Fixed points and cycles

Peter J. Cameron

This paper presents a tapas of results on fixed points and cycles in permutation groups, arising in such disparate areas as matrix group recognition, Brauer groups, Latin squares, and relational databases.

1 Fixed points and orbits

The Orbit-Counting Lemma asserts that the number of orbits of a finite permutation group is equal to the average number of fixed points of its elements (or, in different language, the expected number of fixed points of a random element of the group). In this section, I discuss various extensions of this result.

1.1 A theorem of Boston *et al.*

A *derangement* in a permutation group G (a subgroup of the symmetric group S_n) is an element of G with no fixed points. It is well known that the probability that a random element of the symmetric group S_n is a derangement is very close to 1/e. This was generalised by Boston *et al.* [3] as follows:

Theorem 1.1 *Let G be a subgroup of S_n. For $0 \leq i \leq n$, let p_i be the probability that a random element of G fixes exactly i points, and F_i be the number of orbits of G acting on the set of i-tuples of distinct points. Then the sequences $(p_0, \ldots, p_n)$ and $(F_0, \ldots, F_n)$ determine each other: more precisely, if*

$$P(x) = \sum_{i=0}^{n} p_i x^i \qquad \textit{and} \qquad F(x) = \sum_{i=0}^{n} F_i x^i / i!\,,$$

then we have

$$F(x) = P(x+1).$$

In particular, the probability that a random element of G is a derangement is

$$F(-1) = \sum_{i=0}^{n} (-1)^i F_i / i!\,.$$

Proof Here is the simple proof of this result. The number of elements with i fixed points is $p_i|G|$, and each fixes $i(i-1)\cdots(i-j+1)$ ordered j-tuples of distinct elements. By the Orbit-Counting Lemma,

$$F_j = \sum_{i=0}^{n} p_i i(i-1)\cdots(i-j+1).$$

Multiply by $x^j/j!$, sum over j, reverse the order of summation, and use the Binomial Theorem to give the result. The last line follows from the fact that the probability that a random element is a derangement is $p_o = P(0) = F(-1)$. $\square$

This result is useful because often it is easier to calculate the numbers F_i than the p_i. Boston *et al.* [3] give several examples. Most easily, if $G = S_n$, then $F_i = 1$ for $0 \le i \le n$, and so $F(x)$ is the truncated exponential series; this easily gives the classical formula for the number of derangements.

Independently of Theorem 1.1, Cameron and Cohen [7] have proved lower bounds for the proportion of derangements in a permutation group G in terms of its degree and rank.

1.2 Infinite permutation groups

The probability that an element of an infinite permutation group fixes i points has no meaning. We cannot just count, and the symmetric group is not compact in any natural topology so there is no finite Haar measure. However, sometimes the other side of the equation in Theorem 1.1 makes sense.

An infinite permutation group G on a set Ω is said to be *oligomorphic* if G has only finitely many orbits on Ω^n. For an oligomorphic group G, the numbers F_i are defined for all $i \geq 0$, and $F(x)$ exists as a formal power series (though it may not converge anywhere except the origin).

If $F(-1)$ exists, or can be defined by analytic continuation or some other summation method, then it is a parameter of the infinite group playing the role of the "proportion of derangements". It is not at all clear what this parameter means.

For example, if G is the infinite symmetric group, then $F_i = 1$ for all i, and $F(x) = \mathrm{e}^x$. So $F(-1) = 1/\mathrm{e}$, which happens to be the limiting proportion of derangements in finite symmetric groups.

More striking is the group of all order-preserving permutations of $\mathbb{Q}$. It is easy to see that $F_i = i!$ for this group, so that

$$F(-1) = 1 - 1 + 1 - 1 + 1 - \cdots$$

As Euler remarked, the sum of this series is $\frac{1}{2}$ (for example, by analytic continuation, since $F(x) = 1/(1-x)$ is defined everywhere except at $x = 1$). There is no obvious sense in which half of the elements of this group are derangements!

1.3 Linear groups

The problem of counting derangements in linear or other classical groups has been considered by Neumann and Praeger [20, 21] in connection with matrix group recognition algorithms. Many results about permutation groups have analogues for linear groups. This is the case for Theorem 1.1; so in principle we can calculate the proportion of derangements in any linear group.

Theorem 1.2 *Let G be a subgroup of the general linear group $\mathrm{GL}(n,q)$. For $0 \leq i \leq n$, let P_i be the probability that the fixed points of a random element of G form an i-dimensional subspace, and L_i be the number of orbits of G acting on the set of linearly independent i-tuples. Then the sequences $(P_0, \ldots, P_n)$ and $(L_0, \ldots, L_n)$ determine each other.*

Proof We consider G as a permutation group on the set of q^n vectors of the n-dimensional vector space over $\mathrm{GF}(q)$. Since the fixed points of any element form a subspace, the probabilities p_i of Theorem 1.1 are given by

$$p_i = \begin{cases} P_j & \text{if } i = q^j, \\ 0 & \text{otherwise.} \end{cases}$$

By the theorem, the numbers F_i of G-orbits on i-tuples are determined for all $i \leq q^n$.

Let F_i^* be the number of orbits of G on all i-tuples (elements not necessarily distinct. Then (see Cameron and Taylor [9]),

$$F_i^* = \sum_{j=1}^{i} S(i,j) F_j,$$

where the $S(i,j)$ are *Stirling numbers of the second kind.* In terms of generating functions, if $F^*(x) = \sum F_i^* x^i / i!$, then we have

$$F^*(x) = F(\mathrm{e}^x - 1).$$

This statement has an analogue for linear groups, also found in [9]: if L_i is the number of orbits on linearly independent i-tuples, then

$$F_i^* = \sum_{j=0}^{i} \begin{bmatrix} i \\ j \end{bmatrix}_q L_j.$$

Note that the Gaussian coefficients play the role of q-analogues of the Stirling numbers here. This is because set partitions (counted by Stirling numbers) are the "kernels" of surjective set mappings; the kernel of a linear mapping is completely determined by a single subspace (the corresponding partition being into cosets of that subspace.)

So the numbers L_i determine the F_i^*, and hence the F_i, and hence the P_i; and conversely. $\square$

After this roundabout argument, it is natural to ask if a more direct approach exists. First we require some notation. For any positive integer n and indeterminate q, we define the q-analogues of factorials and powers by

$$\begin{aligned} [n]!_q &:= (q^n - 1)(q^{n-1} - 1) \cdots (q - 1), \\ [1 + x]_q^{[n]} &:= (1 + x)(1 + qx) \cdots (1 + q^{n-1} x). \end{aligned}$$

The *q-binomial theorem* asserts that

$$[1+x]_q^{[n]} = \sum_{i=0}^{n} q^{i(i-1)/2} \begin{bmatrix} n \\ i \end{bmatrix}_q x^i.$$

Theorem 1.3 *Let G be a subgroup of* $\mathrm{GL}(n,q)$*, and let the numbers P_i, L_i be as defined earlier. Then*

$$\sum_{i=0}^{n} \frac{L_i x^i}{[i]!_q} = \sum_{j=0}^{n} P_j [1+x]_q^{[j]}.$$

Proof The proof is the q-analogue of the argument of Boston *et al.* By the Orbit-Counting Lemma we have

$$L_i = \sum_{j=i}^{n} P_j (q^j - 1) \cdots (q^j - q^{i-1}).$$

Multiply both sides by $x^i/[i]!_q$, sum over i, and use the q-binomial theorem. □

This relation can be inverted, to give the P_j explicitly in terms of the L_i. The last displayed equation in the proof can be written as

$$\frac{L_i}{|\,\mathrm{GL}(i,q)|} = \sum_{j=i}^{n} \begin{bmatrix} j \\ i \end{bmatrix}_q P_j,$$

and Möbius inversion over the lattice of subspaces of the projective space (see Rota [22]) gives

Theorem 1.4 *With the hyptheses of Theorem 1.3,*

$$P_i = \sum_{j=i}^{n} (-1)^{j-i} q^{(j-i)(j-i-1)/2} \begin{bmatrix} j \\ i \end{bmatrix}_q \frac{L_j}{|\,\mathrm{GL}(j,q)|}.$$

(I am grateful to Thomas Müller and Shahn Majid for conversations about this.)

Note that, as in the permutation group case, the numbers L_i are often easier to calculate than the P_i. For example, if $G = \mathrm{GL}(n,q)$, then $L_i = 1$ for all $i \leq n$.

The calculation of the L_i is also possible for the classical groups, but the arguments are a bit more complicated. I give details for the symplectic group $\mathrm{Sp}(2m, q)$ in the next subsection as an example.

Problem Calculate the numbers L_i for the "large" linear groups constituting the Aschbacher classes [1].

One could also ask for a similar analysis for projective groups. Note that a fixed point of an element of $\mathrm{PGL}(n, q)$ is spanned by an eigenvector of a correponding element of $\mathrm{GL}(n, q)$. There is a simple characterisation of the numbers of fixed points of elements of $\mathrm{PGL}(n, q)$: the integer m is the number of fixed points of an element of $\mathrm{PGL}(n, q)$ if and only if, when m is written in base q, the digits are non-decreasing and have sum at most n.

1.4 The symplectic group

As promised, in this section the number P_i of orbits on linearly independent i-tuples is computed for the symplectic group $\mathrm{Sp}(2m, q)$.

First note that, by Witt's Lemma [23, p.57],

> Two linearly independent i-tuples $(v_1, \ldots, v_i)$ and $(w_1, \ldots, w_i)$ lie in the same orbit of $G = \mathrm{Sp}(2m, q)$ if and only if the skew-symmetric matrices $(B(v_j, v_k))$ and $(B(w_j, w_k))$ are equal, where B is the form preserved by G.

So we must count the possible Gram matrices of linearly independent i-tuples. First, we decide which matrices are representable.

> An $i \times i$ skew-symmetric matrix of rank $2r$ is the Gram matrix of a linearly independent set in $V(2m, q)$ if and only if $\max\{0, i - m\} \leq r \leq \min\{\lfloor i/2 \rfloor, m\}$.

For clearly $r \geq 0$; and the span of the given vectors has a totally isotropic subspace of dimension $(i - 2r) + r = i - r$, and this cannot exceed m. Moreover, the rank cannot exceed either i or $2m$. For the converse, note first that the condition implies that $i \leq 2m$. It is enough to deal with skew-symmetric matrices in 'standard form'. If $0 \leq r \leq m$ and $i - r \leq m$, then the vectors $e_1, f_1, \ldots, e_r, f_r, e_{r+1}, \ldots, e_{i-r}$ have the required Gram matrix.

Now to count the matrices:

(a) The number of $2r \times 2r$ skew-symmetric matrices of rank $2r$ is

$$N_r := q^{r(r-1)} \prod_{j=1}^{r} (q^{2j-1} - 1).$$

(b) The number of $i \times i$ skew-symmetric matrices of rank $2r$ is

$$M_{i,r} := \begin{bmatrix} i \\ 2r \end{bmatrix}_q N_r$$

for $2r \leq i$.

Here (a) is the number of symplectic forms, most easily computed as the index of $\mathrm{Sp}(2r, q)$ in $\mathrm{GL}(2r, q)$ (see [23, pp.19, 70]); for (b), we choose the null space in $\left[\begin{smallmatrix} i \\ i-2r \end{smallmatrix}\right]_q$ ways, and a symplectic form on the quotient in N_r ways.

We conclude that

$$L_i = \sum_{r=\max\{0,i-m\}}^{\min\{\lfloor i/2 \rfloor, m\}} M_{i,r}.$$

In particular, $L_i = q^{i(i-1)/2}$ for $i \leq m$, and of course $L_i = 0$ for $i \geq 2m$.

1.5 Cycles

In fact Theorem 1.1 is a special case of a much older result. Suppose we are interested in not just the number of fixed points but the cycle structure (the number of cycles of each length) of a random element of G. The probability generating function for this is

$$\frac{1}{|G|} \sum_{g \in G} s_1^{c_1(g)} s_2^{c_2(g)} \cdots,$$

where $s_1, s_2, \ldots$ are indeterminates, and $c_i(g)$ is the number of i-cycles of the element g. This is just the familiar Redfield–Pólya *cycle index*, whose role in orbit-counting is well-known.

In particular, it is known that $F(x)$ (the exponential generating function for orbits of G on ordered i-tuples) is obtained from the cycle index by the substitution $s_1 \leftarrow x+1$, $s_i \leftarrow 1$ for $i > 1$ (which yields Theorem 1.1). A related result is that the ordinary generating function for the number of orbits of G on unordered i-sets (that is, the polynomial $f(x) = \sum f_i x^i$, where f_i is the number of orbits of G on i-sets), is also a specialisation of $Z(G)$, obtained by the substitution $s_i \leftarrow x^i + 1$ for all i.

Some authors (see for example [17, 12]) have considered extensions of the cycle index to linear groups. This would have obvious applications to the material of the preceding section.

2 Cycle partitions

The cycles of a permutation form a partition. So there is a map C from S_n to the set P_n of partitions of $\{1, \ldots, n\}$, which is onto but not one-to-one. Alberto Leporati (personal communication), in connection with work on database query languages [2], asked; what do we know about a permutation group G if we are given the set $C(G)$ of cycle partitions of its elements? I will report briefly on some results, which are discussed more fully in [6].

Theorem 2.1 *The set $C(G)$ determines*

(a) the order of G;

(b) the multiset $C(G)$ (that is, for each $\pi \in P_n$, the number of $g \in G$ with $C(g) = \pi$ is determined);

(c) the cycle index $Z(G)$.

It does not determine G, even up to isomorphism as an abstract group. □

The last assertion is due to Eamonn O'Brien (personal communication), who found two pairs of permutation groups with the same set of cycle partitions (all these groups have degree 16 and order 64).

There is also a recognition problem: given a subset X of P_n, is there a subgroup G of S_n with $C(G) = X$? It is not reasonable to ask whether this problem has a polynomial-time solution, since the input is potentially exponentially large. P. Kolaitis (personal communication) suggested the *polynomial delay model*, where we are allowed to perform a polynomial-time computation after reading each element of the input X. Now the analogues of asking if the problem is in P or NP in this model are as follows,, where 'polynomial' means 'polynomial in n':

(a) Is there an algorithm which decides, with polynomial delay, whether $X = C(G)$ for some group G?

(b) Is the a polynomial-length certificate for a set X, knowing which we can verify the existence of G such that $X = C(G)$ with a polynomial-delay computation?

The certificate in (b) might be a generating set for G. (It is known that any subgroup of S_n can be generated by $n/2$ elements if $n > 2$: see McIver and Neumann [19].)

The question posed in this section makes sense for infinite groups as well. One particular problem is worth stating. It follows from Theorem 2.1(a) that, if H is a subgroup of the finite permutation group G with $C(H) = C(G)$, then in fact $H = G$.

Problem Does the above assertion hold also for infinite permutation groups?

3 Derangements of prime order

The Orbit-counting Lemma immediately implies that a transitive finite permutation group of degree greater than 1 contains a derangement. (The average number of fixed points is equal to 1, and the identity fixes more than one point, so some element fixes fewer than one.) Much more difficult is the following result of Fein *et al.* [11], whose proof uses the Classification of Finite Simple Groups:

Theorem 3.1 *A finite transitive permutation group of degree greater than* 1 *contains a derangement of prime power order.* $\square$

These authors also gave an example to show that the theorem is false if 'prime power' is replaced by 'prime'. Let $G = \mathrm{AGL}(1, p^2)$ and $H = \mathrm{AGL}(1, p)$, where p is a Mersenne prime. Consider G as a permutation group on the cosets of H (equivalently, $G \leq \mathrm{AGL}(2,p)$ acting on the set of lines of the affine plane). The degree is $p(p+1)$, so the only possible prime orders of derangements are 2 and p; and it is easily seen that any conjugacy class of elements of order 2 or p in G meets H, so that all such elements have fixed points.

A permutation group is called *elusive* if it is transitive and has no derangement of prime order. Not many such groups are known. The most surprisingly overlooked example is the Mathieu group M_{11} in its action of degree 12, found recently by Michael Giudici. A number of examples and constructions are presented in [8], including another sporadic example of structure $7^3 : (3^{1+2} : Q_8)$. (The translation complement, taken projectively, is the group of the nine inflexion points of a cubic in the plane of order 7. For us, this group acts as an elusive permutation group of degree 84.) In the direction of characterisations, Giudici [15] has shown:

Theorem 3.2 *Any quasiprimitive elusive group is isomorphic to a wreath product $M_{11} \wr K$, for some transitive permutation group K of degree k, in its product action of degree 12^k.* □

(A permutation group G is *quasiprimitive* if every non-trivial normal subgroup of G is transitive.)

Part of the motivation for studying elusive groups is a conjecture first stated by Marušič and in the present form by Klin, asserting that there is no 2-closed elusive group. (A permutation group $G \leq S_n$ is 2-*closed* if every permutation in S_n which preserves all the orbits of G on ordered pairs belongs to G.)

The automorphism group of a graph, possibly directed and edge-coloured, is necessarily 2-closed. Moreover, if a graph Γ on n vertices has an automorphism g which is a derangement of prime order, then we can get information about Γ by studying a quotient $\Gamma/\langle g\rangle$ on n/p vertices. Our study has turned up no counterexamples to this conjecture.

The set of degrees of elusive groups is multiplicatively closed.

Problem Does the set of degrees of elusive groups have density zero?

Either this question or Klin's conjecture might be settled with less than a complete classification of elusive groups. The known degrees below 100 of elusive groups are 12, 24, 36, 48, 56, 72, 84 and 96.

4 Derangements and Latin squares

Dixon [10] proved that almost all pairs of elements of the symmetric group S_n generate either S_n or A_n (in the sense that the probability that a randomly-chosen pair of elements generates a smaller subgroup tends to zero as $n \to \infty$). Recently, Łuczak and Pyber [18] proved a theorem from which Dixon's result follows. The interpretation of 'almost all' is as just described.

Theorem 4.1 *Almost all elements of S_n lie in no proper transitive subgroup of S_n except possibly A_n.* □

The easier part of the proof of Dixon's theorem is the fact that almost all pairs of elements generate a transitive subgroup; then the conclusion is immediate from Theorem 4.1.

The theorem has another application, to a new proof of the result of [4].

Theorem 4.2 *The rows of a random Latin square of order n, regarded as permutations, almost surely generate S_n.*

Proof The group generated by the rows of a random Latin square is obviously transitive, and the first row is a random permutation (that is, all permutations occur equally often as the first row of a Latin square). The alternating group is excluded by a result of Häggkvist and Janssen [16], according to which the proportion of Latin squares for which all rows are even permutations is exponentially small. □

Problem Does the conclusion of Theorem 4.2 also hold for random *normalised* Latin squares, those for which the first row and column are equal to the identity permutation?

The second row of a normalised Latin square is a derangement. It follows from Theorem 4.1 and the fact that derangements have non-zero probability that almost all derangements lie in no proper subgroup of S_n except possibly A_n. However, this does not settle the question, since derangements do not occur equally often as the second row of normalised Latin squares. Indeed, random normalised Latin squares define a probability measure on derangements, and the problem above asks whether the analogue of Theorem 4.1 holds for this measure.

5 Other topics

Two further topics will be considered here only briefly.

A permutation group G is *cycle closed* if it contains all the cycles of its elements. The finite cycle closed groups are direct products of symmetric groups and cyclic groups of prime order, and it is known that from any permutation group we reach a cycle-closed group in at most three steps (each step consisting of taking the group generated by the cycles of the given group). Interesting open problems remain for infinite groups. See [5] for further information.

The *Parker vector* of a permutation group $G \leq S_n$ is the sequence $(P_1, \ldots, P_n)$, where P_i is the number of orbits of G on the set $\mathcal{C}_i(G)$ of all i-cycles occurring in elements of G (the action is by conjugation). The Parker vector contains some information about the group, and is closely connected with the cycle index, from which it can be calculated. See Gewurz [13, 14] for further information on this topic.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[2] P. Bonizzoni, G. Della Vedova, A. Leporati, D. Lucarella and G. Mauri, A unifying framework to characterize the power of query languages, preprint.

[3] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leavitt, D. T. Ose and D. A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, *Commun. Algebra* **21** (1993), 3259–3275.

[4] P. J. Cameron, Almost all quasigroups have rank 2, *Discrete Math.* **106/107** (1992), 111–115.

[5] P. J. Cameron, Cycle-closed permutation groups, *J. Algebraic Combinatorics* **5** (1996), 315–322.

[6] P. J. Cameron, Partitions and permutations, preprint.

[7] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements of a permutation group, *Discrete Math.* **106/107** (1992), 135–138.

[8] P. J. Cameron, M. R. Giudici, G. A. Jones, W. M. Kantor, M. Klin, D. Marušič and L. A. Nowitz, Transitive permutation groups without semiregular subgroups, in preparation.

[9] P. J. Cameron and D. E. Taylor, Stirling numbers and affine equivalence, *Ars Combinatoria* **20B** (1985), 3–14.

[10] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[11] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[12] H. Fripertinger, Cycle indices of linear, affine, and projective groups, *Linear Algebra Appl.* **263** (1997), 133–156.

[13] D. A. Gewurz, Reconstruction of permutation groups from their Parker vectors, *J. Group Theory*, to appear.

[14] D. A. Gewurz, Parker vectors and cycle indices of permutation groups, in preparation.

[15] M. R. Giudici, Quasiprimitive permutation groups without semiregular subgroups, in preparation.

[16] R. Häggkvist and J. C. M. Janssen, All-even latin squares, *Discrete Math.* **157** (1996), 199–206

[17] J. P. S. Kung, The cycle structure of a linear transformation over a finite field, *Linear Algebra Appl.* **36** (1981), 141–155.

[18] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combinatorics, Probability & Computing* **2** (1993), 505–512.

[19] A. McIver and P. M. Neumann, Enumerating finite groups, *Quart. J. Math.* (2) **38** (1987), 473–488.

[20] P. M. Neumann and C. E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc.* (3) **65** (1992), 555–603.

[21] P. M. Neumann and C. E. Praeger, Derangements and eigenvalue-free elements in finite classical groups, *J. London Math. Soc.* (2) **58** (1999), 564–586.

[22] G.-C. Rota, On the foundations of combinatorial theory, I: Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2** (1964), 340–368.

[23] D. E. Taylor, *The Geometry of the Classical Groups*, Helderman, Berlin, 1992.

Peter J. Cameron
School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS
United Kingdom
`p.j.cameron@qmw.ac.uk`