppose $|G|$ is odd and that 4 does not divide f_0. Then $P_G(x)$ is irreducible.*

Proof. If G is a group acting on a set Ω, then g and g^{-1} have the same number of fixed points for every $g \in G$. Further as the order is odd, there is no element of order 2, so $g \neq g^{-1}$ unless g is the identity. Thus all the f_i for $i < n$ are even. Since by assumption $2^2 = 4$ does not divide f_0, the result follows from Eisenstein's criterion applied at the prime $p = 2$. □

Theorem 4.5. *The fixed-point polynomial for a Frobenius group of prime degree is irreducible. In particular, the automorphism groups of Paley graphs have irreducible fixed-point polynomials.*

Proof. Let G be a Frobenius group of order m and prime degree p. Then the fixed point polynomial of G is $P_G(x) = x^p + (m-p)x + p - 1$. We first shift this polynomial by 1 to get $P_G(x+1) = (x+1)^p + (m-p)x + m - 1$. The prime p divides every coefficient of $(x+1)^p$ with the exceptions of the leading term and the constant term 1. Also p divides m and so divides $m - p$. The combined constant term is m, which is divisible by p but not by p^2 as by Blichfeldt's theorem m divides $p(p-1)$. Thus Eisenstein's criterion shows $P_G(x+1)$ is irreducible. Thus $P_G(x)$ is irreducible. □

Similarly, one may take the calculations of the fixed-point polynomials of Mathieu groups: then MAPLE indicates that these are all irreducible. For the projective planes, we do not have a complete result yet, but in the special case where $p^2 + p + 1$ is also prime, it is not too hard to use Eisenstein's criterion on $P_{\mathrm{PG}_2(p)}(x)$, putting $x = u + 1$, to see that it is irreducible. See [18] for details.

Zhao [35] shows (an application of Rouché's theorem) that if $p(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial of degree n with integer coefficients and if $|a_0|$ is prime with $|a_0| > \sum_{i=1}^{n} |a_i|$ then $p(x)$ is irreducible. We suspect this result will be of use in proving irreducibility results.

5 Location of the roots of fixed-point polynomials

A useful technique for bounding the number of real roots of a polynomial is Descartes' rule of signs: the relevant version for us is that the number of negative roots of a polynomial $P(x) = \sum_{i=0}^{n} f_i x^i$ is at most the number of sign changes in the sequence of non-zero coefficients of $f(-x) = \sum_{i=0}^{n} (f_i(-1)^i)x^i$. Thus Frobenius groups of odd degree (e.g. Paley graphs) have exactly one real root of their fixed-point polynomials (they have one real root for having odd degree, and there is only one change on sign in the coefficients).

Example 5.1 (Symmetric groups)**.** This is a well-understood story. Let $g_n(z) = \sum_{i=0}^{n-1} \frac{z^i}{i!}$, so that the roots of $g_n(z)$ are the roots of $P_{S_{n-1}}(x)$ translated by 1. It thus suffices to understand the roots of $g_n(z)$.

Theorem 5.1. *The roots of $g_n(nz)$ converge, as $n \to \infty$, to the curve $|ze^{1-z}| = 1$ in the complex plane. There is exactly one real root of $P_{S_n}(x)$ if n is odd, and none if n is even. The real root, when it exists, is near c^*n, where c^* is the unique (negative) real solution of $|ce^{1-c}| = 1$, which is approximately -0.278.*

Proof. This is a compilation of results of Szegő[25] and Zemyan[34]. □

See [34] for a picture of the curve and the roots converging to it.

Note also this result on the real root allows us to construct *intransitive* permutation groups whose fixed-point polynomial has many real roots. Indeed take the disjoint union of complete graphs of orders $2n_1+1 < 2n_2+1 < \ldots < 2n_k+1$: the automorphism group is then $S_{2n_1+1} \times S_{2n_2+1} \times \ldots \times S_{2n_k+1}$ and this will have fixed point polynomial the product of the fixed point polynomials on S_{2n_j+1} on K_{2n_j+1}, by Lemma 1.2 part 1. Each of these k polynomials has (exactly) one real root by the above, so overall there will be k real roots.

Example 5.2 (Alternating groups)**.** Again the seeming pattern of roots is a horseshoe of the same general style as for the symmetric group, though we have not formally proved this. As regards real roots, numerical work suggests that there are exactly two real roots of $P_{A_n}(x)$ for n even, one close to $-\frac{n}{\sqrt{2}}$ and the other close to $-c^*n$ where c^* is as in the discussion of the symmetric group: for n odd, it seems there is exactly one real root close to $-\frac{n}{\sqrt{2}}$. Here is a partial result.

Lemma 5.2. *Suppose that $P_{A_{n-1}}(z_n n+1) = 0$ for real z_n. Then if n is even, we get $(z_n) \to \frac{-1}{\sqrt{2}}$. If n is large enough and odd, and there are infinitely many z_n, then $(z_n) \to \frac{-1}{\sqrt{2}}$ if* $\liminf_n \sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n = 0$*, and otherwise* $\liminf_n z_n \geqslant c^*$.

Proof. By the Eneström-Kakeya theorem, any root of $\sum_{i=0}^n a_i z^i$ with $a_i > 0$ for all i lies in the annulus

$$\min_{0\leqslant i\leqslant n-1} \frac{a_i}{a_{i+1}} \leqslant |z| \leqslant \max_{0\leqslant i\leqslant n-1} \frac{a_i}{a_{i+1}}.$$

Recall that

$$P_{A_n}(x) = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(x-1)^i}{i!} + n(x-1)^{n-1} + (x-1)^n.$$

Thus, putting $z = (x-1)$ we have

$$a_i = \frac{1}{2}\frac{n!}{i!} \text{ for } 0 \leqslant i \leqslant n-2,\ a_{n-1} = n,\ a_n = 1$$

so all roots of $P_{A_n}(x)$ have $1 \leqslant |x-1| \leqslant n$; real roots are in $1-n \leqslant x \leqslant 0$. We need to show that there is not a root at $x = 1-n$ for $n \geqslant 2$, in order to apply a result of Dieudonné shortly. The claim that $P_{A_n}(1-n) \neq 0$ will follow if we show

$$P_{A_n}(x) = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-n)^i}{i!} \neq 0.$$

If n is odd, simply note that each two consecutive terms in the sum

$$\frac{(-n)^{2j}}{(2j)!} + \frac{(-n)^{2j+1}}{(2j+1)!} < 0$$

for $2j+1 \leqslant n-2$ is negative: this follows as the numerator is a positive number times $2j+1-n<0$. Similarly, if n is even, the $i=0$ term is positive, and thereafter for any $1 \leqslant 2j-1 \leqslant n-2$ we have

$$\frac{(-n)^{2j-1}}{(2j-1)!}+\frac{(-n)^{2j}}{(2j)!}>0.$$

Thus we need only consider roots of $P_{A_{n-1}}(z_n n+1)$ with $z_n \in (-1,0)$. Dieudonné proved (see. e.g. [33]) that, for any fixed $\eta>0$, if $z \in \{w : |w|<1\} \cap \{w : |w-1| \geqslant \eta\}$ we have $(f_n(z))$ converges uniformly to $1/(1-z)$, where

$$f_n(z)=\frac{n!}{(nz)^n}\left(e^{nz}-\sum_{i=0}^{n-1}\frac{(zn)^i}{i!}\right).$$

Thus for real $z \in (-1,0)$, given $\epsilon>0$ for $n \geqslant N_1(\epsilon)$ we get

$$\begin{aligned}
&\frac{1}{1-z}-\epsilon<f_n(z)<\frac{1}{1-z}+\epsilon\\
\Longrightarrow\ &\frac{1}{1-z}-\epsilon<\frac{n!e^{nz}}{(nz)^n}-\frac{nP_{S_{n-1}}(nz+1)}{(nz)^n}<\frac{1}{1-z}+\epsilon.
\end{aligned}$$

Substituting $P_{A_{n-1}}(x)=\frac{1}{2}(P_{S_{n-1}}(x)+(x-1)^{n-1}+(n-1)(x-1)^{n-2})$ gives

$$\frac{1}{1-z}-\epsilon<\frac{n!e^{nz}}{(nz)^n}-\frac{n(2P_{A_{n-1}}(nz+1)-(nz)^{n-2}(nz+n-1))}{(nz)^n}<\frac{1}{1-z}+\epsilon$$

$$\frac{1}{1-z}-\frac{1}{z}-\frac{1}{z^2}-\epsilon<\frac{n!e^{nz}}{(nz)^n}-\frac{2nP_{A_{n-1}}(nz+1)}{(nz)^n}-\frac{1}{nz^2}<\frac{1}{1-z}-\frac{1}{z}-\frac{1}{z^2}+\epsilon$$

$$\frac{2z^2-1}{(1-z)z^2}-\epsilon<\frac{n!e^{nz}}{(nz)^n}-\frac{2nP_{A_{n-1}}(nz+1)}{(nz)^n}-\frac{1}{nz^2}<\frac{2z^2-1}{(1-z)z^2}+\epsilon.$$

In particular, if $n \geqslant N_1(\epsilon)$ and z_n is such that $P_{A_{n-1}}(nz_n+1)=0$, we get that

$$\frac{2z_n^2-1}{(1-z_n)z_n^2}-\epsilon<\frac{n!e^{nz_n}}{(nz_n)^n}-\frac{1}{nz_n^2}<\frac{2z_n^2-1}{(1-z_n)z_n^2}+\epsilon.$$

Recall that a form of Stirling's approximation says that, for all $n \in \mathbb{N}$,

$$\sqrt{2\pi}n^{n+1/2}e^{-n} \leqslant n! \leqslant en^{n+1/2}e^{-n}.$$

This gives

$$\begin{aligned}
&\sqrt{2\pi n}\frac{n^n}{e^n}\frac{e^{nz_n}}{(-nz_n)^n} \leqslant \frac{n!e^{nz_n}}{(-nz_n)^n} \leqslant e\sqrt{n}\frac{n^n}{e^n}\frac{e^{nz_n}}{(-nz_n)^n}\\
\Longrightarrow\ &\sqrt{2\pi n}\left(\frac{e^{z_n-1}}{-z_n}\right)^n \leqslant \frac{n!e^{nz_n}}{(-nz_n)^n} \leqslant e\sqrt{n}\left(\frac{e^{z_n-1}}{-z_n}\right)^n.
\end{aligned}$$

Thus, if n is even (respectively odd) we get

$$\sqrt{2\pi n}\left(\frac{e^{z_n-1}}{z_n}\right)^n \leqslant \frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}+\epsilon$$
$$e\sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n \geqslant \frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}-\epsilon$$

respectively

$$e\sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n \leqslant \frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}+\epsilon$$
$$\sqrt{2\pi n}\left(\frac{e^{z_n-1}}{z_n}\right)^n \geqslant \frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}-\epsilon. \ (*)$$

In the case when n is even, we see we must have

$$\begin{aligned}&\frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}+\epsilon>0\\ \Longrightarrow\ &(2n+\epsilon n(1-z_n))z_n^2-n+1-z_n>0\\ \Longrightarrow\ &2n(1+\epsilon)z_n^2>n-2\end{aligned}$$

which implies that $\limsup_n z_n \leqslant \frac{-1}{\sqrt{2}}$. We record for future use that taking $\epsilon=0.01$ and $n=200$, that indeed we have $z_n^2>\frac{0.99}{2.02}$ for $n\geqslant 200$ so $z_n<-0.7$ for $n\geqslant 200$.

On the other hand, since $z_n \leqslant \frac{-1}{\sqrt{2}}+\delta$ for n large enough, we have that $\left|\frac{e^{z_n-1}}{z_n}\right|<0.256$ (taking δ small enough) so $\left|\left(\frac{e^{z_n-1}}{-z_n}\right)^n e\sqrt{n}\right|<\epsilon$ for all $n\geqslant N_2(\epsilon)$. Thus

$$\frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}>-2\epsilon$$

for n large enough. Thus again $\liminf_n z_n \geqslant \frac{-1}{\sqrt{2}}$: thus $(z_n)\to\frac{-1}{\sqrt{2}}$.

For n odd, from the formula

$$\sqrt{2\pi n}\left(\frac{e^{z_n-1}}{z_n}\right)^n \geqslant \frac{2z_n^2-1}{z_n^2(1-z_n)}+\frac{1}{nz_n^2}-\epsilon.$$

we note that as n is odd and $z_n<0$ the left-hand side is negative. Thus we must get

$$\frac{2z_n^2-1}{(z_n^2(1-z_n))}+\frac{1}{nz_n^2}<\epsilon$$

which again implies that $\liminf_n z_n \geqslant \frac{-1}{\sqrt{2}}$.

Now suppose that $\liminf \sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n=0$ so that $\sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n>-\epsilon$ for n large enough. Multiplying by e and using the inequalities (*) for n odd,

$$\frac{2z_n^2-1}{(z_n^2(1-z_n))}+\frac{1}{nz_n^2}>-(1+e)\epsilon>-4\epsilon$$

(say) for n large enough. This cannot happen if, for infinitely many n, we have $z_n > \frac{-1}{\sqrt{2}}+\delta$, so we get $\limsup_n z_n \leqslant \frac{-1}{\sqrt{2}}$ so $\lim_{n\to\infty} z_n = \frac{-1}{\sqrt{2}}$.

Otherwise $\liminf_n \sqrt{n}\left(\frac{e^{z_n-1}}{z_n}\right)^n < 0$, i.e. there is some $\epsilon > 0$ such that for all but finitely many n, $\sqrt{n}\left(\frac{e^{z_n-1}}{-z_n}\right)^n > \epsilon$; this would not work if for infinitely many n we had $-e^{z_n-1}/z_n \leqslant 1-\delta$. Thus we cannot have infinitely many $z_n < c^*$ as then we would have

$$\begin{aligned} e^{z_n-1} &< e^{c^*-1} \\ \frac{e^{z_n-1}}{-z_n} &< \frac{e^{c^*-1}}{-c^*} \\ \left|\frac{e^{z_n-1}}{-z_n}\right| &< \left|\frac{e^{c^*-1}}{-c^*}\right| \\ &= \left|\frac{1}{c^*e^{1-c^*}}\right| \\ &= 1 \end{aligned}$$

and so $\liminf_n z_n \geqslant c^*$. (We suspect, as noted above, that the limsup is c^* too, but there is a technical issue about proving it and we do not need it for our argument, so omit the point). □

Lemma 5.3. *For even $n = 2k \geqslant 4$, $P_{A_{2k}}(1-k) < 0$ (so in particular there are at least two real roots).*

Proof. We do the case $k = 2$ by hand. For $k \geqslant 3$, using MAPLE and simplifying, we have

$$P_{A_{2k}}(1-k) = \frac{k(2k-1)}{e^k}\Gamma(2k-1,-k) - k^{2k}$$

where $\Gamma(2k-1,-k) = \int_{-k}^{\infty} e^{-t}t^{2k-2}dt$. Thus we need to prove that

$$\int_{-k}^{\infty} e^{-t}t^{2k-2} < \frac{(k^2e)^k}{k(2k-1)}.$$

We split the integral into

$$\int_0^{\infty} e^{-t}t^{2k-2}dt + \int_{-k}^{0} e^{-t}t^{2k-2}dt \leqslant (2k-2)! + k\sup e^{-t}t^{2k-2}.$$

Easy calculus shows the supremum of $e^{-t}t^{2k-2}$ is attained at $t = (2k-2)$ where the supremum is $e^{-2k-2}(2k-2)^{2k-2}$. So we have to prove that

$$(2k-2)! + ke^{-2k-2}(2k-2)^{2k-2} < \frac{(k^2e)^k}{k(2k-1)}.$$

By Stirling again, it is enough to show that

$$\frac{e(2k-2)^{2k-2+1/2}}{e^{2k-2}} + ke^{-(2k-2)}(2k-2)^{2k-2} < \frac{(k^2e)^k}{k(2k-1)}$$

For this in turn, it is enough to show that

$$(2k)^{2k-2}[e\sqrt{2k-2}+k] < \frac{k^{2k-1}e^{3k-2}}{2k}$$

for which, manipulating, it is enough to show that

$$\left(\frac{e^3}{4}\right)^k > \frac{e^2}{2}[e\sqrt{2k-2}+k]$$

for which it is enough to show that

$$\left(\frac{e^3}{4}\right)^k > 16k.$$

This is easily proved by induction on $k \geqslant 3$. $\square$

Corollary 5.4. *P_{A_n} has exactly two real roots for n even, and exactly one for n odd.*

Proof. We have for $n \leqslant 200$ that the claim holds by (MAPLE) calculation. For $k \geqslant 101$, we prove the following statement $P(k)$ by induction:
$P(k)$: $P_{A_{2k}}(x)$ has two real roots $z_{2k+1}(2k+1)+1$, with exactly one of them having $z_k > -0.5$ and $P_{A_{2k-1}}$ has exactly one real root $z_{2k}(2k)+1$.
For the base case $k = 101$ we have that the lower root of $P_{A_{202}}$ is $-141.896\ldots$ and the upper $-55.288\ldots$ which indeed gives exactly one of the two $z_{203} < -0.5$. Similarly the unique root of $P_{A_{201}}(x)$ is -141.189 which give $z_{202} < -0.7$.

For subsequent cases, suppose we have proved $P(k)$ for $k \leqslant n$. $P_{A_{2n+1}}$ of course has at least one real root; if it had more than one, it would have at least 3. By the estimates in Lemma 5.2, the corresponding z_{2n+2}'s are all < -0.7. Hence both roots of $P_{A_{2n}}$ are between these, so $< -0.7 \times (2k+2)+1$ and so not greater than $-0.5 \times (2k+1)$. This is a contradiction, so $P_{A_{2k+1}}$ has only one root.

Finally, if $P_{A_{2n+2}}$ has more than 2 roots, it has at least 4: thus we would get 3 roots of $P_{A_{2n+1}}$ but we know that this is not true. Thus we need only check that $P_{A_{2n+2}}$ has at least one real root, and that at least one of them has $z_{2n+3} > -0.5$. But this follows from the last Lemma. $\square$

Example 5.3 (Frobenius groups)**.**

Theorem 5.5. *If G is a Frobenius group acting on n points then $P_G(z)$ has one root inside the unit circle, no roots on the unit circle, and $n-1$ roots outside the unit circle.*

Proof. If $n \neq |G|/2$, then $f_1 > f_0 + 1$ and so the result follows by applying Theorem 2.1. We will thus assume that $n = |G|/2$.

To see that there are no roots on the unit circle, assume that $z = e^{i\theta}$ is a root. Then separating $P_G(z) = 0$ into real and imaginary parts gives us the system of equations

$$\begin{aligned} \cos n\theta &= -(n\cos\theta + n - 1) \\ \sin n\theta &= -(n\sin\theta). \end{aligned}$$

Squaring both equations and summing them together gives us the unique solution $\theta = \pi$. This means that $z = -1$. For $z = -1$ to be a root, we must have n be an even number. However, n is also the size of the Frobenius kernel, and the size of any Frobenius complement of G is 2. These orders are not coprime [3, 35.234 p. 191], so G cannot exist in this case.

To see that the roots are distinct, assume that there is a repeated root α. Then $P_G(\alpha) = P'_G(\alpha) = 0$. Since $P'_G(z) = n(z^{n-1} + 1)$, the roots of $P'_G(z)$ occur at $e^{\frac{\pi i(2k+1)}{n-1}}$, where k is an integer between 0 and $n-1$.

Thus α must be one of these roots. Inserting this formula into $P_G(z)$ gives

$$\begin{aligned} P_G\left(e^{\frac{\pi i(2k+1)}{n-1}}\right) &= -e^{\frac{\pi i(2k+1)}{n-1}} + ne^{\frac{\pi i(2k+1)}{n-1}} + n - 1 \\ &= (n-1)\left(e^{\frac{\pi i(2k+1)}{n-1}} + 1\right). \end{aligned}$$

Since $n - 1 \neq 0$, $e^{\frac{\pi i(2k+1)}{n-1}} + 1$ must be zero, which implies that $k = \frac{n}{2} - 1$. However, n must be odd and so k cannot be an integer. Thus, by contradiction, no such α can exist.

There exists one root inside the unit circle, since $P_G(-1) = -2$ and $P_G(0) > 0$. To see that this is the only root, assume that there are two roots α_1, α_2 inside the unit circle. Then

$$\alpha_1^n + n\alpha_1 + n - 1 = 0,\ \alpha_2^n + n\alpha_2 + n - 1 = 0.$$

Subtracting these equations gives $(\alpha_1^n - \alpha_2^n) + n(\alpha_1 - \alpha_2) = 0$. Since the roots must be distinct, $\alpha_1 - \alpha_2 \neq 0$, and so we can divide through to get

$$\sum_{j=0}^{n-1} \alpha_1^{n-j-1}\alpha_2^j + n = 0 \implies \left|\sum_{j=0}^{n-1} \alpha_1^{n-j-1}\alpha_2^j\right| = n.$$

But as $|\alpha_i| < 1$, the triangle inequality gives the contradiction

$$n \leqslant \sum_{j=0}^{n-1} \left|\alpha_1^{n-j-1}\alpha_2^j\right| < \sum_{j=0}^{n-1} 1 = n.$$

Thus there must be a unique root inside the circle as required. □

The question of how many real roots lie outside the unit circle can be answered by applying Descartes' rule of signs. We noted earlier a Frobenius group of odd degree has exactly one real root. For a Frobenius group of even degree, there will be 2 changes in sign. Since we can guarantee the existence of one root inside the unit circle, there must be exactly two real roots and so this other real root must be outside the unit circle.

Note that, as the Paley graph has its one real root close to $-2/p$ for large p, that there can be no extension of the 'obvious' zero-free range of the x-axis (namely, positive x). This is in contrast with chromatic polynomials, which have a zero-free region $(0, 1) \cup (1, 32/27]$ in addition to their 'obvious' zero-free region $x < 0$.

Note that, if $q = 2^r$, with $r \geqslant 2$, then the fixed-point polynomial for the action of the maps $x \to ax + b$ with $a, b \in \mathbb{F}_q$ and $a \neq 0$, similarly has a fixed point polynomial $x^q + q(q-2)x + q - 1$ and this has at most two real roots by the rule of signs, and at least two real roots since its value at 0 is positive, its value at -1 is negative and its value at -2 is easily checked by induction to be positive.

Example 5.4 (Mathieu groups)**.** All eight fixed-point polynomials from Mathieu groups M_n have exactly zero real roots if n is even and exactly one if n is odd: the slightly tedious calculations checking this are in [18]. Note that this result, together with the alternating groups having one/two real roots according as n is odd/even, suggest that it is hard to make a link between a group's being simple and the existence of real roots of its fixed point polynomial.

Example 5.5 (Hyperoctahedral Groups)**.** The roots of the fixed-point polynomial for the hyperoctahedral groups can be described with two theorems. Firstly, all roots lie outside the unit circle.

Theorem 5.6. *All roots of $P_{H_n}(x)$ lie outside the unit circle for all $n > 1$.*

Proof. This is equivalent to the claim that $(2n)! < 2^{2n+1}n!^2$, since then $2f_0 > |H_n|$ and so Theorem 2.1 will apply. The claim follows from the fact that $2^{2n} = \sum_{i=0}^{n} \binom{2n}{i} \geqslant \binom{2n}{n}$. □

Secondly, the roots tend toward the unit circle as $n \to \infty$.

Theorem 5.7. *The modulus of the roots of $P_{H_n}(z)$ tends to 1 as $n \to \infty$.*

Proof. Note that $P_{H_n}(z) = f_{2^n} z^{2^n} + f_{2^{n-1}} z^{2^{n-1}} + \cdots + f_2 z^2 + f_0$.

Let α be a root of $P_{H_n}(z)$ for some n. Then

$$|\alpha|^{2^n} = \left| \sum_{i=0}^{2^{n-1}} f_i \alpha^i \right| \leqslant (2^n n! - 1)\, |\alpha|^{2^{n-1}} \leqslant 2^n n!\, |\alpha|^{2^{n-1}} \implies |\alpha| \leqslant (2^n n!)^{\frac{1}{2^{n-1}}}.$$

We show that $\lim_{n\to\infty}(2^n n!)^{\frac{1}{2^{n-1}}}$ exists and is equal to 1. The crude bound $n! < n^n$ and the sandwich rule make it clear it is enough to show that $\lim_{n\to\infty}(2n)^{\frac{n}{2^{n-1}}} = 1$. But for large enough n, $n/(2^{n-1})$ is $\leqslant 1/(2n)$ and it is known that $(2n)^{\frac{1}{(2n)}} \to 1$, so we indeed get the claim. □

There are clearly no real roots in this case.

Example 5.6 (Projective planes)**.** Again, these polynomials have as few real roots as possible and only one root in the unit circle:

Theorem 5.8. *$P_{\mathrm{PG}_2(p)}(x)$ has exactly one root inside the unit circle, and no roots on it for any prime p. There is only the one real root.*

Proof. Showing this claim is equivalent to showing that f_1 dominates the sum of the other f_i, using Theorem 2.1. By Example 6 and manipulation, we have that this boils down to showing that the polynomial $f(x) = x^8 - 2x^7 - x^6 + x^5 + 2x^4 + 3x^3 + 2x$ is positive for all $x \geqslant 2$. This function f has two real roots, one at $x = 0$ and one near $x \approx -1.1258$, and as it is positive for $x = 1$ the result on roots inside D follows. The unique root inside the unit circle is clearly real.

Thus it remains to show that there are no real roots in $(-\infty, -1]$. Again deal with $p = 2, 3, 5$ as special cases, so that $p \geqslant 7$. Suppose instead that the fixed point polynomial had two or more real roots; being of odd degree, it must have at least three. Since exactly one of these has modulus < 1, the other two are less than -1. Thus there must be a root of the derivative of the fixed point polynomial between them (so also < -1). But the derivative of the fixed point polynomial is $(p^2 + p + 1)x^{p^2+p} + (p + 1)f_{p+1}x^p + f_1$. Putting $u = x^p$, there has to be a root $u < -1$ of the polynomial $g(u) = (p^2+p+1)u^{p+1} + f_{p+1}(p+1)u + f_1$. We now claim that this cannot happen. Noting that $(p^2 + p + 1)u^{p+1}$ is positive, we see that we would have to have $f_{p+1}(p + 1)u + f_1 < 0$, i.e. $u < \frac{-f_1}{(f_{p+1}(p+1))}$, which (by MAPLE checking) is $< -p + 1$. But also we must have that $(p^2 + p + 1)u^{p+1} + f_{p+1}(p + 1)u < 0$ and so must have $u > \left(\frac{-f_{p+1}(p+1)}{(p^2+p+1)}\right)^{\frac{1}{p}}$. Now $\frac{-f_{p+1}(p+1)}{(p^2+p+1)} = -p^5 + p^4 + p^3 - p^2 + p + 1 > -p^5$ so $u > -(p^{\frac{1}{p}})^5$. Now $(p^{\frac{1}{p}})$ is decreasing for $p \geqslant 7$ so is always less than $7^{\frac{1}{7}}$ for $p \geqslant 7$: thus we get $u > -(7^{\frac{5}{7}}) > -5$, but we also must have $u < -6$. This contradiction completes the proof. $\square$

Example 5.7 (Bipartite double cover of a stable graph)**.** Regardless of the choice of G, $P_{\tilde{G}}$ possesses no real roots, since it can be written as a sum of even powers of x (plus a positive constant term). We will also have $f_0(\tilde{G}) > \left|\tilde{G}\right|/2$ as long as $\mathrm{Aut}(G)$ contains a derangement. Thus again there are no roots of $P_{\tilde{G}}$ in the unit circle in this case.

The above example, together with the easily checked fact that the fixed-point polynomial for the automorphism group acting on the complete bipartite graph $K_{n,n}$ is $P_{S_n}(x)^2 + n!^2$, and the above results for hypercubes and dihedral groups, plus some other calculations, leave open the possibility that the fixed point polynomial for the full automorphism group of a vertex-transitive bipartite graph acting on that graph has no real roots. We have no counterexample. (Transitivity would be needed: the fixed-point polynomial for $K_{1,n}$ is x times the fixed-point polynomial for S_{n-1} so has a root at $x = 0$ (and one more root if $n-1$ is odd)). It is easy to see that if a transitive permutation group has blocks of imprimitivity of size 2, then its fixed-point polynomial is a polynomial in x^2 so has no real roots: cases covered by this include the automorphisms of a perfect matching, and some other cases above e.g. hypercubes. However we have no proof in general.

Question. Can the fixed point polynomial for the full automorphism group of a vertex-transitive bipartite graph acting on the vertices of the graph have any real roots?

6 Miscellaneous remarks and future topics

We record here that we have also calculated the fixed-point polynomials for the natural actions on $\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(q)$ on 1-dimensional subspaces of $\mathbb{F}_q^2$. For $q > 3$ odd, the polynomials for $\mathrm{PSL}_2(q)$ have no real roots and again roots converge to the unit circle. (for $q = 3$, $\mathrm{PSL}_2(\mathbb{F}_3) \equiv A_4$ so there are two real roots). Similarly for $\mathrm{PGL}_2(q)$ for q odd there are no real roots. For q even, $\mathrm{PSL}_2(q)$ is equal to $\mathrm{PGL}_2(q)$: their fixed point polynomials have at least one real root being of odd degree, and again one can show that there is only one real root. Details are in [18].

Neumann [23] proved various results to the effect that transitive permutation groups (G, Ω) which are not regular have to have $f_i \neq 0$ for some 'not-too-large' i. For example, he shows transitivity and not being regular imply there is some $1 \leqslant i \leqslant \frac{n}{2}$ such that $f_i > 0$, and that this is best possible: that if further G is primitive, there is some $f_i > 0$ with $1 \leqslant i < (n+3)/4$, and that there are infinitely many n for which there is a primitive non-regular group with $f_i = 0$ for $1 \leqslant i < n^{\frac{1}{3}}$, and also has results on the case where (G, Ω) is primitive and soluble.

We have talked so far about doing this for groups acting on sets. However it is possible to apply the same concept to semigroup actions. For example, if we have the full transformation semigroup T_n of all maps from $[n]$ to itself, it is easy to check that

$$P_{T_n,[n]}(x) = \sum_{i=0}^{n} \binom{n}{i} (n-1)^{n-i} x^i = (x + n - 1)^n$$

as there are $\binom{n}{i}$ ways of choosing i points to fix, and $(n-1)^{n-i}$ ways to derange the remaining $n - i$ points. Note that this polynomial is far from irreducible!

When asking about the irreducibility of polynomials, it is natural to ask also 'what is the Galois group of the polynomial?'. In the case of the fixed-point polynomial for S_n acting on $[n]$, Schur showed that the Galois group is S_n if $n \not\equiv 0 \mod 4$ and A_n otherwise. Using [15] we have found some interesting conjectural patterns for various families of fixed-point polynomials, which can be found in [18]. We can use standard techniques for calculating Galois groups to show that, for example, the Galois group of the fixed-point polynomial for each Mathieu group is the whole of S_n.

Note that in general it will be NP-hard to compute the fixed point polynomials: for even in the special case of the automorphism group of a graph acting on its vertex set, the (easier) problem of working out whether or not f_0 is zero or not is known to be NP-complete by a result of Lubiw. We have not yet investigated tractability in special cases, or approximating the values.

We hope to address some of the above areas, plus calculations of the roots for maximal subgroups of S_n and for the somewhat more general situation of the action of finite groups on themselves by conjugation, in a further paper in this series.

Acknowledgement. We are grateful to Peter Cameron for his helpful comments on an earlier draft of this paper and in particular for outlining the construction of reducible

fixed-point polynomials in [8] to us. We also thank two anonymous referees for helpful comments on an earlier draft of this paper.

References

[1] Miklós Abért and Tamás Hubai. Benjamini-Schramm convergence and the distribution of chromatic roots for sparse graphs. Preprint, available at arXiv:1201.3861.

[2] Albrecht Beutelspacher and Ute Rosenbaum. *Projective Geometry: From Foundations to Applications*. Cambridge University Press, 1998.

[3] Michael Aschbacher. *Finite group theory*. Cambridge University Press, 1986.

[4] László Babai. On the order of uniprimitive permutation groups. *Annals of Mathematics*, 113(3):553–568, 1981.

[5] Reinhold Baer. Homogeneity of projective planes. *American Journal of Mathematics*, 64(1):137–152, 1942.

[6] Arrigo Bonisoli. On collineation groups of finite planes. Socrates Intensive Programme: Finite Geometries and Their Applications.

[7] Nigel Boston, Walter Dabrowski, Tuval Foguel, Paul J. Gies, Judy Leavitt, and David T. Ose. The proportion of fixed-point-free elements of a transitive permutation group. *Communications in Algebra*, 21(9):3259–3275, 1993.

[8] Peter J. Cameron. Personal communication.

[9] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, 1999.

[10] L. Carlitz. A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.*, 11:456–459, 1960.

[11] Robin J. Chapman. An involution on derangements. *Discrete Mathematics*, 231:121–122, 2001.

[12] William Y.C. Chen and Richard P. Stanley. Derangements on the n-cube. *Discrete Mathematics*, 115(1-3):65–75, May 1993.

[13] G. Donati. On the system of fixed points of a collineation in noncommutative projective geometry. *Discrete Mathematics*, 255(1–3):65–70, 2002.

[14] Michael Filaseta. A generalization of an irreducibility theorem of I. Schur. *Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam*, 1:317–396, 1996. Edited by B. C. Berndt, H. G. Diamond and A. J. Hildebrand.

[15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[16] Solomon W. Golomb. Powerful numbers. *American Mathematical Monthly*, 77(8):848–852, October 1970.

[17] D. R. Hughes and F. C. Piper. *Projective Planes*. Graduate Texts In Mathematics. Springer-Verlag, 1973.

[18] Christopher Harden. *Fixed-point Polynomials*. PhD thesis, The University of Essex. To appear.

[19] Christopher C. Heyde and Hans-Jürgen Schuh. Uniform bounding of probability generating functions and the evolution of reproduction rates in birds. *Journal of Applied Probability*, 15:243–250, 1978.

[20] Christopher P. Hughes and Ashkan Nikhegbali. The zeros of random polynomials cluster uniformly near the unit circle. *Compositio Mathematica*, 144:734–746, 2008.

[21] Bill Jackson. Zeros of chromatic and flow polynomials of graphs. *J. Geometry*, 76:95–109, 2003.

[22] Attila Maróti. On the orders of primitive groups. *Journal of Algebra*, 258(2):631–640, December 2002.

[23] Peter M. Neumann. *A study of some finite permutation groups*. PhD thesis, The Queen's College, Oxford, April 1966.

[24] Jim Pitman. Probabilistic bounds on the coefficients of polynomials with only real zeros. *Journal of Combinatorial Theory, Series A*, 77(2):279–303, February 1997.

[25] György Pólya and Gabór Szegő. *Aufgaben und Lehrsätze aus der Analysis*. Springer-Verlag, 1964.

[26] Victor V. Prasolov. *Polynomials*. Springer-Verlag, 2001.

[27] László Pyber. On the orders of doubly transitive permutation groups, elementary estimates. *Journal of Combinatorial Theory, Series A*, 62(2):361–366, 1993.

[28] Ed B. Saff and Richard Varga. Zero-free parabolic regions for sequences of polynomials. *SIAM Journal on Mathematical Analysis*, 7(3):344–357, 1976.

[29] Jesús Salas and Alan D. Sokal. Transfer matrices and partition-function zeroes for antiferromagnetic potts models v. further results for the square-lattice chromatic polynomial. *Journal of Statistical Physics*, 144(5):1028–1122, 2011.

[30] David B. Surowski. Stability of arc-transitive graphs. *Journal of Graph Theory*, 38:95–110, 2001.

[31] Koen Thas. Personal communication.

[32] Timothy Vis. Collineations of projective planes.

[33] Cem Yalçın Yıldırım. On the tails of the exponential series. *Canad. Math. Bull*, 37:278–286, 1994.

[34] Stephen M. Zemyan. On the zeros of the Nth partial sum of the exponential series. *The American Mathematical Monthly*, 113:891–909, December 2005.

[35] Yufei Zhao. Integer polynomials, June 2007. yufeizhao.com/olympiad/intpoly.pdf

A Corrigendum (10 Oct 2014)

An error in this paper was pointed out to the first author by Prof. Peter Cameron [personal communication, June 2014]. This error affects Example 3.6 and, by extension, Example 5.6, and does not affect the rest of the paper. Here we present the corrected polynomial, and then give the correct version of Theorem 5.8.

A.1 Collineation group of $\mathbf{PG_2}(p)$

Let us recall the projective plane $\mathrm{PG}_2(p)$, where p is a prime. The point set of points of $\mathrm{PG}_2(p)$ is defined to be equal to the 1-dimensional subspaces of the finite field $\mathbb{F}_p$. Similarly the line set is defined to be equal to the 2-dimensional subspaces of $\mathbb{F}_p$. The incidence relation in this case is inclusion.

In the original paper, we claimed to calculate the fixed point polynomial for the automorphism group of $\mathrm{PG}_2(p)$ acting on $\mathrm{PG}_2(p)$. However, Prof. Cameron pointed out to us that this calculation is inaccurate. In order to correctly calculate the true polynomial, we note that Donati [13, Theorem 7] has classified all collineations by the number of fixed points, for any finite dimensional projective space over a division ring. For our case, we get the following:

Theorem A.1. *The only non-zero f_is for the automorphism group of $\mathrm{PG}_2(p)$ are f_0, f_1, f_2, f_3, f_{p+1}, f_{p+2}, and $f_{p^2+p+1} = 1$.*

The fact that this group is 2-transitive gives us three linear equations in the non-zero f_is. Since there are six unknown f_is we need to find the values of three of coefficients directly. We start with some definitions.

Definition A.2. *Let α be a collineation of $\mathrm{PG}_2(p)$. Then*

- *a point P is fixed if $\alpha(P) = P$.*
- *a line L is fixed if $\alpha(P) \in L$ for all $P \in L$.*
- *a point P is fixed linewise if all lines through P are fixed.*
- *a line L is fixed pointwise if all points on L are fixed.*

Two of the coefficients come from central collineations. We proceed by defining and then counting these central collineations.

Definition A.3. *A collineation α of $\mathrm{PG}_2(p)$ is called a central collineation if it fixes a line L pointwise and a point P linewise. L is called the axis of α, and P is called the centre of α.*

If the centre of a central collineation lies on its axis, then it is called a elation and it fixes $p + 1$ points. Otherwise the centre lies off the axis, which is called a homology and fixes $p + 2$ points. The converse of this statement is also true.

Theorem A.4. *Let $p \geqslant 3$ and α be a non-identity collineation of* $\mathrm{PG}_2(p)$ *that fixes at least $p+1$ points. Then α is a central collineation.*

Proof. If α fixes a line pointwise, then α can fix at most one point not on this line [6, Proposition 2.2]. Thus it is sufficient to prove that α fixes some line pointwise.

Let L be a line that contains as many fixed points of α as possible. L contains at least two fixed points, since α fixes at least two points. If α fixes two points on a line L, then the entire line is fixed [32, Proposition 3(1)]. Thus if α fixes p points on a line L then α fixes the line pointwise. Thus we may assume that L contains at most $p-1$ fixed points.

Assume that L contains three fixed points, R, S, and T. Since α fixes at least $p+1$ points, there exists (at least) two fixed points P and Q that are not on L. The line PQ is fixed, and intersects with L. This intersection point is also a fixed point of α [32, Proposition 3(2)]. If the intersection point is one of the points R, S or T (WLOG R) then consider the points P, Q, S, and T. Otherwise consider the points P, Q, and any two of R, S, and T. By construction, no three of these fixed points of α are collinear. Thus α fixes an entire subplane [17, Corollary to 4.2]. However, the only subplane of $\mathrm{PG}_2(p)$ is itself [17, p83], and thus α is the identity, which is a contradiction.

Thus L must contain at most two fixed points of α, and so no three fixed points are collinear. Since $p+1 \geqslant 4$ there exist four fixed points, no three of which are collinear, and so again α is the identity [17, Corollary to 4.2]. Thus α fixes a line L pointwise by contradiction. ☐

Central collineations are simple to classify. Further, in the case of $\mathrm{PG}_2(p)$ every central collineation that can exist does [5]. We can thus count them to get the values of f_{p+1} and f_{p+2}.

Theorem A.5 ([2, 3.1.3 Lemma])**.** *A central collineation is uniquely determined by its centre, its axis, and the image of any point P distinct from the centre and not lying on the axis.*

There are two cases to consider. The first case is where the centre lies on the axis, which contributes to f_{p+1}, and the second case is where the centre lies off the axis, which contributes to f_{p+2}. There are p^2+p+1 choices for the line L that forms the axis, and so there are p^2 points lying off of L. Let C be the centre of the central collineation and P be a point distinct from C and not lying on L. Then the line between C and P is fixed and the image of P must also be on this line. Now:

- in the first case there are $p+1$ choices for C. Thus there are $p+1-2$ choices for the image of P, since neither C or P can be the image. Thus $f_{p+1} = (p+1)(p-1)(p^2+p+1)$.
- in the second case there are p^2 choices for C. Note that the line L must always intersect the line between C and P, and so there are $p+1-3 = p-2$ choices for the image of P. Thus $f_{p+2} = p^2(p-2)(p^2+p+1)$.

Finally, we will work out f_3. We will do this by considering a related action on ordered triples of distinct points. A triple (P_1, P_2, P_3) is fixed by g in this action if and only if P_1, P_2, and P_3 are all fixed by g in the original action. This action has exactly two orbits.

Theorem A.6. *Let p be a prime, let V_1, V_2, and V_3 be a sequence of distinct points in $\mathrm{PG}_2(p)$, and let U_1, U_2, and U_3 be another sequence of distinct points in $\mathrm{PG}_2(p)$. Then there exists a collineation α such that $\alpha(V_i) = U_i$ for all $1 \leqslant i \leqslant 3$ under either of the following conditions:*

1. *V_1, V_2, and V_3 are non-collinear, and U_1, U_2, and U_3 are non-collinear*
2. *V_1, V_2, and V_3 are collinear, and U_1, U_2, and U_3 are collinear*

Proof. We start with the non-collinear case. All V_is and U_is are 1-dimensional subspaces of $\mathbb{F}_p$. Since the V_is (respectively U_is) are non-collinear, we have that $V_1 \oplus V_2 \oplus V_3 = \mathbb{F}_p$ (respectively $U_1 \oplus U_2 \oplus U_3 = \mathbb{F}_p$). Let x_i (respectively y_i) generate V_i (respectively U_i). Then x_1, x_2, and x_3 is a basis for $\mathbb{F}_p$, and similarly for y_1, y_2, and y_3. Thus there exists a function α which maps the first basis to the second basis, which is our required collineation.

Now consider the collinear case. Let x_1 and x_2 generate V_1 and V_2 respectively, and let y_1 and y_2 generate U_1 and U_2 respectively. Since both sets of points are collinear, the direct sum of the spaces in both cases is a 2-dimensional space. Thus V_3 is generated by a vector of the form $\lambda_1 x_1 + \mu_1 x_2$, and similarly U_3 is generated by a vector of the form $\lambda_2 y_1 + \mu_2 y_2$. We have that λ_1, λ_2, μ_1, and μ_2 are all non-zero, since V_3 must be a 1-dimensional space distinct from V_1 and V_2 (and again for U_3). Thus there exists a function α such that $\alpha(V_1) = U_1$ and $\alpha(V_2) = U_2$. Therefore there exists α that additionally maps $\lambda_1 x_1 + \mu_1 x_2$ to $\lambda_2 y_1 + \mu_2 y_2$, by replacing x_1 and x_2 with a scalar multiple of themselves (which does not affect the vector space generated by x_1 and x_2). ☐

Note that if g fixes less than 3 points in the original action then it will not fix any ordered triple of distinct points. The identity will fix all $(p^2+p+1)(p^2+p)(p^2+p-1)$ ordered triples of distinct points. So we need only consider the two types of central collineations which we counted above.

If the centre of a central collineation lies on the axis then it fixes $p+1$ points in the original action, and so $(p+1)p(p-1)$ points in the action on ordered triples of distinct points. Otherwise it fixes $p+2$ points in the original action, and so $(p+2)(p+1)p$ points in the action on ordered triples of distinct points. Thus by 2-transitivity we have

$$\begin{aligned}
&2p^3(p^2+p+1)(p-1)^2(p+1)\\
&\quad = p(p+1)(p^2+p+1)(p^2+p-1)\\
&\qquad + p^3(p+2)(p+1)(p-2)(p^2+p+1)\\
&\qquad + p(p+1)^2(p-1)^2(p^2+p+1) + 6f_3
\end{aligned}$$

and so we obtain the value of f_3, which is

$$f_3 = \frac{p^3(p-3)(p-2)(p+1)(p^2+p+1)}{6}.$$

With these coefficients, the system of equations is now solvable. This gives us all the coefficients, and so the description of the fixed point polynomial of the collineation group of $\mathrm{PG}_2(p)$ is complete for $p > 2$, which is

$$\begin{aligned}
P_{\mathrm{Aut}(\mathrm{PG}_2(p))}(x) = x^{p^2+p+1} \\
&+ p^2(p-2)(p^2+p+1)x^{p+2} \\
&+ (p+1)(p-1)(p^2+p+1)x^{p+1} \\
&+ \frac{p^3(p-3)(p-2)(p+1)(p^2+p+1)}{6}x^3 \\
&+ p^2(p+1)(p-1)(p-2)(p^2+p+1)x^2 \\
&+ \frac{p(p-1)^2(p^2+p+1)(p^3+2p+2)}{2}x \\
&+ \frac{p^4(p+1)^2(p-1)^2}{3}.
\end{aligned}$$

This formula also works in the special case of $\mathrm{PG}_2(2)$, which can be verified by hand. For completeness, this polynomial is

$$P_{\mathrm{Aut}(\mathrm{PG}_2(2))}(x) = x^7 + 21x^3 + 98x + 48.$$

A.2 Root location for the collineation group of $\mathrm{PG}_2(p)$

The roots of this polynomial follow a common pattern. There is exactly one root inside the unit circle, and all roots tend towards the unit circle. We start with the latter statement.

Theorem A.7. *For all primes p and any $0 < \rho < 1$ there exist only finitely many roots α of $P_{\mathrm{Aut}(\mathrm{PG}_2(p))}(z)$ outside the annulus $1 - \rho \leqslant |\alpha| \leqslant \frac{1}{1-\rho}$.*

Proof. We use Theorem 2.2 in the original paper to note that the probability of a root lying outside this annulus tends towards zero as $p \to \infty$. To see this, note that

$$\lim_{n\to\infty} \frac{2}{n\rho} L_n(P) = \frac{2}{\rho} \lim_{p\to\infty} \frac{1}{p^2+p+1} \log\left(\frac{p^8 - p^6 - p^5 + p^3}{\sqrt{\frac{p^4(p+1)^2(p-1)^2}{3}}}\right) = 0. \qquad \square$$

We will now focus on the real root.

Theorem A.8. *Let p be a prime. Then $P_{\mathrm{PG}_2(p)}(x)$ has exactly one real root.*

Proof. There exists at least one real root, since $p^2 + p + 1$ is odd for all p. So it is enough to show that the derivative is positive for all x. Note that the derivative of the polynomial is

$$
\begin{aligned}
P'_{\mathrm{Aut}(\mathrm{PG}_2(p))}(x) = \frac{p^2+p+1}{2}(&2x^{p(p+1)} + 2p^2(p^2-4)x^{p+1} \\
&+ 2(p-1)(p+1)^2x^p \\
&+ p^3(p-3)(p-2)(p+1)x^2 \\
&+ 4p^2(p-1)(p-2)(p+1)x \\
&+ p(p^3+2p+2)(p-1)^2)
\end{aligned}
$$

Let $p \geqslant 5$. If this derivative becomes negative, it must do so for some $x < 0$. Consider the case where $-1 \leqslant x < 0$. We can split the constant term to become $p^5(p-2)+p(3p^3-2p^2-2p+2)$. The x^2 and x terms together with constant $p^5(p-2)$ form a quadratic with discriminant

$$-4p^4(p+1)(p-2)^2(p^5-3p^4-4p^3+4p^2+4p-4).$$

Since $p \geqslant 5$ the discriminant is negative, and since the quadratic is positive at $x = 0$ it is positive for all x. Thus the only negative term is x^p. Since

$$p(3p^3-2p^2-2p+2) - 2(p-1)(p+1)^2\,|x|$$

is positive for all $|x| \leqslant 1$ and $p \geqslant 5$, we have that the derivative can be written as a sum of positive terms in the range $-1 \leqslant x < 0$, and is thus positive.

Now consider $x < -1$. As before the x^2, x, and constant terms form a quadratic with negative discriminant, and the quadratic is positive at $x = 0$, and thus the only negative term is x^p. However, note that

$$2p^2(p^2-4)\,|x|^{p+1} - 2(p-1)(p+1)^2\,|x|^p = 2\,|x|^p\,(p^2(p^2-4)\,|x| - (p-1)(p+1)^2).$$

Since $p \geqslant 5$ this is positive for all $x < -1$ and so the derivative can be written as a sum of positive terms in the range $x < -1$. Thus the derivative is positive for all $x \in \mathbb{R}$.

We now deal with the remaining special cases. When $p = 2$ we have

$$P_{\mathrm{PG}_2(2)}(x) = x^7 + 21x^3 + 98x + 48$$

and this polynomial has exactly one real root.

Finally, when $p = 3$ we have

$$P_{\mathrm{PG}_2(3)}(x) = x^{13} + 117x^5 + 104x^4 + 936x^2 + 2730x + 1728.$$

The derivative of this polynomial is

$$P'_{\mathrm{PG}_2(3)}(x) = 13x^{12} + 585x^4 + 416x^3 + 1872x + 2730$$

and since this is positive for all x, $P_{\mathrm{PG}_2(p)}(x)$ has one exactly real root for all primes p as required. □

Theorem A.9. *Let p be a prime. Then $P_{\mathrm{PG}_2(p)}(x)$ has exactly one real root α, and this root lies inside the unit circle.*

Proof. For this statement it is sufficient to prove that $P_{\mathrm{PG}_2(p)}(-1)$ is negative for all primes p. Firstly, let $p = 2$. Then $P_{\mathrm{PG}_2(2)}(-1) = -72$ which is negative as required.

Now consider $p > 2$. Then p is odd, and so we get that

$$P_{\mathrm{PG}_2(p)}(-1) = -\frac{(p+1)(p-1)^2(p^5 - 5p^4 + 3p^3 + 6p^2 + 12p + 6)}{3}.$$

It is thus sufficient to prove that the quintic is positive for all $p > 2$. We note that the quintic evaluated at $p = 3$ is equal to 15. Since the quintic has no positive real root, it must be positive for all positive p, and in particular for all $p > 2$ as required. $\square$