CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

1

Introduction

The focus of this book is the question how many groups of order n are there? This is to be interpreted in the natural way: we define $f(n)$ to be the number of groups of order n up to isomorphism and ask for information about the function f.

The values of $f(n)$ for small values of n are:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$f(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	...

For $1 \leqslant n \leqslant 16$ the groups of order n were classified well over a hundred years ago, and the value of $f(n)$ clearly follows from this classification. The easiest case is when n is a prime—Lagrange's Theorem shows that a group of order n must be cyclic, and so $f(n) = 1$. When n is in the range of the table above, only $n = 16$ requires a lengthy argument to establish a classification. Note that $f(15) = 1$ even though 15 is not prime.

As n increases, the problem of classifying groups of order n becomes hard. The groups of order 2^{10} have only recently been classified, by Besche, Eick and O'Brien [6]. An appendix to their paper lists $f(n)$ when $1 \leqslant n \leqslant 2000$; in particular when $n = 2^{10}$ they count 49 487 365 422 groups! However, the groups of order 2^{11} have not been classified and it is not known how many groups of order 2^{11} there are. (We will show in Chapter 4 that $f(2^{11}) > 2^{44}$.) So if we are to say anything about $f(n)$ when n is large, we must resort to giving estimates for $f(n)$ rather than calculating $f(n)$ exactly.

Graham Higman [45] showed in 1960 that

$$f(p^m) \geqslant p^{\frac{2}{27}m^3 - O(m^2)},$$

Charles Sims [86] proved in 1965 that

$$f(p^m) \leqslant p^{\frac{2}{27}m^3 + O(m^{8/3})}$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

and, as the culmination of a long line of development, Laszlo Pyber [82] proved in 1991 (published in 1993) that

$$f(n) \leqslant n^{\frac{2}{27}\mu(n)^2+O(\mu(n)^{5/3})},$$

where $\mu(n)$ is the highest power to which any prime divides n. Amplification of these results, and their proofs, forms the main part of the work: the results of Higman and Sims are expounded in Part II (incorporating a modification of Sims' argument due to Mike Newman and Craig Seeley [77], which improves the error term significantly) and Pyber's theorem is the subject of Part III. The proofs use a large amount of very attractive theory that is just beyond the scope of an undergraduate course in algebra. All that theory is expounded here, so that our treatment of the theorems of Higman and Sims and of Pyber's theorem in the soluble case is self-contained. Our treatment of the general case of Pyber's theorem in Chapter 16 is not self-contained, however, because it relies ultimately upon the Classification of the Finite Simple Groups (CFSG).

The asymptotics of the function f tell us much, but far from everything, about the groups of order n. To get a clearer picture we consider related matters. For example, context is given by the questions how many semigroups and how many latin squares of order n are there? These questions are treated briefly in Chapter 2. Detail is given by such questions as: how many abelian groups of order n are there? how many of the groups of order n have abelian Sylow subgroups? how many of the groups of order n satisfy a given identical relation? how many are soluble? how many are nilpotent? Questions of this type are treated in Part IV.

Standing conventions:

- most groups considered are finite—if at any point finiteness is not mentioned but seems desirable, the reader is invited to assume it;
- f has already been introduced as the group enumeration function;
- for a class $\mathfrak{X}$ of groups (or of other structures) $f_{\mathfrak{X}}(n)$ denotes the number of members of $\mathfrak{X}$ of order n, up to isomorphism;
- logarithms are to the base 2;
- maps are on the left;
- p always denotes a prime number;
- if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime numbers, then $\lambda(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $\mu(n) = \max\{\alpha_i \mid 1 \leqslant i \leqslant k\}$.

Other notation and conventions are introduced where they are needed.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

I

Elementary results

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

2

Some basic observations

This chapter is devoted to elementary estimates for $f(n)$, the number of groups of order n (up to isomorphism). We begin by looking at some enumeration functions for weaker objects than groups.

Since a binary system is determined by its multiplication table, we find that

$$f(n) \leqslant f_{\text{binary systems}}(n) \leqslant n^{n^2}.$$

At most $n!$ of these multiplication tables are isomorphic to any fixed binary system, since an isomorphism is one of only $n!$ permutations. Hence

$$n^{n^2-n} \leqslant \frac{n^{n^2}}{n!} \leqslant f_{\text{binary systems}}(n) \leqslant n^{n^2}.$$

If we consider binary systems with a unit element, we have

$$n^{n^2-3n+O(1)} \leqslant f_{\text{binary systems with 1}}(n) \leqslant n^{(n-1)^2} = n^{n^2-2n+1}.$$

Recall that a semigroup is a set with an associative multiplication defined on it. For all $\epsilon > 0$,

$$n^{(1-\epsilon)n^2} \leqslant f_{\text{semigroups}}(n) \leqslant n^{n^2}$$

if $n \geqslant n_0(\epsilon)$. To see this, consider the binary systems on $\{0, 1, \ldots, n-1\}$ described by tables of the following form:

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

	0	1	…	$m-2$	$m-1$	m	$m+1$	…	$n-2$	$n-1$
0	0	0	…	0	0	0	0	…	0	0
1	0	0	…	0	0	0	0	…	0	0
⋮	⋮	⋮		⋮	⋮	⋮	⋮		⋮	⋮
$m-1$	0	0	…	0	0	0	0	…	0	0
m	0	0	…	0	0	$*$	$*$	…	$*$	$*$
$m+1$	0	0	…	0	0	$*$	$*$	…	$*$	$*$
⋮	⋮	⋮		⋮	⋮	⋮	⋮		⋮	⋮
$n-1$	0	0	…	0	0	$*$	$*$	…	$*$	$*$

Here the starred entries are arbitrary subject to being at most $m-1$. The associative law holds for this table, since

$$(a_i a_j)a_k = 0 = a_i(a_j a_k).$$

Hence

$$f_{\text{semigroups}}(n) \geqslant m^{(n-m)^2}.$$

(Notice here that we should divide by $n!$, but this again does not make a significant difference.) Setting m to be approximately $n^{1-\frac{1}{2}\epsilon}$ we have

$$f_{\text{semigroups}}(n) \geqslant n^{(1-\frac{1}{2}\epsilon)(n-n^{1-\frac{1}{2}\epsilon})^2}.$$

For sufficiently large n,

$$n^{(1-\frac{1}{2}\epsilon)(n-n^{1-\frac{1}{2}\epsilon})^2} \geqslant n^{(1-\epsilon)n^2}.$$

Thus we get the requisite lower bound.

If we add the condition that all our semigroups contain a unit element, we have similar results to the above.

Daniel Kleitman, Bruce Rothschild and Joel Spencer enumerate semigroups more precisely in [55]. They show that most semigroups can be split into two subsets A and B having the following property: there exists an element $0 \in B$ such that if $x, y \in A$ then $xy \in B$ but if $x \in B$ or $y \in B$ then $xy = 0$. They then use this fact to prove

$$f_{\text{semigroups}}(n) = \left(\sum_{t=1}^{n} g(t)\right)(1+O(1)), \text{ where}$$

$$g(t) = \binom{n}{t} t^{1+(n-t)^2}.$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

The function $g(t)$ maximises at t_0, where $t_0 \sim n/2\log_e n$. Thus we may improve the lower bound we gave above to

$$f_{\text{semigroups}}(n) \geqslant n^{n^2(1-(\log\log n/\log n)-O(1/\log n))},$$

where (for this inequality only) log should denote the natural logarithm—although, as the astute reader will realise, in fact the base of the logarithms does not matter here.

A multiplication table with inverses is a latin square (i.e., in each row and column of the table, an element appears only once). We have

$$n^{\frac{1}{2}n^2-O(n)} \leqslant f_{\text{latin squares}}(n) \leqslant n^{n^2}.$$

The lower bound was proved by Marshall Hall [40]. Using less elementary methods, the lower bound may be improved: Henryk Minc showed in [69] that

$$(n!)^{2n}/n^{n^2} \leqslant f_{\text{latin squares}}(n).$$

His proof uses the Egoryčev–Falikman theorem [26, 32, 70] establishing the van der Waerden conjecture on permanents. Note that there is a constant c such that $n! > c\,(n/e)^n$, and so $f_{\text{latin squares}}(n) > c^2 n^{n^2(1-1/\log n)}$. Much remains to be discovered about this enumeration function. In 2005, Brendan McKay and Ian Wanless [68] state 'At the time of writing, not even the asymptotic value of $f_{\text{latin squares}}(n)$ is known'.

Returning to the group enumeration function, we see that even very elementary methods are enough to show that there are seriously fewer groups than semigroups or latin squares:

Observation 2.1

$$f(n) \leqslant n^{n\log n}.$$

Proof: For a group G, define

$$d(G) = \min\{k \mid \exists\, g_1, \ldots, g_k \in G \text{ such that } G = \langle g_1, \ldots, g_k\rangle\}.$$

We first show that if $|G| = n$ then $d(G) \leqslant \log n$. Let

$$\{1\} = G_0 < G_1 < G_2 < \cdots < G_r = G$$

be a maximal chain of subgroups. Let $g_i \in G_i \setminus G_{i-1}$ for $1 \leqslant i \leqslant r$. Then $\langle g_1, \ldots, g_i\rangle = G_i$, as one easily sees by induction. In particular, G can be generated by r elements. Now by Lagrange's Theorem

$$|G| = \prod_{i=1}^{r} |G_i : G_{i-1}| \geqslant 2^r. \tag{2.1}$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

Hence $r \leqslant \lfloor \log n \rfloor$. Then by Cayley's theorem $G \leqslant \mathrm{Sym}(n)$ and so

$$\begin{aligned} f(n) &\leqslant \text{number of subgroups of order } n \text{ in } \mathrm{Sym}(n) \\ &\leqslant \text{number of } \lfloor \log n \rfloor\text{-generator subgroups of } \mathrm{Sym}(n) \\ &\leqslant \text{number of } \lfloor \log n \rfloor\text{-element subsets of } \mathrm{Sym}(n) \\ &\leqslant (n!)^{\log n} \\ &\leqslant n^{n \log n} \end{aligned}$$

and the result follows.

Recall the notation $\mu(n)$ and $\lambda(n)$ that we introduced at the end of Chapter 1. A factorisation of n has at most $\lambda(n)$ non-trivial factors. Equation (2.1) shows that $r \leqslant \lambda(n)$, and therefore the bound for $d(G)$ can be sharpened to say that $d(G) \leqslant \lambda(n)$. We remark that in fact $d(G) \leqslant \mu(n)+1$, as we will see in Corollary 16.7, but ignoring this for the moment and feeding the simple bound for $d(G)$ into the above argument we get that

$$f(n) \leqslant n^{n\lambda(n)}.$$

That is about as far as one can go with elementary methods. Nevertheless, it already shows that the associative law and the existence of inverses are separately very much weaker than is their combination.

The aim of the remainder of the book is to prove the better bounds on $f(n)$ given in the Introduction, using more sophisticated methods.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

II

Groups of prime power order

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

3

Preliminaries

This chapter contains a brief account of some of the results we will need in the next two chapters. More specifically, we review some basic commutator identities and results on nilpotent groups, discuss the Frattini subgroup of a group and prove some simple enumeration results concerning vector spaces, general linear groups and symplectic groups. We emphasise that all groups are finite in this section—some of the results (and definitions) differ in the infinite case. We assume that the reader has already met a few commutator identities and the idea of a nilpotent group, and so we have included sketch proofs rather than full detail for some of the results. For more detail, see Gorenstein [36, Sections 2.2 and 2.3].

3.1 Tensor products and exterior squares of abelian groups

As preparation for some of our treatment of commutators we recall (without proofs) the definition of tensor product and exterior square of abelian groups. If A, B are abelian groups (which we write additively here) the *tensor product* $A \otimes B$ is defined to be the abelian group which is generated by all symbols $a \otimes b$ for $a \in A$ and $b \in B$ subject to the relations

$$(a_1 + a_2) \otimes b - a_1 \otimes b - a_2 \otimes b = 0,$$
$$a \otimes (b_1 + b_2) - a \otimes b_1 - a \otimes b_2 = 0,$$

which make the operation $\otimes$ bilinear. We identify $a \otimes b$ with its image modulo the relations and then the map $A \times B \to A \otimes B$ (where here $A \times B$ simply denotes the *set* of pairs), $(a, b) \mapsto a \otimes b$, is bilinear. If A is generated by $a_1, \ldots, a_r$ and B is generated by $b_1, \ldots, b_s$ then

$$\{a_i \otimes b_j \mid 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s\}$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

will be a generating set for $A \otimes B$; moreover, the order of $a \otimes b$ divides the greatest common divisor of the orders of a and b.

The *exterior square* $A^{\wedge 2}$ (sometimes written $\bigwedge^2 A$) of A is defined to be the abelian group generated by all symbols $a \wedge b$ for $a, b \in A$ with the same bilinearity relations as the tensor product and, in addition, the relations

$$a \wedge a = 0 \quad \text{for all } a \in A$$

which make $\wedge$ an alternating function of its arguments. Again, we identify $a \wedge b$ with its image modulo the relations and then the two-variable function $(a, b) \mapsto a \wedge b$ is an alternating bilinear map $A \times A \to A^{\wedge 2}$. Note that the equation $b \wedge a = -(a \wedge b)$ follows easily from the defining relations for the exterior square, and that if A is generated by $a_1, \ldots, a_r$ then

$$\{a_i \wedge a_j \mid 1 \leqslant i < j \leqslant r\}$$

is a generating set for $A^{\wedge 2}$.

One of the main properties of the tensor product is that it is universal for bilinear maps. That is, if C is an abelian group and $f : A \times B \to C$ is a bilinear map then there is a unique homomorphism $f^* : A \otimes B \to C$ such that $f^*(a \otimes b) = f(a, b)$ for all $a \in A$, $b \in B$. Similarly, the exterior square is universal for alternating bilinear maps in the sense that if $f : A \times A \to C$ is bilinear and such that $f(a, a) = 0$ for all a then there is a unique homomorphism $f^* : A^{\wedge 2} \to C$ such that $f^*(a \wedge b) = f(a, b)$ for all $a, b \in A$. Another fundamental property is functoriality: the tensor product and exterior square are functorial in the sense that if A_1, A_2, B_1, B_2 are abelian groups and $f : A_1 \to A_2$, $g : B_1 \to B_2$ are homomorphisms then there are homomorphisms $f \otimes g : A_1 \otimes B_1 \to A_2 \otimes B_2$ and $f^{\wedge 2} : {A_1}^{\wedge 2} \to {A_2}^{\wedge 2}$ such that $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$ for all $a \in A_1$, $b \in B_1$ and $f^{\wedge 2}(a \wedge b) = f(a) \wedge f(b)$ for all $a, b \in A_1$.

3.2 Commutators and nilpotent groups

Let G be a group and let $x, y \in G$. The commutator $[x, y]$ of x and y is defined by $[x, y] = x^{-1}y^{-1}xy$. For $x, y, z \in G$, we define $[x, y, z] = [[x, y], z]$. Throughout this section, we will write x^y to mean $y^{-1}xy$.

Lemma 3.1 *Let G be a group.*

(1) *For all $x, y \in G$,*

$$[x, y] = [y, x]^{-1}. \tag{3.1}$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

(2) *For all* $x, y, z \in G$,

$$[xy, z] = [x, z]^y [y, z] = [x, z][x, z, y][y, z], \tag{3.2}$$

$$[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]. \tag{3.3}$$

(3) *For all* $x, y, z \in G$,

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1. \tag{3.4}$$

The proof of this lemma is easy: just use the definition of a commutator to express each side of the above equalities as a product of x, y, z and their inverses.

Corollary 3.2 *Let G be a group.*

(1) *For all* $x, y, z \in G$,

$$[x^{-1}, y] = \left([x, y]^{-1}\right)^{x^{-1}} = [x, y, x^{-1}]^{-1}[x, y]^{-1}, \tag{3.5}$$

$$[x, y^{-1}] = \left([x, y]^{-1}\right)^{y^{-1}} = [x, y, y^{-1}]^{-1}[x, y]^{-1}. \tag{3.6}$$

(2) *For all* $x, y, z \in G$,

$$[x, y, z] = \left([z, x^{-1}, y^{-1}]^{-1}\right)^{xy} \left([y^{-1}, z^{-1}, x]^{-1}\right)^{zy}. \tag{3.7}$$

Proof: The corollary follows from Lemma 3.1 by making the appropriate substitutions. To derive (3.5), replace y by x^{-1} and z by y in (3.2). For (3.6), replace z by y^{-1} in (3.3). To derive (3.7), replace y by y^{-1} in (3.4).

Lemma 3.3 *Let G be a group. Let $x, y \in G$. Suppose that $[y, x]$ commutes with both x and y. Then for all positive integers n*

$$[y, x^n] = [y^n, x] = [y, x]^n, \tag{3.8}$$

$$(xy)^n = x^n y^n [y, x]^{\frac{1}{2}n(n-1)}. \tag{3.9}$$

Proof: The equality (3.8) follows by induction on n, using (3.2) and (3.3) in the inductive step. To establish (3.9), use the fact that $y^i x = xy^i [y^i, x]$.

We will now consider a collection of results related to nilpotency of groups. Let H and K be subgroups of a group G. Then $[H, K]$ is defined to be the subgroup generated by all elements of the form $[h, k]$ where $h \in H$ and $k \in K$. Note that $[H, K] = [K, H]$, by Equation (3.1). The subgroup $[H, K, L]$ is defined by $[H, K, L] = [[H, K], L]$. The following lemma, known as the Three Subgroup Lemma, is often useful.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-0-521-88217-0 — Enumeration of Finite Groups
Simon R. Blackburn , Peter M. Neumann , Geetha Venkataraman
Excerpt
More Information

Lemma 3.4 *Let K, L and M be subgroups of a group G. Then $[K, L, M] \leqslant [M, K, L][L, M, K]$ whenever $[M, K, L]$ and $[L, M, K]$ are normal subgroups of G.*

Proof: Suppose that $[M, K, L]$ and $[L, M, K]$ are normal subgroups of G. The subgroup $[K, L, M]$ is generated by elements of the form $[g, h]$ where $g \in [K, L]$ and $h \in M$. We may express g as a product of commutators of the form $[g', h']$ where $g' \in K$ and $h' \in L$, and then use Equations (3.2) and (3.3) to express $[g, h]$ as a product of conjugates of elements of the form $[x, y, z]$ where $x \in K$, $y \in L$ and $z \in M$. But (3.7) expresses $[x, y, z]$ as a product of a conjugate of an element of $[M, K, L]$ and a conjugate of an element of $[L, M, K]$. Since $[M, K, L]$ and $[L, M, K]$ are normal, we find that each generator of $[K, L, M]$ lies in $[M, K, L][L, M, K]$, so the lemma follows.

The *lower central series* $G_1, G_2, G_3, \ldots$ of a group G is defined by $G_1 = G$ and $G_{i+1} = [G_i, G]$ for every positive integer i. From now on, we will always use G_i to denote the ith term of the lower central series of G. It is not difficult to see, using the definition of the lower central series, that the subgroups G_i are characteristic subgroups of G. Clearly G_i/G_{i+1} is central in G/G_{i+1}. For all normal subgroups N of G, we have that $(G/N)_i = (G_iN)/N$. Moreover, if H is a subgroup of G then H_i is a subgroup of G_i for all positive integers i.

Proposition 3.5 *Let G be a group. Let $A = G/G_2 = G/G'$ and $A_i = G_i/G_{i+1}$. Then A_2 is a homomorphic image of $A^{\wedge 2}$ and A_{i+1} is a homomorphic image of $A_i \otimes A$ for all $i \geqslant 1$.*

Proof: It follows immediately from Lemma 3.1 that the map $A \times A \to A_2$, $(aG', bG') \mapsto [a, b]G_3$ is well-defined and bilinear. It is also alternating since $[a, a] = 1$ for all $a \in G$. Therefore there is a homomorphism $A^{\wedge 2} \to A_2$ such that $aG' \wedge bG' \mapsto [a, b]G_3$ for all $a, b \in G$. This is surjective since G_2 is generated by the commutators $[a, b]$ for $a, b \in G$, and therefore A_2 is a homomorphic image of $A^{\wedge 2}$. The proof that A_{i+1} is a homomorphic image of $A_i \otimes A$ for all $i \geqslant 1$ is similar and we omit it.

Proposition 3.6 *Let G be a group. For all positive integers i and j, we have that $[G_i, G_j] \leqslant G_{i+j}$.*

Proof: We use induction on j. The case when $j = 1$ follows by definition of the lower central series. Assume that $j > 1$ and that $[G_i, G_{j-1}]$ is a subgroup of G_{i+j-1} for any group G and any $i \geqslant 0$. We prove that $[G_i, G_j]$ is a subgroup of G_{i+j} as follows.

© in this web service Cambridge University Press www.cambridge.org