Derangements and p-elements in permutation groups

Peter J. Cameron

Queen Mary University of London

p.j.cameron@qmul.ac.uk

Groups and their Applications
Manchester, 14 February 2007

In the beginning . . .

A derangement is a permutation with no fixed points.

In the beginning . . .

A derangement is a permutation with no fixed points.

1. The proportion of derangements in the symmetric group S_n is approximately $1/e$.
More precisely, the number of derangements in S_n is the nearest integer to $n!/e$.

In the beginning . . .

A derangement is a permutation with no fixed points.

1. The proportion of derangements in the symmetric group S_n is approximately $1/\mathrm{e}$.
More precisely, the number of derangements in S_n is the nearest integer to $n!/\mathrm{e}$.

2. (Jordan) A transitive permutation group of degree $n > 1$ contains a derangement.
In fact (Cameron and Cohen) the proportion of derangements in a transitive group G is at least $1/n$.
Equality holds if and only if G is sharply 2-transitive, and hence is the affine group $\{x \mapsto ax + b : a, b \in F, a \neq 0\}$ over a nearfield F.

In the beginning ...

A derangement is a permutation with no fixed points.

1. The proportion of derangements in the symmetric group S_n is approximately $1/\mathrm{e}$.
More precisely, the number of derangements in S_n is the nearest integer to $n!/\mathrm{e}$.

2. (Jordan) A transitive permutation group of degree $n > 1$ contains a derangement.
In fact (Cameron and Cohen) the proportion of derangements in a transitive group G is at least $1/n$.
Equality holds if and only if G is sharply 2-transitive, and hence is the affine group $\{x \mapsto ax + b : a, b \in F, a \neq 0\}$ over a nearfield F.

The finite nearfields were determined by Zassenhaus. They all have prime power order.

Why do we care?

The presence of derangements in a permutation group has important implications in number theory and topology. See Serre's beautiful paper "On a theorem of Jordan", in *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

Why do we care?

The presence of derangements in a permutation group has important implications in number theory and topology. See Serre's beautiful paper "On a theorem of Jordan", in *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

- Let f be an integer polynomial of degree $n > 1$, irreducible over $\mathbb{Q}$. Then f has no roots mod p for infinitely many primes p (indeed, for at least a proportion $1/n$ of all primes).

Why do we care?

The presence of derangements in a permutation group has important implications in number theory and topology. See Serre's beautiful paper "On a theorem of Jordan", in *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

- Let f be an integer polynomial of degree $n > 1$, irreducible over $\mathbb{Q}$. Then f has no roots mod p for infinitely many primes p (indeed, for at least a proportion $1/n$ of all primes).
- Let $\pi : T \to S$ be a covering map of degree $n \geq 2$, and suppose that T is arcwise connected but not empty. Then there is a continuous closed curve in S which cannot be lifted to T.

Why do we care?

The presence of derangements in a permutation group has important implications in number theory and topology. See Serre's beautiful paper "On a theorem of Jordan", in *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

- Let f be an integer polynomial of degree $n > 1$, irreducible over $\mathbb{Q}$. Then f has no roots mod p for infinitely many primes p (indeed, for at least a proportion $1/n$ of all primes).
- Let $\pi : T \to S$ be a covering map of degree $n \geq 2$, and suppose that T is arcwise connected but not empty. Then there is a continuous closed curve in S which cannot be lifted to T.
- The Fein–Kantor–Schacher theorem (see later) is equivalent to the statement that the relative Brauer group of any finite extension of global fields is infinite. (The proof uses the classification of finite simple groups.)

So find one then . . .

A subgroup of S_n can be generated by at most $n-1$ elements, and such a generating set can be found efficiently (with polynomial delay) (Jerrum). So such a subgroup can be described by $O(n^2 \log n)$ bits.

So find one then . . .

A subgroup of S_n can be generated by at most $n-1$ elements, and such a generating set can be found efficiently (with polynomial delay) (Jerrum). So such a subgroup can be described by $O(n^2 \log n)$ bits.

Problem: Given a subgroup of S_n, does it contain a derangement?

So find one then ...

A subgroup of S_n can be generated by at most $n-1$ elements, and such a generating set can be found efficiently (with polynomial delay) (Jerrum). So such a subgroup can be described by $O(n^2 \log n)$ bits.

Problem: Given a subgroup of S_n, does it contain a derangement?

This problem is NP-complete, even for elementary abelian 2-groups. There is a simple reduction from the known NP-complete problem 3-SAT. Indeed, the argument shows that counting the derangements in a subgroup of S_n is #P-complete.

and in a transitive group ...

Given generators for a subgroup G of S_n, we can check quickly whether H is transitive. If it is (and $n > 1$), then we know that G contains a derangement.

and in a transitive group . . .

Given generators for a subgroup G of S_n, we can check quickly whether H is transitive. If it is (and $n > 1$), then we know that G contains a derangement.

Problem: Suppose that G is transitive. Find a derangement in G.

and in a transitive group . . .

Given generators for a subgroup G of S_n, we can check quickly whether H is transitive. If it is (and $n > 1$), then we know that G contains a derangement.

Problem: Suppose that G is transitive. Find a derangement in G.

There is an efficient randomised algorithm for this problem. Since at least a fraction $1/n$ of the elements of G are derangements, we can do this by random search: in n trials we will have a better-than-even chance of finding one, and in n^2 trials we will fail with exponentially small probability.

and in a transitive group . . .

Given generators for a subgroup G of S_n, we can check quickly whether H is transitive. If it is (and $n > 1$), then we know that G contains a derangement.

Problem: Suppose that G is transitive. Find a derangement in G.

There is an efficient randomised algorithm for this problem. Since at least a fraction $1/n$ of the elements of G are derangements, we can do this by random search: in n trials we will have a better-than-even chance of finding one, and in n^2 trials we will fail with exponentially small probability.

Problem: Can it be done deterministically?

and in a transitive group ...

Given generators for a subgroup G of S_n, we can check quickly whether H is transitive. If it is (and $n > 1$), then we know that G contains a derangement.

Problem: Suppose that G is transitive. Find a derangement in G.

There is an efficient randomised algorithm for this problem. Since at least a fraction $1/n$ of the elements of G are derangements, we can do this by random search: in n trials we will have a better-than-even chance of finding one, and in n^2 trials we will fail with exponentially small probability.

Problem: Can it be done deterministically?

The answer is likely to be "yes" – this is theoretically interesting but the randomised algorithm will almost certainly be more efficient!

Groups with many derangements

Although the lower bound $|G|/n$ for the number of derangements in a transitive group G is attained (by sharply 2-transitive groups), there are many groups with a higher proportion of derangements. For example, if G is regular, than all but one of its elements are derangements!

Groups with many derangements

Although the lower bound $|G|/n$ for the number of derangements in a transitive group G is attained (by sharply 2-transitive groups), there are many groups with a higher proportion of derangements. For example, if G is regular, than all but one of its elements are derangements!

The argument of Cameron and Cohen gives a lower bound of about $(r-1)/n$ for the proportion of derangements in a transitive group G, where r is the permutation rank (the number of orbits of G on ordered pairs).

Groups with many derangements

Although the lower bound $|G|/n$ for the number of derangements in a transitive group G is attained (by sharply 2-transitive groups), there are many groups with a higher proportion of derangements. For example, if G is regular, than all but one of its elements are derangements!

The argument of Cameron and Cohen gives a lower bound of about $(r-1)/n$ for the proportion of derangements in a transitive group G, where r is the permutation rank (the number of orbits of G on ordered pairs).

Can anything be said about families of (say, primitive) groups in which the proportion of derangements is bounded away from zero?

An example

Example: There is a constant $\alpha_k > 0$ so that the proportion of derangements in S_n acting on k-sets tends to α_k as $k \to \infty$. (For example, $\alpha_1 = \mathrm{e}^{-1} = 0.3679\ldots$, while $\alpha_2 = 2\mathrm{e}^{-3/2} = 0.4463\ldots$.

There is a formula for α_k as a sum over subsets of the partitions of k. But most of the terms cancel, so I suspect there is a much simpler formula!

An example

Example: There is a constant $\alpha_k > 0$ so that the proportion of derangements in S_n acting on k-sets tends to α_k as $k \to \infty$. (For example, $\alpha_1 = \mathrm{e}^{-1} = 0.3679\ldots$, while $\alpha_2 = 2\mathrm{e}^{-3/2} = 0.4463\ldots$.

There is a formula for α_k as a sum over subsets of the partitions of k. But most of the terms cancel, so I suspect there is a much simpler formula!

Problem: Is it true that $\alpha_k \to 1$ monotonically as $k \to \infty$?

Prime power order

Theorem: A transitive group of degree $n > 1$ contains a derangement. (Jordan)

The proof is elementary: By the Orbit-counting Lemma, the average number of fixed points is 1; and some element (the identity) fixes more than one point.

Prime power order

Theorem: A transitive group of degree $n > 1$ contains a derangement. (Jordan)

The proof is elementary: By the Orbit-counting Lemma, the average number of fixed points is 1; and some element (the identity) fixes more than one point.

Theorem: A transitive group of degree $n > 1$ contains a derangement of prime-power order. (Fein–Kantor–Schacher)

The proof uses the Classification of Finite Simple Groups, together with detailed analysis of the various families of simple groups.

Prime power order

Theorem: A transitive group of degree $n > 1$ contains a derangement. (Jordan)

The proof is elementary: By the Orbit-counting Lemma, the average number of fixed points is 1; and some element (the identity) fixes more than one point.

Theorem: A transitive group of degree $n > 1$ contains a derangement of prime-power order. (Fein–Kantor–Schacher)

The proof uses the Classification of Finite Simple Groups, together with detailed analysis of the various families of simple groups.

Problem: Find a simple proof!

Prime order

Not every transitive group contains a derangement of prime order.
A simple example is the 1-dimensional affine group over GF(9), acting on the set of 12 lines of the affine plane of order 3.

Prime order

Not every transitive group contains a derangement of prime order.
A simple example is the 1-dimensional affine group over GF(9), acting on the set of 12 lines of the affine plane of order 3.

Call a transitive group elusive if it contains no derangement of prime order.

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

Prime order

Not every transitive group contains a derangement of prime order.
A simple example is the 1-dimensional affine group over GF(9), acting on the set of 12 lines of the affine plane of order 3.

Call a transitive group elusive if it contains no derangement of prime order.

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

A permutation group G is 2-closed if any permutation which fixes every G-orbit on 2-sets belongs to G. For example, the automorphism group of a graph is 2-closed.

Problem: Is it true that there is no 2-closed elusive group? (Klin)

Which prime?

Conjecture: For any prime p, there is a function f_p on the natural numbers such that, if G is a transitive group of degree $n = p^a b$, where $\gcd(p, b) = 1$ and $a \geq f_p(b)$, then G contains a derangement of p-power order.
This was conjectured for $p = 2$ by Isbell in 1959 (in the context of game theory); even that case is still open.

Which prime?

Conjecture: For any prime p, there is a function f_p on the natural numbers such that, if G is a transitive group of degree $n = p^a b$, where $\gcd(p, b) = 1$ and $a \geq f_p(b)$, then G contains a derangement of p-power order.
This was conjectured for $p = 2$ by Isbell in 1959 (in the context of game theory); even that case is still open.

Conjecture: For any prime p, there is a function g_p on the natural numbers such that, if P is a p-group with b orbits each of length greater than $g_p(b)$, then P contains a derangement.
The second conjecture implies the first.

Maillet and Blichfeldt

Theorem (Maillet 1895)

Let G be a permutation group of degree n, and L the set of numbers of fixed points of non-trivial subgroups of G. Then $|G|$ divides $\prod_{l \in L}(n - l)$.

Maillet and Blichfeldt

Theorem (Maillet 1895)

Let G be a permutation group of degree n, and L the set of numbers of fixed points of non-trivial subgroups of G. Then $|G|$ divides $\prod_{l \in L}(n - l)$.

Theorem (Blichfeldt 1904)

Let G be a permutation group of degree n, and L the set of numbers of fixed points of non-identity elements of G. Then $|G|$ divides $\prod_{l \in L}(n - l)$.

Maillet and Blichfeldt

Theorem (Maillet 1895)

Let G be a permutation group of degree n, and L the set of numbers of fixed points of non-trivial subgroups of G. Then $|G|$ divides $\prod_{l \in L}(n - l)$.

Theorem (Blichfeldt 1904)

Let G be a permutation group of degree n, and L the set of numbers of fixed points of non-identity elements of G. Then $|G|$ divides $\prod_{l \in L}(n - l)$.

Blichfeldt claimed that his was just a new proof of Maillet's Theorem but it is actually stronger.

Proof of Maillet's Theorem

The proof is by induction on n. Let $l_0 = \min(L)$.

Proof of Maillet's Theorem

The proof is by induction on n. Let $l_0 = \min(L)$.
If $l_0 \neq 0$, then G fixes l_0 points; removing these fixed points subtracts l_0 from n and from every element of L and leaves $\prod_{l \in L}(n - l)$ unaltered.

Proof of Maillet's Theorem

The proof is by induction on n. Let $l_0 = \min(L)$.
If $l_0 \neq 0$, then G fixes l_0 points; removing these fixed points subtracts l_0 from n and from every element of L and leaves $\prod_{l \in L}(n-l)$ unaltered.
If $0 \in L$, then any point stabiliser satisfies the hypotheses with L replaced by $L \setminus \{0\}$. By induction, the order of any point stabiliser divides $\prod_{l \in L \setminus \{0\}}(n-l)$. Since n divides the least common multiple of the orbit lengths, it follows that $|G|$ divides $\prod_{l \in L}(n-l)$.

Proof of Maillet's Theorem

The proof is by induction on n. Let $l_0 = \min(L)$.
If $l_0 \neq 0$, then G fixes l_0 points; removing these fixed points subtracts l_0 from n and from every element of L and leaves $\prod_{l \in L}(n-l)$ unaltered.
If $0 \in L$, then any point stabiliser satisfies the hypotheses with L replaced by $L \setminus \{0\}$. By induction, the order of any point stabiliser divides $\prod_{l \in L \setminus \{0\}}(n-l)$. Since n divides the least common multiple of the orbit lengths, it follows that $|G|$ divides $\prod_{l \in L}(n-l)$.

Equality implies that the pointwise stabiliser of any set is transitive on the points it moves. Such a group acts on a nice geometry (a matroid, indeed a "perfect matroid design", that is, a matroid in which the cardinality of a flat depends only on its dimension.

Proof of Blichfeldt's Theorem

The function

$$g \mapsto \prod_{l \in L} (\mathrm{fix}(g) - l)$$

is a virtual character which is zero on all non-identity elements. So it is a multiple of the regular character, whence $|G|$ divides its value at the identity.

Proof of Blichfeldt's Theorem

The function

$$g \mapsto \prod_{l \in L} (\mathrm{fix}(g) - l)$$

is a virtual character which is zero on all non-identity elements. So it is a multiple of the regular character, whence $|G|$ divides its value at the identity.

It is not at all clear what the consequence of equality is, apart from saying that the above function is the regular character of G.

Which groups meet the bound?

Any regular permutation group attains both bounds, with $L = \{0\}$.

Which groups meet the bound?

Any regular permutation group attains both bounds, with $L = \{0\}$.
Groups meeting the bound in Maillet's Theorem have been determined by Zil'ber for $|L| \geq 7$ using geometric and model-theoretic methods, and by Maund for $|L| \geq 2$ using the Classification of Finite Simple Groups. There are generic examples (wreath products of regular groups with symmetric groups; alternating groups; extensions of V^r by G, where G is the stabiliser of a tuple of points in a general linear group and V its natural module. In addition there are some sporadic examples with $|L|$ small.

Which groups meet the bound?

Any regular permutation group attains both bounds, with $L = \{0\}$.
Groups meeting the bound in Maillet's Theorem have been determined by Zil'ber for $|L| \geq 7$ using geometric and model-theoretic methods, and by Maund for $|L| \geq 2$ using the Classification of Finite Simple Groups. There are generic examples (wreath products of regular groups with symmetric groups; alternating groups; extensions of V^r by G, where G is the stabiliser of a tuple of points in a general linear group and V its natural module. In addition there are some sporadic examples with $|L|$ small.
The classification of groups meeting Blichfeldt's bound is not known.

Prime power versions

In both Maillet's and Blichfeldt's Theorems (as they both observed), we can take a smaller set L, the set of fixed point numbers of non-trivial elements or subgroups of *prime-power* order.

Prime power versions

In both Maillet's and Blichfeldt's Theorems (as they both observed), we can take a smaller set L, the set of fixed point numbers of non-trivial elements or subgroups of *prime-power* order.
For, with this hypothesis, each Sylow subgroup satisfies the divisibility condition, and so the whole group does.

Problem

Which groups attain the bounds in the prime power versions of Maillet's or Blichfeldt's Theorems?

Partitions

A partition of a finite group G is a set of non-identity proper subgroups such that every non-identity element is contained in exactly one of these subgroups.

Partitions

A partition of a finite group G is a set of non-identity proper subgroups such that every non-identity element is contained in exactly one of these subgroups.
Iwahori and Kondo showed in 1965 that a group G has a partition if and only if it has a permutation representation in which every non-identity element has k fixed points, for some $k > 0$ (the case $|L| = 1$ in Blichfeldt's Theorem).

Partitions

A partition of a finite group G is a set of non-identity proper subgroups such that every non-identity element is contained in exactly one of these subgroups.
Iwahori and Kondo showed in 1965 that a group G has a partition if and only if it has a permutation representation in which every non-identity element has k fixed points, for some $k > 0$ (the case $|L| = 1$ in Blichfeldt's Theorem).
Suzuki showed in 1961 that a non-solvable group having a partition is one of $\mathrm{PGL}(2, q)$, $\mathrm{PSL}(2, q)$ or $\mathrm{Sz}(q)$ for some prime power q.

Local partitions

Analogous results hold for prime power elements. A A local partition of a group is a set of non-identity proper subgroups so that each non-identity local element (element of prime power order) is contained in exactly one of them.

Local partitions

Analogous results hold for prime power elements. A A local partition of a group is a set of non-identity proper subgroups so that each non-identity local element (element of prime power order) is contained in exactly one of them.
Spiga showed that a group has a local partition if and only if it has a permutation representation in which each non-identity local element has k fixed points, for some $k > 0$.

Local partitions

Analogous results hold for prime power elements. A A local partition of a group is a set of non-identity proper subgroups so that each non-identity local element (element of prime power order) is contained in exactly one of them.
Spiga showed that a group has a local partition if and only if it has a permutation representation in which each non-identity local element has k fixed points, for some $k > 0$.
He also found the finite simple groups which have local partitions: in addition to those in Suzuki's list, the Ree groups $R_1(q)$ and the first Janko group J_1 are the only ones.

The set of derangements

The derangements in a transitive permutation group G are the elements whose conjugacy class is disjoint from the point stabiliser.

The set of derangements

The derangements in a transitive permutation group G are the elements whose conjugacy class is disjoint from the point stabiliser.

Thus, if two transitive actions of a group have the same permutation character, then the sets of derangements in the two actions are equal.

The set of derangements

The derangements in a transitive permutation group G are the elements whose conjugacy class is disjoint from the point stabiliser.
Thus, if two transitive actions of a group have the same permutation character, then the sets of derangements in the two actions are equal.

Theorem (Spiga)

If a group of nilpotency class 2 *has two transitive actions with the same set of derangements, then the point stabilisers are isomorphic, and the permutation characters are equal. This is false for nilpotency class* 3*.*

The set of derangements

The derangements in a transitive permutation group G are the elements whose conjugacy class is disjoint from the point stabiliser.
Thus, if two transitive actions of a group have the same permutation character, then the sets of derangements in the two actions are equal.

Theorem (Spiga)

If a group of nilpotency class 2 *has two transitive actions with the same set of derangements, then the point stabilisers are isomorphic, and the permutation characters are equal. This is false for nilpotency class* 3*.*

Spiga conjectured that if two primitive actions of G have the same set of derangements, then one permutation character contains the other.

Fixed points and orbits

Let G be a finite permutation group. Let $P_G(x)$ be the probability generating function for the number of fixed points of a random element of G. Let F_i be the number of orbits of G on i-tuples of distinct elements, and $F_G(x)$ the exponential generating function for the numbers F_n: that is, $F_G(x) = \sum F_i x^i / i!$.

Fixed points and orbits

Let G be a finite permutation group. Let $P_G(x)$ be the probability generating function for the number of fixed points of a random element of G. Let F_i be the number of orbits of G on i-tuples of distinct elements, and $F_G(x)$ the exponential generating function for the numbers F_n: that is, $F_G(x) = \sum F_i x^i / i!$.

Theorem: $F_G(x) = P_G(x+1)$. (Boston *et al.*)

Corollary: The proportion of derangements in G is $F_G(-1)$.

Fixed points and orbits

Let G be a finite permutation group. Let $P_G(x)$ be the probability generating function for the number of fixed points of a random element of G. Let F_i be the number of orbits of G on i-tuples of distinct elements, and $F_G(x)$ the exponential generating function for the numbers F_n: that is, $F_G(x) = \sum F_i x^i / i!$.

Theorem: $F_G(x) = P_G(x+1)$. (Boston *et al.*)

Corollary: The proportion of derangements in G is $F_G(-1)$.

This gives a simple proof that the proportion of derangements in S_n is close to $1/\mathrm{e}$: for $F_i = 1$ for $0 \leq i \leq n$, so $F_G(x)$ is the expontial series truncated to degree n.

First extension

This is a special case of the Shift Theorem for the cycle index of a permutation group.

First extension

This is a special case of the Shift Theorem for the cycle index of a permutation group.

Recall the cycle index: $Z(G) = \dfrac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} s_i^{c_i(g)}$, where $s_1, s_2, \ldots$ are indeterminates and $c_i(g)$ is the number of i-cycles in g. Putting $s_i = 1$ for $i > 1$ gives $P_G(s_1)$, while putting $s_i = 0$ for $i > 1$ gives $s_1^n / |G|$.

First extension

This is a special case of the Shift Theorem for the cycle index of a permutation group.

Recall the cycle index: $Z(G) = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \prod_{i=1}^{n} s_i^{c_i(g)}$, where $s_1, s_2, \ldots$ are indeterminates and $c_i(g)$ is the number of i-cycles in g.

Putting $s_i = 1$ for $i > 1$ gives $P_G(s_1)$, while putting $s_i = 0$ for $i > 1$ gives $s_1^n / |G|$.

The Shift Theorem asserts that, if $G[A]$ denotes the permutation group induced on A by its setwise stabiliser, then

$$\sum_A Z(G[A]) = Z(G; s_i \leftarrow s_i + 1),$$

where the sum is over representatives of the G-orbits on subsets.

Second extension

There is a version of the theorem for linear groups over $\mathrm{GF}(q)$. Replace "number of fixed points" by "dimension of fixed-point space", "number of orbits on tuples of distinct elements" by "number of orbits on linearly independent tuples", and use the q-analogue of the factorial to define the e.g.f.
Shahn Majid interpreted this formula in terms of addition in the "affine braided line", giving a duality between counting fixed points and counting orbits corresponding to interchanging q and q^{-1} in the formulae.
In particular we get a simple formula for the number of derangements in $\mathrm{GL}(d,q)$.

Third extension

A permutation group G on an infinite set is oligomorphic if G has only finitely many orbits on n-tuples for all n. Now the formal power series $F_G(x)$ makes sense for any oligomorphic group G.

Sometimes the series converges, or is summable by some method, at $x = -1$. If so, is there any connection with derangements?

Third extension

A permutation group G on an infinite set is oligomorphic if G has only finitely many orbits on n-tuples for all n. Now the formal power series $F_G(x)$ makes sense for any oligomorphic group G.

Sometimes the series converges, or is summable by some method, at $x = -1$. If so, is there any connection with derangements?

For example,

- if G is the symmetric group, then $F_G(x) = \mathrm{e}^x$, and $F_G(-1) = \mathrm{e}^{-1}$;

Third extension

A permutation group G on an infinite set is oligomorphic if G has only finitely many orbits on n-tuples for all n. Now the formal power series $F_G(x)$ makes sense for any oligomorphic group G.
Sometimes the series converges, or is summable by some method, at $x = -1$. If so, is there any connection with derangements?
For example,

- if G is the symmetric group, then $F_G(x) = \mathrm{e}^x$, and $F_G(-1) = \mathrm{e}^{-1}$;
- if G is the group of order-preserving permutations of $\mathbb{Q}$, then $F_G(x) = \sum x^n = 1/(1-x)$, and $F_G(-1) = \frac{1}{2}$. (Euler)

Random Latin squares

Theorem: The group generated by the rows of a random Latin square of order n is S_n with high probability.

Random Latin squares

Theorem: The group generated by the rows of a random Latin square of order n is S_n with high probability.

The proof uses two important results:

Random Latin squares

Theorem: The group generated by the rows of a random Latin square of order n is S_n with high probability.

The proof uses two important results:

Theorem: The probability that a random element of S_n lies in no proper transitive subgroup of S_n except possibly A_n tends to 1 as $n \to \infty$. (Łuczak–Pyber)

Random Latin squares

Theorem: The group generated by the rows of a random Latin square of order n is S_n with high probability.

The proof uses two important results:

Theorem: The probability that a random element of S_n lies in no proper transitive subgroup of S_n except possibly A_n tends to 1 as $n \to \infty$. (Łuczak–Pyber)

Theorem: The probability that all rows of a random Latin square are even permutations is exponentially small. (Häggkvist–Janssen)

The proof

The first row of a random Latin square is a random permutation. The group generated by the rows is clearly transitive. So the group generated by the rows is S_n or A_n w.h.p. The second theorem rules out A_n.

The proof

The first row of a random Latin square is a random permutation. The group generated by the rows is clearly transitive. So the group generated by the rows is S_n or A_n w.h.p. The second theorem rules out A_n.

Corollary: For almost all finite quasigroups Q, the multiplication group of Q (generated by the left and right multiplications) is the symmetric group.

A quasigroup is just a binary system whose Cayley table is a Latin square. Jonathan Smith developed a character theory of quasigroups, which turns out to be trivial if the multiplication group is 2-transitive.

What about derangements?

Call a Latin square normalised if its first row is the identity permutation. (Then the remaining rows are derangements.) Is it true that, for almost all normalised Latin squares, the group generated by the rows is the symmetric group?

What about derangements?

Call a Latin square normalised if its first row is the identity permutation. (Then the remaining rows are derangements.) Is it true that, for almost all normalised Latin squares, the group generated by the rows is the symmetric group?

Since an element of S_n is a derangement with positive probability, the Łuczak–Pyber theorem holds for random derangements (with the uniform distribution). We'd like to know it for random derangements (where the probability of g is proportional to the number of normalised Latin squares with second row g).

What about derangements?

Call a Latin square normalised if its first row is the identity permutation. (Then the remaining rows are derangements.) Is it true that, for almost all normalised Latin squares, the group generated by the rows is the symmetric group?

Since an element of S_n is a derangement with positive probability, the Łuczak–Pyber theorem holds for random derangements (with the uniform distribution). We'd like to know it for random derangements (where the probability of g is proportional to the number of normalised Latin squares with second row g).

I **conjecture** that this is also true.

Derangements and Latin squares

For a derangement g, let $L(g)$ be the number of Latin squares whose first row is the identity and whose second row is g. (This depends only on the cycle structure of g). I conjecture that the ratio of the maximum and minimum values of $L(g)$ tends to 1 as $n \longrightarrow \infty$.

If true this would resolve the earlier conjecture and would have the corollary that for almost all finite loops, the multiplication group is the symmetric group. (A loop is a quasigroup with identity.)

Derangements and Latin squares

For a derangement g, let $L(g)$ be the number of Latin squares whose first row is the identity and whose second row is g. (This depends only on the cycle structure of g). I conjecture that the ratio of the maximum and minimum values of $L(g)$ tends to 1 as $n \longrightarrow \infty$.

If true this would resolve the earlier conjecture and would have the corollary that for almost all finite loops, the multiplication group is the symmetric group. (A loop is a quasigroup with identity.)

On the next slide are some values of $L(g)$ for the four conjugacy classes of derangements in S_7 and S_8. The agreement is striking!

The cases $n = 7, 8$

The values for $n = 7, 8$ are:

$[7]$	6566400
$[5,2]$	6604800
$[4,3]$	6543360
$[3,2,2]$	6635520

$[8]$	181519810560
$[6,2]$	182125854720
$[5,3]$	181364244480
$[4,2,2]$	183299604480
$[4,4]$	182052126720
$[3,3,2]$	181813248000
$[2,2,2,2]$	186042286080

The case $n = 9$

This table was computed by Ian Wanless.

[9]	113959125225308160
[7, 2]	114140503159603200
[6, 3]	113970892709560320
[5, 4]	113938545628938240
[5, 2, 2]	114303522444410880
[4, 3, 2]	114131854216396800
[3, 3, 3]	113995242201415680
[3, 2, 2, 2]	114460947413729280