Chapter 2
Estimation Problems and Randomised Group Algorithms

Alice C. Niemeyer, Cheryl E. Praeger, and Ákos Seress

2.1 Estimation and Randomization

2.1.1 Computation with Permutation Groups

In 1973, Charles Sims [89] proved the existence of the Lyons–Sims sporadic simple group Ly by constructing its action as a group of permutations of a set of cardinality 8,835,156 on a computer which could not even store and multiply the two generators of Ly in this smallest degree permutation representation for the group! The existence of this finite simple group, together with many of its properties, had been predicted by Richard Lyons [60], but proof of existence was not established until Sims' construction. Leading up to this seminal achievement, Sims [88] had developed concepts and computational methods that laid the foundation for his general theory of permutation group computation.

A.C. Niemeyer (✉)
Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia
e-mail: alice.niemeyer@uwa.edu.au

C.E. Praeger
Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia

King Abdulaziz University, Jeddah, Saudi Arabia
e-mail: cheryl.praeger@uwa.edu.au

Á. Seress
Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia

The Ohio State University, Columbus, OH, USA
e-mail: akos@math.ohio-state.edu

A. Detinko et al. (eds.), *Probabilistic Group Theory, Combinatorics, and Computing*, Lecture Notes in Mathematics 2070, DOI 10.1007/978-1-4471-4814-2_2,

Sims introduced the critical concept of a *base* of a permutation group G on a finite set Ω, namely a sequence of points $\alpha_1, \ldots, \alpha_b$ of Ω such that only the identity of G fixes all of them. For example, the dihedral group $D_{2n} = \langle a, b \rangle$ acting on $\{1, 2, \ldots, n\}$, where $a = (1, 2, \ldots, n)$ and $b = (2, n)(3, n-1)\ldots$, has a base $B = (1, 2)$, since only the identity of D_{2n} fixes both 1 and 2. Moreover the $2n$ elements $g \in D_{2n}$ produce $2n$ distinct image pairs $(1^g, 2^g)$ of the base B—for example, a maps B to $(2, 3)$, b maps B to $(1, n)$.

Sims observed that elements of a permutation group G could always be represented uniquely by the sequence of images of the points of a given base B. He exploited this potentially compact representation of group elements, ingeniously showing how to compute in G with these base images, via a so-called strong generating set of G relative to B. Sims' algorithm to construct a base and strong generating set, called the *Schreier–Sims algorithm*, is of fundamental importance for permutation group computation.

For groups possessing a small base, the Schreier–Sims algorithm is extremely efficient, but for some groups every base has size close to the cardinality $n = |\Omega|$ of the point set. For such groups, the methods are not effective. Examples of such large-base groups include the "giants": the alternating group $\mathrm{Alt}(\Omega) = A_n$ and the symmetric group $\mathrm{Sym}(\Omega) = S_n$, which have minimum-sized bases $(1, 2, \ldots, n-2)$ and $(1, 2, \ldots, n-1)$ respectively.

2.1.2 Recognising the Permutation Group Giants

For computational purposes, a finite permutation group G on Ω is given by a (usually small) set X of generators. The group G consists of all products of arbitrary length of elements from X. Since the Schreier–Sims algorithm is ineffective for computation with the giants $\mathrm{Alt}(\Omega)$ and $\mathrm{Sym}(\Omega)$, it is important to determine in advance (that is, before trying to find a base and strong generating set) whether or not a given permutation group $G = \langle X \rangle$ is one of these giants. Thus the question of identifying the giants $\mathrm{Alt}(\Omega)$ and $\mathrm{Sym}(\Omega)$, given only a generating set of permutations, was a central issue in the development of general purpose group theory computer systems.

Theoretically the problem of detecting these giants had engaged mathematicians from the earliest studies of group theory. Since the seminal work of Camille Jordan in the 1870s, it has been known that there are many kinds of permutations such that the only transitive permutation groups containing them are the giants (we say that $G \leq \mathrm{Sym}(\Omega)$ is *transitive* if each pair of points of Ω can be mapped one to the other by an element of G). The most beautiful of these results that identifies a large family of such elements is Jordan's theorem below.

Let us call a permutation $g \in S_n$ a *Jordan element* if g contains a p-cycle, for some prime p with $n/2 < p < n-2$. For example, $g = (1, 2, 3, 4, 5)(6, 7) \in S_9$ is a Jordan element (with $n = 9$, $p = 5$).

Theorem 2.1. *If a transitive permutation group $G \leq S_n$ contains a Jordan element then G is A_n or S_n.*

Given a set of generators for $G \leq \mathrm{Sym}(\Omega)$, it is easy to test whether G is transitive. Hence, recognising the giants boils down to the question: how prevalent are the Jordan elements in the giants? For a fixed prime $p \in (n/2, n-2)$, the number of elements in S_n containing a p-cycle is

$$\binom{n}{p}(p-1)!(n-p)! = \frac{n!}{p} \text{ (and } \frac{n!}{2p} \text{ in } A_n),$$

so the proportion of Jordan elements in A_n or S_n for this prime p is $1/p$, and therefore the proportion of Jordan elements in A_n or S_n is $\sum_{n/2<p<n-2} \frac{1}{p} \geq \frac{c}{\log n}$ for some constant c. For $n \geq 100$, c can be taken to be $1/5$, which follows by applying an inequality by Dusart [25, p. 414] to determine the number of primes p with $n/2 < p < n-2$. So roughly c out of every $\log n$ independent, uniformly distributed random elements from S_n or A_n will be Jordan. That is to say, we should find a Jordan element with high probability by randomly selecting elements in a giant.

2.1.3 Monte Carlo Algorithms

How do we turn the comments above into a justifiable algorithm? We want to make some multiple of $\log n$ random selections from a transitive group G on n points which we suspect may be S_n or A_n, but as yet we have no proof of this fact. We hope, and expect, to find a Jordan element, thereby uncovering the secret and proving that G really is a giant S_n or A_n.

Formally, we model this process as a *Monte Carlo algorithm*. The Monte Carlo method was invented by Stanislaw Ulam in the 1940s; it was named after Monte Carlo Casino in Monaco which Ulam's uncle visited often (see the account in [62]). The characteristics of a Monte Carlo algorithm are that it completes quickly, but allows a small (user-controlled) probability of "error", that is, of returning an incorrect result. In our context, for a Monte Carlo algorithm, we begin with a prescribed bound on the error probability $\varepsilon \in (0, 1)$. The algorithm typically makes a number $N = N(\varepsilon)$ of random selections, depending on ε, this number being determined in advance to guarantee that the probability of an incorrect result is at most ε.

Here is a worked example of a Monte Carlo algorithm to recognise the giants S_n and A_n among transitive permutation groups on n points.

Algorithm 1: JORDAN

Input: A transitive subgroup $G = \langle x_1, \ldots, x_k \rangle \leq S_n$ and a real number $\varepsilon \in (0, 1)$ (the error probability bound);
Output: true or false;
# We hope the algorithm returns true if G is S_n or A_n – see the comments below;
for *up to* $N = \lceil (\log \varepsilon^{-1})(\log n)/c \rceil$ *random elements* g *from* G **do**
  if g *is a Jordan element* **then**
    return true;
  end
end
Return false;

Comments on the algorithm

1. The procedure completes after at most N repeats of the **if** statement, so it *is* an algorithm! If it returns true then $G = A_n$ or S_n by Jordan's Theorem 2.1. On the other hand, if the algorithm returns false then this may be incorrect, but only if G does equal A_n or S_n, and we failed to find a Jordan element.
2. We have
   Prob(we do not find a Jordan element, given that $G = A_n$ or $G = S_n$) $\leq \left(1 - \frac{c}{\log n}\right)^N < \varepsilon$.
   So Algorithm 1 is a Monte Carlo algorithm with error probability less than ε. This is a special kind of Monte Carlo algorithm: the result true is always correct, and the possibility of an incorrect result is confined to the case where false is returned. Such algorithms are called *one-sided Monte Carlo algorithms*.
3. This probability estimate assumes that the random selections made are independent and uniformly distributed. There are algorithms available for producing "approximately random" elements from a group given by a generating set; see [3,18,24]. We shall not discuss the theoretical details of these algorithms or their practical performance. Rather we assume in our discussion of randomised algorithms that we are dealing with independent uniformly distributed random elements.
4. The design and discussion of this simple algorithm used concepts and results from group theory to prove correctness, and from number theory to establish the bound on the error probability. It is typical to gather and develop methods from a variety of mathematical areas to achieve good algorithm design and analysis.
5. Algorithm 1 is essentially the algorithm used in GAP [37] and MAGMA [15] for testing if a permutation group is a giant. It was first described by Parker and Nikolai [79], preceding Sims' work by a decade. The second author (Praeger) recalls numerous discussions with John Cannon, over a number of years, about the implementation of this algorithm in connection with his development of the computer algebra system CAYLEY (a precursor to MAGMA). There was much to learn about improving the practical performance of the algorithm to avoid its becoming a bottle-neck for permutation group computation. A wider class of "good elements" than the Jordan elements was used, based on generalisations of

Jordan's Theorem (see [94, 13.10] and [83]), and better methods were developed to produce "approximately random" elements.

2.1.4 What Kinds of Estimates and in What Groups?

Notice the role estimates played in Algorithm 1:

a lower bound for the proportion of Jordan elements gives an upper bound on the error probability.

Does it matter if the estimate is far from the true value? We might, for different reasons, propose one of two different answers to this question:

1. We might say "no", because if there are more Jordan elements than our estimates predict, then we simply find one more quickly and the algorithm confirms that "G is a giant" more efficiently.
2. We might say "yes", because if G is not a giant then we force the algorithm to do needless work in testing too large a number of random elements so that the algorithm runs more slowly than necessary on non-giants. Note that the algorithm will never find a Jordan element in a non-giant by Theorem 2.1, so the full quota of random elements will be tested before completion.

For general purpose algorithms such as Algorithm 1, which are used frequently on arbitrary permutation groups, the quality of the estimates really does matter. We should try to make estimates as good as possible, especially when they are used to analyze a time-critical module of a randomised algorithm.

In the computer algebra systems GAP and MAGMA, new algorithms are under development for computation with matrix groups and permutation groups. These employ a tree-like data structure which allows a "divide and conquer" approach, reducing to computations in normal subgroups and quotient groups. This approach (see Sect. 2.4.1) reduces many computational problems to the case of finite simple groups. Accordingly many of the topics chosen in this chapter are of relevance to computing with finite simple groups.

2.1.5 What Group is That: Recognising Classical Groups as Matrix Groups

As a more substantial example for group recognition, we describe an algorithm to recognise a finite classical group in its natural representation. By this, we mean that the algorithm will return the "name" of the group. We give a broad-brush description of the classical recognition algorithm developed in [72] generalising the Neumann–Praeger SL-recognition algorithm in [69].

The algorithm takes as input a subgroup G of a finite n-dimensional classical group $\mathrm{Class}(n, q)$ over a finite field $\mathbb{F}_q$ of order q, such as the general linear group $\mathrm{GL}(n, q)$ or a symplectic group $\mathrm{Sp}(n, q)$, in its natural representation as a group of

matrices acting on the underlying vector space $V(n,q)$. The subgroup G is given by a generating set of $n \times n$ matrices over $\mathbb{F}_q$. The algorithm seeks so-called *ppd elements* in G which we describe as follows.

For an integer $e > 1$, a *primitive prime divisor (ppd)* of $q^e - 1$ is a prime r dividing $q^e - 1$ such that r does not divide $q^i - 1$ for any $i < e$. It has been known for a long time that primitive prime divisors exist unless $q = 2$, $e = 6$, or $e = 2$ and $q + 1$ is a power of 2; see [97]. Superficially, primitive prime divisors seem interesting because the order of the classical group has the form

$$|\operatorname{Class}(n,q)| = q^{\text{some power}} \prod_{\text{various } i} (q^i \pm 1).$$

We define a *ppd-$(q;e)$ element* $g \in \operatorname{Class}(n,q)$ as an element with order divisible by a ppd of $q^e - 1$. The algorithm in [72] seeks two ppd elements, namely a ppd-$(q;e_1)$ and a ppd-$(q;e_2)$ element for $e_1 \neq e_2$ and $e_1, e_2 > n/2$, which satisfy various additional minor conditions described in [72, Sects. 2 and 9]. We call such a pair a *good ppd matrix pair*. Their importance lies in the following deep theorem [72, Theorem 4.8], the proof of which relies heavily on the finite simple group classification.

Theorem 2.2. *If $G \leq \operatorname{Class}(n,q)$ is irreducible on $V(n,q)$ and G contains a good ppd matrix pair, then (essentially) $G = \operatorname{Class}(n,q)$ or G is known explicitly.*

Thus, provided that (a) we can test efficiently whether G is irreducible on $V(n,q)$, (b) good ppd matrix pairs are sufficiently prevalent in $\operatorname{Class}(n,q)$ and are easily identifiable, and (c) the exceptions in Theorem 2.2 are easy to deal with, the good ppd matrix pairs could play the role of the Jordan elements used to identify the permutation group giants in Algorithm 1. We would then have an analogue of Algorithm 1 for classical groups, underpinned by considerably deeper theory than Jordan's Theorem 2.1. It would look like this:

Algorithm 2: RECOGNISECLASSICAL

Input: An irreducible subgroup $G = \langle X_1, \ldots, X_k \rangle \leq \operatorname{Class}(n,q)$ and a real number $\varepsilon \in (0,1)$ (the error probability bound).
Output: true or false
# If the output is true, we are certain that $G = \operatorname{Class}(n,q)$;
# the output false may be incorrect;
for Many*(depending on n, q, ε) random elements $g \in G$* **do**
  determine if g is a ppd element with the additional properties;
  if *a good ppd matrix pair is found* **then**
    if *G is one of the exceptions* **then**
      return false
    else
      return true;
    end
  end
end
return false;

Comments on the algorithm

1. Note that if Algorithm 2 returns true then G really is Class(n, q) by Theorem 2.2; while if it returns false then the result may be incorrect (namely if $G =$ Class(n, q) and we fail to find the good ppd matrix pair).
2. The missing ingredient is our knowledge of the presence of good ppd matrix pairs in Class(n, q), and an estimate of their proportion. We need a positive lower bound on their proportion in order to decide how Many random elements to test to ensure an error probability of at most ε. This is necessary to prove that we have a one-sided Monte Carlo algorithm.

Estimating the proportion of ppd-$(q; e)$ elements in Class(n, q): For the details involved in dealing with the additional properties we refer the reader to [72]. For $G =$ Class(n, q) and $e > n/2$, let ppd(G, e) be the proportion of ppd-$(q; e)$ elements in G. We give a few details for the general linear case.

Lemma 2.3. *Let $G =$ GL(n, q) and let $\frac{n}{2} < e \leq n$. Then $\frac{1}{e+1} \leq ppd(G, e) \leq \frac{1}{e}$.*

Proof. Let $g \in G$ be a ppd-$(q; e)$ element and let r be a ppd of $q^e - 1$ dividing $|g|$. By considering a power of g of order r, we can show that g leaves invariant a unique e-dimensional subspace U of $V(n, q)$, and acts irreducibly on U. Moreover the induced element $g|_U$ is a ppd-$(q; e)$ element in GL(U), and a straightforward counting argument (see [72, Lemma 5.1]) shows that ppd$(G, e) =$ ppd(GL$(U), e)$.

In other words, we may assume that $n = e$ in the proof. With this assumption, we have g irreducible on $V(n, q)$, and each such element lies in a Singer cycle $S = Z_{q^e-1}$ of G. All Singer cycles are conjugate in G, and distinct Singer cycles contain disjoint sets of irreducible elements. Moreover the number of Singer cycles is $|G : N_G(S)| = |G|/(e(q^e - 1))$ (see [69, Lemma 2.1]). Hence ppd(G, e) is equal to $(1/e) \times$ (the proportion of such elements in the cyclic group S).

This immediately gives ppd$(G, e) \leq 1/e$. We need one more observation to obtain the lower bound. Certainly each element of S of order not divisible by r lies in the unique subgroup S_0 of S of index r. Thus each element of $S \setminus S_0$ has order divisible by r, and hence ppd$(G, e) \geq (1/e) \times (1 - 1/r)$. Now e is the least positive integer such that $q^e \equiv 1 \pmod{r}$, and so q has order e modulo the prime r. This implies that e divides $r - 1$, and in particular $r \geq e + 1$. Hence ppd$(G, e) \geq (1/e) \times e/(e + 1) = 1/(e + 1)$. □

A similar argument in [72, Theorem 5.7] shows that the bounds of Lemma 2.3 hold for the other classical groups for almost all values of e. Since each ppd element corresponds to just one e-value (because $e > n/2$), we can find a lower bound for the proportion of ppd elements in G by adding the lower bounds for ppd(G, e) over all relevant e. For GL(n, q), this is $\sum_{n/2<e\leq n} 1/e \sim \log 2$ by Lemma 2.3. For the other classical groups, the values of e occurring all have the same parity (odd for unitary groups and even for symplectic and orthogonal groups), and for these groups the proportion of ppd elements is roughly $(\log 2)/2$ [72, Theorem 6.1].

These lower bounds (or rather, the equivalent ones we obtain in [72] after taking into account the additional conditions on the ppd elements) allow us to decide

how many random selections to make in order to find a good ppd matrix pair with probability at least $1 - 1/\varepsilon$, and hence to determine the value for Many in Algorithm 2.

2.1.6 What Group is That: Recognising Lie Type Groups in Arbitrary Representations

Of course, we do not only encounter the classical groups in their natural representation. If G is a simple group of Lie type, given in any permutation or matrix group representation, and the characteristic p of G is known, then we may proceed by an extension of Algorithm 2. The procedure that we sketch was developed in [6].

Let e_1 and e_2 be the two highest *ppd exponents*, that is, integers e such that G contains elements of order divisible by a primitive prime divisor of $p^e - 1$. It was shown in [6] that for each pair of integers (e_1, e_2), there are at most seven isomorphism types of Lie type groups of characteristic p with e_1, e_2 as the highest ppd exponents in the group. Also, ppd elements with ppd exponents e_1 and e_2 are frequent enough that we encounter them in a random sample of size polynomial in the input length.

To distinguish between the possibilities for G with the same values e_1 and e_2, we consider the third highest ppd exponent in G and elements whose order is divisible by a product of two ppd primes, corresponding to certain chosen ppd exponents. The result is a polynomial-time Monte Carlo algorithm that names the isomorphism type of G, with one exception: a polynomial-size random sample may not distinguish the groups $\mathrm{Sp}(2m, p^f)$ and $O(2m+1, p^f)$, for odd primes p. This last ambiguity was handled by Altseimer and Borovik [1].

2.2 Proportions of Elements in Symmetric Groups

2.2.1 Notation

In this section we fix a set Ω and consider the symmetric group $\mathrm{Sym}(\Omega)$ on Ω. When $\Omega = \{1, \ldots, n\}$ for some positive integer n we write S_n instead of $\mathrm{Sym}(\{1, \ldots, n\})$. Elements of S_n are written in disjoint cycle notation. The *number of cycles* of a given element $g \in S_n$ denotes the number of disjoint cycles g has on $\{1, \ldots, n\}$ including fixed points.

2.2.2 Historical Notes

The study of proportions of permutations has been of interest to mathematicians for a long time. For example, in 1708 Monmort introduced and analyzed a game

of 13 cards which he called "jeu de Treize" (the game of thirteen) in his book on the theory of games [64, pp. 54–64]. He later generalised the game to any number of cards numbered from 1 to n [65, pp. 130–143]. In the game, a player has n turns, each time announcing out loud the number of the turn and picking a card at random from the deck of n cards without replacing it. The game is won if each time the number of the card and the number announced are different. Leonhard Euler in *Solutio Quaestionis curiosae ex doctrina combinationum* [34] describes the game as follows: *Data serie quotcunque litterarum* a, b, c, d, e *etc., quarum numerus sit* n*, invenire quot modis earum ordo immutari possit, ut nullo in eo loco reperiatur, quem initio occupaverat.* This can be translated as *Given an arbitrary series (sequence) of letters* $a, b, c, d, e, \ldots$*, let the number of which be* n*, find in how many ways their order may be changed so that none reappears in the same place which it originally occupied.*[1] In [33] Euler showed that the number of solutions is the integer closest to $n!/e$. Earlier solutions had already been given; for example, Monmort presented a solution by Nicolas Bernoulli [65, pp. 301–302]. De Moivre also mentions the game already in the first edition of [23], and gives a solution in [23, Problem 35].

Today this problem is often called the hat-swapping problem: *Suppose n men each put a hat on a hat rack in a restaurant. When they leave they each choose a random hat. What is the probability that no man chooses his own hat?*

Nowadays we call a permutation in S_n which has no fixed points on $\{1, \ldots, n\}$ a *derangement*, and we would rephrase the game of thirteen, Euler's question or the hat-swapping problem as: How many derangements are there in S_n?

In this section we will focus on certain other proportions of elements in S_n. The proportions that we focus on arise either from algorithmic applications for permutation groups or from applications to classical groups of Lie type (see Sect. 2.3.2).

2.2.3 Orders of Permutations

The order of a permutation can easily be read off from its disjoint cycle notation; namely it is the least common multiple of the cycle lengths. One of the oldest results on the order of an element in a symmetric group is due to Landau, who determined how large the order of an element in S_n can be asymptotically.

Theorem 2.4 (Landau [51]).

$$\lim_{n\to\infty} \frac{\log\left(\max_{g\in S_n}(\mathrm{ord}(g))\right)}{\sqrt{n\log(n)}} = 1.$$

[1] Translation by Peter M. Neumann, The Queen's College, University of Oxford.

Although the order of an element in S_n can be as large as the previous theorem suggests, Erdős and Turán were able to prove, in the first of a series of papers [27–32] on the subject of the statistics of permutations, that most elements have much smaller order.

Theorem 2.5 (Erdős and Turán [27]). *For $\varepsilon, \delta > 0$ there is a number $N_0(\varepsilon, \delta)$ such that for all $n \geq N_0(\varepsilon, \delta)$,*

$$\frac{|\{g \in S_n \mid (1/2 - \varepsilon)\log^2(n) \leq \log(\mathrm{ord}(g)) \leq (1/2 + \varepsilon)\log^2(n)\}|}{n!} \geq 1 - \delta.$$

Erdős and Turán proved many more insightful results on the order of elements in symmetric groups. For example, in [28] they investigated prime divisors of the order of elements in symmetric groups. In [29] they described for any x the limiting behaviour as n tends to infinity of the proportion of elements g in S_n for which $\log(\mathrm{ord}(g)) \leq \frac{1}{2}\log^2(n) + x\log^{3/2}(n)$. In [30] they considered, among other problems, the number of different values that $\mathrm{ord}(g)$ can have as g ranges over the elements of S_n.

Goh and Schmutz [39] prove that the logarithm of the average order of a random permutation in S_n is $c\sqrt{n/\log(n)}$, where $c = 2\sqrt{2\int_0^\infty \log\log\left(\frac{e}{1-e^{-t}}\right)dt}$. This constant is approximately 2.99.

2.2.4 Number of Cycles

Let $a(n)$ denote the average number of cycles of the elements in S_n. In a seminal paper [40], Gončarov examined various properties of random permutations. Among many other results, he proved that the average number of cycles of a permutation in S_n is close to $\log(n)$.

Theorem 2.6 (Gončarov [40]).

$$a(n) = \sum_{i=1}^{n} \frac{1}{i} = \log(n) + \gamma + o(1)$$

for $n \to \infty$.

Plesken and Robertz [82] generalised these results to A_n and to wreath products of groups with imprimitive action.

2.2.5 Generating Functions

One very powerful method of obtaining information about certain combinatorial quantities is to employ generating functions.

Given a sequence $(a_n)_{n\in\mathbb{N}}$ of real numbers, the *Ordinary Generating Function* for a_n is

$$A(z) := \sum_{n\geq 0} a_n z^n.$$

For example, a_n could be the number of certain elements in S_n.

A very intuitive way to view generating functions is given in the following quote from Wilf's aptly named book *generatingfunctionology* [96]: "A generating function is a clothesline on which we hang up a sequence of numbers for display." Here we just highlight some of the ways in which generating functions can shed light on some of our problems. To understand the power and beauty of the subject of generating functions we refer the reader to both Wilf's book [96] and a recent book on analytic combinatorics by Flajolet and Sedgewick [35]. Both books also contain various interesting results on proportions of permutations.

Several types of generating functions can be defined, and the type of generating function chosen to attack a particular problem depends on the circumstances. In our situation *exponential generating functions* are of particular interest. They are of the form

$$A(z) := \sum_{n\geq 0} \frac{a_n}{n!} z^n$$

and ensure that the coefficients $\frac{a_n}{n!}$ of z^n are manageable in situations where a_n is expected to grow almost as fast as $n!$. For example, if a_n is the number of elements with a particular property in S_n, then this number could grow rapidly and using an ordinary generating function would quickly produce unwieldy coefficients. However, dividing by the order of the group S_n ensures that the coefficients $a_n/n!$ are proportions of elements in S_n and thus all less than 1.

We study generating functions as elements of the ring of formal power series. Analytic questions, convergence etc. do not concern us just yet. Generating functions can be manipulated in various ways, and this theory is described in the above mentioned books. Here we just state, as an example, how two generating functions can be multiplied:

$$\left(\sum_{n=0}^{\infty} a_n z^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n z^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) z^n.$$

The usefulness of taking a generating function approach in our situation can be highlighted with the following example. A further example, that estimates the proportion of regular semisimple elements in general linear groups, is given in Sect. 2.3.6.

2.2.5.1 Example

Let $b \geq 1$ be a fixed integer and let a_n denote the number of permutations in S_n all of whose cycles have length at most b.

We would like to study the exponential generating function describing the numbers a_n. So let

$$A(z) := \sum_{n\geq 0} \frac{a_n}{n!} z^n.$$

One very effective way of studying a generating function is to start from a recursive equation for the coefficients a_n, and we employ this method here. Our first task is to find a suitable recursion for a_n. Recall that we write permutations in disjoint cycle notation. We are interested in finding an expression for the number a_n of permutations in S_n all of whose cycles have length at most b in terms of a_m for integers m smaller than n. We employ a combinatorial trick which has been used e.g. in Beals et al. [9, Theorem 3.7].

We enumerate the permutations in S_n all of whose cycles have length at most b according to the length d of the cycle containing the point 1. For a fixed d, we have $\binom{n-1}{d-1}$ choices for the remaining points of the cycle of length d containing 1. On these d points we can put any one of $(d-1)!$ different cycles and we have a_{n-d} choices for the permutation on the remaining $n-d$ points. Thus we obtain the recursion

$$\frac{a_n}{n!} = \frac{1}{n} \sum_{d=1}^{\min\{b,n\}} \frac{a_{n-d}}{(n-d)!}.$$

Note in particular that $a_n = n!$ for $n \leq b$, which is in agreement with this recursion. The recursion implies that

$$\begin{aligned} A(z) := \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n &= 1 + \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{d=1}^{\min\{b,n\}} \frac{a_{n-d}}{(n-d)!} \right) z^n \\ &= 1 + \sum_{d=1}^{b} \sum_{n=d}^{\infty} \frac{1}{n} \frac{a_{n-d}}{(n-d)!} z^n = 1 + \sum_{d=1}^{b} \sum_{n=0}^{\infty} \frac{1}{n+d} \frac{a_n}{n!} z^{n+d}. \end{aligned}$$

A very useful trick when working with generating functions is to take the derivative. This yields in our case

$$A'(z) = \sum_{d=1}^{b} \sum_{n=0}^{\infty} \frac{a_n}{n!} z^{n+d-1} = \sum_{d=1}^{b} z^{d-1} \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n = \sum_{d=1}^{b} z^{d-1} A(z).$$

Thus

$$\frac{A'(z)}{A(z)} = \sum_{d=1}^{b} z^{d-1}$$

and so

$$\log(A(z)) = \sum_{d=1}^{b} \frac{z^d}{d}.$$

Therefore we see that our generating function is

$$A(z) = \exp(\sum_{d=1}^{b} \frac{z^d}{d}).$$

While this has yielded a very succinct way of describing the number of elements of interest, it does not as yet yield the desired upper and lower bounds for the proportion of such elements. Thus we would like to know whether generating functions can tell us about the limiting behaviour of the coefficients.

An elaborate theory of the asymptotic behaviour of the coefficients of the generating functions exists. We mention here briefly a subject called "Saddlepoint Analysis". The theory is described in the above mentioned books (see also the papers by Moser and Wyman [67, 68] and Bender [11]). We quote here one result from Flajolet and Sedgewick's book, which helps in the situation of our example. The quoted result is based on a more general theorem by W.K. Hayman [43] (see also Theorem VIII.4 of [35]). In line with the literature, we denote the coefficient of z^n in the generating function $A(z)$ by $[z^n]A(z)$. The operator $z\frac{d}{dz}$ is defined by $z\frac{d}{dz} : P(z) \mapsto zP'(z)$.

Theorem 2.7 (see Corollary VIII.2 of [35]). *Let* $P(z) = \sum_{j=1}^{n} a_j z^j$ *have non-negative coefficients and suppose* $\gcd(\{j \mid a_j \neq 0\}) = 1$. *Let* $F(z) = \exp(P(z))$. *Then*

$$[z^n]F(z) \sim \frac{1}{\sqrt{2\pi\lambda}} \frac{\exp(P(r))}{r^n},$$

where r *is defined by* $rP'(r) = n$ *and* $\lambda = \left(z\frac{d}{dz}\right)^2 P(r)$.

2.2.5.2 Example of Saddlepoint Analysis

Recall that $A(z) = \exp(\sum_{d=1}^{b} \frac{z^d}{d})$ is the exponential generating function for the number of elements all of whose cycles have length at most b.

Let $P(z) = \sum_{d=1}^{b} \frac{z^d}{d}$. Then $P(z)$ is a polynomial in z with non-negative coefficients and satisfies $\gcd(\{d \mid \text{coefficient of } z^d \text{ is nonzero}\}) = 1$. The first step in applying Saddlepoint Analysis is to estimate r determined by the equation $n = rP'(r)$. We have $n = rP'(r) = r\sum_{d=1}^{b} r^{d-1} = \sum_{d=1}^{b} r^d \geq r^b$, and so $r \leq \sqrt[b]{n}$.

The next step is to estimate λ, where $\lambda = \left(r\frac{r}{dr}\right)^2 P(r) = r\sum_{d=1}^{b} dr^{d-1} = \sum_{d=1}^{b} dr^d \leq b\sum_{d=1}^{b} r^d = bn$.

Hence we have $r \leq n^{1/b}$, $\lambda \leq bn$ and $P(r) = \sum_{d=1}^{b} \frac{r^d}{d} \geq \frac{1}{b}\sum_{d=1}^{b} r^d = \frac{n}{b}$, implying

$$[z^n]A(z) \sim \frac{1}{\sqrt{2\pi\lambda}} \frac{\exp(P(r))}{r^n} \geq \frac{1}{\sqrt{2\pi bn}} \left(\frac{e}{n}\right)^{n/b}.$$

2.2.6 *Solutions to $x^m = 1$ in Symmetric and Alternating Groups*

The number of solutions to an equation of the form $x^m = 1$ for a fixed integer m in symmetric and alternating groups of degree n has received quite a lot of attention in the literature. More recently, interest in such equations has been rekindled due to algorithmic applications. In particular, it has also been important for algorithmic applications to find the asymptotic behaviour of the number of solutions of equations of the form $x^m = 1$ where m is allowed to grow with n.

We begin by outlining some of the results in the literature. For m fixed let

$$c(n,m) = \frac{1}{n!}|\{g \in S_n \mid g^m = 1\}|.$$

Let

$$C_m(z) = \sum_{n=0}^{\infty} c(n,m) z^n$$

be the corresponding generating function.

Theorem 2.8 (Jacobsthal [47]). *For a prime p we have*

$$C_p(z) = \exp\left(z + \frac{z^p}{p}\right) \text{ and } c(n,m) = \sum_{\lambda=1}^{[n/p]} \frac{1}{(n-\lambda p)!\lambda! p^\lambda}.$$

The number $n!c(n,2)$ of solutions to the equation $x^2 = 1$ in symmetric groups of degree n deserves particular attention, since it is also the sum of the degrees of the irreducible representations of S_n. Chowla et al. [20] examined $c(n,2)$ and showed that $n \cdot c(n,2) = c(n-1,2) + c(n-2,2)$. Thus they deduced that $1/\sqrt{n} \leq c(n,2) \leq 1/\sqrt{n} + \frac{1}{n}$ and found the dominant term of the asymptotic expansion for $c(n,2)$.

Later, Chowla et al. [21] were able to generalise Jacobsthal's expansion of $C_p(x)$ to $C_m(x)$ where m can be an arbitrary fixed integer, and they asked for an asymptotic formula for $c(n,m)$.

Theorem 2.9 (Chowla et al. [21]).

$$C_m(z) = \exp\left(\sum_{d|m} \frac{z^d}{d}\right).$$

Moser and Wyman [66, 67] derived an asymptotic formula in terms of a contour integral for $c(n,2)$ and derived the first order term of the asymptotic value of $c(n,p)$. Moreover, they were able to obtain corresponding results for alternating groups.

Theorem 2.10 (Moser and Wyman [66, 67]). *For a prime $p > 2$,*

$$c(n,p) \sim \frac{1}{n!}\frac{1}{\sqrt{p}}\left(\frac{n}{e}\right)^{n(1-\frac{1}{p})} e^{n^{\frac{1}{p}}}.$$

Herrera [44] gives the following recursive formula for the number $n!b(n,m)$ of elements in S_n of order m:

$$n!b(n,m) = \sum_s \frac{(n-1)!}{(n-s)!}\sum_t b(n-s,t), \quad \text{where } \gcd(t,s) = m.$$

Other authors (e.g. Chernoff [19], Mineev and Pavlov [63], and Pavlov [80]) studied the number of elements in S_n or A_n satisfying an equation of the form $x^m = a$ for some element $a \in S_n$.

In 1986 Volynets [92], Wilf [95] and Pavlov [81] independently determined the limiting behaviour of $c(n,m)$ for fixed m, and n tending to infinity. The following theorem is Wilf's formulation of the result.

Theorem 2.11. *Let m be a fixed positive integer. Define $\varepsilon(n,m) = 0$ if m is odd and $\varepsilon(n,m) = 1/(2m^2n)$ if m is even; and let*

$$\tau = \frac{1}{n^{1/m}}\left(1 + \frac{1}{nm}\sum_{d|m, d<m} n^{d/n} + \varepsilon(n,m)\right).$$

Then for $n \to \infty$ we have

$$c(n,m) \sim \frac{\tau^n}{\sqrt{2\pi mn}}\exp\{\sum_{d|m}\frac{1}{d\,\tau^d}\}.$$

The above result has been generalised in the literature in various directions and we shall mention some of these.

2.2.6.1 Families of *m*

Ben-Ezra [10] generalised these formulae as follows. Let Π be a set of primes and let Π' denote the set of all primes not in Π. Further, let $C_\Pi(z)$ denote the generating function for the proportion $c(n,\Pi)$ of all elements whose order only involves primes in Π, and let $C_{\Pi'}(z)$ denote the generating function for the proportion $c(n,\Pi')$ of all elements whose order only involves primes in Π'. For a finite set B of integers, define $||B|| = 1$ if $B = \varnothing$ and $||B|| = \prod_{b\in B} b$ otherwise. Then

Theorem 2.12 (Ben-Ezra [10]).

1. $C_{\Pi}(z) = \prod_{\substack{B\subseteq\Pi' \\ |B|<\infty}} (1 - z^{||B||})^{\frac{(-1)^{|B|+1}}{||B||}}$.
2. $C_{\Pi'}(z) = \prod_{\substack{B\subseteq\Pi \\ |B|<\infty}} (1 - z^{||B||})^{\frac{(-1)^{|B|+1}}{||B||}}$.

2.2.6.2 Growing *m*

The first author to consider an equation of the form $x^m = 1$ in symmetric groups of degree n in which m is not assumed to be fixed was Warlimont [93], who considers the case $m = n$. In particular, he shows that

Theorem 2.13 (Warlimont [93]).

$$\frac{1}{n} + \frac{2c}{n^2} \leq c(n,n) \leq \frac{1}{n} + \frac{2c}{n^2} + O\left(\frac{1}{n^{3-o(1)}}\right),$$

where $c = 0$ if n is odd and $c = 1$ if n is even.

In 1990 Erdős and Szalay [26] considered the case where m lies in the range $\log(n)/(2\log\log(n)) \leq m \leq n^{(1/4)-\varepsilon}$, and derived an asymptotic formula for $c(n,m)$.

Volynets [92] proved the following result via the Saddlepoint method.

Theorem 2.14 (Volynets [92]). *For primes p, and for positive integers n such that n and p tend to ∞ and $p/n \to 0$,*

$$c(n,p) = \frac{1}{n!}\left(\frac{n}{e}\right)^{n(1-1/p)} p^{1/2} \sum_{k=0}^{\infty} \frac{(n^{1/p})^{m+kp}}{(m+kp)!}(1+o(1)),$$

where $m = n - p[n/p]$. In particular, if $n^{1/p}/p^2 \to 0$ then

$$c(n,p) = \frac{1}{n!}\left(\frac{n}{e}\right)^{n(1-1/p)} p^{1/2} e^{n^{1/p}}(1+o(1)),$$

while if $n^{1/p}/p \to 0$ then

$$c(n,p) = \frac{1}{n!}\left(\frac{n}{e}\right)^{n(1-1/p)} p^{1/2} \frac{n^{m/p}}{m!}(1+o(1)).$$

Finally A.V. Kolchin [49] proved the following theorem using the method of generalised schemes of allocation (see [50, Chap. 5]).

Theorem 2.15 (Kolchin [49]). *For d, n positive integers such that $d\log\log(n)/\log(n) \to 0$ and for $\delta = 0$ if d is odd and $\delta = 1/(2d)$ when d is even, the following holds:*

$$c(n,d) = \frac{1}{n!}\frac{n^{n(1-1/d)}}{e^n}\frac{1}{\sqrt{d}}\exp\left\{\sum_{j|d}\frac{n^{j/d}}{j} - \delta\right\}(1+o(1)).$$

Another generalisation of the above to the case where the cycle lengths are elements of particular sets can be found in [90]. Finally we would like to refer the interested reader to V.F. Kolchin's book on random graphs [50], which contains many references and notes to the above mentioned, and other, results on random permutations.

2.2.7 The Münchausen Method (Bootstrapping)

The previous results highlight how difficult it is to obtain the overall limiting behaviour for $c(n,m)$ when $m \le \ell n$ for some constant ℓ and m is allowed to grow with n. However, for our algorithmic applications (see Sect. 2.2.8 below), we require good upper bounds for $c(n,m)$ in the case where $m = r(n-k)$ for $r \in \{1,2,3\}$ and $k \le 6$.

To obtain bounds for $c(n,m)$ in cases where $n-1 \le m \le \ell n$ for some constant ℓ, we return to more basic methods and highlight some of the ideas in a proof of the limiting behaviour of $c(n,m)$ in such cases.

A popular folk tale tells the story of how Baron Münchausen found himself stuck in a swamp while riding his horse. He then managed to save himself and his horse by pulling himself out of the swamp by his own ponytail.

We employ a similar strategy to obtain good estimates for our required proportions. We begin by deriving a first crude estimate and then using this to refine our estimates. This method (also called bootstrapping) was employed in [9] and later in [73].

The overall estimate for $c(n,m)$ is obtained in two steps. The first step yields a very crude estimate. This in turn is employed in a second step to yield a more refined estimate.

$$\text{Define } \gamma(m) := \begin{cases} 2 & \text{for } 360 < m \\ 2.5 & \text{for } 60 < m \le 360 \\ 3.345 & \text{for } m \le 60. \end{cases}$$

A first crude estimate for $c(n,m)$ is given in the following theorem.

Theorem 2.16. *Let $m,n \in \mathbb{N}$ with $m \ge n-1$. Then*

$$c(n,m) \le \frac{1}{n} + \frac{\gamma(m)m}{n^2}.$$

Proof-Idea for Crude Estimate

The proof of our first crude estimate relies on a simple idea. It divides the problem of estimating $c(n,m)$ into several smaller problems by considering the following proportions in S_n (see [9]) according to how many cycles the numbers 1, 2 and 3 lie in. Define proportions

1. $c^{(1)}(n,m)$ of those $g \in S_n$ which have $1,2,3$ in the same g-cycle.
2. $c^{(2)}(n,m)$ of those $g \in S_n$ which have $1,2,3$ in two g-cycles.
3. $c^{(3)}(n,m)$ of those $g \in S_n$ which have $1,2,3$ in three g-cycles.

Then it is clear that

$$c(n,m) = c^{(1)}(n,m) + c^{(2)}(n,m) + c^{(3)}(n,m).$$

For each i with $i \in \{1,2,3\}$, we can now hope to use the extra knowledge about the elements that contribute to the proportion $c^{(i)}(n,m)$ to obtain a first estimate for this proportion.

For example, we show how we can obtain an estimate for $c^{(1)}(n,m)$. Elements $g \in S_n$ contributing to this proportion must contain a cycle C of length d with the following properties:

1. $d \mid m$ and $3 \leq d$.
2. The cycle C of length d contains 1,2,3.
3. The remaining cycles of g all have lengths dividing m.

Now we can obtain an expression for $c^{(1)}(n,m)$ by considering all allowable cycle lengths d and counting the number of cycles C on d points that contain the points 1, 2 and 3 and ensuring that the remaining $n-d$ points all have lengths dividing m. As C has to contain 1, 2 and 3, we have $n-3$ points left to choose the remaining $d-3$ points of C; and having chosen a set of d points (which contains the points 1, 2 and 3), we have $(d-1)!$ ways of arranging them into different cycles. The number of permutations on the remaining $n-d$ points all of whose cycle lengths divide m is $c(n-d,m)(n-d)!$. Hence

$$\begin{aligned} c^{(1)}(n,m) &= \frac{1}{n!} \sum_{d \mid m, d \geq 3} \binom{n-3}{d-3} (d-1)! c(n-d,m)(n-d)! \\ &= \frac{(n-3)!}{n!} \sum_{d \mid m, 3 \leq d \leq n} (d-1)(d-2) c(n-d,m). \end{aligned}$$

As we are currently only interested in obtaining a first crude estimate, we apply a very rough upper bound on $c(n-d,m)$, by replacing it with the constant 1. We therefore find

$$\begin{aligned} c^{(1)}(n,m) &\le \frac{(n-3)!}{n!} \sum_{d|m, 3\le d\le n} (d-1)(d-2) \\ &\le \frac{(n-3)!}{n!} \sum_{m/n\le t\le m/3} (\frac{m}{t}-1)(\frac{m}{t}-2) \\ &\le \frac{(n-3)!}{n!} \left((n-1)(n-2) + \int_{m/n}^{m/3} \frac{m^2}{t^2}\, dt \right) \\ &\le \frac{(n-3)!}{n!} \{(n-1)(n-2) + mn - 3m\} \\ &< \frac{1}{n} + \frac{m}{n^2}. \end{aligned}$$

We can employ similar estimates to obtain crude upper bounds for $c^{(2)}(n,m)$ and $c^{(3)}(n,m)$, which we omit here. Having obtained a first crude estimate, we now insert this estimate when trying to get a better estimate for $c(n,m)$.

2.2.7.1 The Pull

Enumerating g by the g-cycle of length d on 1 and recalling that $n-1 \le m$ yields

$$\begin{aligned} c(n,m) &= \frac{1}{n} \sum_{\substack{d|m \\ 1\le d\le n}} c(n-d,m) \\ &\le \frac{1}{m} + \frac{1}{n} \sum_{\substack{d|m \\ 1\le d\le m/2}} c(n-d,m). \end{aligned}$$

For example, in the case where $m = n$ or $m = n-1$, inserting the crude estimate for $c(n-d,m)$ in the equations above we find that

$$\begin{aligned} c(n,m) &\le \frac{1}{m} + \frac{1}{n} \sum_{\substack{d|m \\ 1\le d\le m/2}} \left(\frac{1}{n-d} + \frac{\gamma(m)m}{(n-d)^2} \right) \\ &\le \frac{1}{m} + \frac{d(m)(2+4\gamma(m))}{n^2}, \end{aligned}$$

where $d(m)$ denotes the number of positive integer divisors of m. The above results allow us to prove the following strong corollaries.

Corollary 2.17. *Let $n \ge 19$. Let $f \in \{n-3, n-2\}$ be odd. Then*

1. *The conditional probability that a random element g has an n-cycle given that it satisfies $g^n = 1$ is at least $1/2$.*

2. *The conditional probability that a random element g has an f-cycle given that it satisfies $g^{2f} = 1$ and $|g^f| = 2$ is at least* $1/3$.

Finally, we highlight some of the results proved in [75] estimating $c(n, m)$, where $m = rn$ for a fixed value of r. The proof of this theorem relies on ideas similar to those outlined above, combined with an idea of Warlimont's [93] dividing cycles of permutations into large and small cycles.

Theorem 2.18. *For positive integers r, n with r fixed and n sufficiently large,*

$$c(n, rn) = \frac{1}{n} + \frac{a(r)}{n^2} + O\left(\frac{1}{n^{\frac{5}{2}-o(1)}}\right)$$

where $a(r) = \sum_{i,j}(1 + \frac{i+j}{2r})$, $1 \leq i, j \leq r^2$, $ij = r^2$ and $r + i, r + j$ divide rn. Moreover, the conditional probability that an element $g \in S_n$ is an n-cycle, given that its order divides rn, is at least $1 - \frac{a(r)}{n} - O\left(\frac{1}{n^{3/2-o(1)}}\right)$.

2.2.8 Algorithmic Applications of Proportions in Symmetric Groups

Warlimont's result is very useful for algorithmic purposes. It tells us that most permutations g satisfying the equation $g^n = 1$ are n-cycles. Moreover, it also identifies the cycle structure of the second most abundant set of permutations satisfying the equation $g^n = 1$; namely permutations which consist of two cycles of length $n/2$, and these only occur when n is even. This translates into the algorithm below to find an n-cycle. Note that the algorithm works in *any permutation or matrix group representation* of S_n, where we may not easily recognise the cycle structure of an element in the natural representation. Such algorithms are called *black box group algorithms*; for a formal definition, see Sect. 2.4.2.

Suppose we are given a group G and we believe G might be isomorphic to S_n under a putative, yet unknown, isomorphism $\lambda : G \to S_n$. We find an element $g \in G$ which would map to an n-cycle under λ with high probability by Algorithm 3 below.

Algorithm 3: FINDNCYCLE

Input: G a group, $n \geq 19$ an integer, $0 < \varepsilon < 1$ real;
Output: **g** or **fail;**
# If the output is **g**, then $g^n = 1$;
for *up to* $n \log(\varepsilon^{-1})$ *random elements* $g \in G$ **do**
  if $g^n = 1$ **then**
    return g;
  end
end
Return **fail**;

The algorithm takes as input a real ε such that $0 < \varepsilon < 1$, and this input is used to control the probability of failure. We require that the probability that G is isomorphic to S_n and the algorithm returns **fail** to be at most ε. Note that on each random selection, the probability of finding an n-cycle is $1/n$. Hence the probability of failing to find an n-cycle in $N(\varepsilon)$ random selections is $(1-1/n)^{N(\varepsilon)}$ and we have $(1-1/n)^{N(\varepsilon)} < \varepsilon$ when $N(\varepsilon) \geq \log(\varepsilon^{-1})/(-\log(1-1/n))$. In particular, this is the case when $N(\varepsilon) \geq n\log(\varepsilon^{-1})$.

Thus the above algorithm returns with probability at least $1-\varepsilon$ an element $g \in G$ satisfying $g^n = 1$. Therefore, if $G \cong S_n$ then with probability at least $1/2$ this element is an n-cycle, by the above corollary.

Niemeyer and Praeger [74] generalise Warlimont's result and consider the case where $m \geq n$, namely $rn \leq m < (r+1)n$ for fixed positive integers r.

Algorithm 3 is part of a procedure which decides whether a black box group G is isomorphic to the full symmetric group S_n for a given natural number n. The full algorithm is described in [9]. First, we have to describe a presentation for the group S_n.

Theorem 2.19 (Coxeter and Moser, 1957).

$$\langle r, s \mid r^n = s^2 = (rs)^{(n-1)} = [s, r^j]^2 = 1 \text{ for } 2 \leq j \leq n/2 \rangle$$

is a presentation for S_n. Moreover, if some group G has generators r, s satisfying this presentation and $r^2 \neq 1$ then G is isomorphic to S_n.

Definition 2.20. The transposition y *matches* the n-cycle x if y moves two adjacent points in x.

Lemma 2.21. *For $n \geq 5$, an n-cycle and a matching transposition satisfy the presentation in Theorem 2.19.*

Now we are ready to sketch the algorithm BBRecogniseSn of [9].

Algorithm 4: BBRecogniseSn

Input: $G = \langle X \rangle$ a black box group, $n \geq 5$;
Output: true and a map $\lambda : G \to S_n$, **or fail**;
repeat
1. find $r \in G$ with $r^n = 1$.
   # is $\lambda(r)$ an n-cycle?
2. find $h \in G$ with $h^{2m} = 1$ where $m \in \{n-2, n-3\}$ odd.
   # is $\lambda(h^m)$ a transposition?
3. find a random conjugate s of h^m with $[s, s^g] \neq 1$.
   # does $\lambda(s)$ interchange two points of $\lambda(r)$?

until *repeated too often*;
if *r or s not found* **then return fail**;
else
define λ by

- $\lambda(r) = (1, \ldots, n)$ and
- $\lambda(s) = (1, 2)$.

Return true and $\lambda : G \to S_n$;
end

We test whether $\langle r, s\rangle \cong S_n$ via the presentation described in Theorem 2.19.

Theorem 2.22. *Given a black box group G isomorphic to S_n, the probability that the algorithm* BBRecogniseSn(G, n, ε) *returns* ***fail*** *is at most ε. The cost of the algorithm is*

$$O((n\xi + n\log(n)\mu)\log(\varepsilon^{-1})),$$

where ξ is the cost of finding a random element in a black box group and μ the cost of a black box group operation.

2.2.9 Restrictions on Cycle Lengths

An extensive amount of literature exists on the topic of random permutations whose cycle lengths lie in a given set $\mathscr{L}$ or lie in a particular arithmetic progression. Early work includes that of Touchard [91], Gončarov [40] and Gruder [42].

Let $\mathscr{L}$ be a set of natural numbers. Let $d_{\mathscr{L}}(n)$ denote the proportion of elements in S_n all of whose cycle lengths lie in $\mathscr{L}$ and let $d_{\mathscr{L}}(n,k)$ denote the proportion of elements in S_n with exactly k cycles all of whose lengths lie in $\mathscr{L}$. A generating function for $d_{\mathscr{L}}(n)$ can be found in [91]. This proportion has been studied by many authors; we just mention briefly some of Gruder's results.

Theorem 2.23 (Gruder [42]).

$$d_{\mathscr{L}}(n,k) = \frac{1}{k!} \sum_{\substack{(x_1,\ldots,x_k)\in\mathscr{L}^k \\ x_1+\cdots+x_k=n}} \frac{1}{x_1\cdots x_k}.$$

Put $H(z) = \sum_{a\in\mathscr{L}} \frac{z^a}{a}$ and let $D(z) = \sum_{n=0}^{\infty} d_{\mathscr{L}}(n) z^n$.

Theorem 2.24 (Gruder [42]).

1. $D(z) = \exp(H(z))$.
2. $D(z)^x = \exp(xH(z)) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} d_{\mathscr{L}}(n,k)x^k\right) z^n$.

Bolker and Gleason [13] obtain an explicit asymptotic formula for $d_{\mathscr{L}}(n)$ when $\mathscr{L}$ is an arithmetic progression.

Let $p_a(n)$ denote the proportion of elements in S_n all of whose cycle lengths are at least a for some $a \geq 2$.

Theorem 2.25 (Gruder [42]).

1. $\lim_{n\to\infty} \frac{1}{p_a(n)} = \exp(1 + \frac{1}{2} + \cdots + \frac{1}{a-1})$.
2. $\log\left(\lim_{a\to\infty} \lim_{n\to\infty} \frac{1}{p_a(n)}\right) = \gamma$, *where* $\gamma = \lim_{n\to\infty}\left(\sum_{i=1}^{n} \frac{1}{i} - \log(n)\right)$ *is the Euler constant.*

V.F. Kolchin summarises many of the asymptotic results known about this case in his book [50]. We refer the interested reader to [50] and references therein.

Finally, we mention one particular proportion that has been of considerable interest in various applications. For positive integers b, let $p_{\neg b}(n)$ denote the proportion of elements in S_n with no cycle of length divisible by b. This proportion was first studied for primes b in [28], where Erdős and Turán give an explicit formula for it. This formula immediately generalises to arbitrary positive integers b. For a prime b, Erdős and Turán also give the limiting distribution of $p_{\neg b}(n)$. Many other authors have also considered this proportion; for example [12], [14, Sect. 2], [38]. Here we quote a result from [8, Theorem 2.3(b)].

Theorem 2.26. *Let $n \geq b$. Then*

$$\left(\frac{b}{n}\right)^{1/b} \frac{(1-\frac{1}{n})}{\Gamma(1-\frac{1}{b})} \leq p_{\neg b}(n) \leq \left(\frac{b}{n}\right)^{1/b} \frac{(1+\frac{2}{n})}{\Gamma(1-\frac{1}{b})}.$$

Ben-Ezra [10] obtained a similar result for $b = 2$. A formula for the proportion of elements in A_n with no cycle of length divisible by b is also given in [8]. Maróti [61] generalises this, and gives a formula for the proportion of elements of order not divisible by b in arbitrary permutation groups.

The above estimates have proved to be very useful in deriving proportions of certain elements in finite classical groups of Lie type. Suppose G is a finite classical group of Lie type given in natural dimension n with $n \geq 2$. Using the method outlined in Sect. 2.3.4, [58] shows that the proportion of elements in G for which some power is an involution with a large 1-eigenspace of dimension d with $n/3 \leq d \leq 2n/3$ is at least $c/\log(n)$ for some constant c.

2.3 Estimation Techniques in Lie Type Groups

We start with a seemingly simple result about permutation groups, discuss the deep Lie-theoretic analysis underpinning it, and indicate how this approach has led to a powerful estimation technique for Lie type groups.

2.3.1 p-Singular Elements in Permutation Groups

The following beautiful and surprising result of Isaacs et al. [46] was published in 1995.

Theorem 2.27 (Isaacs, Kantor and Spaltenstein [46]). *Let $G \leq S_n$ and let p be a prime dividing $|G|$. Then there is at least 1 chance in n that a uniformly distributed random permutation in G has order a multiple of p.*

This result is about *any permutation group*—not necessarily primitive, nor even transitive. It is best possible for such a general result, since if $n = p$ then in the

affine group AGL(1, p) there are exactly $p-1$ elements of order divisible by p out of a total of $p(p-1)$ elements in the group.

The only known proof of Theorem 2.27 requires the finite simple group classification. The proof strategy is first to make an elementary reduction to the case where G is a nonabelian simple group. Then the simple groups are dealt with. There are no difficulties with the alternating groups A_n and the sporadic simple groups. This leaves the finite simple groups of Lie type to be considered, and this is where the authors of [46] "wave a magic wand" with a sophisticated argument from the theory of Lie type groups. We (Niemeyer and Praeger) were at first baffled by this proof, as well as fascinated by what it achieved, so set about trying to understand it. Along the way there was help from Klaus Lux and Frank Lübeck. With Frank Lübeck we made our first full-blown application of the theory in [58] to estimate the proportion of a certain family of even ordered elements in classical groups. We discovered that this beautiful theory had been introduced by Gus Lehrer [54,55] to count various element classes and representation theoretic objects associated with Lie type groups. Recently Arjeh Cohen and Scott Murray [22] also used this approach to develop algorithms for computing with finite Lie algebras.

Our objective became: to formalise the ideas into a framework for estimating proportions of a wide class of subsets of finite Lie type groups. The framework was first set out in [58] and in general in [76]. We describe it in the next subsection.

2.3.2 *Quokka Subsets of Finite Groups*

For a finite group G and a prime p dividing $|G|$, each group element g can be written uniquely as a commuting product $g = us = su$, where u is a p-element and s is a p'-element (that is, ord(u) is a power of p while ord(s) is coprime to p). This is called the *Jordan p-decomposition* of g.

To find this decomposition write $\mathrm{ord}(g) = p^a b$ where $p \nmid b$ and $a \geq 0$. Then since p^a and b are coprime, there are integers r, t such that $rp^a + tb = 1$. It is straightforward to check that the elements $u = g^{tb}$ and $s = g^{rp^a}$ have the required properties, and that u, s are independent of the choices for r, t. This decomposition is critical for defining the kinds of subsets amenable to this approach for estimation.

Definition 2.28. Let G be a finite group and p a prime dividing $|G|$. A non-empty subset Q of G is called a *quokka set*, or a *p-quokka set* if we wish to emphasise the prime p, if the following two properties hold:

(a) Q is closed under conjugation by elements of G.
(b) For $g \in G$ with Jordan p-decomposition $g = us = su$, $g \in Q$ if and only if $s \in Q$.

A natural place to find p-quokka sets is in finite Lie type groups in characteristic p; for example, in $G = \mathrm{GL}(n,q)$ with q a power of p. Here, in a Jordan p-decomposition $g = us = su$, the element u is unipotent and s is semisimple. The elements u, s are called the *unipotent part* and the *semisimple part* of g, respectively. Some of the subsets already discussed in this chapter turn out to be quokka sets. We give an example.

Example 2.29. Let $G = \mathrm{GL}(n,q)$ or $\mathrm{SL}(n,q)$, with q a power of p, let e be an integer such that $e > n/2$, and suppose that $q^e - 1$ has a primitive prime divisor. Then the subset Q of ppd-$(n,q;e)$ elements of G is a p-quokka set. To see this, note that Q is closed under conjugation since conjugate elements have the same order. Also, for a Jordan p-decomposition $g = us = su$, a ppd r of $q^e - 1$ divides $\mathrm{ord}(g)$ if and only if r divides $\mathrm{ord}(s)$.

2.3.3 Estimation Theory for Quokka Sets

The standard reference for the concepts discussed below is Roger Carter's book [17], and an account of the required theory is given in [76].

The groups: We start with a connected reductive algebraic group G defined over the algebraic closure $\overline{\mathbb{F}_q}$ of the finite field $\mathbb{F}_q$ of order q, where q is a power of a prime q_0. A Frobenius morphism $F : G \to G$ defines a finite group of Lie type $G^F = \{g \in G \mid F(g) = g\}$ as its fixed point subgroup. We use the following example to illustrate the concepts as they arise. For the algebraic group $G = \mathrm{SL}(n, \overline{\mathbb{F}_q})$ and Frobenius morphism $F : (a_{ij}) \mapsto (a_{ij}^q)$, the finite group of Lie type is $G^F = \mathrm{SL}(n,q)$, since the fixed field of the map $a \mapsto a^q$ is $\mathbb{F}_q$.

Maximal tori: A *torus* in an algebraic group is a subgroup T that is isomorphic to a direct product of a finite number of copies of the multiplicative group of $\overline{\mathbb{F}_q}$. In particular, T is abelian. A torus T is F-stable if $F(T) = T$, and T is a maximal torus if T is closed and not properly contained in another torus. All F-stable maximal tori in G are conjugate. In our example $G = \mathrm{SL}(n, \overline{\mathbb{F}_q})$, the subgroup T_0 of diagonal matrices in G is a maximal torus that is isomorphic to a direct product of $n-1$ copies of $(\overline{\mathbb{F}_q})^*$.

The Weyl group: Choose an F-stable maximal torus T_0 in G. The *Weyl group* W is defined as the quotient $N_G(T_0)/T_0$. Since F-stable maximal tori are conjugate, the group W is independent of the choice of T_0. In our example $G = \mathrm{SL}(n, \overline{\mathbb{F}_q})$, with T_0 the subgroup of diagonal matrices, $N_G(T_0)$ is the subgroup of monomial matrices in G, and $W = N_G(T_0)/T_0$ is isomorphic to the group of $n \times n$ permutation matrices, so $W \cong S_n$.

F-conjugacy: Elements $v, w \in W$ are said to be *F-conjugate* if there is an element $x \in W$ such that $v = x^{-1} w F(x)$. Notice that we abuse notation a little in this definition, since $x \in W$ is a coset $x = x_0 T_0$ and by $F(x)$ we mean $F(x_0)T_0$

(which is well defined since T_0 is F-stable). In our example $G = \mathrm{SL}(n, \overline{\mathbb{F}_q})$, F-conjugation is ordinary conjugation (since each $x \in W$ has a representative monomial matrix with entries 0 or ± 1, and hence x is fixed by F).

A crucial correspondence and the Quokka Theorem: For an F-stable maximal torus T of G, the intersection $T^F = T \cap G^F = \{g \in T \mid F(g) = g\}$ is called a *maximal torus* of G^F; although all F-stable maximal tori of G are G-conjugate, there are usually several G^F-conjugacy classes of F-stable maximal tori T^F, and the structure of the T^F is governed by the Weyl group. *There is a 1–1 correspondence between G^F-conjugacy classes of F-stable maximal tori and F-conjugacy classes of the Weyl group.* This is a crucial ingredient in proving the main theorem below. Let $\mathscr{C}$ be the set of F-conjugacy classes in W, and for $C \in \mathscr{C}$, let T_C^F denote a representative F-stable maximal torus of G^F corresponding to C.

Theorem 2.30. *Let G, F, T_0, W and $\mathscr{C}$ be as above, and let $Q \subset G^F$ be a quokka set. Then*

$$\frac{|Q|}{|G^F|} = \sum_{C \in \mathscr{C}} \frac{|C|}{|W|} \cdot \frac{|T_C^F \cap Q|}{|T_C^F|}.$$

Bounds on proportions: Essentially Theorem 2.30 allows us to separate an estimation problem within a Lie type group G^F into two simpler problems, one within the Weyl group and the other within various maximal tori. The expression for $\frac{|Q|}{|G^F|}$ in Theorem 2.30 as an exact summation can lead to usable bounds. Suppose that $\hat{\mathscr{C}}$ is a union of F-conjugacy classes and that ℓ_Q is a positive constant such that $\frac{|T_C^F \cap Q|}{|T_C^F|} \geq \ell_Q$ for all $C \in \hat{\mathscr{C}}$. Then Theorem 2.30 implies that $\frac{|Q|}{|G^F|} \geq \ell_Q \frac{|\hat{\mathscr{C}}|}{|W|}$. Similarly, if u_Q is such that $\frac{|T_C^F \cap Q|}{|T_C^F|} \leq u_Q$ for all $C \in \hat{\mathscr{C}}$, then $\frac{|Q|}{|G^F|} \leq u_Q \frac{|\hat{\mathscr{C}}|}{|W|}$.

A worked example: Let $G = \mathrm{SL}(n, \overline{\mathbb{F}_q})$ and let Q be the quokka set of ppd$(n, q; e)$ elements of G, for some $e \in (n/2, n)$—see Example 2.29. We use this "quokka theory" to re-derive Lemma 2.3. The Weyl group is $W \cong S_n$, and each maximal torus T_C^F containing an element of Q is of the form

$$T_C^F = Z_{q^e-1} \times \text{ other cyclic factors.} \tag{2.1}$$

As we discussed in the last paragraph of the proof of Lemma 2.3, for each such torus, the proportion $\frac{|T_C^F \cap Q|}{|T_C^F|}$ lies between $1 - \frac{1}{e+1}$ and 1. The F-conjugacy class C in W corresponding to such a torus consists of certain elements of $W = S_n$ containing an e-cycle, and all classes C with this property correspond to tori T_C^F as in (2.29). Let $\hat{\mathscr{C}}$ be the subset of W of all elements containing an e-cycle. Then $|\hat{\mathscr{C}}|/|W| = 1/e$, and as we discussed above, $|Q|/|G^F|$ lies between $(1 - \frac{1}{e+1})\frac{1}{e} = \frac{1}{e+1}$ and $\frac{1}{e}$.

r-abundant elements: The original impetus to study the work of Isaacs et al. [46] so closely came from efforts of Niemeyer and Praeger to understand whether, for a prime r, the lower bound given in [46] for the proportion of r-singular elements in

finite classical groups was close to the true proportion. (An *r-singular element* is one with order a multiple of r.) Niemeyer conducted a computer experiment on general linear groups $G = \mathrm{GL}(n, p^a)$, for various dimensions n and primes p and r, where r divides $|G|$ and $r \neq p$, to discover the kinds of r-singular elements in G which appeared frequently on repeated independent random selections from G. It turned out that a good proportion of the r-singular elements that we found left invariant, and acted irreducibly on, a subspace of dimension greater than $n/2$. Moreover, their frequency seemed to be roughly proportional to $1/e$, where e is the smallest positive integer such that r divides $p^{ae} - 1$. We decided to call these elements *r-abundant*. It seemed at first that the r-abundant elements alone occurred with frequency greater than the lower bound predicted in [46]. However, it was pointed out to us by Klaus Lux that, hidden in the proofs in [46] was a lower bound on the proportion of r-singular elements of the form c/e for some constant c, with e as above. If $e > n/2$ then these r-singular elements are the ppd-$(n, p^a; e)$ elements used in the classical recognition algorithm in [72], and in general r-abundant elements are as easily recognisable as ppd elements from properties of their characteristic polynomials: namely, there is an irreducible factor $f(x)$ of degree greater than $n/2$ and a multiple of e, such that x has order a multiple of r modulo $f(x)$ in the polynomial ring $\mathbb{F}_{p^a}[x]$. A detailed study of r-abundant elements was carried out by Niemeyer and Praeger with Tomasz Popiel [71] to prove that the experimentally observed proportion of r-singular elements in general linear groups is correct, and to find and prove analogues for other finite classical groups. The r-abundant elements form a quokka set, and their proportion was determined [71, Theorem 1.1] using Theorem 2.30. For the general linear group $\mathrm{GL}(n, p^a)$, the proportion is

$$\left(1 - \frac{1}{r^{t-1}(r+1)}\right) \cdot \frac{\ln(2)}{e}$$

with an error term of the form c/n for some constant c, where r^t is the largest power of r dividing $p^{ae} - 1$. It would be interesting to know if r-abundant elements could be useful algorithmically to identify classical groups. To aid our understanding of such elements, Sabina Pannek is undertaking a Ph.D. project to find which maximal subgroups of finite classical groups contain elements with an irreducible invariant subspace of the natural module of more than half the dimension.

2.3.4 Strong Involutions in Classical Groups

In [53], Leedham-Green and O'Brien introduced a new Las Vegas algorithm to find standard generators for a finite simple n-dimensional classical group H in odd characteristic in its natural action. (Recall that a randomised algorithm is called *Las Vegas* if the output, if it exists, is always correct; the algorithm may report failure with a small probability.) The algorithm of [53] proceeds by constructing recursively various centralisers of involutions (elements of order 2), the details of

Table 2.1 The classical groups for Theorem 2.31 and Corollary 2.32

S	X	n
$\mathrm{SL}(\ell+1,q)$	$\mathrm{GL}(\ell+1,q)$	$\ell+1$
$\mathrm{SU}(\ell+1,q)$	$\mathrm{GU}(\ell+1,q)$	$\ell+1$
$\mathrm{Sp}(2\ell,q)$	$\mathrm{GSp}(2\ell,q)$	2ℓ
$\mathrm{SO}(2\ell+1,q)$	$\mathrm{GO}(2\ell+1,q)$	$2\ell+1$
$\mathrm{SO}^{\pm}(2\ell,q)$	$\mathrm{GO}^{\pm}(2\ell,q)^0$	2ℓ

which are discussed further in Sect. 2.4.3. The issue we address here is how to find an appropriate involution. Leedham-Green and O'Brien wished to work with an involution whose centraliser would be essentially a product of two smaller classical groups, each of roughly half the dimension. They called such involutions "strong": an involution is *strong* if its fixed point subspace has dimension in $[n/3, 2n/3)$, or equivalently if its -1-eigenspace has dimension in $(n/3, 2n/3]$. Let I denote the subset of strong involutions in H. Leedham-Green and O'Brien constructed elements of I by making independent, uniformly distributed random selections from H to find an element of even order which powered up to a strong involution. We call such elements *preinvolutions*. To estimate how readily a preinvolution can be found by random selection, we need to estimate the size of the set

$$\mathrm{P}(H, I) = \{h \in H \mid \mathrm{ord}(h) \text{ is even}, h^{\mathrm{ord}(h)/2} \in I\}. \tag{2.2}$$

Leedham-Green and O'Brien estimated that it would require $O(n\xi + n^4 \log n + n^4 \log q)$ elementary field operations (that is, additions, multiplications or inversions) to compute a strong involution in H, where ξ is an upper bound on the number of elementary field operations required to produce an independent, uniformly distributed random element of H; see [53, Theorem 8.27]. Underpinning this complexity estimate was their estimate that the proportion of preinvolutions in H was at least c/n, for a constant c.

Niemeyer and Praeger, with Frank Lübeck, used the approach described in Sect. 2.3.3 to obtain an improved estimate for this proportion [58, Theorem 1.1]. They considered any n-dimensional classical group H satisfying $S \leq H \leq X$, where S, X, n are as in one of the lines of Table 2.1 with q odd. Here $\mathrm{GO}^{\pm}(2\ell,q)^0$ denotes the connected general orthogonal group—the index 2 subgroup of $\mathrm{GO}^{\pm}(2\ell,q)$ that does not interchange the two $\mathrm{SO}^{\pm}(2\ell,q)$-classes of maximal isotropic subspaces.

Theorem 2.31. *Let H satisfy $S \leq H \leq X$, with S, X, n as in one of the lines of Table 2.1, with q odd and $\ell \geq 2$, and let $I \subset H$ be the set of strong involutions. Then*

$$\frac{|\mathrm{P}(H,I)|}{|H|} \geq \frac{1}{5000 \log_2(\ell)}.$$

The weak constant of $1/5000$ arises from the fact that the estimation only considered one class of elements that power up to a strong involution, and from the fact that it determined one constant that is valid uniformly for all classical groups.

A more detailed analysis taking into account a wider family of preinvolutions would yield a larger value for the constant.

Lübeck, Niemeyer and Praeger also obtained similar lower bounds for projective groups: note that, for $Z_0 \leq Z(X)$, since the subset I of involutions in Theorem 2.31 contains no central elements, the set $\overline{I} := IZ_0/Z_0$ is a subset of involutions in the projective group $\overline{H} := HZ_0/Z_0$.

Corollary 2.32. *With the above notation,* $|\mathrm{P}(\overline{H}, \overline{I})|/|\overline{H}| \geq 1/(5000 \log_2 \ell)$.

Using this new lower bound reduces the complexity of computing a strong involution in [53] to $O(\log(n)\xi + n^4 \log n + n^4 \log q)$; that is, replacing the first summand $n\xi$ by $\log(n)\xi$. It seems to be typical that whenever "quokka theory" is applicable, it produces superior estimates to more intuitive geometric methods.

In Sect. 2.4.3, the algorithm in [53] will be discussed further. Here we just mention that the proof of [58, Theorem 1.1] could have been given for a more general class of involutions called "balanced involutions". For constants α, β such that $0 < \alpha < 1/2 < \beta < 1$, an (α, β)-*balanced involution* in an n-dimensional classical group H is one with fixed point subspace having dimension in $[\alpha n, \beta n)$. The resulting lower bound on the proportion of (α, β)-balanced involutions in H would be $c/\log_2(n)$, for a constant c depending only on α and β.

2.3.5 More Comments on Strong Involutions

Before leaving this topic we make some comments about the proof of Theorem 2.31. First, it is not difficult to see that $\mathrm{P}(H, I)$ is a quokka set: it is non-empty since $I \neq \emptyset$; it is conjugacy closed since I is a union of H-conjugacy classes; and finally, since q is odd, if $g = us = su$ is the Jordan p-decomposition then $g^{\mathrm{ord}(g)/2} = s^{\mathrm{ord}(s)/2}$, and hence $g \in \mathrm{P}(H, I)$ if and only if $s \in \mathrm{P}(H, I)$.

To obtain the lower bound in Theorem 2.31 we used Theorem 2.30. A special subset $\mathscr{C}_0$ of F-conjugacy classes of W was examined, for which it was possible both to estimate $w_0 := |\cup_{C \in \mathscr{C}_0} C|/|W|$ and to find a good positive lower bound on $|T_C^F \cap \mathrm{P}(H, I)|$ for each $C \in \mathscr{C}_0$. To give an understanding of this subset of W, while avoiding the technicalities associated with small dimensions and the other types of classical groups, we confine our attention to $H = \mathrm{GL}(n, q)$ with $n \geq 7$. Here $\mathscr{C}_0$ is a set of conjugacy classes in $W = S_n$. We choose a particular positive integer a as follows, and take $W_0 := \cup_{C \in \mathscr{C}_0} C$ to consist of all permutations with a single cycle of length $2^a k \in (n/3, 2n/3]$, for some integer k, and no other cycle of length divisible by 2^a. For $a_0 = \log_2 \ln 2 + \log_2 \log_2 n$, we take a to be the integer in the interval $[a_0 - 1/2, a_0 + 1/2)$. We note for later use that, since $n \geq 7$, we have $a \geq 1$ and $(13/4) \cdot 2^a \leq n$.

First we show that $|T_C^F \cap \mathrm{P}(H, I)|/|T_C^F| \geq 1/2$, for $C \in \mathscr{C}_0$ with a cycle of length $2^a k$ as above. Each torus T_C^F in the H-conjugacy class of tori corresponding to C is of the form $Z \times A$, where Z is cyclic of order $q^{2^a k} - 1$ leaving invariant a subspace U of dimension $2^a k$ and acting as a Singer cycle on U, and for each $x \in A$, the 2-part of $\mathrm{ord}(x)$ (that is, the highest power of 2 dividing $\mathrm{ord}(x)$) is

strictly less than the 2-part of $q^{2^a k} - 1$. Now half of the elements $z \in Z$ are such that the 2-part of ord(z) is equal to the 2-part of $q^{2^a k} - 1$, and for each such z, and any $x \in A$, the element zx has even order, and $(zx)^{|zx|/2}$ is the unique involution z_0 in Z. The element z_0 acts as $-I$ on the subspace U and has fixed point subspace of dimension $n - 2^a k \in [n/3, 2n/3)$; that is to say, z_0 is a strong involution and $zx \in \mathrm{P}(H, I)$. Thus $|T_C^F \cap \mathrm{P}(H, I)|/|T_C^F| \geq 1/2$.

Theorem 2.30 now implies that

$$\frac{|\mathrm{P}(H, I)|}{|H|} \geq \frac{1}{2} \cdot \frac{|W_0|}{|W|},$$

so it remains to estimate the size of W_0. A straightforward counting argument yields

$$\frac{|W_0|}{|W|} = \sum_k \frac{p_{\neg 2^a}(n - 2^a k)}{2^a k}, \tag{2.3}$$

where the sum is over integers k such that $n/3 < 2^a k \leq 2n/3$, and $p_{\neg 2^a}(n - 2^a k)$ is the proportion of elements in $S_{n-2^a k}$ with no cycle of length divisible by 2^a. By Lemma 4.2(a) of [58], which is based on Theorem 2.26,

$$p_{\neg 2^a}(n - 2^a k) > \frac{1}{4}(n - 2^a k)^{-1/2^a} > \frac{1}{4} n^{-1/2^a}.$$

Thus each summand in (2.3) is at least $3/(8n^{1+1/2^a})$ since $2^a k \leq 2n/3$. The number of summands in (2.3) is at least $(2n/3 - n/3)/2^a - 1 = n/(3 \cdot 2^a) - 1$, which is at least $n/(39 \cdot 2^a)$ (since $(13/4) \cdot 2^a \leq n$). Hence

$$\frac{|\mathrm{P}(H, I)|}{|H|} \geq \frac{1}{2} \cdot \frac{|W_0|}{|W|} \geq \frac{1}{2} \cdot \frac{n}{39 \cdot 2^a} \cdot \frac{3}{8n^{1+1/2^a}} = \frac{1}{208} \cdot \frac{1}{2^a \cdot n^{1/2^a}},$$

which is greater than $\frac{1}{208} \frac{1}{3 \log_2(n)} = \frac{1}{624 \log_2(n)}$. This proves Theorem 2.31 for $H = \mathrm{GL}(n, q)$.

The family W_0 of elements of the Weyl group W gives a far better lower bound than bounds obtained by geometric arguments. However we have not considered all conjugacy classes in W, and indeed it seems that, for this problem, application of "quokka theory" does not yield an upper bound. It is reasonable to ask how good the lower bound of Theorem 2.31 is. To attempt to answer this question, we quote a few sentences from [58, p. 3399].

> We did some numerical experiments for small $q \in \{3, 5, 9, 13\}$ and groups from the theorem up to dimension 1000. We computed many pseudo-random elements and checked if they powered up to an involution with a fixed point space of dimension in the right range. The proportion of these elements is not a monotonic function in the dimension, but the trend was that the proportion was about 25% for small dimensions and went down to about 15% in dimension 1000 (independently of the type of the group and q). Further, statistical tests on the data from the groups H we sampled strongly indicates that $P(H, I)/|H| = O(1/\log(\ell))$. This seems to suggest at least that we cannot expect that there is a lower bound independent of the rank of the group.

2.3.6 Regular Semisimple Elements and Generating Functions

Let H be an n-dimensional classical group in odd characteristic, as in one of the lines of Table 2.1. The methods described in Sect. 2.3.4 show how to find a strong involution efficiently, or more generally, how to find an (α, β)-balanced involution z. The problem of constructing the centraliser $C_H(z)$ of such an involution will be discussed in Sect. 2.4. In this section we explore an estimation problem connected with part of the construction. An essential component in finding $C_H(z)$ is to take random conjugates z^g to find a "nice product" $y := zz^g$, where "nice" means "close to regular semisimple". This procedure is discussed in the seminal paper [78] by Christopher Parker and Rob Wilson. They estimate that $O(n)$ random products will produce a nice product with high probability. The approach taken by Praeger and Seress [86], and described in this section, shows that only $O(\log n)$ random products are required.

Written in an appropriate basis, the product $y = zz^g$ of an involution z and a random conjugate z^g of z has the following form, where y_0 has no ± 1-eigenvectors:

$$y := zz^g = \begin{pmatrix} I_r & 0 & 0 \\ 0 & y_0 & 0 \\ 0 & 0 & -I_s \end{pmatrix}.$$

Typically, the dimension r is close to $2m - n$, where m is the maximum of the dimensions of the ± 1-eigenspaces of z, and s is close to 0. The question arises: what kind of matrix do we expect for y_0 "typically"? Let us restrict attention to the simplest case where $H = \mathrm{GL}(n, q)$ with q odd. By considering the results of computer experiments on various (α, β)-balanced involutions and their random conjugates for various n and odd q, we discovered that often y_0 is "regular semisimple". *For the following discussion, let us assume that* $y = y_0$.

An element y of $\mathrm{GL}(n, q)$ is called *semisimple* if is diagonalisable over some extension field of $\mathbb{F}_q$ (see [17, p. 11]), and this is equivalent to its minimal polynomial $m_y(t)$ being multiplicity free. Also y is called *regular* if its centraliser in the corresponding general linear group over the algebraic closure of $\mathbb{F}_q$ has minimal possible dimension, namely n (see [17, p. 29]). It turns out that an element y of a general linear group is regular if and only if $m_y(t) = c_y(t)$, where $c_y(t)$ denotes the characteristic polynomial of y. These two conditions for elements of finite classical groups are discussed and compared in [69, Note 8.1]. The *regular semisimple elements* are those which are both regular and semisimple. In fact, for elements y of $H = \mathrm{GL}(n, q)$, y is regular semisimple if and only if the characteristic polynomial $c_y(t)$ for its action on $V(n, q)$ satisfies

$$c_y(t) = \text{a product of pairwise distinct irreducible polynomials.}$$

Looking into the analysis of this situation in the paper [78], it is clear that Parker and Wilson recognised that regular semisimple elements y occur frequently. Moreover,

the proportion of regular semisimple elements in the full n-dimensional matrix algebra was estimated by Neumann and Praeger [70]. The main result of [86] (cf. Theorem 2.34) is a strengthening of the estimates in [70, 78].

The characteristic polynomial $c_y(t)$ has two special properties: firstly, when $y = y_0$ the element y has no ± 1-eigenvectors, so $c_y(t)$ is not divisible by $t \pm 1$. Secondly, since $y^z = z^{-1}(zz^g)z = z^g z = y^{-1}$, the characteristic polynomials of y and y^{-1} are equal. Now $c_{y^{-1}}(t) = c_y^*(t)$ is the conjugate polynomial of $c_y(t)$ where, for an arbitrary polynomial $f(t)$ with $f(0) \neq 0$, its conjugate polynomial is $f^*(t) := f(0)^{-1} t^{\deg f} f(t^{-1})$. Thus $c_y(t) = c_y^*(t)$ is self-conjugate. We have seen that conjugation by z inverts y, and similarly conjugation by z^g inverts y. Inverting a regular semisimple matrix pins down the conjugacy class of the involution z, as shown in [86, Lemma 3.1]. For n even and q odd, let $\mathscr{C} \subseteq \mathrm{GL}(n,q)$ denote the the conjugacy class of involutions with fixed point space of dimension $n/2$.

Lemma 2.33. *Let $z, y \in \mathrm{GL}(n,q)$ with q odd, such that y is regular semisimple with characteristic polynomial $c_y(t)$ coprime to $t^2 - 1$, and z is an involution inverting y. Then n is even, $z \in \mathscr{C}$, and zy is also an involution which inverts y.*

By Lemma 2.33, we have a bijection $(z', z) \mapsto (y, z)$ between the sets

$$X = \left\{ (z, z') \in \mathscr{C} \times \mathscr{C} \;\middle|\; \begin{array}{l} y := zz' \text{ regular semisimple} \\ \text{with } c_y(t) \text{ coprime to } t^2 - 1 \end{array} \right\}$$

and

$$Y = \left\{ (y, z) \;\middle|\; \begin{array}{l} y, z \in \mathrm{GL}(n,q), z^2 = 1, y^z = y^{-1} \\ y \text{ regular semisimple, and} \\ c_y(t) \text{ coprime to } t^2 - 1 \end{array} \right\}.$$

The set X is relevant for algorithmic purposes, while the set Y is more amenable to estimation techniques. For the algorithm, we are given (that is to say, we have already found) the involution $z \in \mathscr{C}$, and we want to know the proportion of $z' \in \mathscr{C}$ such that $(z, z') \in X$. This is

$$\frac{|\{z' \in \mathscr{C} \mid (z, z') \in X\}|}{|\mathscr{C}|} = \frac{|X|}{|\mathscr{C}|^2} = \frac{|Y|}{|\mathscr{C}|^2} = \frac{|\mathrm{GL}(n,q)|}{|\mathscr{C}|^2} \cdot \frac{|Y|}{|\mathrm{GL}(n,q)|}$$

and the first factor on the right of the equality, namely $\frac{|\mathrm{GL}(n,q)|}{|\mathscr{C}|^2} = \frac{|\mathrm{GL}(n/2,q)|^4}{|\mathrm{GL}(n,q)|}$, lies between $(1 - q^{-1})^7$ and $(1 - q^{-1})^2$. Thus the essential problem is to estimate

$$ss(n,q) := \frac{|Y|}{|\mathrm{GL}(n,q)|}.$$

Parker and Wilson [78] give a heuristic that estimates this quantity as being at least c/n if we require in addition that y has odd order. Our approach gives a surprisingly precise answer; see [86, Theorem 1.2]. Since n is even we consider $ss(2d, q)$.

Theorem 2.34. *For a fixed odd prime power q, the limit of $ss(2d,q)$ as $d \to \infty$ exists and*

$$ss(\infty,q) := \lim_{d\to\infty} ss(2d,q) = (1-q^{-1})^2.$$

Moreover $|ss(2d,q) - ss(\infty,q)| = o(q_0^{-d})$ for any q_0 such that $1 < q_0 < \sqrt{q}$.

Corollary 2.35. *There exists $c > 0$ with the property that for any $z \in \mathscr{C}$ the proportion of $z' \in \mathscr{C}$ such that $(z,z') \in X$ is bounded below by c.*

We use generating functions discussed in Sect. 2.2.5 to study the quantities $ss(2d,q)$. We define

$$S(u) = \sum_{d=0}^{\infty} ss(2d,q)u^d \quad \text{where} \quad ss(0,q) = 1.$$

Since y is regular semisimple, $c_y(t)$ is multiplicity-free, and since y is inverted by the involution z, we have a factorisation

$$c_y(t) = \left(\prod_{i=1}^{r} f_i(t)\right) \times \left(\prod_{j=1}^{s} g_j(t)g_j^*(t)\right) \tag{2.4}$$

where each $f_i = f_i^*$ has even degree, and each $g_j \neq g_j^*$, with the f_i, g_j, g_j^* pairwise distinct monic irreducibles. We use this decomposition to find in [86, Lemma 3.2] that the number of pairs $(y',z) \in Y$ such that y' has characteristic polynomial $c_y(t)$ is equal to

$$\frac{|\operatorname{GL}(2d,q)|}{\left(\prod_{i=1}^{r}(q^{\frac{1}{2}\deg f_i}-1)\right)\left(\prod_{j=1}^{s}(q^{\deg g_j}-1)\right)}.$$

Summing over all possible $c_y(t)$ gives an expression for $ss(2d,q)|\operatorname{GL}(2d,q)|$. Comparing the expression we obtain for $ss(2d,q)$ by this process with the coefficient of u^d in the infinite product

$$\prod_{f=f^*,\ \text{irred.}} \left(1 + \frac{u^{\frac{1}{2}\deg f}}{q^{\frac{1}{2}\deg f}-1}\right) \times \prod_{\{g,g^*\},\, g\neq g^*,\ \text{irred.}} \left(1 + \frac{u^{\deg g}}{q^{\deg g}-1}\right),$$

we see that the two expressions are the same. Hence $S(u)$ is equal to this infinite product. The contribution to the infinite product from each irreducible polynomial f or conjugate pair $\{g,g^*\}$ of non-self-conjugate polynomials depends only on the degrees of the polynomials. Thus

$$S(u) = \prod_{m\geq 1}\left(1 + \frac{u^m}{q^m-1}\right)^{N^*(q;2m)} \times \prod_{m\geq 1}\left(1 + \frac{u^m}{q^m-1}\right)^{M^*(q;m)} \tag{2.5}$$

where the exponents are

$$\begin{aligned} N^*(q;m) &= \#\,\text{monic irreducible self-conjugate polynomials over} \\ &\quad\ \mathbb{F}_q \text{ of degree } m. \\ M^*(q;m) &= \#\ \text{(unordered) conjugate pairs of monic irreducible} \\ &\quad\ \text{non-self-conjugate polynomials over } \mathbb{F}_q \text{ of degree } m. \end{aligned}$$

It turned out that a somewhat similar infinite product arose when Praeger was studying separable matrices in finite unitary groups with Jason Fulman and Peter Neumann in [36]. A similar analysis to that given in [36] for these matrices yielded:

1. $S(u)$ is analytic for $|u| < 1$ with a simple pole at $u = 1$.
2. $S(u) = (1-u)^{-1}H(u)$, with $H(u)$ analytic for $|u| < \sqrt{q}$.

Completing the analysis we found the asymptotic behaviour of the $ss(2d, q)$, as in Theorem 2.34.

2.4 Computing Centralisers of Involutions

The results in the previous section play a significant role in the analysis of algorithms to compute centralisers of involutions. In general the problem of computing centralisers is of great importance in theoretical computer science and in group theory. In computer science, the main interest stems from the connection with the *graph isomorphism problem*.

Problem 2.36. *(ISO)* Given: graphs $\Gamma_1(V_1, E_1)$ and $\Gamma_2(V_2, E_2)$.
Find: an edge-preserving bijection between V_1 and V_2, or prove that no such bijection exists.

ISO is polynomial-time reducible to the following computational problems with permutation groups.

Problem 2.37. *(STAB)* Given: a permutation group $G \leq \mathrm{Sym}(\Omega)$ and a subset $\Delta \subseteq \Omega$.
Find: the set stabiliser $\mathrm{Stab}_G(\Delta) = \{g \in G \mid \Delta^g = \Delta\}$.

Problem 2.38. *(INT)* Given: permutation groups $G, H \leq \mathrm{Sym}(\Omega)$.
Find: the intersection $G \cap H$.

Problem 2.39. *(CENT)* Given: permutation groups $G, H \leq \mathrm{Sym}(\Omega)$.
Find: the centraliser $C_G(H) = \{g \in G \mid h^g = h \text{ for all } h \in H\}$.

Problems 2.37–2.39 are in the same class of the complexity hierarchy, which means that they can be reduced to each other in time polynomial in the input length [59].

The reduction of ISO is easiest to STAB or INT. First, we notice that $\Gamma_1(V_1, E_1)$ and $\Gamma_2(V_2, E_2)$ are isomorphic if and only if $\Gamma_1 \cup \Gamma_2$ (disjoint copies of Γ_1 and Γ_2) has an automorphism that exchanges V_1 and V_2. Therefore, it is enough to compute automorphism groups of graphs. Given a graph $\Gamma(V, E)$, define Ω as the set of unordered pairs in V. Then E corresponds to a subset $\Delta \subseteq \Omega$, and $\mathrm{Sym}(V)$ acts as a group G on Ω. We can compute $\mathrm{Aut}(\Gamma)$ as $\mathrm{Aut}(\Gamma) = \mathrm{Stab}_G(\Delta)$ or $\mathrm{Aut}(\Gamma) = G \cap (\mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Omega \setminus \Delta))$.

Although, using backtrack methods (see e.g. [87, Chap. 9]), ISO and CENT are usually easy to solve in practice, no polynomial-time solution is known for Problems 2.36–2.39. Special cases with polynomial-time solutions are of great theoretical and practical interest.

In group theory, the most important case of centraliser computations is to construct *centralisers of involutions*. On the theoretical side, a major tool in the study and classification of finite simple groups is the investigation of their involution centralisers [41]. On the computational side, in the last decade involution centraliser computations became prevalent [1, 7, 45, 53, 56, 78]. In the next subsections, we describe some applications of centraliser computations; Bray's algorithm [16] for computing centralisers of involutions; and efforts to analyze Bray's algorithm.

2.4.1 Applications of Centralisers of Involutions Computations

A recent active area of computational group theory is the so-called *matrix group recognition project*. Let V be a finite dimensional vector space over a finite field $\mathbb{F}_q$. Given $G = \langle S \rangle \leq \mathrm{GL}(V)$, the goal is to compute quantitative and structural information about G such as the order, a composition series, and important characteristic subgroups like the largest solvable normal subgroup of G.

There are two main approaches to matrix group recognition. The *geometric approach*, initiated by Neumann and Praeger [69] and currently led by Leedham-Green and O'Brien [52,77], is based on Aschbacher's classification of matrix groups [2]. Aschbacher defines nine categories of matrix groups G. In seven of these categories, there is a natural normal subgroup $N \lhd G$ that can be used to divide the recognition problem into two smaller subproblems on N and G/N. Based on that result, the geometric approach tries to find a homomorphism $\varphi : G \to H$ into an appropriate permutation or matrix group H, and recursively recognise $\mathrm{Im}(\varphi)$ and $\mathrm{Ker}(\varphi)$. In contrast, the *black-box group approach* of Babai and Beals [4] aims for the abstract group theoretic structure of G. Babai and Beals define a series of characteristic subgroups, present in all finite groups, and initiate a program that tries to compute a composition series going through these characteristic subgroups.

Both approaches eventually lead to simple (or quasisimple) matrix groups, where further divide-and-conquer is impossible. For such groups, a major issue is the solution of the *constructive membership problem*.

2.4.2 Constructive Membership in Lie Type Groups

Definition 2.40. A *black-box group* G is a group whose elements are encoded by bit strings (strings consisting of 0s and 1s) of uniform length. Moreover, there are oracles for the following tasks. Given strings representing $g, h \in G$, we can compute a string representing gh; a string for g^{-1}; and we can decide whether $g = 1$.

A *black-box algorithm* is an algorithm that, given G by a set of generators, uses only the black-box oracles.

The definition of black-box groups covers the "concrete" representations of groups as permutation groups or matrix groups defined over finite fields. Note that if G is a black-box group and N is a *recognisable* normal subgroup (i.e., given a string representing some $g \in G$, we can decide whether $g \in N$), then G/N is also a black-box group. This observation plays a crucial role in recursive algorithms, allowing us to work in factor groups. Also note that we require only that N is recognisable, but N is not necessarily *constructed* (i.e., we may not have a generating set for N in hand). Examples of recognisable normal subgroups that may be hard to construct are the centre and the largest soluble normal subgroup of G. Black-box groups were introduced by Babai and Szemerédi [5]. For an introduction to the basic black-box group algorithms, see [87, Chap. 2].

A black-box group algorithm does not use specific features of the group representation, nor particulars of how group operations are performed. For example, we lose all information stored implicitly in the cycle structure of a permutation, or in the characteristic polynomial of a matrix. In practice, and also in some theoretical considerations, we often allow oracles for some other operations; an example is an oracle to compute element orders.

The very reasonable and justified question arises: why do we handicap ourselves with black-box group algorithms? One answer is that in certain situations, we cannot do more than the black-box operations. For example, to generate random elements in a matrix group, so far every algorithm takes repeated products and inverses of the given generators, and after a while declares the last element constructed as a random element of the input group [3, 18, 24]. Bray's algorithm (see Sect. 2.4.4) for computing centralisers of involutions is another example of a black-box group algorithm, with a possible enhancement using element order oracles. Another, more unusual answer is that elements of a permutation group can be described as unique words in a strong generating set (SGS), constructed in a canonical way. The group operations are performed using the images of elements of the base associated with the SGS. For the important class of small-base groups, these group operations are much faster than permutation multiplication, but the algorithms using this representation are strictly black-box. For details, we refer to [87, Chap. 5.4].

Next, we define the notion of a straight-line program (SLP). Expressing elements of a group G in a given set of generators may result in words of length proportional to $|G|$; intuitively, SLPs are shortcuts, to reach group elements faster from a set of generators. By [5], every $g \in G$ can be reached from any set of generators by an SLP of length at most $(1 + \log |G|)^2$.

Definition 2.41. Given $G = \langle S \rangle$ and $g \in G$, a *straight-line program (SLP)* reaching g from S is a sequence of expressions $W = (w_1, \ldots, w_m)$ such that, for $i = 1, 2, \ldots, m$,

1. w_i is a symbol for some $s \in S$; or
2. $w_i = (w_j, w_k)$ for some $j, k < i$; or
3. $w_i = (w_j, -1)$ for some $j < i$.

We define the evaluation of W the natural way: $\text{eval}(w_j, w_k) = \text{eval}(w_j)\text{eval}(w_k)$ and $\text{eval}(w_j, -1) = \text{eval}(w_j)^{-1}$; and require that $\text{eval}(w_m) = g$.

Finally, we are ready to define the constructive membership problem.

Definition 2.42. A *constructive membership algorithm for a group* G is a black-box group algorithm that, given the black-box group $G = \langle S \rangle$ and $g \in G$, constructs an SLP reaching g from S.

The main result of this subsection is the following theorem by Holmes et al. [45].

Theorem 2.43 ([45]). *Let G be a black-box group equipped with an order oracle. There is a black-box Monte Carlo algorithm which reduces the constructive membership problem for G to three instances of the same problem for centralisers of involutions of G.*

Proof. Let $G = \langle S \rangle$ and $g \in G$. An algorithm constructing an SLP reaching g from S consists of the following steps.

1. Find $h \in G$ with $\text{ord}(gh) = 2\ell$. Define $z := (gh)^\ell$.
2. Find an involution $x \in G$ with $\text{ord}(xz) = 2m$. Define $y := (xz)^m$.
3. Construct $X = C_G(x)$.
4. Solve the constructive membership problem for $y \in X$.
5. Construct $Y = C_G(y)$.
6. Solve the constructive membership problem for $z \in Y$.
7. Construct $Z = C_G(z)$.
8. Solve the constructive membership problem for $gh \in Z$.
9. Compute and return an SLP for g.

To prove the correctness of the algorithm, observe that z, constructed in Step 1, is an involution centralising gh. In Step 2, y is in the centre of the dihedral group $\langle x, z \rangle$, so x is an involution centralising y and y is an involution centralising z. Hence Steps 3, 5 and 7 compute centralisers of involutions, and the constructive membership problems in Steps 4, 6 and 8 indeed try to reach elements of G that are in the appropriate subgroups. Finally, note that the construction of x provides an SLP reaching x from S and, consequently, we have SLPs reaching y, then z, then gh from S. Also, in Step 1, we construct an SLP reaching h from S. Hence, in Step 9, we can construct an SLP reaching g from S. □

Remark 2.44. We note that the hypothesis of Theorem 2.43 that G has an order oracle can be relaxed. The only places in the algorithm where the order oracle is used are in Steps 1 and 2. For example, at the construction of z in Step 1, we

can proceed the following way. Instead of computing ℓ, we can raise gh to an appropriate multiple of the odd part of $|G|$. To find such a multiple (without knowing $|G|$), it is enough to know a superset of primes occurring in $|G|$ or, in the case of a matrix group $G \leq \mathrm{GL}(n,q)$, we can work with the set of *pseudoprimes*: these are the largest divisors of the numbers $q^e - 1$ for $e \leq n$, that are relatively prime to $q^j - 1$ for all $j < e$. The pseudoprimes can be computed in polynomial time (polynomial in terms of n and $\log q$). For details, see [4]. The use of the order oracle in Step 2 can be avoided in exactly the same way.

In [45], Holmes et al. show that if G is a simple group of Lie type then the algorithm described in Theorem 2.43, not counting the time requirement of Steps 4, 6 and 8, runs in polynomial time. However, we cannot apply the theorem recursively to the groups in these steps, because they are not simple. Therefore, we need a recursive scheme involving all groups, not only the simple ones. Such a scheme is designed by Babai et al. in [7]; Theorem 2.43 is a crucial ingredient in the following result.

Theorem 2.45 ([7]). *There is a randomised polynomial-time algorithm, employing certain number-theoretical oracles, which, given a matrix group $G \leq \mathrm{GL}(n,q)$ of odd characteristic, solves the constructive membership problem in G.*

The required *number-theoretical oracles* are the *factorisation of integers* of the form $q^e - 1$, for $1 \leq e \leq n$, and the *solution of the discrete logarithm problem*: given $a, b \in \mathbb{F}_{q^e}^*$, decide whether $a \in \langle b \rangle$; and, if the answer is affirmative, then find an integer x such that $a = b^x$. In polynomial-time algorithms for matrix groups, it is customary to assume the use of these number theory oracles as they are already needed in finding a composition series and the order of a 1×1 matrix group over $\mathbb{F}_q$. We note that Theorem 2.45 extends to matrix groups defined over fields of characteristic 2, with some restrictions on the composition factors of G. It is expected that these restrictions will be removed in the near future, as constructive membership algorithms in all simple groups are in the offing.

2.4.3 Constructive Recognition of Lie Type Groups

Membership testing is an important first step in exploring a permutation or matrix group G; however, for studying the structure of G and constructing important subgroups, it is beneficial to identify the composition factors of G with standard copies of these factor groups. For alternating and classical groups, the standard copy is the natural permutation and matrix representation, respectively. For exceptional groups, the definition of a standard copy is not so clear-cut: we may choose the smallest-dimensional matrix representation, or a Bruhat decomposition, or any other representation we may be able to control. Here we only give a formal definition for classical groups, taken from [48].

Definition 2.46. *Constructive recognition* of a black-box group $G = \langle S \rangle$ isomorphic to a simple classical group defined on some vector space over a field of given characteristic p is an algorithm that verifies that there is, indeed, an isomorphism, and finds the following:

(i) The field size $q = p^e$, as well as the type and the dimension d of G.
(ii) A new set S^* generating G, a vector space $\mathbb{F}_q^d$, and a monomorphism $\lambda\colon G \to \mathrm{PSL}(d,q)$, specified by the image of S^*, such that $G\lambda$ acts projectively on $\mathbb{F}_q^d$ as a classical group defined on $\mathbb{F}_q^d$.

Moreover, the data structures underlying (ii) yield deterministic algorithms for each of the following:

(iii) Given $g \in G$, find $g\lambda$ and a straight-line program from S^* to g.
(iv) Given $h \in \mathrm{PGL}(d,q)$, decide whether or not $h \in G\lambda$; and, if it is, find $h\lambda^{-1}$ and a straight-line program from S^* to $h\lambda^{-1}$.
(v) Find a form on $\mathbb{F}_q^d$ involved in the definition of G as a classical group, if $G \ncong \mathrm{PSL}(d,q)$.

Although Definition 2.46 is formulated in the general context of black-box groups, of course it can be applied to any given permutation or matrix representation of G. The simplest but most important case is when G is already given in its natural representation, and the only task is to find "nice" generators S^* such that each element of G can be reached easily from S^*. For classical groups of odd characteristic, this task has been accomplished by Leedham-Green and O'Brien by a highly efficient algorithm [53]. A rough outline of their procedure is given in Algorithm 5.

Algorithm 5: ConstructiveRecognition

Input: $G = \langle S \rangle \leq \mathrm{GL}(V) \cong \mathrm{GL}(n,q)$, q odd, G is a classical group in its natural representation;
Output: A data structure for constructive recognition of G;
(1) **repeat**
  $y :=$ random element of G;
until $\mathrm{ord}(y)$ *is even and* $x := y^{\mathrm{ord}(y)/2}$ *has* ± 1*-eigenspaces* E_1, E_{-1} *with* $\dim(E_i) \in (n/3, 2n/3)$;
(2) Construct $H = C_G(x)$;
(3) Recursively solve constructive recognition for the restriction of H to its action on E_1 and E_{-1};
(4) Use the result of Step (3) to obtain nice generators and data structure for constructive recognition of G;

The following simple lemma from [84] implies that Step (3) is indeed a recursive call.

Lemma 2.47. *Let G, x, E_1, E_{-1} be as in Algorithm 5, with G classical but not linear. Then $V = E_1 \perp E_{-1}$, and both E_1 and E_{-1} are nondegenerate (and of even dimension if G is symplectic).*

Proof. For $u \in E_1$ and $w \in E_{-1}$, we have $(u, w) = (u, w)^x = (u, -w)$ and hence $(u, w) = 0$. Thus $E_1 \subseteq E_{-1}^{\perp}$. Since the bilinear form is nondegenerate, $\dim(E_1) = n - \dim(E_{-1}) = \dim(E_{-1}^{\perp})$ and hence $E_1 = E_{-1}^{\perp}$. Therefore, $E_{-1} \cap E_{-1}^{\perp} = 0$ so E_{-1}, and similarly also E_1, are nondegenerate. In particular, E_1 and E_{-1} both have even dimension if G is symplectic. □

Since, for $i \in \{1, -1\}$, x acts as a scalar matrix on E_i, Lemma 2.47 implies that the restriction of H to E_i is a classical group of the same type as G and Step (3) is indeed a recursive call. Note that the requirement $\dim(E_i) \in (n/3, 2n/3)$ ensures that $C_G(x)$ can be split into two parts of roughly equal size, thereby ensuring that the depth of the recursion is logarithmic in n.

To analyze Algorithm 5, for the first two steps we have to estimate (i) the proportion of elements y as in Step (1); and (ii) give a running time estimate for the construction of involution centralisers. Task (i) has been accomplished in Sect. 2.3.4. In the next two subsections, we describe and analyze an algorithm for computing involution centralisers.

2.4.4 Computation of an Element Centralising an Involution

In this subsection we describe an algorithm by Bray [16] that constructs an element in the centraliser of a given involution.

Algorithm 6: CENTRALISINGELEMENT

Input: $G = \langle S \rangle$ and an involution $x \in G$;
Output: An element of $C_G(x)$;
(1) $g :=$ random element of G;
(2) $y := x \cdot x^g$ and $m := \mathrm{ord}(y)$;
(3) **if** *m is even* **then**
    return $\zeta(g) := y^{m/2}$
else
    return $\zeta(g) := y^{(m+1)/2} g^{-1}$
end

We note that the order computation in Step (2) may be avoided, using a superset of primes occurring in G, or pseudoprimes (see Remark 2.44).

Lemma 2.48. *The output of Algorithm 6 is correct: no matter which $g \in G$ is chosen in Step* (1)*, we have $\zeta(g) \in C_G(x)$.*

Proof. For any $g \in G$, the group $D := \langle x, x^g \rangle$ is dihedral, of order $2m$. If m is even then $\zeta(g) \in Z(D)$; in particular, $\zeta(g)$ centralises $x \in D$.

If m is odd then, using that $x^2 = 1$, we obtain

$$x^{y^{\frac{m+1}{2}}} = (xg^{-1}xg)^{\frac{m-1}{2}} x (xg^{-1}xg)^{\frac{m+1}{2}} = x^g.$$

Comparison of the leftmost and rightmost terms gives $\zeta(g) = y^{\frac{m+1}{2}} g^{-1} \in C_G(x)$. □

We say that $g \in G$ is of *even type* if $y = xx^g$ has even order, and $g \in G$ is of *odd type* if $y = xx^g$ has odd order. Note that for any $c \in C_G(x)$, $x^{cg} = x^g$, so $xx^g = xx^{cg}$ and consequently g and cg have the same type. Moreover, $(xx^g)^c = xx^{gc}$ so xx^g and xx^{gc} are conjugate, have the same order, and g and gc have the same type. Combining the last two observations, we obtain that *in a double coset* $C_G(x) \cdot g \cdot C_G(x)$, *all elements have the same type*.

Lemma 2.49. (i) *If g is chosen from the uniform distribution on the set of odd type elements of G then $\zeta(g)$ is a uniformly distributed random element of $C_G(x)$.*

(ii) *If g is chosen from the uniform distribution on the set of even type elements of G and $\zeta(g)$ is in the conjugacy class $\mathscr{C}$ of involutions in $C_G(x)$ then $\zeta(g)$ is a uniformly distributed random element of $\mathscr{C}$.*

Proof. (i) Suppose that g is of odd type. For $c \in C_G(x)$, we have $y^{\frac{m+1}{2}}(cg)^{-1} = y^{\frac{m+1}{2}} g^{-1} c^{-1}$ and so $\zeta(cg) = \zeta(g)c^{-1}$. Hence, as cg runs through the coset $C_G(x) \cdot g$, $y^{\frac{m+1}{2}} g^{-1} c^{-1}$ runs through $C_G(x)$. This implies that if g runs through the elements of G of odd type then each element of $C_G(x)$ occurs as $\zeta(g)$ exactly the same number of times.

(ii) Suppose now that g is of even type. Then $\zeta(g) = (xx^g)^{m/2}$ is an involution; let $\mathscr{C}$ denote its conjugacy class in $C_G(x)$. As gc runs through the coset $g \cdot C_G(x)$, $\zeta(gc) = (xx^{gc})^{m/2} = ((xx^g)^{m/2})^c$ covers each element of $\mathscr{C}$ the same number of times. Hence each element of a fixed conjugacy class $\mathscr{C}$ of involutions in $C_G(x)$ has the same chance to occur as $\zeta(g)$ for some g of even type. □

2.4.5 Computation of the Full Centraliser

In order to compute a set X of generators of $C_G(x)$ for a given group G and involution $x \in G$, we may construct a sequence $(g_1, \ldots, g_m)$ of random elements in G and take $X := \{\zeta(g_i) \mid 1 \leq i \leq m\}$. By Lemma 2.48, we always have $\langle X \rangle \leq C_G(x)$, but when can we stop? How large should m be so that, with high probability, X generates the entire group $C_G(x)$?

By Lemma 2.49, random elements g_i of odd type are highly desirable, since then $\zeta(g_i)$ is a uniformly distributed random element of $C_G(x)$. Such a random element

$\zeta(g_i) \in C_G(x)$, added to an already constructed proper subgroup $H < C_G(x)$, increases H with probability $1 - 1/|C_G(x) : H| \geq 1/2$, so if we know an upper bound ℓ for the length of subgroup chains in $C_G(x)$ then we may estimate how many elements g_i of odd type we need to encounter. For polynomial-time computations, the trivial bound $\ell \leq \log_2 |G|$ suffices, but sometimes we have much better estimates for the number of required random generators. In particular, in the especially important case when G is a simple group of Lie type defined over a field of odd characteristic, the structure of involution centralisers is known. Consequently, for any involution $x \in G$, the number of uniformly distributed random elements needed to generate $C_G(x)$ with probability greater than $1 - \varepsilon$ can be bounded by a function of ε, independent of G and x [57]. Therefore, the following seminal result of Parker and Wilson [78] has great importance in the analysis of many matrix group algorithms.

Theorem 2.50 ([78]). *There exists a positive constant c such that:*

(i) *If G is a simple exceptional group of Lie type defined over a field of odd order, and x is any involution in G, then the probability that a uniformly distributed random element $g \in G$ is of odd type is bounded below by c.*

(ii) *If G is a simple classical group defined over a field of odd order, with natural module of dimension n, and x is any involution in G, then the probability that a uniformly distributed random element $g \in G$ is of odd type is bounded below by c/n. Moreover, the order of magnitude $1/n$ for a lower bound is best possible.*

Parker and Wilson [78, p. 886] give an indication of how big the constants can be: "The constants c that can be obtained from our proofs are of the order of $1/1000$, but we have made no attempt to calculate them explicitly, as we conjecture that the best possible constants are nearer $1/4$."

The basic idea of the proof of Theorem 2.50 is to identify a set of dihedral subgroups D of twice odd order in G, each D containing the given involution x. If the random conjugate x^g falls into one of these subgroups D then xx^g has odd order and g is of odd type. In order to avoid double counting, we also require that generators of the maximal cyclic normal subgroup of D be *regular semisimple* in a suitable subgroup $H \leq G$. (Here H depends on D but H is also of Lie type. We require the generators of D to be regular semisimple as elements of this Lie type group, as defined in Sect. 2.3.6.)

While Theorem 2.50 is sufficient to prove polynomial running time of centraliser of involution computations in Lie type simple groups, the scarcity of elements of odd type raises the the following questions. Is there an algorithm that uses the lower quality random elements $\zeta(g_i) \in C_G(x)$, obtained from g_i of even type, to generate $C_G(x)$? Can the asymptotic running time of this algorithm be faster than the construction of $C_G(x)$ using the uniformly distributed $\zeta(g_i)$ obtained from g_i of odd type? To formulate this problem precisely, we need some definitions.

We consider finite classical groups H of dimension n over a finite field $\mathbb{F}_q$ of odd order q. We denote by H^* the generalized Fitting subgroup of H (for example $H^* = \mathrm{SL}(n, q)$ if $H = \mathrm{GL}(n, q)$). Let α, β be real numbers such that $0 < \alpha <$

$1/2 < \beta < 1$, and let $x \in H$ be of order 2. Recall that x is called an (α, β)-*balanced involution* in H if the subspace $E_1(x)$ of fixed points of x in the underlying vector space has dimension r where $\alpha n \leq r < \beta n$. For a given sequence $\mathscr{X} = (\mathscr{C}_1, \ldots, \mathscr{C}_m)$ of conjugacy classes of (α, β)-balanced involutions in H, a c-tuple $(g_1, \ldots, g_m)$ is a *class-random sequence from* $\mathscr{X}$ if g_i is a uniformly distributed random element of $\mathscr{C}_i$ for each $i = 1, \ldots, m$, and the g_i are mutually independent.

Given a classical group $G \leq \mathrm{GL}(n, q)$ and an involution $x \in G$, the centraliser $C_G(x)$ modulo x is the direct product of two classical groups $H^{(1)}$ and $H^{(-1)}$, acting on $E_1(x)$ and $E_{-1}(x)$, respectively. If $g \in G$ is of even type then $\zeta(g)$ acts as an involution $g^{(J)}$ on E_J, for $J \in \{1, -1\}$, and if $(g_1, \ldots, g_m)$ is a sequence of uniformly distributed random elements of even type in G then Lemma 2.49 implies that $(g_1^{(J)}, \ldots, g_m^{(J)})$ is a class-random sequence from some conjugacy classes of involutions $\mathscr{X}^{(J)} = (\mathscr{C}_1^{(J)}, \ldots, \mathscr{C}_m^{(J)})$.

With an application in Algorithm 5 in mind, we propose the following problems. We use the notation and definitions of the previous paragraphs.

Problem 2.51. Given a classical group $G \leq \mathrm{GL}(n, q)$ and a $(1/3, 2/3)$-balanced involution x in G, estimate the probability p that for a uniformly distributed $g \in G$ of even type, $g^{(J)}$ is an (α, β)-balanced involution in $H^{(J)}$, for *both* $J \in \{1, -1\}$. Here α, β are constants, chosen appropriately.

Problem 2.52. Let $G \leq \mathrm{GL}(n, q)$ be a classical group and let $\mathscr{X} = (\mathscr{C}_1, \ldots, \mathscr{C}_m)$ be a sequence of conjugacy classes of (α, β)-balanced involutions in G. Estimate the minimum value of m such that, with high probability, a class-random sequence from $\mathscr{X}$ generates a subgroup of G containing G^*.

If the product $(1/p)m$, for the probability p from Problem 2.51 and the minimum value m from Problem 2.52, satisfies $(1/p)m = o(n)$ then the elements $\zeta(g)$ obtained from even type g generate $C_G(x)$ asymptotically faster than the elements $\zeta(g)$ obtained from odd type g.

Problem 2.52 has been solved for all classical groups.

Theorem 2.53 ([84]). *Let α, β be real numbers such that $0 < \alpha < 1/2 < \beta < 1$. Then there exist integers $m = m(\alpha, \beta)$ and $n(\alpha, \beta)$ such that, for G, n, q as above, with q odd, if $n > n(\alpha, \beta)$ and $\mathscr{X} = (\mathscr{C}_1, \ldots, \mathscr{C}_m)$ is a given sequence of conjugacy classes of (α, β)-balanced involutions in G, then a class-random sequence from $\mathscr{X}$ generates a subgroup containing G^* with probability at least $1 - q^{-n}$.*

The basic idea of the proof of Theorem 2.53 is standard: if a class-random sequence $(g_1, \ldots, g_m)$ does not generate G^* then all g_i belong to some maximal subgroup $M < G$, with M not containing G^*. Since g_i is uniformly distributed in its conjugacy class, we have to estimate the ratios $|M \cap \mathscr{C}_i|/|\mathscr{C}_i|$ for all maximal subgroups M. Maximal subgroups are characterised by Aschbacher's theorem [2]; it turns out that the most difficult case is when M is reducible (has a proper invariant subspace).

Much less is known about Problem 2.51. At present, a solution is known only in the case when $G^* = \mathrm{SL}(n, q)$.

Theorem 2.54 ([85]). *There exist c and n_0 such that if $n > n_0$, $\mathrm{SL}(n,q) \leq G \leq \mathrm{GL}(n,q)$, x is a $(1/3,2/3)$-balanced involution of G, and $g \in G$ is a uniformly distributed random element among the elements of G of even type, then with probability at least $c/\log n$, $g^{(1)}$ and $g^{(-1)}$ are $(1/6,2/3)$-balanced involutions on the eigenspaces $E_1(x)$ and $E_{-1}(x)$ respectively.*

The proof of Theorem 2.54 uses a significant enhancement of the generating function method described in Sect. 2.3.6, and also some ideas from [58].

Acknowledgements This chapter forms part of our Australian Research Council Discovery Project DP110101153. Praeger and Seress are supported by an Australian Research Council Federation Fellowship and Professorial Fellowship, respectively. Niemeyer thanks the Lehrstuhl D für Mathematik at RWTH Aachen for their hospitality, and acknowledges a DFG grant in SPP1489. All three of us warmly thank the de Brún Centre for Computational Algebra at National University of Ireland, Galway, for their hospitality during the Workshop on Groups, Combinatorics and Computing in April 2011, where we presented the short lecture course that led to the development of this chapter. We are very grateful to Peter M. Neumann for many thoughtful comments and advice, and his translation of Euler's words in Sect. 2.2.2.

References

1. C. Altseimer, A.V. Borovik, *Probabilistic Recognition of Orthogonal and Symplectic Groups*, in Groups and Computation, III, vol. 8, Columbus, OH, 1999 (Ohio State University Mathematical Research Institute Publications/de Gruyter, Berlin, 2001), pp. 1–20
2. M. Aschbacher, On the maximal subgroups of the finite classical groups. Invent. Math. **76**(3), 469–514 (1984)
3. L. Babai, *Local Expansion of Vertex-Transitive Graphs and Random Generation in Finite Groups*, in 23rd ACM Symposium on Theory of Computing (ACM, New York, 1991), pp. 164–174
4. L. Babai, R. Beals, *A Polynomial-Time Theory of Black Box Groups. I*, in Groups St. Andrews 1997 in Bath, I. London Mathematical Society Lecture Note Series, vol. 260 (Cambridge University Press, Cambridge, 1999), pp. 30–64
5. L. Babai, E. Szemerédi, *On the Complexity of Matrix Group Problems I*, in 25th Annual Symposium on Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, 1984), pp. 229–240
6. L. Babai, W.M. Kantor, P.P. Pálfy, Á. Seress, Black-box recognition of finite simple groups of Lie type by statistics of element orders. J. Group Theor. **5**(4), 383–401 (2002)
7. L. Babai, R. Beals, Á. Seress, *Polynomial-Time Theory of Matrix Groups*, in 41st ACM Symposium on Theory of Computing, Bethesda, MD, 2009 (ACM, New York, 2009), pp. 55–64
8. R. Beals, C.R. Leedham-Green, A.C. Niemeyer, C.E. Praeger, Á. Seress, Permutations with restricted cycle structure and an algorithmic application. Combin. Probab. Comput. **11**(5), 447–464 (2002)
9. R. Beals, C.R. Leedham-Green, A.C. Niemeyer, C.E. Praeger, Á. Seress, A black-box group algorithm for recognizing finite symmetric and alternating groups. I. Trans. Am. Math. Soc. **355**(5), 2097–2113 (2003)
10. D.E.-C. Ben-Ezra, Counting elements in the symmetric group, Int. J. Algebra Comput. **19**(3), 305–313 (2009)
11. E.A. Bender, Asymptotic methods in enumeration. SIAM Rev. **16**, 485–515 (1974)

12. E.A. Bertram, B. Gordon, Counting special permutations. Eur. J. Comb. **10**(3), 221–226 (1989)
13. E.D. Bolker, A.M. Gleason, Counting permutations. J. Comb. Theor. Ser. A **29**(2), 236–242 (1980)
14. M. Bóna, A. McLennan, D. White, Permutations with roots. Random Struct. Algorithm **17**(2), 157–167 (2000)
15. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997)
16. J.N. Bray, An improved method for generating the centralizer of an involution. Arch. Math. (Basel) **74**(4), 241–245 (2000)
17. R.W. Carter, *Finite Groups of Lie Type* (Wiley Classics Library, Wiley, Chichester, 1993), Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication
18. F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer, E.A. O'Brien, Generating random elements of a finite group. Comm. Algebra **23**(13), 4931–4948 (1995)
19. W.W. Chernoff, Solutions to $x^r = \alpha$ in the alternating group. Ars Combin. **29**(C), 226–227 (1990) (Twelfth British Combinatorial Conference, Norwich, 1989)
20. S. Chowla, I.N. Herstein, W.K. Moore, On recursions connected with symmetric groups. I. Can. J. Math. **3**, 328–334 (1951)
21. S. Chowla, I.N. Herstein, W.R. Scott, The solutions of $x^d = 1$ in symmetric groups. Norske Vid. Selsk. Forh. Trondheim **25**, 29–31 (1952/1953)
22. A.M. Cohen, S.H. Murray, An algorithm for Lang's Theorem. J. Algebra **322**(3), 675–702 (2009)
23. A. de Moivre, *The Doctrine of Chances: Or, A Method of Calculating the Probability of Events in Play*, 2nd edn. (H. Woodfall, London, 1738)
24. J.D. Dixon, Generating random elements in finite groups. Electron. J. Comb. **15**(1), Research Paper 94 (2008)
25. P. Dusart, The kth prime is greater than $k(\ln k + \ln\ln k - 1)$ for $k \geq 2$. Math. Comp. **68**(225), 411–415 (2009)
26. P. Erdős, M. Szalay, *On Some Problems of the Statistical Theory of Partitions*, in Number Theory, vol. I, Budapest, 1987. Colloq. Math. Soc. János Bolyai, vol. 51 (North-Holland, Amsterdam, 1990), pp. 93–110
27. P. Erdős, P. Turán, On some problems of a statistical group-theory. I. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **4**, 175–186 (1965)
28. P. Erdős, P. Turán, On some problems of a statistical group-theory. II. Acta Math. Acad. Sci. Hung. **18**, 151–163 (1967)
29. P. Erdős, P. Turán, On some problems of a statistical group-theory. III. Acta Math. Acad. Sci. Hung. **18**, 309–320 (1967)
30. P. Erdős, P. Turán, On some problems of a statistical group-theory. IV. Acta Math. Acad. Sci. Hung. **19**, 413–435 (1968)
31. P. Erdős, P. Turán, On some problems of a statistical group theory. VI. J. Indian Math. Soc. **34**(3–4), 175–192 (1970/1971)
32. P. Erdős, P. Turán, On some problems of a statistical group theory. V. Period. Math. Hung. **1**(1), 5–13 (1971)
33. L. Euler, *Calcul de la probabilité dans le jeu de rencontre*. Mémoires de l'Academie des Sciences de Berlin, 7 (1751) 1753, pp. 255–270. Reprinted in Opera Omnia: Series 1, vol. 7, pp. 11–25. Available through The Euler Archive at www.EulerArchive.org.
34. L. Euler, *Solutio Quaestionis curiosae ex doctrina combinationum*. Mémoires de l'Académie des Sciences de St.-Petersbourg, 3:57–64, 1811. Reprinted in Opera Omnia: Series 1, vol. 7, pp. 435–440. Available through The Euler Archive at www.EulerArchive.org.
35. P. Flajolet, R. Sedgewick, *Analytic Combinatorics* (Cambridge University Press, Cambridge, 2009)
36. J. Fulman, P.M. Neumann, C.E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Am. Math. Soc. **176**(830), vi+90 (2005)

37. The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.5.2(beta), 2011, http://www.gap-system.org/
38. S.P. Glasby, Using recurrence relations to count certain elements in symmetric groups. Eur. J. Comb. **22**(4), 497–501 (2001)
39. W.M.Y. Goh, E. Schmutz, The expected order of a random permutation. Bull. Lond. Math. Soc. **23**(1), 34–42 (1991)
40. V. Gončarov, On the field of combinatory analysis. Am. Math. Soc. Transl. **19**(2), 1–46 (1962)
41. D. Gorenstein, R. Lyons, R. Solomon, *The Classification of the Finite Simple Groups*. Mathematical Surveys and Monographs, vol. 40 (American Mathematical Society, Providence, 1994)
42. O. Gruder, Zur Theorie der Zerlegung von Permutationen in Zyklen. Ark. Mat. **2**(5), 385–414 (1953)
43. W.K. Hayman, A generalisation of Stirling's formula. J. Reine Angew. Math. **196**, 67–95 (1956)
44. R.B. Herrera, The number of elements of given period in finite symmetric groups. Am. Math. Mon. **64**, 488–490 (1957)
45. P.E. Holmes, S.A. Linton, E.A. O'Brien, A.J.E. Ryba, R.A. Wilson, Constructive membership in black-box groups. J. Group Theor. **11**(6), 747–763 (2008)
46. I.M. Isaacs, W.M. Kantor, N. Spaltenstein, On the probability that a group element is p-singular. J. Algebra **176**(1), 139–181 (1995)
47. E. Jacobsthal, Sur le nombre d'éléments du groupe symétrique S_n dont l'ordre est un nombre premier. Norske Vid. Selsk. Forh. Trondheim **21**(12), 49–51 (1949)
48. W.M. Kantor, Á. Seress, Black box classical groups. Mem. Am. Math. Soc. **149**(708), viii+168 (2001)
49. A.V. Kolchin, Equations that contain an unknown permutation. Diskret. Mat. **6**(1), 100–115 (1994)
50. V.F. Kolchin, *Random Graphs*. Encyclopedia of Mathematics and Its Applications, vol. 53 (Cambridge University Press, Cambridge, 1999)
51. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*, 2nd edn. (Chelsea Publishing Co., New York, 1953), With an appendix by Paul T. Bateman
52. C.R. Leedham-Green, *The Computational Matrix Group Project*, in Groups and Computation, III, vol. 8, Columbus, OH, 1999 (Ohio State University Mathematical Research Institute Publications/de Gruyter, Berlin, 2001), pp. 229–247
53. C.R. Leedham-Green, E.A. O'Brien, Constructive recognition of classical groups in odd characteristic. J. Algebra **322**(3), 833–881 (2009)
54. G.I. Lehrer, Rational tori, semisimple orbits and the topology of hyperplane complements. Comment. Math. Helv. **67**(2), 226–251 (1992)
55. G.I. Lehrer, The cohomology of the regular semisimple variety. J. Algebra **199**(2), 666–689 (1998)
56. M.W. Liebeck, E.A. O'Brien, Finding the characteristic of a group of Lie type. J. Lond. Math. Soc. (2) **75**(3), 741–754 (2007)
57. M.W. Liebeck, A. Shalev, The probability of generating a finite simple group. Geom. Dedicata **56**(1), 103–113 (1995)
58. F. Lübeck, A.C. Niemeyer, C.E. Praeger, Finding involutions in finite Lie type groups of odd characteristic. J. Algebra **321**(11), 3397–3417 (2009)
59. E.M. Luks, *Permutation Groups and Polynomial-Time Computation*, in Groups and computation, New Brunswick, NJ, 1991. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 11 (American Mathematical Society, Providence, 1993), pp. 139–175
60. R. Lyons, Evidence for a new finite simple group. J. Algebra **20**, 540–569 (1972)
61. A. Maróti, Symmetric functions, generalized blocks, and permutations with restricted cycle structure. Eur. J. Comb. **28**(3), 942–963 (2007)
62. N. Metropolis, The beginnings of the Monte Carlo method. Los Alamos Sci. **15** (Special Issue), 125–130 (1987)

63. M.P. Mineev, A.I. Pavlov, The number of permutations of a special form. Mat. Sb. (N.S.) **99(141)**(3), 468–476, 480 (1976)
64. P.R. de Monmort, *Essay d'analyse sur les jeux de hazard* (J. Quillau, Paris, 1708)
65. P.R. de Monmort, *Essay d'analyse sur les jeux de hazard*, 2nd edn. (J. Quillau, Paris, 1713)
66. L. Moser, M. Wyman, On solutions of $x^d = 1$ in symmetric groups. Can. J. Math. **7**, 159–168 (1955)
67. L. Moser, M. Wyman, Asymptotic expansions. Can. J. Math. **8**, 225–233 (1956)
68. L. Moser, M. Wyman, Asymptotic expansions. II. Can. J. Math. **9**, 194–209 (1957)
69. P.M. Neumann, C.E. Praeger, A recognition algorithm for special linear groups. Proc. Lond. Math. Soc. (3) **65** (3), 555–603 (1992)
70. P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields. J. Lond. Math. Soc. (2) **52**, 263–284 (1995)
71. A.C. Niemeyer, T. Popiel, C.E. Praeger, Abundant p-singular elements in finite classical groups, preprint (2012) http://arxiv.org/abs/1205.1454v2
72. A.C. Niemeyer, C.E. Praeger, A recognition algorithm for classical groups over finite fields. Proc. Lond. Math. Soc. (3) **77** (1), 117–169 (1998)
73. A.C. Niemeyer, C.E. Praeger, On the frequency of permutations containing a long cycle. J. Algebra **300**(1), 289–304 (2006)
74. A.C. Niemeyer, C.E. Praeger, On permutations of order dividing a given integer. J. Algebr. Comb. **26**(1), 125–142 (2007)
75. A.C. Niemeyer, C.E. Praeger, On the proportion of permutations of order a multiple of the degree. J. Lond. Math. Soc. (2) **76**(3), 622–632 (2007)
76. A.C. Niemeyer, C.E. Praeger, Estimating proportions of elements in finite groups of Lie type. J. Algebra **324**(1), 122–145 (2010)
77. E.A. O'Brien, *Algorithms for Matrix Groups*, in Groups St. Andrews 2009 in Bath, vol. 2. London Mathematical Society Lecture Note Series, vol. 388 (Cambridge University Press, Cambridge, 2011), pp. 297–323
78. C.W. Parker, R.A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers. J. Algebra **324**(5), 885–915 (2010)
79. E.T. Parker, P.J. Nikolai, A search for analogues of the Mathieu groups. Math. Tables Aids Comput. **12**, 38–43 (1958)
80. A.I. Pavlov, An equation in a symmetric semigroup. Trudy Mat. Inst. Steklov. **177**, 114–121, 208 (1986); Proc. Steklov Inst. Math. 1988(4), 121–129, Probabilistic problems of discrete mathematics
81. A.I. Pavlov, On permutations with cycle lengths from a fixed set. Theor. Probab. Appl. **31**, 618–619 (1986)
82. W. Plesken, D. Robertz, The average number of cycles. Arch. Math. (Basel) **93**(5), 445–449 (2009)
83. C.E. Praeger, On elements of prime order in primitive permutation groups. J. Algebra **60**(1), 126–157 (1979)
84. C.E. Praeger, Á. Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions. J. Group Theor. **14**(4), 521–545 (2011)
85. C.E. Praeger, Á. Seress, Balanced involutions in the centralisers of involutions in finite general linear groups of odd characteristic (in preparation)
86. C.E. Praeger, Á. Seress, Regular semisimple elements and involutions in finite general linear groups of odd characteristic. Proc. Am. Math. Soc. **140**, 3003–3015 (2012)
87. Á. Seress, *Permutation Group Algorithms*. Cambridge Tracts in Mathematics, vol. 152 (Cambridge University Press, Cambridge, 2003)
88. C.C. Sims, *Computational Methods in the Study of Permutation Groups*, in Computational Problems in Abstract Algebra, Proceedings of the Conference, Oxford, 1967 (Pergamon, Oxford, 1970), pp. 169–183
89. C.C. Sims, *The Existence and Uniqueness of Lyons' Group*, in Finite groups '72, Proceedings of the Gainesville Conference, University of Florida, Gainesville, FL, 1972. North–Holland Mathematical Studies, vol. 7 (North-Holland, Amsterdam, 1973), pp. 138–141

90. A.N. Timashev, Random permutations with cycle lengths in a given finite set. Diskret. Mat. **20**(1), 25–37 (2008)
91. J. Touchard, Sur les cycles des substitutions. Acta Math. **70**(1), 243–297 (1939)
92. L.M. Volynets, The number of solutions of the equation $x^s = e$ in a symmetric group. Mat. Zametki **40**(2), 155–160, 286 (1986)
93. R. Warlimont, Über die Anzahl der Lösungen von $x^n = 1$ in der symmetrischen Gruppe S_n. Arch. Math. (Basel) **30** (6), 591–594 (1978)
94. H. Wielandt, *Finite Permutation Groups*, Translated from the German by R. Bercov (Academic, New York, 1964)
95. H.S. Wilf, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n. Bull. Am. Math. Soc. (N.S.) **15** (2), 228–232 (1986)
96. H.S. Wilf, *Generatingfunctionology*, 2nd edn. (Academic, Boston, 1994)
97. K. Zsigmondy, Zur Theorie der Potenzreste. Monatsh. für Math. U. Phys. **3**, 265–284 (1892)

http://www.springer.com/978-1-4471-4813-5

Probabilistic Group Theory, Combinatorics, and Computing
Lectures from the Fifth de Brún Workshop
Detinko, A.; Flannery, D.; O'Brien, E. (Eds.)
2013, XIII, 107 p., Softcover
ISBN: 978-1-4471-4813-5