Elusive groups and the polycirculant conjecture

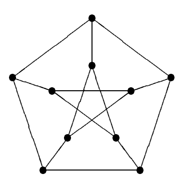
Peter J. Cameron

Queen Mary, University of London

p.j.cameron@qmw.ac.uk

Barcelona, February 2001

The Petersen graph



Norman Biggs' notation for this graph is as follows:

Three remarkable graphs

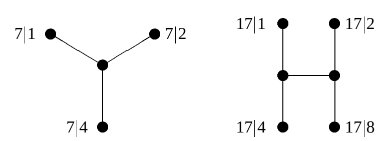
N. L. Biggs, Three remarkable graphs, *Canad. J. Math.* **25** (1973), 397–411.

There are exactly three graphs which are

- trivalent,
- distance-transitive,
- vertex-primitive,
- not K_4.

They are the Petersen graph, the Coxeter graph, and the Biggs–Smith graph. The second and third are shown on the next slide.

Three remarkable graphs



These graphs, with 10, 28 and 102 vertices respectively, are called I, Y and H by Biggs for obvious reasons.

Semiregular automorphisms

An automorphism of a graph is *semiregular* if it permutes the vertices in cycles of the same length.

Biggs' graphs I, Y, H have semiregular automorphisms of order 5, 7 and 17 respectively.

As these examples show, the existence of a semiregular automorphism may lead to a very compact description of a graph.

The polycirculant conjecture

A graph is called a *circulant* if it has an automorphism permuting the vertices in a single cycle. More generally, a graph is a *polycirculant* if it has a non-identity semiregular automorphism.

For example, the Petersen graph is a polycirculant, but not a circulant.

The following conjecture is due to D. Marušič, *Discrete Math.* **36** (1981), 69–81, and independently to D. Jordan, *Dresdner Reihe Forsch.* **9** (1988).

The polycirculant conjecture: *Every vertex-transitive finite graph is a polycirculant.*

2-closure and Klin's conjecture

Let G be a permutation group on a set Ω. The 2-*closure* of G is the set of all permutations p of Ω with the property that, for any two points $\alpha,\beta\in\Omega$, there exists $g\in G$ such that $(\alpha,\beta)p=(\alpha,\beta)g$. That is, it is the largest permutation group which has the same orbits on 2-sets as G does.

A permutation group is 2-*closed* if it is equal to its 2-closure.

The automorphism group of a (di)graph is 2-closed. The converse is false.

M. Klin, BCC Problem 15.12, generalised the polycirculant conjecture as follows:

Conjecture: *Every transitive 2-closed finite permutation group of degree greater than 1 contains a non-identity semiregular element.*

Fixed-point-free permutations

The context of Klin's conjecture is the following old theorem of C. Jordan in 1872:

Theorem 1 *Every transitive finite permutation group of degree greater than 1 contains a non-identity fixed-point-free element.*

The proof is elementary. By the Orbit-counting Lemma, the average number of fixed points of the elements of G is equal to 1. But the identity has more than one fixed point; so some element has less than one.

Fixed-point-free elements, continued

B. Fein, W. M. Kantor and M. Schacher, *J. Reine Angew. Math.* **328** (1981), 39–57, improved Jordan's Theorem:

Theorem 2 *Every transitive finite permutation group of degree greater than* 1 *contains a non-identity fixed-point-free element of prime-power order.*

Sketch proof: There is an elementary reduction to the case where G is a simple group. Then apply the Classification of Finite Simple Groups and analyse in detail the various cases. The proof is definitely not "elementary"!

Note that, to prove Klin's conjecture, it would suffice to replace "prime-power" by "prime" in this theorem. However, this is false, though examples are not very common.

Elusive permutation groups

A transitive permutation group is said to be *elusive* if it contains no non-trivial semiregular element (equivalently, no fixed-point-free element of prime order).

Our attack on Klin's conjecture is:

- Try to determine the elusive permutation groups.
- Check whether these groups can be 2-closed.

The advantage is that previous attempts fail because we don't know enough about what extra properties a 2-closed group must have.

Examples of elusive groups

Example Let p be a Mersenne prime. The field $\mathrm{GF}(p^2)$ can be identified with the affine plane over $\mathrm{GF}(p)$. Let

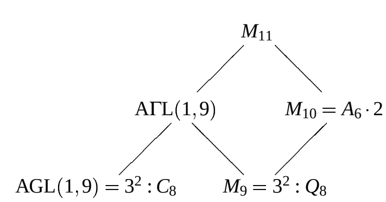
$$G = \mathrm{AGL}(1,p^2) = \{x \mapsto ax+b : a,b \in \mathrm{GF}(p^2), a \neq 0\}$$

acting on the $p(p+1)$ lines of $\mathrm{AG}(2,p)$. The only primes dividing $p(p+1)$ are 2 and p; elements of order p are translations, and so have fixed lines; elements of order 2 clearly have fixed lines.

Example The Mathieu group M_{11} has an action on 12 points, in which it is 3-transitive. Inspection of the character table shows that no element of order 2 or 3 is fixed-point-free.

Elusive groups of degree 12

All elusive groups of degree 12 are conjugate to subgroups of M_{11}, and together with their inclusions are shown in the diagram below.



Degrees of elusive groups

Many more examples exist. Rather than describing the constructions in detail, I sketch what is known about the degrees of elusive groups.

- The set of degrees of elusive groups is multiplicatively closed.
- For any Mersenne prime p, any positive integer n, and any number m such that $2^m > p$, there is an elusive group of degree $2^m p^n$. These arise from the examples of degree $p(p+1)$ by means of a doubling construction and a Hensel lift.
- There is a *sporadic* elusive group of degree 84, from which examples of degree $7^n \cdot 12$ can be constructed for all $n > 0$.

Degrees of elusive groups

The numbers less than 100 which are known to be degrees of elusive groups are

$$12, 24, 36, 48, 56, 72, 84, 96.$$

Problem: Is it true that the set of degrees of elusive groups has density zero?

Remark: None of the known constructions of elusive groups produces an example which is 2-closed.

Characterisations

Theorem 3 *(Giudici) A primitive elusive permutation group is isomorphic to the wreath product $M_{11} \wr K$, for some transitive permutation group K (and so has degree 12^k).*

More generally, Giudici has found all elusive groups which have a transitive minimal normal subgroup: the list is the same.

Giudici has also determined the elusive groups which have a non-soluble minimal normal subgroup. The complete determination of elusive groups has not yet been found.

Isbell's conjecture

This problem arises in game theory. Von Neumann and Morgenstern analysed so-called *simple n-person* games by the family of *winning coalitions*, sets of players who can force a win if they cooperate. This family has the following obvious properties:

- A superset of a winning coalition is a winning coalition.
- A set is a winning coalition if and only if its complement is not a winning coalition.

An n-person game is obviously fair if there is a group of symmetries of the game which permutes the players transitively. Call such a game *symmetric*. For which n do symmetric simple n-person games exist?

Isbell's conjecture

Isbell (1959) noted that a symmetric simple n-person game exists if and only if there is a transitive permutation group of degree n which contains no fixed-point-free element of 2-power order. In 1960 he conjectured that such a group exists if and only if $n = 2^a \cdot b$, where b is odd and a is sufficiently large in terms of b.

Note that, by Fein–Kantor–Schacher, there is always a fixed-point-free element of some prime power order. It seems plausible that, if the prime 2 dominates the degree, then we can choose this prime to be 2. In this form, the conjecture can be extended to any prime in place of 2.

However, after more than 40 years and CFSG, the conjecture is still wide open!

A related question

As is well known, the proportion of derangements (fixed-point-free elements) in the symmetric group is very close to $1/\mathrm{e}$.

No such result is true for arbitrary transitive groups. However, Cameron and Cohen showed that the proportion of fixed-point-free elements in a transitive group of degree n is at least $1/n$. Moreover, if equality holds, then the group is sharply 2-transitive, and hence n is a power of a prime p and every fixed-point-free element in G has order p.

Problem: Find a lower bound, in terms of n, for the proportion of fixed-point-free elements of prime power order in a transitive permutation group of degree n.