Asymptotic Group Theory

Aner Shalev

What is the probability that two randomly chosen permutations of $1, \ldots, n$ generate the group S_n of all permutations of $1, \ldots, n$? How many subgroups of index n can a group with two generators have? What can be said about a group of order 2^n which has a nonidentity commutator of length $n - 10$? These questions all concern different aspects of a field which is very active nowadays and which may be called asymptotic group theory.

Roughly speaking, asymptotic group theory can be thought of as groups viewed from some distance. The finer details disappear, and the rough lines become the main focus. If in group theory one often aims at full classification (say, classifying finite simple groups or doubly transitive permutation groups), then in asymptotic group theory we would be happy with a classification up to finitely many (unspecified) exceptions. If in group theory one often likes to compute certain invariants, in asymptotic group theory we would be happy with finding out the asymptotic behavior of these invariants. If in group theory one often studies a single finite group, in asymptotic group theory we often study an infinite family of finite groups or sometimes the set of finite quotients of some given infinite group.

The topic of asymptotic group theory is motivated by and interrelated with many fields of mathematics and other areas; these include combinatorics, computer science, probability theory, geometry, as well as some branches of logic, algebra, and analysis.

It is impossible to cover all aspects of the field in this short expository paper; important aspects such as Cayley graphs and random walks on groups, word growth of groups, permutation groups, and algorithmic applications will not be discussed. We will be content with sampling recent progress in three areas and providing some references for further reading. In the first section we shall focus on random generation and the recent use of probability in proving existence theorems in finite groups. In the following section we will turn to infinite groups and to the enumeration of their finite index subgroups. The last section combines finite groups with infinite groups; it describes the so-called coclass theory for p-groups and pro-p groups, with a few tips on the more general subject of slim objects.

The Unbearable Ease of Generating (Some) Groups

What does a random permutation look like? At first sight it is not at all clear whether this is a meaningful question. We can talk about the average number of cycles of a permutation in S_n, or its average order, for instance. But if we draw a graph of the function that assigns to m the number of permutations in S_n with precisely m cycles, what will its shape be? Will it have a well-defined peak? The answer to this and various related questions was provided in a series of seven papers by Erdős and Turán (starting with [ET1]), which could be regarded as one of the milestones of asymptotic group theory. Erdős and Turán discovered various concentration phenomena. In particular they showed that most (at least $(1 - \epsilon)n!$) permutations in S_n have roughly $\log n$ (more precisely, between $(1 - \epsilon)\log n$ and $(1 + \epsilon)\log n$) cycles and have order roughly $n^{\frac{1}{2}\log n}$ (more precisely, between $n^{(\frac{1}{2}-\epsilon)\log n}$ and $n^{(\frac{1}{2}+\epsilon)\log n}$). As for the question of the shape of the graph described above and of similar graphs, it turns out to have the shape of a bell: the distributions of

Aner Shalev is professor of mathematics at the Institute of Mathematics, The Hebrew University of Jerusalem. His e-mail address is shalev@math.huji.ac.il.

the number of cycles and of the logarithm of the order of a permutation in S_n converge to Gaussian normal distributions when n tends to infinity with known mean values and variances.

The work of Erdős and Turán on statistical aspects of S_n has gradually gained various applications. While the Erdős-Turán theory explores properties of a single random permutation, some of these applications concern properties of a randomly chosen pair (or a longer sequence) of permutations. For example, a nineteenth-century conjecture of Netto asserts that almost all pairs of permutations in A_n (the group of even permutations) generate A_n. This was confirmed by J. D. Dixon [D] in 1969, and one of the ingredients in the proof is the Erdős-Turán theory. While this beautiful result settles a vintage conjecture, there is a more modern aspect of it which is relevant in group-theoretic algorithms: it is very easy to find generating pairs in A_n; after a few random choices you are very likely to end up with one. Is this property shared by other important groups? For instance, by the finite simple groups?

The classification of finite simple groups was one of the major tasks of group theory in the second half of the twentieth century. Announced in 1980, it asserts that the finite simple groups split into four major families: the abelian ones (cyclic of prime order), the alternating ones (A_n), the groups of Lie type (such as the classical group $PSL_n(q)$ on the one hand and the exceptional group $E_8(q)$ on the other), and the sporadic ones (a specific list of 26 groups). Since the problems we shall discuss are trivial for the abelian simple groups, let us agree that by simple groups we mean simple nonabelian. Also, since these problems are of an asymptotic nature, we may exclude the finitely many sporadic groups from the discussion and focus on alternating groups and the finite simple groups of Lie type.

In [D] Dixon generalized Netto's conjecture as follows.

Conjecture *(Dixon 1969): Two randomly chosen elements of a finite simple group G generate G with probability $\to 1$ as $|G| \to \infty$.*

Here G and its Cartesian powers are regarded as probability spaces with respect to the uniform distribution, and the random elements are chosen independently (allowing repetitions). Denote by $P(G)$ the respective generation probability, namely, the number of generating pairs $(x, y) \in G \times G$ divided by $|G|^2$ (the number of all ordered pairs).

It turns out that the maximal subgroups of the ambient group G provide a key to the solution of Dixon's conjecture. To understand their relevance, suppose $x, y \in G$ are chosen at random. If these elements do not generate G, then they both lie in some maximal (proper) subgroup M of G. Given M, the probability that x, y lie in M is $(|M|/|G|)^2$. Summing up over all maximal subgroups M of G, we obtain the following upper bound on the non-generation probability:

$$1 - P(G) \leq \sum_{\substack{M \subset G \\ M \text{ maximal}}} |G : M|^{-2}.$$

Define a "zeta function" associated with G by

$$\zeta_G(s) = \sum_{\substack{M \subset G \\ M \text{ maximal}}} |G : M|^{-s}.$$

Then, in order to confirm Dixon's conjecture, it suffices to show that, for finite simple groups G, $\zeta_G(2) \to 0$ as $|G| \to \infty$. Roughly speaking, this would follow if we could show that simple groups do not have many maximal subgroups (so the sum in question has few summands) and that the indices of these subgroups are usually rather large (so that these summands are usually small).

The study of the maximal subgroups of the finite simple groups is an ongoing project dating back to the nineteenth century. Two major results, by O'Nan-Scott and by Aschbacher respectively, describe the maximal subgroups of alternating groups and of classical groups (see [KlLi] and the references therein). Extensions for nonclassical simple groups of Lie type were provided by Seitz and others. These descriptions do not add up to full classification (except for a few families of simple groups G), but they do provide enough information to deduce the following result by applying some additional tools (see [KL], [LiSh1]).

Theorem 1 *(Dixon 1969, Kantor-Lubotzky 1990, Liebeck-Shalev 1995). For finite simple groups G, $\zeta_G(2) \to 0$ as $|G| \to \infty$. Therefore Dixon's conjecture holds.*

It is intriguing that the asymptotic behavior of $\zeta_G(s)$ for smaller values of s provides a key to the solution of several other problems. Given positive integers r, s, denote by $P_{r,s}(G)$ the probability that randomly chosen elements $x, y \in G$ of orders r, s generate G. One of the main motivations for the study of probabilities of this type comes from the study of the modular group $PSL_2(\mathbb{Z})$. This group has fundamental importance in geometry and analysis, and the determination of its finite simple quotients has been an ongoing project over the past hundred years or so. It is well known that $PSL_2(\mathbb{Z}) \cong C_2 * C_3$, the free product of groups of orders 2 and 3 respectively. This means that a group G is a quotient of $PSL_2(\mathbb{Z})$ if and only if G can be generated by elements x, y satisfying $x^2 = y^3 = 1$. Such groups are termed $(2, 3)$-generated.

Which of the finite simple groups have this property? The groups A_n ($n \geq 9$) do, as shown by Miller in 1901. It was not until 1967 that the proof that the simple groups of type $PSL_2(q)$ ($q \neq 9$) are

$(2,3)$-generated was completed (we note that $PSL_2(9)$ and A_8 are not $(2,3)$-generated). Since then the $(2,3)$-generation property has been established by Tamburini, Di Martino, Vavilov, Wilson, and others for more families of simple groups, such as $PSL_n(q)$ for odd q (or large n), but the problem remained unsolved for various other families. It is only through the application of probabilistic methods (and character methods for exceptional groups) that a full asymptotic solution has been provided, as follows.

***Theorem 2** (Liebeck-Shalev 1996, Lübeck-Malle 1999). All finite simple groups, except the symplectic groups $PSp_4(2^k)$, $PSp_4(3^k)$, the Suzuki groups $Sz(2^k)$, and finitely many other groups, can be obtained as quotients of the modular group $PSL_2(\mathbb{Z})$.*

The explicit exceptions above are genuine: it can be shown that these groups are not $(2,3)$-generated, and so they cannot be obtained as quotients of the modular group. However, there are some additional exceptions which the theorem does not list; all we know is that there are finitely many of them. This is typical of results proved using a probabilistic approach.

Let us now discuss in some detail the way Theorem 2 was proved. In view of the $(2,3)$-generation of A_n $(n \geq 9)$, it remains to consider finite simple groups G of Lie type. The exceptional groups of Lie type were dealt with by Lübeck and Malle using character theory and computer calculations. So let G be a classical group.

To show that G is $(2,3)$-generated (with some exceptions), we apply the so-called probabilistic method, proving the existence of an object with some required properties not by explicit constructions but by showing that "most" objects in a certain "universe" have these properties. This method has a rich history in many areas of mathematics, such as combinatorics and number theory, though it is relatively new in finite group theory.

Thus, instead of explicitly constructing a pair x, y generating G which consists of an involution and an element of order 3, we choose at random an involution $x \in G$ and an element $y \in G$ of order 3, and we hope to show that, as $|G| \to \infty$, x and y generate G with probability tending to 1, or at least to some positive number. If we can show this for a family of classical groups G, it would follow that all sufficiently large groups in that family are $(2,3)$-generated. In other words, we are interested in estimating the probabilities $P_{r,s}(G)$ defined above, with particular attention to $(r,s) = (2,3)$.

Again, information on maximal subgroups is of great help. Given a positive integer r and a finite group H, let $i_r(H)$ denote the number of elements of order r in H. Now, let $x, y \in G$ be randomly chosen elements of orders r, s respectively. If x, y do not generate G, then they both lie in some maximal subgroup M of G. Given M, the probability that $x \in M$ is $i_r(M)/i_r(G)$, and the probability that $y \in M$ is $i_s(M)/i_s(G)$. Letting M range over all maximal subgroups of G and using the independence of x, y, we obtain the following elementary upper bound on the nongeneration probability:

$$1 - P_{r,s}(G) \leq \sum_{\substack{M \subset G \\ M \text{ maximal}}} \frac{i_r(M) i_s(M)}{i_r(G) i_s(G)}.$$

The next stage is to try to count the elements of given order in classical groups G and in their maximal subgroups M. In the important case $(r,s) = (2,3)$ our (rather painstaking) computations show that for some absolute constant c we have

$$\frac{i_2(M)}{i_2(G)} \leq c|G:M|^{-2/5},$$

and (with few exceptions such as $PSp_4(q)$)

$$\frac{i_3(M)}{i_3(G)} \leq c|G:M|^{-8/13}.$$

Plugging this into the upper bound above, we obtain

$$\begin{aligned} 1 - P_{2,3}(G) &\leq c^2 \sum_{\substack{M \subset G \\ M \text{ maximal}}} |G:M|^{-2/5} |G:M|^{-8/13} \\ &= c^2 \zeta_G(2/5 + 8/13) = c^2 \zeta_G(66/65). \end{aligned}$$

We see that, as in the case of Dixon's conjecture, the problem now boils down to estimating values of $\zeta_G(s)$. We show the following [LiSh2].

***Theorem 3** (Liebeck-Shalev 1996). Let G be a finite simple classical group. Then for any fixed $s > 1$ we have $\zeta_G(s) \to 0$ as $|G| \to \infty$. Therefore $P_{2,3}(G) \to 1$ as $|G| \to \infty$, provided $G \neq PSp_4(q)$.*

We conjecture that the first assertion in the theorem holds for all finite simple groups. This is the case for alternating groups, and so it remains to prove it for exceptional groups of Lie type. It is easy to see that $s \leq 1$ implies $\zeta_G(s) \to \infty$ as $|G| \to \infty$, so 1 can be viewed as a singular point here. The fact that $2/5 + 8/13$ is strictly bigger than 1 (just barely!) is therefore a key to our random $(2,3)$-generation result. We also show that, for $p \geq 5$ and $G = PSp_4(p^k)$, we have $P_{2,3}(G) \to 1/2$ as $|G| \to \infty$. Theorem 2 for classical groups now clearly follows, using this result and Theorem 3. For more details, see [LiSh2].

Recall that the proof of Theorem 1 was based on estimating $\zeta_G(2)$, while the proof of Theorem 2 is based, among other things, on estimating $\zeta_G(66/65)$. It is intriguing that other generation results can be obtained by studying $\zeta_G(s)$ for other values of s. For instance, it can be shown that the probability that a randomly chosen involution and a randomly chosen additional element generate a finite simple classical group G is at least $1 - c\zeta_G(7/5)$, which tends to 1 by Theorem 3 above, and the probability that G is generated by three randomly chosen involutions is at least $1 - c\zeta_G(6/5)$, which also tends to 1. Similar methods have recently yielded the following yet-unpublished result.

Theorem 4 *(Liebeck-Shalev 2000). Let r, s be primes, not both 2. Let G be a finite simple classical group of sufficiently large dimension. Then $P_{r,s}(G) \to 1$ as $|G| \to \infty$.*

Here sufficiently large means larger than some function $f(r, s)$ (which can be computed explicitly) of the respective primes r, s.

We conclude this section by mentioning briefly some other recent applications of the probabilistic method in the theory of finite groups. Not all results in this field are of an asymptotic nature. Instead of studying the behavior of certain generation probabilities when the group order tends to infinity, some authors obtained lower bounds on such probabilities which hold for *all* finite simple groups. As an important example, consider the following result which was proved by Guralnick and Kantor a few years ago and which will appear in the near future.

Theorem 5 *(Guralnick-Kantor). In every finite simple group G there is a conjugacy class C such that, for any nonidentity element $g \in G$, the probability that g and a random element of C generate G is at least* $1/10$.

This theorem has several interesting applications. One of them is the following positive solution to a problem which has been open for many years regarding the so-called one-and-a-half generation of finite simple groups: every nonidentity element of a finite simple group can be extended to a generating pair. This result is yet another indication of the ease with which generators for finite simple groups can be found.

Probabilistic ideas were also useful in settling some conjectures in the theory of finite permutation groups, such as Cameron's conjecture on base size and the Guralnick-Thompson conjecture concerning genus of permutation groups. See [LiSh3], [Sh2] and the references therein. They have also been extremely useful in computational group theory in designing efficient algorithms for permutation groups, matrix groups, and so-called black-box groups, as shown in recent works by Babai, Kantor, Leedham-Green, Neumann, Praeger, Seress and others. It seems that the role of probability in finite group theory, which was evident in the past decade, will only gain further momentum in the years to come.

Subgroup Growth

The connection between generation and maximal subgroups may serve as a natural bridge between random generation and subgroup growth. This connection can be made precise in the language of profinite groups. A profinite group is an inverse (projective) limit of an inverse system of finite groups. For example, the additive group $\mathbb{Z}_p$ of the p-adic integers is a profinite group, being the inverse limit of the cyclic groups C_{p^k} $(k \geq 1)$ with the natural epimorphisms between them. Matrix groups over $\mathbb{Z}_p$ (or other profinite rings), as well as Galois groups of infinite field extensions, form other important examples of profinite groups. The notion of a profinite group is most natural in asymptotic group theory and can be viewed as a way to encode information on infinitely many finite groups.

A profinite group G can be viewed as a topological group, and when we talk about generation and subgroups we mean topological generation and closed subgroups. As a compact group, each profinite group admits an invariant measure, the so-called Haar measure, of finite total measure. If we normalize the measure so that the total measure is 1, then the measure is unique, and it turns the group G, as well as its Cartesian powers G^k, into probability spaces.

Given G and k, let $P(G, k)$ denote the measure in G^k of the set of generating k-tuples, namely, of k-tuples $(x_1, \ldots, x_k)$ such that $\langle x_1, \ldots, x_k \rangle = G$. Let us say that G is *positively finitely generated* if $P(G, k) > 0$ for some k. This notion, as well as the arguments below, are due to Mann [M]. Which profinite groups are positively finitely generated? This problem is still open in a structural sense. But we do have a nonstructural characterization. In order to state it we need some notation.

Given G and n, let $m_n(G)$ denote the number of maximal subgroups of index n in G. We may define the profinite analogue of the "zeta function" discussed earlier, namely,

$$\zeta_G(s) = \sum_{\substack{M \subset G \\ M \text{ maximal}}} |G : M|^{-s} = \sum_{n > 1} m_n(G) n^{-s}.$$

Of course this series need not converge for a given (or any) value of s, and so $\zeta_G(s)$ is not always well defined. The convergence of this sum for some s is equivalent to polynomial growth of $m_n(G)$, namely, to the existence of a positive number α satisfying $m_n(G) \leq n^\alpha$ for all n. In this case we say that G has *polynomial maximal subgroup growth.*

Now, arguing exactly as in the previous section, one obtains the following basic upper bound for the nongeneration probability:

$$1 - P(G, k) \leq \zeta_G(k).$$

If G has polynomial maximal subgroup growth, then it is easy to choose a positive integer k so that

$\zeta_G(k) < 1$. In view of the upper bound above, this implies $P(G, k) > 0$, so G is positively finitely generated. A more difficult argument, based on the classification of finite simple groups and on other tools, shows that the converse also holds: positively finitely generated groups have polynomial maximal subgroup growth. So we have the following characterization [MSh].

***Theorem 6** (Mann-Shalev 1996). A profinite group is positively finitely generated if and only if it has polynomial maximal subgroup growth.*

To this category belong all finitely generated prosolvable groups [M] as well as other groups, although a structural characterization has yet to be found.

More satisfactory results have been obtained in a related context, namely, when one counts all subgroups of G of given index and not just the maximal ones. Suppose now that G is not a profinite group, but an infinite, finitely generated discrete group. Let $a_n(G)$ denote the number of index n subgroups of G. Counting finite index subgroups has its earliest origin in counting finite sheeted covers of manifolds (corresponding to finite index subgroups of the fundamental group). It is not hard to verify that a free group on $d > 1$ generators has about $n \cdot (n!)^{d-1}$ index n subgroups, and so the subgroup growth of certain groups is super-exponential. We are interested in understanding groups with much slower subgroup growth. We say that G has *polynomial subgroup growth* if for some α we have $a_n(G) \le n^\alpha$ for all n. It is natural to assume here that G is *residually finite*, namely, that the intersection of all finite index subgroups of G is trivial (otherwise, factoring out this intersection yields a group with the same subgroup growth properties). Which finitely generated groups have polynomial subgroup growth? It is easy to see that the abelian ones and the nilpotent ones have this property. But not all solvable groups have polynomial subgroup growth; for example, the subgroup growth of the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is exponential. Again, what emerges here is a fascinating relation with generation properties. We say that G has rank at most r if every finitely generated subgroup of G can be generated by r elements. If such a number $r < \infty$ exists, we say that G has *finite rank*.

A celebrated result, by Lubotzky, Mann, and Segal [LMS], provides the following characterization.

***Theorem 7** (Lubotzky-Mann-Segal 1993). Let G be a finitely generated residually finite group. Then G has polynomial subgroup growth if and only if G has finite rank.*

In fact the result is more detailed, providing a full structural characterization. The groups of polynomial subgroup growth are precisely those having a finite index subgroup which is a solvable minimax group. The proof of this definitive result uses many tools: the classification of finite simple groups, the theory of algebraic groups, the theory of p-adic Lie groups, as well as some number theory. It can be considered as somewhat analogous to Gromov's celebrated theorem on groups of polynomial (word) growth. In both cases one invokes a slow growth assumption and concludes that the ambient group is rather tame (virtually nilpotent in case of word growth, and virtually solvable in case of subgroup growth). In the next section we will encounter a similar phenomenon with yet another notion of growth.

We note that when we turn to profinite groups, the assumption of polynomial subgroup growth does not lead to such strong conclusions. Profinite groups of polynomial subgroup growth need not be virtually solvable and need not have finite rank. Still, these groups have been fully characterized [SSh]. For more background on subgroup growth, see Lubotzky [Lu] and the references therein.

We end this section by briefly mentioning related zeta functions. Recall that a function $\zeta_G(s)$ encoding the growth of maximal subgroups of G was defined and used in the context of random generation. Similarly, consider the function defined by the sum

$$\sum_H |G : H|^{-s} = \sum_{n \ge 1} a_n(G) n^{-s},$$

where H ranges over all finite index subgroups of G. There are many deep results concerning the behavior of such functions, covering aspects such as rationality, analytic continuation, etc. For an up-to-date account of this rich theory, developed by du Sautoy, Grunewald, Segal, Smith, and others, we refer the reader to Chapter 9 of [DSSh].

Slim Is Beautiful

The condition that a group G has at most n^α subgroups of index n can be regarded as a kind of slimness condition. Other slimness conditions have been studied in the past two decades; this section is devoted to one of them, which leads to a fascinating theory, the so-called coclass theory for finite p-groups and infinite pro-p groups.

A pro-p group is an inverse limit of finite p-groups. As such it is a special type of profinite group. For such a group G, let γ_n be the nth term of its lower central series, namely, the subgroup generated by all length n commutators in G. Thus $\gamma_1 = G$, $\gamma_2 = G'$ (the derived subgroup), and so on. The lower central series $\{\gamma_n\}$ of a pro-p group G is a descending chain of normal subgroups, and there is great interest in its rate of descent. A natural way to measure this is to consider the orders of the quotients G/γ_n. These orders need not be finite, but when they are all finite and grow rather slowly, then the coclass theory is set into motion and can reveal a great deal about the ambient group G.

How small can $|G/\gamma_n|$ be? Suppose G is an infinite pro-p group (formally, finite p-groups are also pro-p groups). Then one can easily show that $|G/\gamma_n| \geq p^n$ for all $n \geq 2$. Moreover, these inequalities are best possible, since there are pro-p groups satisfying $|G/\gamma_n| = p^n$ for all $n \geq 2$. Such a pro-p group, which could be considered the slimmest among all pro-p groups, is usually termed a pro-p group of *maximal class*. The dihedral pro-2 group, namely, the extension of the additive group of the 2-adic integers $\mathbb{Z}_2$ by an involution acting as multiplication by -1, provides such an example.

One may relax this condition slightly and consider pro-p groups G satisfying $|G/\gamma_n| \leq p^{n+r-1}$ for all $n \geq 2$, where r is some fixed positive integer. If there exists such an integer r, we say that G has *finite coclass*. The minimal such r is then defined to be *the coclass of* G. The coclass of a finite p-group G can be defined in exactly the same way. An equivalent definition can be given as follows. Suppose G is a group of order p^n and nilpotency class c (this means that c is the maximal length of non-identity commutators in G). Then G has coclass $n-c$. If such a group G has coclass 1, we also say that G is of maximal class (indeed, its class is $n-1$, the maximal nilpotency class of a group of order p^n).

Groups of maximal class were studied by Blackburn in the 1950s, and then by Shepherd, Leedham-Green, and McKay in the 1970s. A surprising phenomenon which was discovered in these investigations is that these groups, which are on the one hand furthest away from abelian groups, are in some other sense rather close to being abelian. The evidence gathered from the theory of p-groups of maximal class led Leedham-Green and Newman in 1980 to propose a series of powerful and challenging conjectures, which can be viewed as an attempt to classify finite p-groups asymptotically, using the coclass as the primary invariant.

The classification of finite simple groups was briefly mentioned and applied in previous sections, but can one classify finite p-groups? The collection of finite p-groups seems chaotic in many ways. For instance, while there are at most two simple groups of any given finite order (up to isomorphism), there are $p^{(2/27+o(1))n^3}$ groups of order p^n, as shown by Higman and Sims. The attempt to classify p-groups using the nilpotency class as the main invariant fails already when we reach groups of class two. The coclass philosophy can be phrased as follows: if you cannot start with the beginning, start with the end! (namely, with groups with very large nilpotency class). And strangely enough, it works: in many ways the attempt to describe p-groups of large class (small coclass) turned out to be more successful than that of describing p-groups of small class.

The coclass conjectures, stated in [LGN] in decreasing strength, from conjecture A to conjecture E, had an enormous impact on the theory of finite p-groups and infinite pro-p groups. While they did not result in the classification of p-groups up to isomorphism (an impossible task), they did result in some weak classification in the sense of division into classes, each of which is surprisingly well behaved.

Let us state here three of these conjectures.

Conjecture D: Given p and r, there are only finitely many isomorphism types of infinite pro-p groups of coclass r.

Conjecture C: Pro-p groups of finite coclass are solvable.

Conjecture A: For some function f, every finite p-group of coclass r has a normal subgroup of class at most 2 (1, if $p=2$) and index at most $f(p,r)$.

Some of these conjectures may be reformulated as combinatorial statements on the structure of certain graphs. Thus, let Γ be a (directed) graph whose vertices are all finite p-groups of coclass r, where (H,G) is an edge if there is an epimorphism from H to G whose kernel has order p. Then Conjecture D is tantamount to saying that there are only finitely many infinite chains in Γ.

It is a remarkable consequence of Conjecture C that every pro-p group G of finite coclass has the structure of a p-adic prespace group; this means that G is an extension of a free finitely generated p-adic module by a finite p-group, so in particular it is virtually abelian. Such groups can be viewed as a p-adic analogue of crystallographic groups, appearing in chemistry. For this and more details, see [LGN].

There is a certain counterintuitive aspect in some of the conjectures in that they assert that groups of small coclass, that is, of very large nilpotency class, are in a sense almost abelian.

A major breakthrough in the study of these conjectures is the discovery, by Leedham-Green, that pro-p groups of finite coclass are p-adic analytic. This means that they have the structure of a p-adic Lie group, namely, a p-adic manifold, with the group operations being expressed by analytic functions. It is intriguing that pro-p groups of polynomial subgroup growth were also shown to be p-adic analytic and that this fact was instrumental in proving Theorem 7 above.

The theory of p-adic analytic groups was developed by Lazard in the 1960s and then by Lubotzky, Mann, and others in the 1980s (see [DDMS]). It is a powerful theory which is acquiring more and more applications. Two main features of p-adic analytic pro-p groups are that they are linear (namely, can be embedded in some group of matrices over a field) and that their structure is intimately related to the structure of some Lie algebras which can be associated with them. Using these features and some other tools, it was shown in [Do] and [LG1] (for $p > 3$) and then in [ShZ] (for all p, using a simpler method) that Conjecture C holds. In view of previous remarks this can be stated as follows.

***Theorem 8** (Donkin, Leedham-Green, Shalev, Zelmanov). Let G be a pro-p group satisfying $|G/\gamma_n| \leq p^{n+c}$ for some constant c and for all n. Then G has an abelian subgroup of finite index.*

Further work led to the proof of Conjecture A and thereby of all of the coclass conjectures. The proof in [LG2] was given first. Like some results mentioned in the first section, this proof (based on limit arguments) said something about *almost all* finite p-groups of coclass r, not about all of them; consequently it did not result in explicit bounds for the function f occurring in Conjecture A. An effective proof, which does provide explicit bounds, was subsequently given in [Sh1]. For instance, it follows from [Sh1, 1.7] that a group of order 2^n containing a nonidentity commutator of length $n - 10$ (i.e., having coclass at most 10) has an abelian subgroup of index at most $2^{2^{25}}$ (this awful bound can be improved if n is large).

The success of the coclass project led people to examine similar slimness conditions for other objects, such as torsion-free nilpotent groups and Lie algebras, as well as weaker slimness conditions for pro-p groups. Some results have been obtained by Zelmanov, Caranti and Newman, and others. See, for instance, Chapter 1 (§6) and Chapter 2 (§7) of [DSSh]. Zelmanov's approach brings many tools from the theory of (associative and nonassociative) rings into play and uses the notion of Gelfand-Kirillov dimension, which is a way to measure growth of rings. In fact, there is a long and independent tradition of studying slim rings, with results by Artin, Small, Stafford, and Warfield on associative rings, and of Vergne, Kac, and Mathieu on Lie algebras. These trends in ring theory and in group theory, which developed independently, are now becoming rather interrelated.

One of the main challenges in the group-theoretic part of this project is to understand pro-p groups G satisfying $|G/\gamma_n| \leq p^{cn}$ for all n. These groups are not as slim as groups of finite coclass, but they are not much fatter. Is there a hope of understanding their structure? It seems that each time someone tries to formulate a conjecture about these mildly slim groups, some constructions (such as the so-called Nottingham group and Grigorchuk groups) are quickly shown to refute it. The pessimist would argue that there are too many (and too wild!) examples to allow a general structure theory, while the optimist sees a glimmer of light at the end of the tunnel. Both would agree that the study of slim objects is one of the exciting current trends in asymptotic group theory.

References

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

[DDMS] J. D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, *Analytic Pro-p Groups*, 2nd edition, Cambridge University Press, 1999.

[Do] S. Donkin, Space groups and groups of prime power order. VIII. Pro-p groups of finite coclass and p-adic Lie algebras, *J. Algebra* **111** (1987), 316–342.

[DSSh] M.P.F. du Sautoy, D. Segal, and A. Shalev (eds.), *New Horizons in Pro-p Groups*, Progr. Math., Birkhäuser, 2000.

[ET1] P. Erdős and P. Turán, On some problems of a statistical group theory. I, *Z. Wahrscheinlichkeitstheorie Verw. Gabiete* **4** (1965), 175–186.

[KL] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.

[K1Li] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[LG1] C. R. Leedham-Green, Pro-p groups of finite coclass, *J. London Math. Soc.* **50** (1994), 43–48.

[LG2] ——, The structure of finite p-groups, *J. London Math. Soc.* **50** (1994), 49–67.

[LGN] C. R. Leedham-Green and M. F. Newman, Space groups and groups of prime power order I, *Arch. Math.* **35** (1980), 193–202.

[LiSh1] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.

[LiSh2] ——, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Ann. of Math.* **144** (1996), 77–125.

[LiSh3] ——, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.

[Lu] A. Lubotzky, Counting finite index subgroups, *Groups '93 – Galway/St. Andrews*, London Math. Soc. Lecture Note Series, vol. 212, Cambridge University Press, Cambridge, 1995, pp. 368–404.

[LMS] A. Lubotzky, A. Mann, and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82** (1993) 363–371.

[M] A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429–459.

[MSh] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel. J. Math.* **96** (1997), 449–468 (Amitsur memorial issue).

[SSh] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math. Soc.* **55** (1997), 320–334 (Hartley memorial issue).

[Sh1] A. Shalev, The structure of finite p-groups: Effective proof of the coclass conjectures, *Invent. Math.* **115** (1994), 315–345.

[Sh2] ——, Simple groups, permutation groups, and probability, *Proc. International Congress of Mathematicians, Berlin, 1998*, Vol. II, Berlin, 1998, pp. 129–137.

[ShZ] A. Shalev and E. I. Zelmanov, Pro-p groups of finite coclass, *Math. Proc. Cambridge Philos. Soc.* **111** (1992), 417–421.