Mathematical Reports

MARCH / MARS 2002

IN THIS ISSUE / DANS CE NUMÉRO

24
No 1

C. R. Math. Rep. Acad. Sci. Canada Vol. **24** (1), 2002 pp. 1–15

PROBABILISTIC GROUP THEORY

JOHN D. DIXON

Presented by V. Dlab, FRSC

ABSTRACT. This survey discusses three aspects of the ways in which probability has been applied to the theory of finite groups: probabilistic statements about groups; construction of randomized algorithms in computational group theory; and application of probabilistic methods to prove deterministic theorems in group theory. It concludes with a brief summary of related results for infinite groups.

RÉSUMÉ. Cet article donne un aperçu sur trois aspects des façons dont la probabilité est appliquée à la théorie des groupes finis: les faits probabilistiques des groupes; la construction d'algorithmes aléatoires dans la computation; et l'application des moyens probabilistiques pour obtenir les théorèmes déterministiques dans la théorie des groups. On termine avec un bref sommaire de résultats se rapportant aux groupes infinis.

In the past 20 years, and particularly during the last decade, there has been a growing interest in the use of probability in finite groups. It has been my experience that many pure mathematicians still look on probability theory as an "applied" subject (perhaps because of the way it is taught in our universities), and are dubious about the validity of using probabilistic reasoning in their own discipline. Kolmogorov's axiomatization [51] of probability theory still seems to be a well kept secret. However, no-one should be uncomfortable in a discussion of the applications of probability theory to finite groups, since in these cases the probabilistic statements can be always be simply understood in terms of proportions.

In the current article I shall consider three aspects of the ways in which probability has been applied to problems in group theory. These are: probabilistic statements about groups which give some alternative description of the structure of the group and its elements (Sections 1 and 2); applications of probability to construct algorithms in computational group theory (Section 3); and applications of probabilistic methods to prove deterministic theorems in group theory (see Section 4). The last section (Section 5) deals with some related results in infinite groups.

Since my focus is on group theory, I shall ignore several very important areas where the primary interest is in probability theory such as random walks on

Received by the editors September 18, 2001.
AMS subject classification: 20-02, 20D60, 20F69, 20-04.

groups and amenable groups (but see Section 3.2). There is also interesting recent work on probability and conjugacy classes of the classical groups (see [36] and [37]).

There are two surveys by Shalev (see [74] and [76]) which partially overlap with this paper.

1. Probabilistic questions about elementary properties of groups.

1.1. *"Statistics" of the symmetric group.* During the 1960's Erdős and Turán published a series of papers [31], [32], [33] and [34] on the "statistics" of the symmetric group S_n. A typical result describes the probability distribution of the logarithm of the order of a random element x from S_n; they prove that the distribution of $\ln(\mathrm{ord}(x))$ is asymptotically normal with mean $\frac{1}{2}\ln^2 n$ and variance $\frac{1}{3}\ln^3 n$. This contrasts sharply with the classical result of E. Landau that the maximum of $\ln(\mathrm{ord}(x))$ is $(1+o(1))\sqrt{n\ln(n)}$ (see [68]). The results of Erdős and Turán have been refined and extended in a number of other papers such as [17], [7], [29], [45], [30], [11] (see also [73]). All of these results are essentially combinatorial and do not use significant group properties of S_n. A little more group theory is used to prove the results in [23].

Similar results for the finite classical linear groups are found in [35].

1.2. *Group laws.* An earlier example of a probabilistic statement about groups describes how commutative a nonabelian group can be (I am not sure who first made this observation):

- If G is a nonabelian finite group with $k(G)$ conjugacy classes, then

$$\frac{|\{(x,y)\in G\times G \mid xy=yx\}|}{|G|^2} = \frac{k(G)}{|G|} \le \frac{5}{8}.$$

This can be interpreted as saying that, for any finite nonabelian group, the probability that two elements chosen at random from G commute is at most $5/8$ (the bound is achieved when G is nonabelian group of order 8). Elementary extensions of this result can be found in [43], [77] and [78].

NOTE. We are assuming (as we shall generally assume for finite groups throughout this paper) that random elements are chosen independently with the uniform distribution on G. Thus every pair (x,y) has the same probability $1/|G|^2$ of being chosen.

This suggests the following general question:

- Let $w := w(X_1, X_2, \ldots, X_m)$ be a nontrivial word. Does there exist a constant $\eta < 1$ (depending on w) such that, if $w = 1$ is not a law for a finite group G, then a random m-tuple $(x_1, x_2, \ldots, x_m)$ of elements from G satisfies $w(x_1, x_2, \ldots, x_m) = 1$ with probability $\le \eta$?

Of course the theorem quoted above is just the case when $w(X,Y) = X^{-1}Y^{-1}XY$. Although the question has been answered positively in some special

cases, for example, for some words representing nilpotent varieties and metabelian varieties (unpublished work), the problem appears to be open in the general case. For results related to nilpotent varieties see the recent paper [38].

Some related results are known. For example, [41] shows that if G is a finite group which is not solvable, then the probability that two random elements generate a solvable subgroup is at most $11/30$. A further result appears in [21] (see Section 4.2). Both of these results require the classification of finite simple groups for their proofs.

2. Generators.

2.1. *Generating the symmetric group.* In 1969 I was reading the classical book of E. Netto [66] and came across the following claim (p. 90 of the English translation):

> If we arbitrarily select two or more substitutions of n elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group. In the case of two substitutions the probability in favor of the symmetric group may be taken as about $\frac{3}{4}$, and in favor of the alternating, but not symmetric, group as about $\frac{1}{4}$. In order that any given substitutions may generate a group which is only a part of the $n!$ possible substitutions, very special relations are necessary, and it is highly improbable that arbitrarily chosen substitutions [...] should satisfy these conditions. The exception most likely to occur would be that all the given substitutions were severally equivalent to an even number of transpositions and would consequently generate the alternating group.

Perhaps Netto was expressing his frustration after trying to generate interesting subgroups of S_n from random permutations. He gives no supporting evidence for his claim.

Let A_n denote the alternating group. Then Netto's conjecture can be written:

$$p_n := \frac{|\{(x,y) \in S_n \times S_n \mid \langle x,y\rangle \geq A_n\}|}{|S_n|^n} \to 1 \quad \text{as } n \to \infty$$

where $\langle x,y\rangle$ denotes the subgroup generated by x and y. Since $|S_n : A_n| = 2$ for $n \geq 2$, we have $\langle x,y\rangle \leq A_n$ for exactly $\frac{1}{4}$ of the pairs, so the rest of his claim follows easily. Netto's conjecture can be rephrased as "almost all pairs of elements of S_n generate either A_n or S_n as $n \to \infty$" or

- the probability p_n that two elements chosen at random from S_n generate either A_n or S_n tends to 1 as $n \to \infty$.

Netto's conjecture was proved in [22] where it is shown that $p_n > 1 - 2(\ln \ln n)^{-2}$ for all sufficiently large n. The proof consists of two main steps. Let x, y be random elements of S_n. Then it is shown that:

(i) the probability that $\langle x, y\rangle$ is a primitive subgroup of S_n is $1-1/n+O(1/n^2)$; and

(ii) the probability that neither $\langle x\rangle$ nor $\langle y\rangle$ contains a p-cycle for some prime $p < n-2$ is $< 1.8(\ln\ln n)^{-2}$ for all n large enough.

The result now follows by applying a classical theorem of Jordan: a primitive subgroup of S_n which contains a p-cycle for some prime $p < n-2$ must contain A_n.

The result in [22] was progressively refined in [13] and in [12]. Finally, assuming the classification of finite simple groups, Babai [5] proved that $p_n = 1 - 1/n + O(1/n^2)$ as conjectured in [22].

2.2. *Generating finite simple groups.* It follows from Netto's conjecture that almost all pairs of elements from A_n generate all of A_n as $n \to \infty$. At the end of [22] the author made the conjecture that a similar result might be true for the other finite simple groups. More precisely, as S runs through the finite nonabelian simple groups:

- if x, y are random elements from S, then the probability that $\langle x, y\rangle = S$ tends to 1 as $|S| \to \infty$.

This was a rash conjecture in 1969 since the proof that every finite simple group is 2-generator is based on the classification of finite simple groups (announced in 1980). However it turned out to be very fruitful. Naturally the complete proof of this conjecture was much more difficult than the special case where $G = A_n$. The general proof follows a different approach (closer to the one used in [5] for Netto's conjecture). We shall describe this approach now.

In 1936 Philip Hall [44] introduced the *Eulerian function* $\varphi(G, d)$ which is defined to be equal to the number of d-tuples from G which generate the finite group G. (The ordinary Euler function $\varphi(n)$ counts the number of 1-tuples which generate the cyclic group of order n.) He proved that his function has the form

$$\varphi(G, d) = \sum_{H \le G} \mu(G, H)|H|^d$$

where the sum is over all subgroups H of G and μ denotes the Möbius function on the lattice of subgroups of G. (Specifically μ is defined recursively by $\mu(G, G) = 1$ and $\sum_{H \le K \le G} \mu(G, K) = 0$ for all subgroups $H < G$.) The *zeta function* $\zeta(G, s)$ for G is then defined to be the reciprocal of the finite Dirichlet series

$$P(G, s) := \frac{\varphi(G, s)}{|G|^s} = \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s} \quad \text{where} \quad a_h(G) := \sum_{H \le G, |G:H|=n} \mu(G, H).$$

Clearly, $P(G, d)$ is the probability that a random d-tuple of elements from G generates G, and for specific groups Hall's formula may be used to compute this probability exactly (see [1] and [46]). The general zeta function has a number of

interesting properties, many of which are not well understood. See, for example, [14].

A lot of information about G is usually required if we want to calculate $P(G,s)$ exactly. However, in many cases a useful estimate can be obtained by using just the terms involving the maximal subgroups of G. If M is maximal in G, then $\mu(G,M) = -1$, and for all $s \geq 0$ we have the inequality

$$P(G,s) \geq 1 - \sum_{m=2}^{\infty} \frac{b_m(G)}{m^s}$$

where $b_m(G)$ is the number of maximal subgroup of index m in G. If we are lucky, then sufficient knowledge of the maximal subgroups of G may lead to a nontrivial estimate on $P(G,d)$ for sufficiently large d.

For example, in the alternating group A_n the maximal subgroups which are not primitive are easily described, and the maximal subgroups of A_n which are primitive are known to have small orders (see [26, Section 8.5 and Theorem 5.6B]). It is therefore possible to show that $P(A_n,2) \to 1$ as $n \to \infty$. This is the idea behind the proof in [5] although it is not stated in exactly this way. Indeed it is now known [55] that there are exactly $n/2 + o(n)$ conjugacy classes of maximal subgroups in A_n, and Babai's theorem follows easily from this because every proper subgroup of A_n has index at least n.

In [49] and [53] Kantor, Lubotzky, Liebeck and Shalev completed the proof of the conjecture in [22] by showing that as S runs over the finite simple groups, $P(S,2) \to 1$ as $|S| \to \infty$. Their proof uses detailed knowledge of the maximal subgroups of the various classes of simple groups and is, of course, dependent on the classification. As we shall see later (Section 4.2), the theorem which they proved has applications to problems which seem to have nothing to do with probabilistic questions.

In the past few years much more has been proved about this problem and related questions. For example, Liebeck and Shalev [56] proved a conjecture of Kantor and Lubotzky for finite nonabelian simple groups S:

- If x is random element and y is a random involution from S then $S = \langle x, y \rangle$ with probability approaching 1 as $|S| \to \infty$.

Guralnick and Kantor [42] have also proved:

- In each finite nonabelian simple group S there is a conjugacy class C such that for each fixed element $x \neq 1$ from S and a random element y from C, the probability that $\langle x, y \rangle = S$ is at least $1/10$.

3. Algorithms. A probabilistic algorithm is an algorithm which, at some stages, does not prescribe a determined step but "tosses a coin" to decide what the next step should be. The effect of introducing randomization into the execution of an algorithm can often speed up the running time of the algorithm as well as simplify its programming. Randomized algorithms of this type have been used

over the past 40 years, and have become increasingly important in solution of computational problems in combinatorics and algebra. A good general reference is [65]. The paper [15] gives a good overview of probabilistic algorithms applied to groups (see also [16] and [50]).

Of particular interest are *Monte Carlo algorithms.* These are randomized algorithms whose reliability (probability of returning the correct answer) can be increased arbitrarily at the expense of extra time. A Monte Carlo algorithm which never returns an incorrect answer (but may sometimes return "fail" to indicate that it cannot find the solution) is called a *Las Vegas algorithm.*

3.1. *An example: the structure of U_n.* An example of a Las Vegas algorithm which may be familiar is a *pseudo-prime test.* These are fast tests used to determine when a large integer n is composite and to give convincing evidence for primality when the integer is prime. The tests are based on recognizing distinguishing properties of the group $\mathbb{U}_n$ of units of the ring $\mathbb{Z}/n\mathbb{Z}$. We take a few moments to describe one of these tests here (see [72]).

Let $n > 1$ be an odd integer. Then we can represent the group $\mathbb{U}_n$ by the set of integers k with $1 \leq k < n$ with greatest common divisor $\mathrm{GCD}(k, n) = 1$ with the operation $\cdot$ of multiplication modulo n. If n is prime, then $\mathbb{U}_n$ is a cyclic group of order $n-1$ whose unique element of order 2 is $n-1$. If n is not prime then: either n is a prime power and so $|\mathbb{U}_n|$ does not divide $n-1$; or else n has at least two odd prime divisors and so $\mathbb{U}_n$ at least two elements of order 2. Suppose that n is not prime, and write $n - 1 = 2^t m$ where $t \geq 1$ and m is odd. We say that an integer k with $1 \leq k < n$ is a *witness* to the compositeness of n if any of the following hold:

(i) $\mathrm{GCD}(k, n) \neq 1$;
(ii) k has order not dividing $n-1$; or
(iii) k has even order $2h$ in $\mathbb{U}_n$ but k^h is not equal to $n-1$.

We can check these three conditions as follows: a particular value of k is a witness unless $k^m = 1$ or one of the elements $k^m, k^{2m}, \ldots, k^{2^{t-1}m}$ is equal to $n-1$. (The usefulness of this criterion depends on the fact that there is a fast way to compute powers of k modulo n; see, for example, [65].)

We now have a Las Vegas algorithm for checking compositeness of an odd integer. Choose a random integer k from the interval $1 \leq k < n$ and test to see whether k is a witness to the compositeness of n. If n is composite, then it can be proved that a randomly chosen k will be a witness with probability at least $1/2$. If we find a witness, then we know that n is composite and so we are finished. The test can never give us a proof that n is prime. However, if we perform d independent repetitions of the test on n and do not find a witness, then we should become increasingly convinced that n is prime since the probability that this event happens for a composite n is $\leq (1/2)^d$. This pseudo-prime test (or a similar test) is widely used in programs such as Maple as an inexpensive partial substitute for primality testing.

A similar search for witnesses can be used to determine whether or not a given finite set of matrices from $\mathrm{GL}(d,q)$ generates a subgroup containing $\mathrm{SL}(d,q)$ or one of the other classical groups (see [67], [69], [70] and [75]).

3.2. *Finding random elements.* A problem which arises in many probabilistic algorithms in group theory is:

- If we are given a set of generators for a group G, how can we efficiently generate random elements of G?

In some cases this can be done easily; an important case is when the group is given as a permutation group and a stabilizer chain and strong generating set are known. However, in other cases, when we have less information about G or a less structured generating set, the problem may be much more difficult.

In practice we do not require that the probability distribution be exactly uniform, but it should be close to uniform. Consideration of this problem leads to the analysis of random walks on the group (more precisely, on the Cayley graph associated with the set of generators) which can be described in terms of Markov chains. Measuring the efficiency of the algorithms to generate near random elements then reduces to determining how fast the Markov chain converges. This in turn uses some interesting linear representation theory (see [20] for an excellent introduction). Along similar lines we note that [2] discusses the problem of random walks on S_n and explains why 6 random riffle shuffles of an ordinary deck of cards are not sufficient to randomize the deck, but 7 shuffles suffice.

The general problem of generating random elements in a group is by no means satisfactorily solved, and it is clear that naïve methods of computing random elements are not adequate (see [6] and [71]). The problem is particularly important when G is a group of matrices over a finite field.

We remark that Babai, Luks and Seress have introduced a simple technique called *random subproducts* which can sometimes be used to substitute for the problem of finding random elements. This is based on the following easily proved proposition (see [15, Prop. 2.1]):

- If H is a proper subgroup of G and $x_1,\dots,x_m$ is a set of generators of G, then with probability $\geq 1/2$ a random element from the set

$$\{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_m^{\varepsilon_m} \mid \varepsilon_1,\varepsilon_2,\dots,\varepsilon_m \in \{0,1\}\}$$

  does *not* lie in H.

3.3. *Recognizing S_n.* Let $f(X)$ be a monic separable polynomial of degree n with integer coefficients, and let $G = \mathrm{Gal}(f)$ denote the Galois group of the splitting field of f where G is considered as a permutation group on the set of n roots. For each prime p we can consider the factorization

$$f(X) = f_1(X)f_2(X)\cdots f_r(X) \pmod p$$

where the $f_i(X)$ are monic irreducible modulo p. Suppose that p does not divide the discriminant $\mathrm{disc}(f)$ of f (so the factors $f_i(X)$ are distinct) and let $n_1 \leq n_2 \leq \cdots \leq n_r$ be the degrees of the factors. Then Frobenius showed that G contains permutations with cycle type $(n_1, n_2, \ldots, n_r)$ (see [82, Sect. 61]); and later Chebotarev showed that, in a suitable sense, the proportion of p which give rise to a particular cycle type is equal to the proportion of permutations in G with that cycle type (see [81]). This theorem is used to help identify the Galois groups of irreducible polynomials.

Van der Waerden also proved that "almost all" irreducible polynomials over the rationals have the full symmetric group as their Galois group. It is therefore worthwhile having a quick test to determine whether this is true for $\mathrm{Gal}(f)$. This leads to the following heuristic. For a sequence of "random" primes p find the associated cycle type $(n_1, n_2, \ldots, n_r)$ which must appear in $\mathrm{Gal}(f)$ according to Frobenius' theorem. Try to determine whether the existence of these cycle types in $\mathrm{Gal}(f)$ implies that $\mathrm{Gal}(f)$ is the full symmetric group. Recalling that two elements of S_n have the same cycle type exactly when they are conjugate in S_n, and taking into consideration Chebotarev's theorem, we have the following (slightly idealized question) about recognizing when we have the full symmetric group.

We shall say that a list $x_1, x_2, \ldots, x_d$ from a group G *invariably generates* G if $\langle y_1, y_2, \ldots, y_d \rangle = G$ whenever y_i is conjugate to x_i in G for $i = 1, 2, \ldots, d$. We then ask:

- Given $d \geq 2$ what is the probability that d random elements of S_n invariably generate S_n?

This problem was first posed by John McKay (private communication). He conjectured from numerical experiments that the expected number of random elements required to invariably generate S_n is a constant (about 5) independent of n. It is shown in [25] that $O\big((\ln n)^{1/2}\big)$ random elements are enough, and soon after that Luczak and Pyber [59] improved this to show that for each $\varepsilon > 0$ there exists a constant C (depending on ε but independent of n) such that C random elements of S_n invariably generate S_n with probability at least $1 - \varepsilon$. A good value of C is still not known.

3.4. *Other algorithmic problems.* There are many other algorithmic problems in which probabilistic methods play a part. For example, suppose that we are given a permutation group G. How difficult is it to find an element of order p in G? One answer is given by [47] where it is shown:

- If G is a permutation group of degree n, and p is a prime which divides $|G|$, then the probability that a random element of G has its order divisible by p is at least $1/n$.

Thus there is a good probability that a randomly chosen element will have its order divisible by p, and then some power of this element has order p. Surprisingly, the proof uses the classification of finite simple groups.

The paper [52] proposes a probabilistic algorithm for determining when a linear group has a tensor product decomposition, [79] describes a probabilistic algorithm to find the structure of a finite abelian group, and [64] considers the discrete logarithm problem in $\mathrm{GL}(n,q)$.

4. Applications to deterministic theorems. A famous theorem of Georg Cantor states that, because the set of real numbers is uncountable and the set of algebraic real numbers is countable, therefore the set of transcendental real numbers is uncountable; in particular, transcendental real numbers exist. In 1947 Paul Erdős [28] popularized similar arguments (they had occasionally been used earlier by other authors) to prove existence theorems in finite structures. This extension of the pigeonhole principle is now called the *probabilistic method* (see [3]) and has been used with great success in combinatorics. Recently probabilistic methods have been successfully applied to problems in group theory.

The possibility of such applications was predicted by Paul Turán. In a letter dated (Budapest. 16.3.1970) to the author, Turán concludes with:

> *My "Einstellung" with statistical group theory will be perhaps more understandable by repeating how I came to the idea of statistical group theory. My "old age dream" (an expression, imitating "Kronecker's Jugendtraum") is to disprove Burnside's conjecture (if G is finitely generated and for all elements x we have with the same n $x^n = e$ then G is finite) by finding for such groups an appropriate representation in a space so that one could find that in this space the "points" belonging to finite groups form a "small" set. But I could not find a good representation so far.*

So far no-one has succeeded in tackling Burnside's problem in this way, but in recent years there have been a number of successful applications of probabilistic group theory somewhat along the lines which Turán describes. We discuss some of these.

4.1. *The* $(2,3)$*-generator problem.* The *(2,3)-generator problem* was open for nearly a century. It arose from the study of groups acting on Riemann surfaces and asks:

- Which finite simple groups S can be generated by two elements x, y of orders 2 and 3, respectively?

The modular group $\mathrm{PSL}(2,\mathbb{Z})$ is isomorphic to a free product $\langle x\rangle * \langle y\rangle$ of a group of order 2 and a group of order 3. Therefore the $(2,3)$-generator problem is equivalent to: which simple groups S are homomorphic images of $\mathrm{PSL}(2,\mathbb{Z})$?

It is easily verified that A_n is $(2,3)$-generated for all $n > 8$, but for the other families of simple groups the problem is more complicated. In 1996 that it was shown that the simple groups $\mathrm{PSL}(d,q)$ are $(2,3)$-generated for odd q except when $d = 2$ and $q = 9$ (see [18] and [19]). At that time it was conjectured that, with a finite number of exceptions, every finite simple group was $(2,3)$-generated.

A strengthened form of this conjecture was tackled by Liebeck and Shalev [54] who proved:

- If S runs over the finite classical simple linear groups which are *not* of the form $\mathrm{PSp}(4,q)$, then the probability that two random elements of order 2 and 3, respectively, generate S tends to 1 as $|S| \to \infty$. Moreover, the corresponding probability as S runs over the groups $\mathrm{PSp}(4,q)$ with $q \neq 2^k$ or 3^k is $1/2$.

Unexpectedly, it turned out that the groups from the two infinite families $\mathrm{PSp}(4,2^k)$ and $\mathrm{PSp}(4,3^k)$ fail to be $(2,3)$-generated. However, Liebeck and Shalev's result shows that, except for these families, all finite simple classical groups—with finitely many possible exceptions—are $(2,3)$-generated (what the exceptions may be is still unknown).

Since then Lübeck and Malle [57] settled the $(2,3)$-generation problem for exceptional groups of Lie type using more direct methods. They show that, except for $G_2(2)'$ and the Suzuki groups, all of these groups are $(2,3)$-generated.

4.2. *Residual properties of free groups.* A group G is called *residually-$\mathcal{C}$* for a class $\mathcal{C}$ of groups if for each $x \neq 1$ in G there is a normal subgroup N of G with $x \notin N$ and G/N isomorphic to a group in $\mathcal{C}$. It is well known that any free group F of rank ≥ 2 is residually finite; indeed F is a residually finite p-group for each prime p. In 1969 Magnus [60] asked the question:

- Is it true that F residually-$\mathcal{X}$ for every infinite set $\mathcal{X}$ of finite nonabelian simple groups?

Equivalently, is it true that for each $x \neq 1$ in F there exists a normal subgroup N_x such that $x \notin N_x$ and F/N_x is isomorphic to one of the groups S in $\mathcal{X}$?

The problem is easily reduced to the case where F has rank 2 since every free group of rank > 2 is residually free of rank 2. After several partial solutions, Magnus' question was completely answered in the affirmative by Weigel in a series of three long papers ([85], [83] and [84]). More recently, a stronger probabilistic version of Weigel's theorem has been proved in [21] (both theorems require the classification of finite simple groups). We can explain the latter result as follows.

Let F be the free group on two generators X, Y and let $w(X,Y)$ be a nontrivial word in F. In order to prove Magnus' conjecture it is necessary to show that there exists $S \in \mathcal{X}$ and a homomorphism of F onto S such that $w(X,Y)$ is not mapped onto the identity of S. Equivalently, there exist $x, y \in S$ such that $S = \langle x, y \rangle$ and $w(x,y) \neq 1$. In [21] the following is proved.

- Let $w(X,Y)$ be a nontrivial word in F. Then, as S runs over the set of all finite nonabelian simple groups, the probability that two random elements x, y from S generate S and satisfy $w(x,y) \neq 1$ tends to 1 as $|S| \to \infty$.

Weigel's theorem clearly follows from this. The proof is simplified because we already know (see Section 2.2) that x, y generate S with probability tending to 1, so it is enough to show that $w(x,y) \neq 1$ also with probability tending to 1 as

$|S| \to \infty$. This is done by considering separately each family in a finite set of infinite families of nonabelian simple groups.

We illustrate the proof for the family of alternating groups A_n (the easiest case). Assume that $w(X,Y)$ is a reduced word of length $r \geq 1$, and write $w(X,Y) = w_1(X,Y)\cdots w_r(X,Y)$ where $w_i(X,Y) \in \{X, X^{-1}, Y, Y^{-1}\}$ for each i. Suppose that s of these factors are X or X^{-1} and t of the factors are Y or Y^{-1} and assume that $n \geq r+2$. Let α_0 be a fixed element from the set Ω on which A_n acts. Now for each $(r+1)$-tuple $(\alpha_0, \alpha_1, \ldots, \alpha_r)$ of distinct points in Ω, there exist $(n-s)!/2$ values of $x \in A_n$ such that $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ for the indices where $w_i(X,Y) \in \{X, X^{-1}\}$, and $(n-t)!/2$ values of y such that $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ for the indices where $w_i(X,Y) \in \{Y, Y^{-1}\}$. Since $\alpha_0^{w(x,y)} = \alpha_r \neq \alpha_0$ for such choices of x and y, we must have $w(x,y) \neq 1$. Since there are $(n-1)!/(n-r-1)!$ $(r+1)$-tuples of distinct points starting with α_0, this guarantees that there are at least $\frac{1}{4}(n-s)!\,(n-t)!\,(n-1)!/(n-r-1)!$ pairs (x,y) from A_n for which $w(x,y) \neq 1$. This latter number is asymptotic to $[\frac{1}{2}n!]^2$ and so the probability that two random elements from A_n satisfy $w(x,y) \neq 1$ tends to 1 as $n \to \infty$. In particular, this gives a simple solution to Magnus' question in the special case whenever $\mathcal{X}$ is an infinite set of alternating groups.

5. Infinite groups and the ubiquity of free subgroups. When we consider infinite groups, even the statement of probabilistic questions becomes a little subtle. First we need a suitable probability distribution defined on the group. For some groups this can be done very naturally. For example, there is a natural probability distribution on a profinite group defined in terms of the uniform distribution on its finite quotients (its Haar measure). In this context Mann and Shalev ([62] and [61]) have considered the problem (for integers $k \geq 1$):

- For which profinite groups G is there a positive probability that the (closed) subgroup generated by a random k-tuple of elements from G is equal to G?

In particular, they show that, if G satisfies this condition for some k, then G also satisfies the condition of polynomial maximal subgroup growth. Related theorems are proved in [58], [8] and [48].

If we have no natural probability distribution on our group, it may still be possible to make "almost all" statements in a sense similar to "almost all real numbers are transcendental". These are not probabilistic statements, but they have much the same flavour as "probability 1" statements.

An early example of such a theorem is due to Epstein [27] who proved that

- If G is a simple Lie group, then almost all k-tuples from G generate a free group of rank k.

In this case "almost all" means all but a set of measure 0 in the natural measure on G. If G is not compact, this measure does not define a probability distribution on G.

In 1990 the author proved in [24] a parallel result on the ubiquity of free subgroups in the infinite symmetric group of countably infinite degree

- If $k \geq 2$, then almost all k-tuples from Sym($\mathbb{N}$) generate a subgroup which is free of rank k. Moreover, almost all of these subgroups are m-transitive for every $m \geq 1$.

This gave a nonconstructive proof of the existence of highly transitive free subgroups of Sym($\mathbb{N}$) (examples of such subgroups had been constructed earlier in [63]). For $G = \text{Sym}(\mathbb{N})$ there is no natural measure. However, we can define a simple metric d on G by setting $d(x, y) := 2^{-t}$ if xy^{-1} fixes $0, 1, \ldots, t-1$ but does not fix t. Under this metric G is a complete metric space and also a topological group. In particular, the Baire category theorem holds in G^k, and so it makes sense to consider meagre sets (= sets of the "first category") as "null". So in this context we say that a subset of G^k includes *almost all* k-tuples in G if its complement is meagre.

The result above has been extended by Glass and others (see [39], [80] and [40]). The proper setting for these theorems appears to be in the context of metrizable topological groups which are Polish spaces (see [10]) since these are precisely the spaces in which a Baire category theorem holds.

Other theorems on the ubiquity of free subgroups in other contexts are found in [9] and [4].

ACKNOWLEDGEMENT. This work was supported in part by NSERC under Grant A7171.

REFERENCES

1. Vincenzo Acciaro, *The probability of generating some common families of finite groups.* Utilitas Math. **49**(1996), 243–254.
2. D. Aldous and P. Diaconis, *Shuffling cards and stopping times.* Amer. Math. Monthly **93**(1986), 333–348.
3. Noga Alon and Joel H. Spencer, *The probabilistic method.* Wiley-Interscience, New York, 2000.
4. G. N. Arzhantseva and A. Yu. Ol'shanshij, *The class of groups all of whose subgroups with lesser number of generators are free is generic.* Math. Notes **59**(1996), 350–355 (transl. from Mat. Zametki **59**(1996), 489–496.
5. László Babai, *The probability of generating the symmetric group.* J. Combin. Theory Ser. A **52**(1989), 148–153.
6. László Babai and Igor Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm".* Proc. Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, 2000), ACM, New York, 2000, 627–635.
7. M. R. Best, *The distribution of some variables on symmetric groups.* Nederl. Akad. Wetensch. Proc. Ser. A **73**=Indag. Math. **32**(1970), 385–402.
8. Meenaxi Bhattacharjee, *The probability of generating certain profinite groups by two elements.* Israel J. Math. **86**(1994), 311–329.
9. ———, *The ubiquity of free subgroups in certain inverse limits of groups.* J. Algebra **172**(1995), 134–146.
10. N. Bourbaki, *General topology (part 2).* Hermann, Paris, 1966.
11. J. D. Bovey, *An approximate probability distribution for the order of the elements of the symmetric group.* Bull. London Math. Soc. **12**(1980), 41–46.
12. ———, *The probability that some power of a permutation has small degree.* Bull. London Math. Soc. **12**(1980), 47–51.

13. John Bovey and Alan Williamson, *The probability of generating the symmetric group.* Bull. London Math. Soc. **10**(1978), 91–96.
14. Kenneth S. Brown, *The coset poset and probabilistic zeta function of a finite group.* J. Algebra **225**(2000), 989–1012.
15. Gene Cooperman and Larry Finkelstein, *Combinatorial tools for computational group theory.* in: Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **11**, Amer. Math. Soc., Providence, RI, 1993,, 53–86.
16. Gene Cooperman and George Havas, *Elementary algebra revisited: randomized algorithms.* In: Randomization methods in algorithm design (Princeton, NJ, 1997), DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **43**, Amer. Math. Soc., Providence, RI, 1999, 37–44.
17. J. Dénes, P. Erdős, and P. Turán, *On some statistical properties of the alternating group of degree n.* Enseign. Math. (2) **15**(1969), 89–99.
18. L. Di Martino and N. A. Vavilov, $(2,3)$*-generation of* $\mathrm{SL}(n,q)$. *I.* Comm. Algebra **22**(1994), 1321–1347.
19. ———, $(2,3)$*-generation of* $\mathrm{SL}(n,q)$. *II.* Comm. Algebra **24**(1996), 487–515.
20. Persi Diaconis, *Group representations in probability and statistics.* Institute of Mathematical Statistics, Hayward, CA, 1988.
21. J. D. Dixon, L. Pyber, A. Seress and A. Shalev, *Residual properties of free groups and probabilistic methods.* Submitted for publication.
22. John D. Dixon, *The probability of generating the symmetric group.* Math. Z. **110**(1969), 199–205.
23. ———, *Maximal abelian subgroups of the symmetric group.* Canad. J. Math. **23**(1971), 426–438.
24. ———, *Most finitely generated permutation groups are free.* Bull. London Math. Soc. **22**(1990), 222–226.
25. ———, *Random sets which invariably generate the symmetric group.* Discrete Math. **105**(1992), 25–39.
26. John D. Dixon and Brian Mortimer, *Permutation groups.* Springer, New York, 1996.
27. D. B. A. Epstein, *Almost all subgroups of a Lie group are free.* J. Algebra **19**(1971), 261–262.
28. P. Erdős, *Some remarks on the theory of graphs.* Bull. Amer. Math. Soc. **53**(1947), 292–294.
29. P. Erdős and R. R. Hall, *Probabilistic methods in group theory. II.* Houston J. Math. **2**(1976), 173–180.
30. ———, *Some new results in probabilistic group theory.* Comment. Math. Helv. **53**(1978), 448–457.
31. P. Erdős and P. Turán, *On some problems of a statistical group-theory. I.* Z. Wahrschein. Verw. Gebeite **4**(1965), 175–186.
32. ———, *On some problems of a statistical group-theory. II.* Acta Math. Acad. Sci. Hungar. **18**(1967), 151–163.
33. ———, *On some problems of a statistical group-theory. III.* Acta Math. Acad. Sci. Hungar. **18**(1967), 309–320.
34. ———, *On some problems of a statistical group-theory. IV.* Acta Math. Acad. Sci. Hungar. **19**(1968), 413–435.
35. Jason Fulman, *Cycle indices for the finite classical groups.* J. Group Theory **2**(1999), 251–289.
36. ———, *A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups.* J. Algebra **212**(1999), 557–590.
37. ———, *A probabilisitic approach to conjugacy classes in the finite symplectic and orthogonal groups.* J. Algebra **234**(2000), 207–224.
38. J. E. Fulman, M. D. Galloy, G. J. Sherman and J. M. Vanderkam, *Counting nilpotent pairs in finite groups.* Ars Combin. **54**(2000), 161–178.
39. A. M. W. Glass, *The ubiquity of free groups.* Math. Intelligencer **14**(1992), 54–57.

40. A. M. W. Glass, Stephen H. McCleary and Rubin Matatyahu, *Automorphism groups of countable highly homogeneous partially ordered sets*. Math. Z. **214**(1993), 55–66.
41. R. M. Guralnick and J. S. Wilson, *The probability of generating a finite soluble group*. Proc. London Math. Soc (3) **81**(2000), 405–427.
42. Robert M. Guralnick and William M. Kantor, *Probabilistic generation of finite simple groups*. J. Algebra **234**(2000), 743–792.
43. W. H. Gustafson, *What is the probability that two group elements commute?* Amer. Math. Monthly **80**(1973), 1031–1034.
44. Philip Hall, *The eulerian functions of a group*. Quart. J. Math. **7**(1936), 134–151.
45. R. R. Hall, *Extensions of a theorem of Erdős-Rényi in probabilistic group theory*. Houston J. Math. **3**(1977), 225–234.
46. Ishai Ilani, *Zeta functions related to the group* $\mathrm{SL}_2(\mathbb{Z}_p)$. Israel J. Math. **109**(1999), 157–172.
47. I. M. Isaacs, W. M. Kantor and N. Spaltenstein, *On the probability that a group element is p-singular*. J. Algebra **176**(1995), 139–181.
48. Moshe Jarden and Alexander Lubotzky, *Random normal subgroups of free profinite groups*. J. Group Theory **2**(1999), 213–224.
49. William M. Kantor and Alexander Lubotzky, *The probability of generating a finite classical group*. Geom. Dedicata **36**(1990), 67–87.
50. William M. Kantor and A. Seress (eds.), *Groups and Computation III*. Proc. 3rd Internat. Conf. (Ohio State University, 1999), Walter de Gruyter, Berlin, 2001.
51. A. Kolmogorov, *Foundations of the theory of probability*. Chelsea, New York, NY, 1956 (transl. of "Grundbegriffe der Wahrscheinlichkeitsrechnung", 1933).
52. C. R. Leedham-Green and E. A. O'Brien, *Recognizing tensor products of matrix groups*. Internat. J. Algebra Comput. **7**(1997), 541–559.
53. Martin W. Liebeck and Aner Shalev, *The probability of generating a finite simple group*. Geom. Dedicata **56**(1995), 103–113.
54. ———, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem*. Ann. of Math. (2) **144**(1996), 77–125.
55. ———, *Maximal subgroups of symmetric groups*. J. Combin. Theory Ser. A **75**(1996), 341–352.
56. ———, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*. J. Algebra **184**(1996), 31–57.
57. Frank Lübeck and Gunter Malle, $(2,3)$*-generation of exceptional groups*. J. London Math. Soc. (2) **59**(1999), 109–102.
58. Alexander Lubotzky, *Random elements of a free profinite group generate a free subgroup*. Illinois J. Math. **37**(1993), 78–84.
59. Tomasz Luczak and László Pyber, *On random generation of the symmetric group*. Combin. Probab. Comput. **2**(1993), 505–512.
60. W. Magnus, *Residually finite groups*. Bull. Amer. Math. Soc. **75**(1969), 305–316.
61. Avinoam Mann, *Positively finitely generated groups*. Forum Math. **8**(1996), 429–459.
62. Avinoam Mann and Aner Shalev, *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*. Israel J. Math. **96**(1996), 449–468.
63. T. P. McDonough, *A permutation representation of a free group*. Quart. J. Math. Oxford (2) **28**(1977), 353–356.
64. Alfred J. Menezes and Yi-Hong Wu, *The discrete logarithm problem in* $\mathrm{GL}(n,q)$. Ars Combin. **47**(1997), 23–32.
65. Rajeev Motwani and Prabhakar Raghavan, *Randomized algorithms*. Cambridge Univ. Press, Cambridge, 1995.
66. E. Netto, *Substitutionentheorie and ihre Anwendungen auf die Algebra*. Teubner, Leipzig, 1882; English transl. 1892, second edition, Chelsea, New York, 1964.
67. Peter M. Neumann and Cheryl E. Praeger, *A recognition algorithm for special linear groups*. Proc. London Math. Soc. (3) **65**(1992), 555–603.
68. J.-L. Nicolas, *Sur l'ordre maximum d'un élément dans le groupe* S_n *des permutations*. Acta Arith. **14**(1967/68), 315–332.

69. Alice C. Niemeyer and Cheryl E. Praeger, *Implementing a recognition algorithm for classical groups.* In: Groups and computation, II (New Brunswick, NJ, 1995), Amer. Math. Soc., Providence, RI, 1997, 273–296.

70. ———, *A recognition algorithm for classical groups over finite fields.* Proc. London Math. Soc. (3) **77**(1998), 117–169.

71. Igor Pak, *What do we know about the product replacement algorithm?* Groups and Computation III (Ohio State University, 1999), Walter de Gruyter, Berlin, 2001, 301–347.

72. M. O. Rabin, *Probabilistic algorithm for primality testing.* J. Number Theory **12**(1980), 128–138.

73. Vladamir N. Sachov, *Probabilistic methods in combinatorial analysis.* Cambridge Univ. Press, Cambridge, 1997.

74. Aner Shalev, *Simple groups, permutation groups and probability.* In: Proc. International Congress of Mathematicians, vol. II (Berlin, 1998), Doc. Math. **1998**, 129–137 (electronic).

75. ———, *A theorem on random matrices and some applications.* J. Algebra **199**(1998), 124–141.

76. ———, *Asymptotic group theory.* Notices Amer. Math. Soc. **48**(2001), 383–389.

77. Gary Sherman, *What is the probability an automorphism fixes a group element?* Amer. Math. Monthly **82**(1975), 261–264.

78. ———, *A probabilistic estimate of invariance for groups.* Amer. Math. Monthly **85**(1978), 361–363.

79. Edlyn Teske, *A space efficient algorithm for group structure computation.* Math. Comp. **67**(1998), 1637–1663.

80. J. K. Truss, *Joint embeddings of infinite permutation groups.* Algebra Logic Appl. **9**(1997), 121–134.

81. N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören.* Math. Annalen **95**(1926), 191–228.

82. B. L. van der Waerden, *Modern algebra.* Ungar, New York, 1948.

83. T. Weigel, *Residual properties of free groups II.* Comm. Algebra **20**(1992), 1395–1425.

84. ———, *Residual properties of free groups III.* Israel J. Math. **77**(1992), 65–81.

85. ———, *Residual properties of free groups.* J. Algebra **160**(1993), 16–41.

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
K1S 5B6
email: jdixon@math.carleton.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 24 (1), 2002 pp. 16–20

ON THE SPECTRAL THEORY APPROACH TO COUNTING HYPERBOLIC LATTICE POINTS IN THIN REGIONS

C. J. MOZZOCHI

Presented by M. Ram Murty, FRSC

ABSTRACT. In this paper we establish rigorously for the modular group the unexpected result that if one employs the spectral expansion of automorphic kernels in the expected way exactly and precisely analogous to the technique of Hoheisel for counting primes in short intervals, it is not possible for one to get results concerning the counting of hyperbolic lattice points in thin regions even as good as those obtained directly and routinely from the spectral expansion for $P(X)$ itself.

RÉSUMÉ. Nous établissons rigoureusement dans cet article, pour le cas du groupe modulaire, le fait surprenant que si l'on emploie le développement spectral des noyaux automorphes de manière précisément analogue à la technique de Hoheisel pour le comptage des nombres premiers dans de petits intervalles, il n'est pas possible d'obtenir des résultats concernant le comptage de points entiers dans le plan hyperbolique dans des petites régions qui soient même aussi bons que ceux obtenus directement à partir du développement spectral de $P(X)$.

1. Introduction. For the hyperbolic circle problem the object is to estimate for fixed $z \in H$ and $w \in H$

$$P(X) = \#\left\{\gamma \in \Gamma \;\middle|\; u(\gamma z, w) \leq \frac{X-2}{4}\right\}$$

where w is the center of the hyperbolic circle of radius $\frac{X-2}{4}$ and

$$u(z_1, z_2) = \frac{|z_1 - z_2|^2}{4 \operatorname{Im} z_1 \operatorname{Im} z_2}.$$

Several authors have carefully investigated this problem, for example, Iwaniec [5], Huber [4], Patterson [7], Phillips and Rudnick [8] and Chamizo [1], [2]. In Section 2 we state explicitly some results of Iwaniec and Chamizo.

For the problem of hyperbolic lattice points in thin regions the object, in analogy with Hoheisel's theorem for primes in short intervals, is to determine the smallest exponent δ where $0 < \delta \leq 1$ such that

$$P(X+h) - P(X) \sim ch \quad \text{as} \quad X \to \infty$$

Received by the editors February 2, 2000.
AMS subject classification: 11F03, 11F11, 11F12, 11F72.

where $h = X^{\delta}$ and c is a fixed positive constant.

We have not been able to find anything in the literature concerning this problem.

We note the following conventional definitions where $s = \sigma + it$, $0 \le \sigma \le 1$, $t \in \mathbf{R}$. For notation and definitions, see [5].

$$F_s(u) := F(s, 1-s; 1, -u)$$
$$h(t) := 4\pi \int_0^{\infty} F_s(u)k(u)\,du,$$
$$K(z,w) := \sum_{\gamma\in\Gamma} k\big(u(z,\gamma w)\big).$$

$K(z,w)$ is called the *automorphic kernel.* The spectral expansion of the automorphic kernel is given by:

THEOREM 1.1. *Let $K(z,w)$ be an automorphic kernel given by a point-pair invariant $k(z,w) = k\big(u(z,w)\big)$ whose Selberg/Harish-Chandra transform $h(t)$ satisfies*

$$h(t) \text{ is even,}$$
$$h(t) \text{ is holomorphic in the strip } |\operatorname{Im} t| \le \frac{1}{2} + \epsilon,$$
$$h(t) \ll (|t|+1)^{-2-\epsilon} \text{ in the strip.}$$

Then,

$$K(z,w) = \frac{1}{2}\sum h(t_j)u_j(z)\overline{u}_j(w) + \sum_a \frac{1}{4\pi}\int_{-\infty}^{\infty} h(r)E_a\left(z, \frac{1}{2}+ir\right)\overline{E}_a\left(w, \frac{1}{2}+ir\right)dr \tag{1}$$

which converges absolutely and uniformly on compacta.

For a proof *cf.* [5, p. 113].

By the definition of $K(z,w)$ it is immediate that questions about $P(X)$ reduce to evaluating $K(w,z)$ by means of Theorem 1.1 for a properly chosen function $k(u)$.

2. Preliminary results. In the sequel the following theorems and lemmas will be utilized.

THEOREM 2.1. *Let $T \ge 1$ and $z \in H$. We have*

$$\sum_{|t_j|<T} |u_j(z)|^2 + \sum_a \int_{-T}^{T} \left|E_a\left(z, \frac{1}{2}+it\right)\right|^2 dt \ll T^2 + Ty_{\Gamma}(z)$$

where

$$y_\Gamma(z) = \max_a \max_{\gamma\in\Gamma}(\operatorname{Im}\sigma_a^{-1}\gamma z)$$

and where the implied constant depends on the group Γ *alone.*

For a proof *cf.* [5, p. 110].

In the sequel to simplify the notation we denote the sum (1)

$$\sum\!\!+\int_{T_1\le|t|\le T_2} h(t)$$

and we let

$$t_1 \text{ be the smallest } t_j \text{ in } [T_1, T_2],$$
$$F(t) = t^2 + t.$$

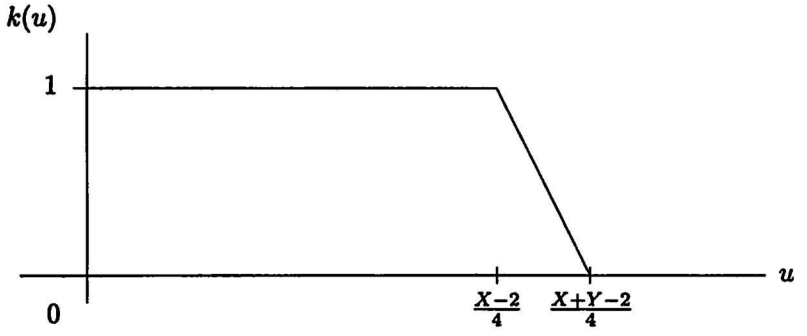
LEMMA 2.1. *Let* $H(t)$ *be decreasing and such that* $|h(t)| \le H(t)$. *Then*

$$\sum\!\!+\int_{T_1\le|t|\le T_2} h(t) \ll \int_{T_1}^{T_2} H(t)(t+1)\,dt + H(T_2)F(T_2) + H(T_1)F(T_1) + H(t_1)F(t_1)$$

where the implied constant is a function of z, w *and* Γ.

The proof follows in a straightforward way by Cauchy's inequality and partial summation.

For each X we define $k(u) = k_x(u)$



where $X \ge 2Y \ge 2$.

LEMMA 2.2. *The Selberg/Harish-Chandra transform of* $k(u)$ *defined above satisfies*

$$h(t) = \pi^{1/2}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s+1)}X^s + O(Y + X^{1/2}) \tag{2}$$

if $\frac{1}{2} < s \leq 1$ *where the implied constant depends on* s, *and*

$$h(t) \ll |s|^{-5/2}(\min(|s|, T) + \log X)X^{1/2} \tag{3}$$

if $\operatorname{Re} s = \frac{1}{2}$ *where* $T = XY^{-1}$ *and the implied constant is absolute.*

(*Cf.* [5, p. 191].)

THEOREM 2.2. *Let* Γ *be a finite volume group. For* $X \geq 2$ *we have*

$$P(X) = \sum_{\frac{1}{2} < s_j \leq 1} \pi^{1/2} \frac{\Gamma(s_j - \frac{1}{2})}{\Gamma(s_j + 1)} u_j(z)\overline{u}_j(w)X^{s_j} + O(X^{2/3}). \tag{4}$$

This follows in a straightforward manner from Lemma 2.1 and Lemma 2.2. (*Cf.* [5, p. 192]).

In the folklore it is believed that $\frac{2}{3}$ can be replaced with $\frac{1}{2}$, which would be best possible.

In [1] and [2] Chamizo shows that $\frac{2}{3}$ can be replaced with $\frac{1}{2}$ on average over a large enough number of radii X or starting points z (or by symmetry, centers w).

3. Restriction to the modular group. Using Theorem 1.1 with $k(u)$ defined as above and using the fact that for the modular group we only have to consider $s_0 = 1$, which corresponds to the lowest eigenvalue $\lambda_0 = 1$ with constant eigenfunctions $u_0(z) = u_0(w) = |F|^{-1/2}$ so it contributes $\pi|F|^{-1}X = 3X$ to the main term. Hence in this case if the error in the circle problem is $O(X^\theta)$, one can take $h = X^{\theta+\epsilon}$ for every $\epsilon > 0$, in the problem of hyperbolic lattice points in thin regions.

By direct estimation and calculation, by our choice of $k(u)$ we have by Theorem 1.1 for the modular group

$$\begin{aligned} &|P(X+h) - P(X) - 3h| \\ &\quad \leq |M(X+h) - M(X)| + |E_1(X)| + |E_1(X+h)| \\ &\quad\quad + |E_2(X)| + |E_2(X+h)| + |E_3(X)| + |E_3(X+h)| + |E_4(X)| \\ &\quad\quad + |E_4(X+h)| + |E_5(X)| + |E_5(X+h)| + |E_6(X)| + |E_6(X+h)|. \end{aligned} \tag{5}$$

Let $s = \frac{1}{2} + it$. Suppose one could show for each $\epsilon > 0$ and for each $\epsilon_1 > 0$ there exists $X_0(\epsilon, \epsilon_1)$ such that if $X \geq X_0(\epsilon, \epsilon_1)$, $X \ll u \ll X$, $1 \leq t \leq X^{1/2-\epsilon_1}$

$$|F_s(u)| \ll \frac{X^\epsilon}{t\sqrt{u}} \tag{6}$$

where the implied constant depends only on ϵ and ϵ_1.

Then we obtain the desired asymptotic formula with $h = X^{2/3+\epsilon_3}$.

4. Observations. It can be shown *cf.* [5, p. 26],

$$F_s(u) = \frac{1}{\pi}\int_0^{\pi}\Big(1+2u+2\big(u(u+1)\big)^{1/2}\cos\theta\Big)^{-s}\,d\theta.$$

We assume the hypothesis of (6). Then integrating by parts once and rearranging terms combined with the trivial observation $E(X) \ll X^{\epsilon/2-1}$ uniformly in t and u, we obtain for $X \geq X_0(\epsilon)$

$$F_s(u) \ll \frac{X^{2-\epsilon}}{t\sqrt{u}}$$

for any $\epsilon > 0$ for $X \ll u \ll X$ and $1 \leq t \leq X^{1/2-\epsilon}$.

We see no way to improve this estimate vis-a-vis restrictions on s, t and u.

We define $I(t,u) := \int_a^b e^{itP(u,\theta)}q(u,\theta)\,d\theta$.

THEOREM 4.1. *For any fixed u if $P'(u,\theta)$ has no zero in $[a,b]$, then*

$$I(t,u) = \frac{ie^{iP(u,q)}q(a)}{tP'(u,a)} - \frac{ie^{itP(u,b)}q(b)}{tP'(u,b)} + o\left(\frac{1}{t}\right) t \to \infty$$

cf. Section 11.3 *in* [6].

It is not difficult to see that Theorem 4.1 implies that (6) is not true.

ACKNOWLEDGEMENT. I would like to thank Henryk Iwaniec for suggesting that I investigate this problem, for several helpful conversations, and for one crucial suggestion.

REFERENCES

1. F. Chamizo, *The large sieve in Riemann surfaces.* Acta Arith. (4) **77**(1966), 303–313.
2. ———, *Some applications of the large sieve in Riemann surfaces.* Acta. Arith. (4) **77**(1996), 315–337.
3. K. Chandrasekharan, *Arithmetical Functions.* Springer-Verlag, Berlin-Heidelberg, 1970.
4. H. Huber, *Uber eine neue Klasse automorpher Functionen und ein Gitterpunktproblem in the hyperbolischen Ebene.* Comment. Math. Helv. **30**(1956), 20–62.
5. H. Iwaniec, *Introduction to the Spectral Theory of Automorphic Forms.* Rev. Math. Iberoamericana, Madrid, 1995.
6. F. W. J. Olver, *Asymptotics and Special Functions.* Academic Press, New York-London, 1974.
7. S. J. Patterson, *A lattice-point problem in hyperbolic space.* Mathematika **22**(1975), 81–88.
8. R. Phillips and Z. Rudnick, *The circle problem in the hyperbolic plane.* J. Funct. Anal. (1) **121**(1994), 78–116.

P.O. Box 1424,
Princeton, NJ 08542
USA
cjm@ix.netcom.com

C. R. Math. Rep. Acad. Sci. Canada Vol. 24 (1), 2002 pp. 21–25

GROUP ACTIONS AND THE FUNCTIONAL EQUATION OF THE MEAN SUN

HARALD FRIPERTINGER

Presented by J. Aczél, FRSC

ABSTRACT. A generalization of the functional equation $g(s+t)x(u) = g(s)x(t+u)$ $(\forall s,t,u \in R)$ of the mean sun is studied, where a group G acts on a set X, $(R,+)$ is a not necessarily commutative group and both $x\colon R \to X$ and $g\colon R \to G$ are unknown functions, which will be determined by the equation.

RÉSUMÉ. Une généralisation de l'équation fonctionnelle $g(s+t)x(u) = g(s)x(t+u)$ $(\forall s,t,u \in R)$ du soleil moyen est examinée, où une groupe agit sur un ensemble X, $(R,+)$ est un groupe, mais pas nécessairement commutatif, et $x\colon R \to X$ et aussi $g\colon R \to G$ sont des fonctions inconnues lesquelles seront déterminées par l'équation fonctionnelle.

Local solar time is measured by a sundial. When the center of the sun is on an observer's meridian, the observer's local solar time is zero hours (noon). Because the earth moves with varying speed in its orbit at different times of the year and because the plane of the earth's equator is inclined to its orbital plane, the length of the solar day is different depending on the time of year. It is more convenient to define time in terms of the average of local solar time. Such time, called mean solar time, may be thought of as being measured relative to an imaginary sun (the mean sun) that lies in the earth's equatorial plane and about which the earth orbits with constant speed. Every mean solar day is of the same length.[1]

In [5], [2] it is shown that the mean sun satisfies the functional equation

$$M(\lambda+t,\phi)^T y(s) = M(\lambda,\phi)^T y(s+t) \quad \forall s,t,\lambda \in \mathbb{R}, -\pi/2 < \phi < \pi/2$$

where $y(s)$ is a vector of length 1 which is the direction from the center of the earth to the sun at the time s (one day corresponds to 2π) expressed in a geocentric coordinate system. As a basis of this system we can choose two orthogonal vectors in the equatorial plane and one vector along the axis of the earth. $M(\lambda,\phi)$ is the matrix

$$M(\lambda,\phi) = \begin{pmatrix} -\sin\lambda & -\sin\phi\cos\lambda & \cos\phi\cos\lambda \\ \cos\lambda & -\sin\phi\sin\lambda & \cos\phi\sin\lambda \\ 0 & \cos\phi & \sin\phi \end{pmatrix}.$$

[1] http://www.infoplease.com/ce6/society/A0845838.html

Received by the editors January 8, 2001.
Supported by the Fonds zur Förderung der wissenschaftlichen Forschung P14342-MAT.
AMS subject classification: 39-02, 20A05.

Then $M(\lambda,\phi)y(s)$ is the direction from the earth to the sun expressed in a local coordinate system on the surface of the earth in the point of longitude λ and latitude ϕ.

In the present paper we investigate a generalization of this equation for fixed ϕ. To be more precise we will deal with the following problem:

Let $(G,\cdot)$ be a group acting on a set X (*cf.* [1], [3], [4], [6]) and let $(R,+)$ be a not necessarily commutative group. Find all functions $x\colon R\to X$ and $g\colon R\to G$ which satisfy

$$g(s+t)x(u)=g(s)x(t+u),\quad \forall s,t,u\in R. \tag{1}$$

The group R is a generalization of $\mathbb{R}$, the matrices expressing the change of the coordinate system are now elements of the group G and X represents a generalization of the set of all vectors in $\mathbb{R}^3$.

To begin with we will collect some properties of the functions g and x. Later we determine all solutions g and x of (1). In a first step we replace g by another function $h\colon R\to G$ defined by

$$h(r):=g(0)^{-1}g(r).$$

It is easy to prove that $h(0)=1\in G$ and

$$h(s)x(u)=x(s+u)\quad \forall s,u\in R. \tag{2}$$

LEMMA 1. *If the functions $x\colon R\to X$ and $h\colon R\to G$ satisfy (2) then for arbitrary $g_0\in G$ the function $g\colon R\to G$ defined by $g(r):=g_0h(r)$ satisfies (1).*

PROOF. $g(s+t)x(u)=g_0h(s+t)x(u)=g_0x(s+t+u)=g_0h(s)x(t+u)=g(s)x(t+u)$. ∎

Furthermore the function h satisfies

$$h(s+t)x(u)=h(s)h(t)x(u)\quad \forall s,t,u\in R, \tag{3}$$

since $h(s+t)x(u)=g(0)^{-1}g(s+t)x(u)=g(0)^{-1}g(s)x(t+u)=h(s)h(t)x(u)$.

For the rest of the paper we will work with h instead of g. For $x\in X$ let G_x denote the stabilizer of x, *i.e.*,

$$G_x:=\{g\in G\mid gx=x\},$$

which is a subgroup of G. From (3) we deduce that $\big(h(s)h(t)\big)^{-1}h(s+t)\in G_{x(u)}$ for all $u\in R$ and all $s,t\in R$. In other words

$$\big(h(s)h(t)\big)^{-1}h(s+t)\in\bigcap_{u\in R}G_{x(u)}=:\hat{G}.$$

Using this for $t=-s$ we see that there exists $g_s\in\hat{G}$ such that $h(s)^{-1}=h(-s)g_s$ and for $s=-t$ there is $g'_t\in\hat{G}$ such that $h(t)^{-1}=g'_th(-t)$.

Let $H:=\langle h(R)\rangle$ and $\tilde{G}:=\hat{G}\cap H$ then the following lemma holds.

LEMMA 2. *The subgroup $\tilde{G}$ of H is normal.*

PROOF. It is clear that $\tilde{G}$ is a subgroup of H. We only have to prove that it is a normal subgroup. From the definition of H we know that

$$H = \left\{ \prod_{i=1}^{n} h(r_i)^{j_i} \;\middle|\; n \in \mathbb{N}, r_i \in R, j_i \in \{1, -1\} \right\}.$$

So it is enough to prove that $h(r)\tilde{G}h(r)^{-1} \leq \tilde{G}$ and $h(r)^{-1}\tilde{G}h(r) \leq \tilde{G}$ for all $r \in R$. Let $r, u \in R$ and $g \in \tilde{G}$ then there is a $g'_r \in \hat{G}$ such that $h(r)gh(r)^{-1}x(u) = h(r)gg'_r h(-r)x(u) = h(r)gg'_r x(-r+u) = h(r)x(-r+u) = x(r-r+u) = x(u)$ since $gg'_r \in \hat{G}$ stabilizes each element of the form $x(t)$. This means, since g was an arbitrary element of $\tilde{G}$, that

$$h(r)\tilde{G}h(r)^{-1} \leq G_{x(u)} \quad \forall u \in R$$

so $h(r)\tilde{G}h(r)^{-1} \leq \hat{G} \cap H = \tilde{G}$. For the second part of the proof similar arguments can be used. ∎

This permits to define a function φ from R to the factor group $H/\tilde{G}$ by

$$\varphi(r) := h(r)\tilde{G} =: \overline{h(r)}.$$

LEMMA 3. *The mapping φ is a surjective group homomorphism.*

PROOF. For $s, t \in R$ we know from (3) that $h(s)h(t) \in h(s+t)\tilde{G}$. So

$$\varphi(s+t) = h(s+t)\tilde{G} = h(s)h(t)\tilde{G} = h(s)\tilde{G}h(t)\tilde{G} = \varphi(s)\varphi(t).$$

In order to prove that φ is surjective let

$$y := \left(\prod_{i=1}^{n} h(r_i)^{j_i} \right) \tilde{G} = \overline{\prod_{i=1}^{n} h(r_i)^{j_i}} \in H/\tilde{G}.$$

Then

$$y = \prod_{i=1}^{n} \overline{h(r_i)^{j_i}} = \prod_{i=1}^{n} \overline{h(r_i)}^{j_i} = \prod_{i=1}^{n} \varphi(r_i)^{j_i} = \prod_{i=1}^{n} \varphi(j_i \cdot r_i) = \varphi\left(\sum_{i=1}^{n} j_i \cdot r_i \right)$$

and $\sum_{i=1}^{n} j_i \cdot r_i \in R$. ∎

Even the following result is true.

LEMMA 4. *If a subgroup N of $G_{x(0)}$ is a normal subgroup of H then N is a subgroup of $\tilde{G}$.*

PROOF. It is enough to prove that N is a subgroup of $G_{x(u)}$ for all $u \in R$, because then N is a subgroup of $\hat{G}$. By assumption $N \leq H$, so $N \leq \tilde{G}$. From (2) it is clear that $x(u) = h(u)x(0)$ for all $u \in R$, so $G_{x(u)} = G_{h(u)x(0)} = h(u)G_{x(0)}h(u)^{-1}$. Since N is a normal subgroup of H it is obvious that $N = h(u)Nh(u)^{-1} \leq h(u)G_{x(0)}h(u)^{-1} = G_{x(u)}$. ∎

So far we derived necessary conditions for solutions of (2). Conversely consider a group G acting on a set X. Let H be a subgroup of G, x_0 an arbitrary element of X and $\tilde{G}$ a normal subgroup of H such that $\tilde{G}$ is a subgroup of the stabilizer G_{x_0}. Then the factor group $H/\tilde{G}$ acts on the orbit $H(x_0) := \{hx_0 \mid h \in H\}$ in the following way:

$$H/\tilde{G} \times H(x_0) \to H(x_0) \quad (\bar{h}, kx_0) \mapsto (hk)x_0. \tag{4}$$

In order to prove that this action is well defined consider an arbitrary $g \in \tilde{G}$. Since $\tilde{G}$ is a normal subgroup of H there exists $g' \in \tilde{G}$ such that $gk = kg'$. From

$$(hg)kx_0 = h(gk)x_0 = h(kg')x_0 = (hk)g'x_0 = (hk)x_0$$

we derive that the action of $\bar{h}$ on $H(x_0)$ does not depend on the special choice of the representative of $\bar{h}$. Furthermore it is clear that $\bar{1}kx_0 = 1kx_0 = kx_0$ and $(\bar{h}_1\bar{h}_2)kx_0 = \overline{h_1h_2}kx_0 = (h_1h_2)kx_0 = h_1(h_2k)x_0 = \bar{h}_1(h_2kx_0) = \bar{h}_1(\bar{h}_2kx_0)$ for all $\bar{h}_1, \bar{h}_2 \in H/\tilde{G}$. Moreover $\tilde{G}$ is a subgroup of all the stabilizers G_{hx_0} for all $h \in H$ since

$$\tilde{G} = h\tilde{G}h^{-1} \leq hG_{x_0}h^{-1} = G_{hx_0}.$$

LEMMA 5. *Let $\varphi: R \to H/\tilde{G}$ be a homomorphism. When defining the two functions x and h by $x(r) := \varphi(r)x_0$, and $h(r)$ being an arbitrary element in the coset $\varphi(r)$ for $r \in R$ then h and x satisfy (2).*

PROOF. $h(s)x(u) = \varphi(s)\varphi(u)x_0 = \varphi(s+u)x_0 = x(s+u)$ for all $s, u \in R$. ∎

These results are summarized in the following:

THEOREM 6. *The functions $x: R \to X$ and $h: R \to G$ satisfy (2) if and only if there exist $x_0 \in X$, a subgroup H of G, a normal subgroup $\tilde{G}$ of H which is a subgroup of the stabilizer G_{x_0} and a homomorphism $\varphi: R \to H/\tilde{G}$ such that*

$$x(r) = \varphi(r)x_0 \quad \textit{and} \quad h(r) \in \varphi(r) \quad \forall r \in R$$

where the natural action of the factor group $H/\tilde{G}$ the orbit $H(x_0)$ is described by (4).

ACKNOWLEDGEMENT. The author wants to express his thanks to Professor Jens Schwaiger for useful comments and hints while preparing this article.

REFERENCES

1. P. M. Cohn, *Algebra.* Vol. 3, 2nd edition, J. Wiley & Sons, Chichester, 1991.
2. H. Fripertinger and J. Schwaiger, *Some applications of functional equations in astronomy.* Grazer Mathematische Berichte **344**(2001), 1–6.
3. S. Lang, *Algebra.* Addison Wesley, Reading, Massachusetts, 3rd edition, 1993.
4. K. Meyberg, *Algebra. Teil 1.* 2nd edition, Carl Hanser Verlag, München, Wien, 1980.
5. J. Schwaiger, *Some applications of functional equations in astronomy.* In: Report of the meeting (The Thirty-seventh International Symposium on Functional Equations, May 16–23, 1999, Huntington, WV), Aequationes Math. **60**(2000), 185.
6. M. Suzuki, *Group Theory I.* Grundlehren Math. Wiss. **247**, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

Institut für Mathematik
Karl Franzens Universität Graz
Heinrichstr. 36/4
A-8010 Graz
Austria
email: harald.fripertinger@kfunigraz.ac.at

C. R. Math. Rep. Acad. Sci. Canada Vol. **24** (1), 2002 pp. 26–32

MAXIMAL ABELIAN SUBALGEBRAS OF $\mathcal{O}_N$

E. J. BEGGS AND P. GOLDSTEIN

Presented by G. A. Elliott, FRSC

ABSTRACT. We consider maximal abelian subalgebras of $\mathcal{O}_n$ which are globally invariant under the standard circle action. It turns out that these are all contained in the fixed point algebra of the circle action. Then we consider shift invariant maximal abelian subalgebras of the fixed point algebra, which are also invariant under a "second shift" map, and show that these are just infinite tensor products of diagonal matrices in the standard UHF picture of the fixed point algebra.

RÉSUMÉ. Nous considérons les sous-algèbres maximales abéliennes d'$\mathcal{O}_n$ qui sont globalement invariantes sous l'action standard du cercle. Il se trouve qu'elles sont toutes contenues dans l'algèbre des points fixes sous l'action du cercle. Nous considérons ensuite les sous-algèbres maximales abéliennes de l'algèbre des points fixes qui sont invariantes sous le shift et "deuxième shift" opérateur, et démontrons qu'elles sont seulement les produits tensoriels infinis des matrices diagonales dans la forme UHF standard de l'algèbre des points fixes.

1. Introduction. Here we are concerned with certain abelian subalgebras of the Cuntz algebra $\mathcal{O}_n = C^*(s_1, \ldots, s_n)$. As usual, for $\mu = i_1 \cdots i_k$, $i_j \in \{1, \ldots, n\}$, we let $|\mu| = k$ be the length of μ and denote $s_{i_1} \cdots s_{i_k}$ by s_μ. The set of all finite words in $\{1, \ldots, n\}$ is denoted by $\mathcal{W}(n)$. The fixed point algebra of the standard circle action $\omega_t(s_i) = ts_i$, $i = 1, \ldots, n$, $t \in \mathbb{T}$ on $\mathcal{O}_n$ is called the "zero grade", $\mathcal{O}_n^0$. Let $\sigma(x) = \sum_{i=1}^n s_i x s_i^*$ be the canonical endomorphism on $\mathcal{O}_n$. The C^*-subalgebra $\mathcal{D}$ of $\mathcal{O}_n$ defined as

$$\mathcal{D} = C^*\{s_\mu s_\mu^*; \mu \in \mathcal{W}(n)\} \tag{1}$$

is an abelian subalgebra of $\mathcal{O}_n^0$ (*cf.* [3]) and $\sigma(\mathcal{D}) \subset \mathcal{D}$. In fact, $\mathcal{D}$ is maximal abelian in both $\mathcal{O}_n^0$ and $\mathcal{O}_n$ (*cf.* [4, 2.18]). Let $\psi: \mathcal{O}_n \to M_n \otimes \mathcal{O}_n$ be the isomorphism (*cf.* [2]), given by

$$x \overset{\psi}{\mapsto} \begin{bmatrix} s_1^* x s_1 & \cdots & s_1^* x s_n \\ \vdots & & \vdots \\ s_n^* x s_1 & \cdots & s_n^* x s_n \end{bmatrix}, \tag{2}$$

Received by the editors May 11, 2001.
AMS subject classification: 46L35, 46L55, 46L06.

and define a unital endomorphism $\tilde{\sigma}\colon \mathcal{O}_n \to \mathcal{O}_n$—the "second shift"—by the formula

$$\tilde{\sigma}(x) = \sum_{i,j,k} s_i s_k s_i^* x s_j s_k^* s_j^*. \tag{3}$$

This map is determined by the following diagram

$$\begin{array}{ccc} \mathcal{O}_n & \xrightarrow{\psi} & M_n \otimes \mathcal{O}_n \\ {\scriptstyle\tilde{\sigma}}\downarrow & & {\scriptstyle \mathrm{id}\otimes\sigma}\downarrow \\ \mathcal{O}_n & \xleftarrow{\psi^{-1}} & M_n \otimes \mathcal{O}_n, \end{array} \tag{4}$$

and it follows easily that $\tilde{\sigma}(1) = 1$ and $\tilde{\sigma}(s_i s_\mu s_\nu^* s_j^*) = s_i \sigma(s_\mu s_\nu^*) s_j^*$, for all $\mu, \nu \in \mathcal{W}(n)$, $|\mu| = |\nu|$. Finally, for $u = [u_{ij}]_{i,j=1}^n$ a unitary in $M_n(\mathbb{C})$, let $U = \sum_{i,j} u_{ij} s_i s_j^*$. Then U is a unitary in $\mathcal{O}_n$, and the map $s_i \mapsto U s_i$, $i = 1, \ldots, n$ extends to an isomorphism of $\mathcal{O}_n$, denoted α_U.

The subject of the present work is to give a characterisation of $\mathcal{D}$ in the above terms. More precisely, we prove (proofs of the following two theorems are at the end of Section 4):

THEOREM 1.1. *Let A be a maximal abelian subalgebra of $\mathcal{O}_n$ such that $\omega(A) \subset A$, $\sigma(A) \subset A$ and $\tilde{\sigma}(A) \subset A$. Then there is an automorphism α_U of $\mathcal{O}_n$, determined by a unitary $U \in M_n(\mathbb{C})$, such that $\alpha_U(A) = \mathcal{D}$. Furthermore, α_U commutes with ω, σ and $\tilde{\sigma}$.*

THEOREM 1.2. *Let A be a maximal abelian subalgebra of $\mathcal{O}_n$ such that $A \cap \mathcal{O}_n^0$ is maximal abelian in $\mathcal{O}_n^0$, $\sigma(A) \subset A$ and $\tilde{\sigma}(A) \subset A$. Then there is an automorphism α_U of $\mathcal{O}_n$, determined by a unitary $U \in M_n(\mathbb{C})$, such that $\alpha_U(A) = \mathcal{D}$. Furthermore, α_U commutes with ω, σ and $\tilde{\sigma}$.*

The paper is organised as follows. In Section 2, we show that an algebra which is maximal in the class of abelian algebras that are invariant under the action of the circle is indeed maximal abelian. In Section 3, we describe maximal abelian subalgebras that are invariant under two shift maps. Both Sections 2 and 3 are done in a slightly more general setting. Finally, in Section 4, we apply these results to the particular case of $\mathcal{O}_n$ and easily obtain the stated characterisation of the abelian subalgebra A.

ACKNOWLEDGEMENTS. The authors would like to thank G. Elliott, D. E. Evans, R. Exel, S. Stratila, S. Wassermann and N.-C. Wong for useful comments, and the referee for several helpful remarks that substantially improved the paper. This research was supported by an EPSRC Research Assistantship (P.G.).

2. Maximal abelian $\mathbb{T}$-invariant $*$-subalgebras. Take a C^*-algebra B, and let $\omega\colon \mathbb{T} \longrightarrow \mathrm{Aut}(B)$ be a homomorphism that is continuous in the topology of pointwise convergence. This means that for each $b \in B$ the map $t \mapsto \omega_t(b)$

is continuous, and the triple $(B, \mathbb{T}, \omega)$ is called a C^*-dynamical system (*cf.* [6, 7.4.1]). Consider the class of $*$-subalgebras A of B which are abelian and globally $\mathbb{T}$-invariant, and consider a subalgebra which is maximal in this class. Our task is to show that such an algebra is actually maximal abelian.

The main result of this section is 2.5. For convenience we assume that B is a subalgebra of $B(H)$ for some Hilbert space H. Some of the results and techniques used in this section are standard in the Arveson spectral theory for the action of a compact abelian group (*cf.* [1]). Furthermore, Theorem 2.5 remains valid for a general abelian compact group G instead of $\mathbb{T}$. We are grateful to the referee for pointing out these facts.

DEFINITION 2.1. Let $(B, \mathbb{T}, \omega)$ be a C^*-dynamical system, and define $B_n = \{b \in B : \omega_t(b) = t^n b, \text{ for all } t \in \mathbb{T}\}$. Let $\pi_n : B \to B$ be defined as

$$\pi_n(b) = \int_{\mathbb{T}} t^{-n} \omega_t(b)\, dt,$$

where dt is the Haar measure on $\mathbb{T}$ (*i.e.*, normalised Lebesgue measure). Then each B_n is a closed linear subspace in B, each π_n is a linear contraction with image B_n, B_0 is a subalgebra and π_0 is a conditional expectation to B_0. Furthermore, we have $\pi_m(b) = \delta_{n,m} b$, $b \in B_n$.

Let A be an abelian, $\mathbb{T}$-invariant $*$-subalgebra of B. It follows immediately that the commutant $A' \cap B$ of A in B is a $\mathbb{T}$-invariant $*$-subalgebra of B, and the image of $A' \cap B$ under π_n is contained in $A' \cap B$. Throughout this section, we assume that A is maximal among abelian $\mathbb{T}$-invariant $*$-subalgebras of B.

PROPOSITION 2.2. *The image of $A' \cap B$ under π_n is contained in A for all $n \in \mathbb{Z}$.*

PROOF. Suppose that $b \in A' \cap B$. By considering $b + b^*$ and $i(b - b^*)$ we may suppose that $\pi_0(b)$ is Hermitian and fixed by the circle action. Hence, the algebra generated by A and $\pi_0(b)$ is an abelian circle invariant $*$-subalgebra of B, and so $\pi_0(b) \in A$ by maximality. For $n \neq 0$, $\pi_n(b) \in A'$, and $\pi_n(b)\pi_n(b)^*$ and $\pi_n(b)^*\pi_n(b)$ are Hermitian circle invariant elements of $A' \cap B$. By the first part we then have $\pi_n(b)\pi_n(b)^*, \pi_n(b)^*\pi_n(b) \in A$. The next lemma shows that $\pi_n(b)$ is normal, and the above maximality argument applied to the algebra generated by A, $\pi_n(b)$ and $\pi_n(b)^*$ yields $\pi_n(b) \in A$. ∎

We initially proved the next lemma using polar decomposition. The following much simpler proof is due independently to S. Wassermann and N.-C. Wong:

LEMMA 2.3. *Let $x \in B$ commute with both xx^* and x^*x. Then x is normal.*

PROOF. We need to show that $xx^* - x^*x = 0$. Since $xx^* - x^*x$ is selfadjoint, that is equivalent to $(xx^* - x^*x)^2 = 0$. Now, the assumption implies $x^*xxx^* = x(x^*x)x^*$ and $xx^*x^*x = x^*(xx^*)x$, and we are done. ∎

PROPOSITION 2.4. $A' \cap B \subset A''$.

PROOF. As pointed out by the referee, this follows from Proposition 2.2 and norm-convergence of the Cesàro means of the Fourier expansion. For details, see [1, 2.2.33], or [5, Theorem VIII.2.2]. Alternatively, we can use a Fourier series argument in the following, more pedestrian, way. Take $b \in A' \cap B$. For any $\xi, \eta \in H$ we define a continuous function $f: \mathbb{T} \to \mathbb{C}$ by $f(t) = \langle \xi, \omega_t(b)(\eta) \rangle$. We get Fourier coefficients $f_n = \langle \xi, \pi_n(b)(\eta) \rangle$, where $\sum_{n=-m}^{m} t^n f_n \longrightarrow f(t)$ in the $L^2(\mathbb{T})$ topology as $m \to \infty$. Since $B \subset B(H)$, we can put $\eta = c(\kappa)$ for some $c \in A'$ and $\kappa \in H$. Then, as $\pi_n(b) \in A$, we see that $f_n = \langle \xi, c\pi_n(b)(\kappa) \rangle = \langle c^*\xi, \pi_n(b)(\kappa) \rangle$. Now we can write

$$\sum_{n=-m}^{m} t^n f_n \to \langle c^*\xi, \omega(b)(\kappa) \rangle = \langle \xi, c\omega(b)(\kappa) \rangle, \quad t \in \mathbb{T}, \quad m \to \infty$$

in the $L^2(\mathbb{T})$ topology. The two limits are the same in $L^2(\mathbb{T})$, so $\langle \xi, c\omega_t(b)(\kappa) \rangle = \langle \xi, \omega_t(b)c(\kappa) \rangle$ almost everywhere in $\mathbb{T}$. By continuity they are the same at $t = 1$, so $cb = bc$. ∎

THEOREM 2.5. *Let $(B, \mathbb{T}, \omega)$ be a C^*-dynamical system, and suppose that A is a maximal among abelian $\mathbb{T}$-invariant $*$-subalgebras of B. Then A is a maximal abelian subalgebra of B.*

PROOF. From Proposition 2.4, $A' \cap B$ is an abelian $\mathbb{T}$-invariant $*$-subalgebra of B which contains A. Maximality of A yields $A = A' \cap B$. ∎

The following example—due to R. Exel—shows that the previous theorem does not hold for a dynamical system (B, G, ω) with G non-abelian:

EXAMPLE 2.6. Consider the adjoint action of SU_2 on $M_2(\mathbb{C})$. The subalgebra consisting of the complex multiples of the identity is maximal among the class of abelian SU_2-invariant $*$-subalgebras. However, it is not maximal abelian, as it is properly contained in the diagonal matrices.

3. Maximal abelian $*$-subalgebras of $\mathcal{O}_n$ contained in the zero grade. Let B be a unital C^*-algebra with a given isomorphism $\psi: B \to M_n \otimes B$ with $\psi(1) = I_n \otimes 1$, I_n being the identity matrix in M_n. We define isomorphisms $\psi_m: B \to (M_n)^{\otimes m} \otimes B$ $(m \geq 0)$ recursively, beginning with $\psi_0: B \to B$ the identity, $\psi_1 = \psi$, and continuing by defining ψ_{m+1} to be the composition

$$B \xrightarrow{\psi_m} (M_n)^{\otimes m} \otimes B \xrightarrow{\mathrm{id}^{\otimes m} \otimes \psi} (M_n)^{\otimes m+1} \otimes B,$$

where $\mathrm{id}: M_n \to M_n$ is the identity map. Now we define an algebra map κ_m: $M_n^{\otimes m} \to B$ by $\kappa_m(x) = \psi_m^{-1}(x \otimes 1)$. Since $\psi(1) = I_n \otimes 1$ we get the commutative diagram

$$\begin{array}{ccc} M_n^{\otimes m} & \xrightarrow{\kappa_m} & B \\ \downarrow \mathrm{id} \otimes I_n & & \downarrow \mathrm{id}_B \\ M_n^{\otimes m+1} & \xrightarrow{\kappa_{m+1}} & B. \end{array}$$

We can define shift maps $\sigma_m: B \to B$ $(m \geq 1)$ by the composition

$$B \xrightarrow{\psi_{m-1}} (M_n)^{\otimes m-1} \otimes B \xrightarrow{\mathrm{id}^{\otimes m-1} \otimes f} (M_n)^{\otimes m} \otimes B \xrightarrow{\psi_m^{-1}} B,$$

where $f: B \to M_n \otimes B$ is the algebra map $f(b) = I_n \otimes b$.

Let $E_{ij} \in M_n$ be the matrix with entry 1 in row i column j, and zeros elsewhere. Define a linear map $e_{ij}: M_n \to \mathbb{C}$ by $e_{ij}(E_{kl}) = \delta_{ik}\delta_{jl}$. Now we can define a map $\chi_{mij}: B \to B$ $(m \geq 1)$ by

$$B \xrightarrow{\psi_m} (M_n)^{\otimes m} \otimes B \xrightarrow{\mathrm{id}^{\otimes m-1} \otimes e_{ij} \otimes \mathrm{id}_B} (M_n)^{\otimes m-1} \otimes B \xrightarrow{\psi_{m-1}^{-1}} B.$$

PROPOSITION 3.1. *For all $b \in B$ and $y \in M_n \otimes B$, $(e_{ij} \otimes \mathrm{id}_B)\big(f(b).y\big) = b.\big((e_{ij} \otimes \mathrm{id}_B)(y)\big)$ and $(e_{ij} \otimes \mathrm{id}_B)\big(y.f(b)\big) = \big((e_{ij} \otimes \mathrm{id}_B)(y)\big).b$.*

PROOF. Take $y = y_1 \otimes y_2 \in M_n \otimes B$. Then

$$\begin{aligned}(e_{ij} \otimes \mathrm{id}_B)\big(f(b).y\big) &= (e_{ij} \otimes \mathrm{id}_B)\big((I \otimes b)(y_1 \otimes y_2)\big) = (e_{ij} \otimes \mathrm{id}_B)(y_1 \otimes by_2) \\ &= e_{ij}(y_1)by_2 = b.\big((e_{ij} \otimes \mathrm{id}_B)(y)\big).\end{aligned}$$

The other identity is proved in the same manner. ∎

COROLLARY 3.2. *For all $b, c \in B$, $\chi_{mij}\big(\sigma_m(b).c\big) = b.\chi_{mij}(c)$ and $\chi_{mij}\big(c.\sigma_m(b)\big) = \chi_{mij}(c).b$.*

PROPOSITION 3.3. *Suppose that A is a maximal abelian $*$-subalgebra of B, obeying the condition $\sigma_m(A) \subset A$. Then for all $1 \leq i, j \leq n$, $\chi_{mij}(A) \subset A$. Furthermore, $\sigma_1(A) \subset A$ implies $\psi_m(A) \subset M_n^{\otimes m} \otimes A$.*

PROOF. For the first part, take $a \in A$, and note that $\sigma_m(a').a = a.\sigma_m(a')$, for all $a' \in A$. Applying χ_{mij} to this we get $a'.\chi_{mij}(a) = \chi_{mij}(a).a'$, so $\chi_{mij}(a) \in A$ by maximality. For the second part, note that $\psi(a) = \sum_{ij} E_{ij} \otimes \chi_{1ij}(a)$, so $\psi(A) \subset M_n \otimes A$. The rest follows by induction. ∎

DEFINITION 3.4. Take a character $\phi: A \to \mathbb{C}$, and extend it to a state $\phi: B \to \mathbb{C}$. Then we define a map $\phi_m: B \to M_n^{\otimes m}$ by

$$B \xrightarrow{\psi_m} M_n^{\otimes m} \otimes B \xrightarrow{\mathrm{id}^{\otimes m} \otimes \phi} M_n^{\otimes m}.$$

Since $\phi_m(1) = 1$, it follows from [6, 3.1.6] that ϕ_m is a contraction. On the other hand, using Proposition 3.3, this is clearly a unital homomorphism when restricted to A. We denote by D the image of $\phi_1: A \to M_n$.

PROPOSITION 3.5. *If $\sigma_1(A) \subset A$, then $\phi_{m+1}(A) \subset M_n \otimes \phi_m(A)$. If $\sigma_2(A) \subset A$, then $(\mathrm{id} \otimes e_{ij} \otimes \mathrm{id}^{\otimes m-1})\phi_{m+1}(A) \subset \phi_m(A)$ for $m \geq 1$.*

PROOF. For the first inclusion, we can write ϕ_{m+1} as

$$A \xrightarrow{\psi_1} M_n \otimes A \xrightarrow{\mathrm{id}\otimes\phi_m} M_n^{\otimes m+1},$$

so we see that $\phi_{m+1}(A) \subset M_n \otimes \phi_m(A)$. For the second inclusion, note that $(\mathrm{id}\otimes e_{ij}\otimes \mathrm{id}^{\otimes m-1})\circ\phi_{m+1} = \phi_m \circ \chi_{2ij}\colon B \to M_n^{\otimes m}$, and use $\chi_{2ij}(A) \subset A$. ∎

COROLLARY 3.6. *If $\sigma_1(A) \subset A$ and $\sigma_2(A) \subset A$, then $\phi_m(A) \subset D^{\otimes m}$.*

PROOF. This is proved by induction. First note that $\phi_1(A) = D$. Now assume that $\phi_m(A) \subset D^{\otimes m}$. By the previous proposition we see that $\phi_{m+1}(A) \subset D \otimes M_n \otimes D^{\otimes m-1}$ and $\phi_{m+1}(A) \subset M_n \otimes D^{\otimes m}$. ∎

Define $C \subset B$ to be the closure of the union of the subalgebras $\kappa_m(M_n^{\otimes m})$ (for $B = \mathcal{O}_n$, C is just the zero grade) and let D^∞ stand for the closure of the union of $\kappa_m(D^{\otimes m})$ for $m \geq 1$.

PROPOSITION 3.7. *Given $c \in C$ and $\epsilon > 0$, there is an $m \geq 1$ so that $|\kappa_m(\phi_m(c)) - c| < \epsilon$.*

PROOF. There is an $m \geq 1$ and an $x \in M_n^{\otimes m}$ so that $|c - \kappa_m(x)| < \epsilon/2$. Since $\phi(1) = 1$ we get $\phi_m(\kappa_m(x)) = x$, and since ϕ_m is a contraction, $|\phi_m(c) - x| < \epsilon/2$. Finally as κ_m is a contraction, $|\kappa_m(\phi_m(c)) - \kappa_m(x)| < \epsilon/2$. ∎

THEOREM 3.8. *Suppose that $A \cap C$ is maximal abelian in C. Then $A \cap C = D^\infty$ and D is maximal abelian in $M_n(\mathbb{C})$.*

PROOF. Corollary 3.6 and Proposition 3.7 show that $A \cap C \subset D^\infty$. Since D^∞ is abelian and $A \cap C$ is maximal, it follows that $A \cap C = D^\infty$. Hence, D is maximal abelian in $M_n(\mathbb{C})$. ∎

4. Maximal abelian $\mathbb{T}$-invariant $*$-subalgebras of $\mathcal{O}_n$. In this section, we apply results from Sections 2 and 3 to maximal abelian subalgebras of $\mathcal{O}_n$ that are invariant under the standard circle action. The notation is as in the introduction. The next lemma is probably well known, but we couldn't find a reference:

LEMMA 4.1. *Let x be in $\mathcal{O}_n^k$ (i.e., $\omega_t(x) = t^k x$), for $k \neq 0$. If x is normal, then $x = 0$.*

PROOF. Suppose $k > 0$. Let $y = x(s_1^*)^k \in \mathcal{O}_n^0$, and let τ be the faithful normalised trace on $\mathcal{O}_n^0 \cong M_{n^\infty}(\mathbb{C})$. Then $yy^* = xx^*$, $y^*y = s_1^k x^* x (s_1^*)^k$, and $\tau(yy^*) = \tau(y^*y)$ imply $\tau(xx^*) = n^{-k}\tau(x^*x)$. If $xx^* = x^*x$, then $\tau(x^*x) = n^{-k}\tau(x^*x)$, hence $\tau(x^*x) = 0$. ∎

THEOREM 4.2. *If A is a maximal among abelian $\mathbb{T}$-invariant $*$-subalgebras of $\mathcal{O}_n$, then $A \subset \mathcal{O}_n^0$.*

PROOF. By the previous lemma, $\pi_k(a) = 0$ for all $a \in A$ and $k \neq 0$. By Fourier analysis we get

$$\sum_{k=-m}^{m} t^k \langle \xi, \pi_k(a)(\eta) \rangle \to \langle \xi, \omega_t(a)(\eta) \rangle, \quad t \in \mathbb{T}$$

in the $L^2(\mathbb{T})$ topology as $m \to \infty$. But then $\langle \xi, \omega_t(a)(\eta) \rangle$ is constant on $\mathbb{T}$, so $\omega_t(a) = a$. ∎

PROOF OF THEOREM 1.1. By Theorem 4.2, $A \subset \mathcal{O}_n^0$. The result then follows from Theorem 3.8, with $B = \mathcal{O}_n^0$, $\sigma = \sigma_1$ and $\tilde{\sigma} = \sigma_2$, while u is any unitary in $M_n(\mathbb{C})$ that diagonalises subalgebra D. ∎

PROOF OF THEOREM 1.2. We apply Theorem 3.8, with $B = \mathcal{O}_n$, and σ and $\tilde{\sigma}$ as in the previous theorem. That shows that $D^\infty \subset A$. Since D^∞ is maximal abelian in $\mathcal{O}_n$ (*cf.* [4, 2.18]), $A = D^\infty$. ∎

REFERENCES

1. O. Bratteli, *Derivations, Dissipations and Group Actions on C^*-algebras.* Lecture Notes in Math. **1229**, Springer-Verlag, Berlin, 1986.
2. M.-D. Choi, *A simple C^*-algebra generated by two finite-order unitaries.* Canad. J. Math **31**(1979), 867–880.
3. J. Cuntz, *Simple C^*-algebras generated by isometries.* Comm. Math. Phys. **57**(1977), 173–185.
4. J. Cuntz and W. Krieger, *A class of C^*-algebras and topological Markov chains.* Invent. Math. **56**(1980), 251–268.
5. K. R. Davidson, *C^*-Algebras by Example.* Fields Institute Monographs **6**, Amer. Math. Society, 1996.
6. G. K. Pedersen, *C^*-algebras and their automorphism groups.* London Math. Soc. Monographs **14**, Academic Press, 1979.
7. M. Pimsner, *A class of C^*-algebras generalizing both Cuntz-Krieger algebras and crossed products by $\mathbb{Z}$.* Fields Institute Communications **12**, Amer. Math. Soc., 1997, 189–212.

Department of Mathematics
University of Wales Swansea
Swansea SA2 8PP
UK
email: e.j.beggs@swan.ac.uk

School of Mathematics
Cardiff University
Cardiff CF4 4YH
UK
email: goldsteinp@cf.ac.uk