FUNDAMENTA
MATHEMATICAE
144 (1994)

The prevalence of permutations with infinite cycles

by

Randall Dougherty (Columbus, Ohio)
and **Jan Mycielski** (Boulder, Colo.)

Abstract. A number of recent papers have been devoted to the study of prevalence, a generalization of the property of being of full Haar measure to topological groups which need not have a Haar measure, and the dual concept of shyness. These concepts give a notion of "largeness" which often differs from the category analogue, comeagerness, and may be closer to the intuitive notion of "almost everywhere." In this paper, we consider the group of permutations of natural numbers. Here, in the sense of category, "almost all" permutations have only finite cycles. In contrast, we show that, in terms of prevalence, "almost all" permutations have infinitely many infinite cycles and only finitely many finite cycles; this set of permutations comprises countably many conjugacy classes, each of which is non-shy.

Let G be a Polish topological group, i.e., a second countable complete metrizable topological group. [Concerning this concept, let us recall that, by a theorem of Birkhoff and Kakutani (see [5]), every first countable topological group G has a left- (or right-) invariant metrization. Also, if G is an absolute $\mathbb{G}_\delta$ (i.e., it has any complete metrization), and G has a two-sided invariant metric, then this invariant metric must be complete.]

A universally measurable subset A of a Polish group G will be called *prevalent* iff there exists a Borel probability measure μ over G (not necessarily invariant) such that

$$\mu(xAy) = 1 \quad \text{for all } x, y \in G \,.$$

(Recall that, if G is not compact, then no invariant Borel probability measure over G exists.) A complement of a prevalent set is called *shy*. These concepts were introduced by Christensen [1] (for abelian groups), and a substantial body of theorems about them was established in [2], [3], [4], and [6]. The main results of these papers (for Polish groups) are:

1991 *Mathematics Subject Classification*: Primary 20B07.
The first author was supported by NSF grant number DMS-9158092 and by a fellowship from the Sloan Foundation.

(1) The class of shy sets is countably additive ([1]; see also [6]).

(2) If G is locally compact, then the class of shy sets is equal to the class of (universally measurable) sets of Haar measure zero ([1]; see also [6]).

(3) If G is not locally compact, and G has an invariant metric (e.g., if G is abelian), then every compact (or σ-compact) subset of G is shy (see [2]).

But many problems are still open; see [1] and [6]. For example, we do not know whether a subgroup of G which is universally measurable and is not shy must be clopen, although this must be so for abelian G by Theorem 2 of [1].

Many of the main results of this theory are of the form "such and such a set is prevalent (or shy)." For example, the set of nowhere differentiable functions in the additive group $C[0,1]$ of continuous functions is prevalent [3].

The purpose of this note is to prove two such theorems about the group S_∞ of all permutations of the countable set $\omega = \{0,1,2,\ldots\}$. The group S_∞ is Polish since it has the complete second countable metrization

$$d(p,q) = (\max\{n : p(k) = q(k) \text{ and } p^{-1}(k) = q^{-1}(k) \text{ for all } k < n\})^{-1}$$

relative to which the operations pq and p^{-1} are continuous.

Theorem 1. *The set of permutations with infinitely many infinite cycles and only finitely many finite cycles is prevalent.*

This theorem should be contrasted with the well-known fact that the set of permutations which have an infinite cycle is meager (i.e., first category) in S_∞.

The set of permutations in Theorem 1 comprises countably many conjugacy classes of permutations, one for each finite list of sizes for the finite cycles in the permutation. We will now see that each of these conjugacy classes is non-shy.

Theorem 2. *For any finite partial permutation p_0 of ω, the set of permutations extending p_0 which have no finite cycles other than those completed in p_0 is not shy.*

Since the intersection of a prevalent set and a non-shy set is non-shy, it follows from Theorems 1 and 2 that, for any finite list of finite cycle sizes (with repetition permitted), the conjugacy class consisting of those permutations with finite cycles of sizes specified by the list and infinitely many infinite cycles is not shy. (For other examples of families of disjoint sets which are not shy, see [2].)

Proof of Theorem 1. Let X be this set of permutations. We will find a probability measure μ on S_∞ such that any double translate gXh of X has μ-measure 1. In fact, it will suffice to show that $\mu(gX) = 1$ for all left translates gX of X, because X is fixed under conjugation, and hence

$gXh = ghh^{-1}Xh = ghX$. Equivalently, we can show that $\mu(g^{-1}X) = 1$ for all permutations g.

Fix natural numbers k_n for $n \in \omega$ which grow so quickly that $k_{n+1} > k_n > 2n + 1$ for all n and $\sum_{n=0}^{\infty} n/k_n$ converges. We define the measure μ somewhat informally, by describing how to choose a permutation p at random with the distribution μ. To do so, successively choose $p(0)$, $p^{-1}(0)$, $p(1)$, $p^{-1}(1)$, and so on as follows. Choose $p(0)$ from the natural numbers less than k_0 with equal probability for each. Then, if $p^{-1}(0)$ has not yet been determined (i.e., if $p(0) \neq 0$), choose $p^{-1}(0)$ from the natural numbers less than k_0 other than 0, with equal probability. In general, at stage n, if $p(n)$ has not yet been determined (i.e., $p^{-1}(m) \neq n$ for $m < n$), choose $p(n)$ randomly from the available numbers less than k_n (those which are not already in the range of p) with equal probability for each; then, if $p^{-1}(n)$ has not yet been determined, choose $p^{-1}(n)$ randomly from the numbers less than k_n which are not already in the range of p^{-1}, with equal probability for each. After all stages are complete, p will be a permutation of ω.

Let p_0 be a finite partial permutation that can arise at the beginning of some stage n_0 of the above construction; that is, suppose $p_0(m)$ and $p_0^{-1}(m)$ are defined and less than k_m for $m < n_0$, no other parts of p_0 are defined, and p_0 and p_0^{-1} are one-to-one.

Claim. *If p_0 is a partial permutation as above, g is a permutation of ω, and M is a natural number, then there is a natural number N such that the conditional probability under μ, under the condition of extending p_0, that a permutation p will be such that gp has no finite cycles including a number greater than N and no two of the numbers $N+1, \ldots, N+M$ are in the same cycle of gp is at least* $1/2$.

Proof. Since $\sum_{n=0}^{\infty} n/k_n$ converges, we have $\lim_{n\to\infty} n/k_n = 0$, so

$$\lim_{n\to\infty} (k_n - 2n - 1)/k_n = 1\,,$$

so $\sum_{n=0}^{\infty} n/(k_n - 2n - 1)$ converges. Therefore, we can choose a natural number r so large that $r > n_0$, $r > p_0(m)$ and $r > p_0^{-1}(m)$ for $m < n_0$, and

$$\sum_{n=r}^{\infty} \frac{2n+2+M}{k_n - 2n - 1} \le \frac{1}{4}\,.$$

Choose $N \ge k_r$ so large that $g(m) < N$ for $m < k_r$.

We must show that the conditional probability that gp has a finite cycle including a number greater than N or the numbers $N+1, \ldots, N+M$ are not in distinct cycles of gp is at most $1/2$. If either of these events occurs, then it occurs after finitely many stages of the construction of p; there must be a particular stage at which the bad gp-cycle or the gp-path from $N+i$ to $N+j$ is completed. Note that neither event can occur before stage r, because

N was chosen to be so large that there is no $k \geq N$ such that $g(p(k))$ or $p^{-1}(g^{-1}(k))$ is defined before stage r.

Suppose the construction has reached stage n. If $p(n)$ is already defined, then we do nothing in the first half of stage n. If $p(n)$ is not yet defined, then $p(n)$ is chosen at random (uniformly) from $k_n - x$ possibilities, where x is the number of natural numbers less than k_n which are already in the range of p; clearly $0 \leq x \leq 2n$. The only ways in which the definition of $p(n)$ can complete a bad event are: $p(n) = g^{-1}(n)$, so we get a fixed point of gp; $g(p(n))$ is the last link of a gp-path from $N+i$ to $N+j$, so $p(n) = g^{-1}(N+j)$; $g(p(n))$ completes a cycle of gp of length greater than 1; or $g(p(n))$ completes a gp-path from $N+i$ to $N+j$ but is not the last link in this path. In the last two cases, the number $g(p(n))$ must already be in the domain of p, so $p(n)$ must be $g^{-1}(t)$ for some t for which $p(t)$ was defined earlier; there are at most $2n$ such t's. Therefore, there are at most $1+M+2n$ possible values for $p(n)$ which can complete a bad event, so the probability that one of these is chosen is at most $(1+M+2n)/(k_n - x)$, which is less than $(2n+2+M)/(k_n-2n-1)$. This was true no matter what the previous construction had been, so, for $n \geq r$, the conditional probability assuming p extends p_0 that a bad event is completed in the first half of stage n is at most $(2n+2+M)/(k_n-2n-1)$.

Similarly, the choice of $p^{-1}(n)$ can complete a bad event only if the chosen value is $g(n)$, one of the numbers $N+i$ for $1 \leq i \leq M$, or a number $g(t)$ where t was already in the range of p, so the probability that this occurs is at most $(2n+2+M)/(k_n-2n-1)$. Therefore, the conditional probability that a bad event is completed during stage n is at most $2(2n+2+M)/(k_n-2n-1)$; since bad events cannot be completed before stage r, the conditional probability that a bad event ever occurs is at most

$$\sum_{n=r}^{\infty} 2\frac{2n+2+M}{k_n-2n-1} \leq \frac{1}{2},$$

as desired. This completes the proof of the claim. ■

Next, we show by induction on i that, if p_0, g, and M are as in the claim, then the conditional probability (under the condition of extending p_0) that a permutation p is such that gp has only finitely many finite cycles and at least M infinite cycles is at least $1-2^{-i}$. The case $i=0$ is trivial. Now suppose that we have the result for $i-1$. Given p_0, g, and M, choose N as in the claim. If a permutation p is such that gp has no finite cycles with a member greater than N and the numbers $N+1, \ldots, N+M$ are in distinct cycles of gp, then clearly gp has only finitely many finite cycles and at least M infinite cycles. If p does not have these properties, then there must be a first stage n at which the construction of p causes the completion of a gp-cycle with a member greater than N or a gp-path from $N+i$ to

$N + j$ for some i, j with $1 \le i, j \le M$; let p_1 be the part of p that has been constructed by the end of stage n. As p varies over all bad permutations extending p_0, the collection of resulting p_1's is a countable collection of finite partial permutations extending p_0, and any two of these partial permutations must disagree somewhere (since the permutations were truncated at the first stage where a bad event occurred), so no permutation p can extend more than one of these partial permutations. Therefore, the sum over all such p_1 of the conditional probability of reaching p_1 given that one has reached p_0 is the conditional probability of reaching a bad permutation given that one has reached p_0, which is at most $1/2$. For each such p_1, the conditional probability of reaching a permutation with infinitely many finite cycles or fewer than M infinite cycles given that one has reached p_1 is at most $2^{-(i-1)}$ by the induction hypothesis. Now one can sum over all such p_1 to see that the conditional probability of reaching a permutation with infinitely many finite cycles or fewer than M infinite cycles given that one has reached p_0 is at most $(1/2)2^{-(i-1)} = 2^{-i}$. This completes the induction.

If we now fix p_0 to be the empty partial permutation but let i be arbitrary, we see that the (unconditional) probability that a permutation gp, where p is chosen according to the distribution μ, will have only finitely many cycles and at least M infinite cycles is 1. Since this is true for all M, the probability that gp has infinitely many cycles is 1. This shows that $\mu(g^{-1}X) = 1$ for all permutations g, so we are done. ∎

Proof of Theorem 2. Let X be this set of permutations. We will show that, for any probability measure μ on S_∞, there is a permutation g such that $\mu(g^{-1}X) > 0$.

Fix such a measure μ. Let D be the domain of p_0. Since there are only countably many possibilities for the restriction of a permutation to D, there must exist a function q_0 with domain D such that the set of permutations extending q_0 has positive μ-measure; fix such a q_0, and let a be the measure of $\{p : q_0 \subseteq p\}$. Clearly q_0 is one-to-one.

If $S(n, m)$ is the set of permutations p such that $p(n) < m$ and $p^{-1}(n) < m$, then, for each n, S_∞ is the increasing union of the sets $S(n, m)$ as m varies, so $\lim_{m\to\infty} \mu(S(n, m)) = 1$. Therefore, we can define a function $F : \omega \to \omega$ so that, for each n, $\mu(S(n, F(n))) > 1 - 2^{-n-2}a$; we may also ensure that F is an increasing function. It follows that, if Y is the set of all permutations p such that p extends q_0 and $p(n), p^{-1}(n) < F(n)$ for all n, then $\mu(Y) > 0$. We will construct a permutation g such that $gY \subseteq X$; this will imply that $\mu(g^{-1}X) \ge \mu(Y) > 0$, as desired.

We will construct g in stages. To start with, for each t in the range of q_0, let $g(t) = p_0(q_0^{-1}(t))$. This guarantees that $gp \supseteq p_0$ for any $p \in Y$.

Also, using this part of g alone, the only completed cycles of gp are those completed in p_0.

Now, for $n = 0, 1, 2, \ldots$ in order, proceed as follows. If $g(n)$ has not yet been defined, choose r to be greater than n and greater than any value $g^{-1}(m)$ previously defined, and let $g(n) = F(r)$. It follows that, for p in Y, $p(g(n))$ cannot be less than r, since p^{-1} maps numbers less than r to numbers less than $F(r)$. Hence, $g(n)$ cannot be in the the domain of the part of gp which was previously defined, and $g(n)$ also cannot be $p^{-1}(n)$, so this definition of $g(n)$ cannot complete a new finite cycle of gp. Once $g(n)$ is defined in this way, we can proceed to define $g^{-1}(n)$ similarly, if it is not already known: choose r to be greater than n and greater than any value $g(m)$ previously defined (including $g(n)$), and let $g^{-1}(n) = F(r)$. Since $p \in Y$ maps numbers less than r to numbers less than $F(r)$, $p^{-1}(g^{-1}(n))$ must be at least r, so this definition of $g^{-1}(n)$ cannot complete a new finite cycle of gp.

This completes the recursive definition of g. For any p in Y, there can be no finite cycles in gp other than those already present in p_0. Therefore, $gY \subseteq X$, as desired. ■

References

[1] J. P. R. Christensen, *On sets of Haar measure zero in abelian Polish groups*, Israel J. Math. 13 (1972), 255–260.

[2] R. Dougherty, *Examples of non-shy sets*, this volume, 73–88.

[3] B. R. Hunt, *The prevalence of continuous nowhere differentiable functions*, to appear.

[4] B. R. Hunt, T. Sauer, and J. A. Yorke, *Prevalence: a translation-invariant "almost every" on infinite-dimensional spaces*, Bull. Amer. Math. Soc. 27 (1992), 217–238.

[5] D. Montgomery and L. Zippin, *Topological Transformation Groups*, Interscience Publ., New York, 1955.

[6] J. Mycielski, *Some unsolved problems on the prevalence of ergodicity, instability and algebraic independence*, Ulam Quart. 1 (3) (1992), 30–37.

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
COLUMBUS, OHIO 43210-1320
U.S.A.
E-mail: RLD@MATH.OHIO–STATE.EDU

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO
BOULDER, COLORADO 80309-0395
U.S.A.

Received 4 April 1993