CAMBRIDGE

Cambridge University Press
978-1-107-65750-2 - How Groups Grow
Avinoam Mann
Excerpt
More information

1
Introduction

Let G be a finitely generated group, generated by $x_1, \ldots, x_d$, say. Each element $x \in G$ can be written as a *word* in the generators, i.e. as a product $y_1 \cdots y_n$, where each y_i is either one of the generators or its inverse. The number n is called the *length* of the word. (The identity element is represented by the empty word, which has length zero.) Usually, the same element can be represented by many words. Of all of these, we choose one of minimal length (this word is not necessarily unique) and call this length the *length* $l(x)$ of x. We write $a_G(n)$ for the number of elements of length n, and $s_G(n)$ for the number of words of length at most n, i.e. $s_G(n) = \sum_{i=0}^{n} a_G(i)$. We term $a_G(n)$ and $s_G(n)$ the *growth functions* of G. More specifically, $a_G(n)$ is the *strict growth function* and $s_G(n)$ is the *cumulative growth function* of G. Our interest is in these two functions, their properties, and their relationship with the structure and properties of G. The subscript G will be often omitted, if it is clear from the context which group is meant.

Example 1 G is finite iff $a_G(n)$ is eventually 0, equivalently iff $s_G(n)$ is eventually constant. On the other hand, if G is infinite, then $a(n) > 0$ for each n, and $s(n) \geq n + 1$.

Exercise 1.1 Prove the statements just made about the growth functions of infinite groups.

Example 2 If $G = \mathbb{Z}$ is infinite cyclic, then $a(n) = 2$ for all n (except for $n = 0$; $a_G(0) = 1$ for all groups).

Example 3 Let $G = F^d$ be free of rank d. Then each element has a unique expression as a reduced word. A word of length $n+1$ is obtained by multiplying one of length n, say $y_1 \cdots y_n$, by any generator or its

CAMBRIDGE

Cambridge University Press
978-1-107-65750-2 - How Groups Grow
Avinoam Mann
Excerpt
More information

inverse, except for y_n^{-1}. Thus $a(n+1) = a(n)(2d-1)$, so we have $a(0) = 1$, $a(1) = 2d$, and $a(n) = 2d(2d-1)^{n-1}$ for $n \geq 1$.

If G is any d-generator group, words of length $n+1$ are obtained from ones of length n in the same way as in this example, but they need not all represent distinct elements of G, and they may also be equal to shorter words. Thus we have:

Proposition 1.1 *If G is generated by d elements, then for $n > 0$ we have $a(n) \leq 2d(2d-1)^{n-1}$.*

Before proceeding, let us clarify our use of the notion “a generating set”. We do not insist that such a set be minimal in any sense. Thus, it need not consist of the minimal possible number of generators, and it is possible that a proper subset of it is still a generating set. However, we insist that no generator is equal to another, or to the inverse of another. Indeed, if this assumption is not met, we can omit a generator that is equal to another without changing the growth functions.

Exercise 1.2 Let G have d generators and the same growth function as F^d. Then $G \cong F^d$.

Example 4 Let G be the free product of $2d$ groups of order 2, generated by $x(1), \ldots, x(2d)$. Then each element has a unique expression as a product $x(i_1) \cdots x(i_n)$, in which no two consecutive factors have the same index. It follows that the growth function is the same as in the previous example. In particular, the group $D_\infty := C_2 * C_2$ has the same growth function as $\mathbb{Z}$ (C_n denotes a cyclic group of order n). That group is known as the *infinite dihedral group*. If the two cyclic factors are generated by x and y, say, then $z = xy$ has an infinite order, generates an infinite cyclic subgroup C of index 2, and $D_\infty = CC_2$, where the last factor may be either of the two cyclic free factors.

Example 5 Take G to be the free product of d copies of $\mathbb{Z}$ and e copies of C_2. The growth function is (for $n > 0$) $a(n) = k(k-1)^{n-1}$, where $k = 2d + e$. It follows that there is no bound on the number of groups with the same growth function.

Proposition 1.2 *If the growth function of G is $a(n) = k(k-1)^{n-1}$, then G is (isomorphic to) one of the groups of the last example.*

Proof Let the generators of G be $x_1, \ldots, x_d, y_1, \ldots, y_e$, where the y_i are the generators that have order 2. Then $k = 2d + e$ (consider $a(1)$). Let H be a free product of d copies of $\mathbb{Z}$ and e copies of C_2. Then there is a homomorphism from H to G, mapping the generators of the factors $\mathbb{Z}$ in H to the x_i, and mapping the generators of order 2 in H to the y_j. Since the two groups have the same growth function, the map is 1–1, and $G \cong H$. QED

Problem 1 Can there be infinitely many groups with the same growth function?

Problem 2 What properties do groups with the same growth function have in common?

The last example shows that the growth function does not determine G. But neither does G determine its growth function, because it may have different sets of generators, a point that we have ignored so far.

Example 6 Let $G = \mathbb{Z}$, and consider the two numbers $\{2, 3\}$. This is a set of generators, since each integer can be written as $2r + 3s$. Suppose that in that expression $r \geq 3$, then we can replace it by $2(r-3) + 3(s+2)$, reducing the length from $r + s$ to $r + s - 1$ (if $s \geq 0$. For negative s the reduction is even bigger). Similarly, if $r \leq -3$, we replace the above expression by $2(r+3) + 3(s-2)$ (note that in this case the term $2r$ contributes $|r| = -r$ to the length). This implies that the minimal length is obtained when we write our integer in the form $3k, 3k + 2$, or $3(k-1) + 2{\cdot}2$, if it is positive, the lengths being $k, k+1$, and $k+1$, respectively. For negative numbers the minimal expression is $3k, 3k-2$, or $3(k+1) - 2{\cdot}2$, with lengths $|k|$ and $|k|+1$. There is a slight exception for the integers $1 = 3 - 2$ and $-1 = 2 - 3$, the only ones for which the minimal expressions have r and s of different signs. It follows that $a(0) = 1$, $a(1) = 4$, $a(2) = 8$, and $a(n) = 6$ for $n \geq 3$. Any pair of coprime integers is a set of generators of Z, and the growth function relative to it can be computed similarly. For example, for the generators $\{2, 5\}$ the expression of minimal length would be one of $5k, 5k+2, 5k-2, 5k+4, 5k-4$, with lengths $k, k+1, k+1, k+2, k+2$, and growth function $a(n) = 10$ (for $n \geq 3$).

Exercise 1.3 If $\mathbb{Z}$ is generated by r and s, with $0 < r < s$, then the corresponding growth function is $a(n) = 2s$, provided n is large enough.

As another illustration, consider the infinite dihedral group D_∞, and take as generators x and z, using the notation of Example **4.** It is easy to see that each element can be written uniquely in the form z^k or $z^k x$, and that this is a shortest presentation. It follows that $a(1) = 3$ and $a(n) = 4$ for $n \geq 2$.

To formalize the relationship between two growth functions of the same group, we introduce the following concept.

Definition Two functions f and g from $\mathbb{N}$ to $\mathbb{N}$, or from $\mathbb{N}$ to $\mathbb{R}$, or from $\mathbb{R}$ to $\mathbb{R}$, are *equivalent* if there exists a real positive number A such that $f(x) \leq Ag(Ax)$ and $g(x) \leq Af(Ax)$.

Proposition 1.3 *Two growth functions of the same group are equivalent.*

Proof Let $s = s_{G,X}$ and $t = s_{G,Y}$ be two growth functions of G. Express each element of Y as a word in the elements of X, and each element of X as a word in the elements of Y, and let A be the maximal length of the resulting set of words. It is then clear that for each $x \in G$ we have $l_X(x) \leq Al_Y(x)$, and it follows that $t(n) \leq s(An)$. Similarly, $s(n) \leq t(An)$. QED

In analogy with Problem 2, we may ask, what properties do groups with equivalent growth functions have in common? But this seems too general. Thus, if we define a function $f(n)$ to be of *exponential growth*, if there exist numbers $a, b > 1$ such that $a^n \leq f(n) \leq b^n$, then all functions of exponential growth are equivalent to each other. In particular all groups of exponential growth (i.e. groups with growth functions of exponential type) have equivalent growth functions, but, as we shall see, this class of groups includes groups of widely differing structures.

Example 7 Let $G = \mathbb{Z}^d$, a free abelian group, with the natural set of d free generators. Each element can be written uniquely in the form $x_1^{e_1} \cdots x_d^{e_d}$. Writing a_d for $a_{\mathbb{Z}^d}$, and s_d similarly, we see easily that $a_d(n) = a_{d-1}(n) + 2\sum_{k=1}^{n} a_{d-1}(n-k)$. Using the known formulas for sums of powers of the first n integers, and induction on d, we obtain that $a_d(n)$ and $s_d(n)$ are polynomials in n of degrees of $d-1$ and d, respectively. For example, $a_2(n) = 4n$ and $a_3(n) = 4n^2 + 4n + 2$ $(n > 0)$.

Example 8 Let $G = H \times K$ be a direct product. Given sets of generators of H and K, their union is a set of generators for G, and for an element $x = (u, v) \in G$ we have $l_G(x) = l_H(u) + l_K(v)$. It follows that $a_G(n) = \sum_{r=0}^{n} a_H(r)a_K(n-r)$. This equality reminds us of the multiplication rule for polynomials, or power series, and suggests the following:

Definition The *strict generating growth function* of G is the infinite series $A_G(X) = \sum_0^\infty a(n)X^n$. We will often refer to it simply as the *generating growth function*.

The *cumulative generating growth function* of G is $S_G(X) = \sum s(n)X^n$.

Proposition 1.4

(a) $A(X) = (1 - X)S(X)$.

(b) *If* $G = H \times K$, *and* G, H, K *have generating growth functions* $A(X)$, $B(X)$, *and* $C(X)$ *respectively, then* $A(X) = B(X)C(X)$.

Here part (**b**) is just a reformulation of the formula in Example 8, and part (**a**) is the analytic form of the equality $a_n = s_n - s_{n-1}$. The equivalent form $s_n = a_0 + a_1 + \cdots + a_n$ is expressed analytically by the formula $S(X) = A(X)(1 + X + X^2 + \cdots)$.

The series $A_G(X)$ is sometimes written as $\sum_{a \in G} X^{l(a)}$.

Part (**b**) enables an alternative approach to Example 7. It also implies that given two groups H and K, the growth function of their direct product depends only on the growth functions of the factors. Thus, if two groups G and H have the same growth function, and K is any group, then $G \times K$ and $H \times K$ also have the same growth function. Moreover, the three groups $G \times G$, $G \times H$, and $H \times H$ have the same growth function. By taking direct products with more than two factors, it seems that we can again find any number of different groups with the same growth function. But we need to be careful! We said "seems" above, because it is possible for two finitely generated groups to be non-isomorphic but have isomorphic direct squares. The most popular theorem on uniqueness of direct decompositions, the Krull–Schmidt theorem, often does not apply in our context. A very general uniqueness theorem is proved in [Ku 56, section 47]. It implies, e.g., that in a group with trivial centre any two direct decompositions into directly indecomposable groups are isomorphic. It follows that if we take for G and H two non-isomorphic groups with the same growth function of the type discussed in Examples 4 and 5 above, then, with one exception, two direct products of G and H are isomorphic only if they have the same number of factors of each isomorphism type. The exception occurs when G and H are $\mathbb{Z}$ and D_∞. For that case, see the following exercise.

Exercise 1.4

(a) Show that two direct products of copies of $\mathbb{Z}$ and of D_∞ are isomorphic only if they have the same number of factors of either type.

(Hint: consider the maximal finite subgroups of the direct product,

Cambridge University Press
978-1-107-65750-2 - How Groups Grow
Avinoam Mann
Excerpt
More information

and the factor groups over the subgroup generated by all these subgroups. An alternative approach: consider the factors groups G/G^2 and G/G^3. Here G is the direct product, and G^n is the subgroup generated by all nth powers in G).

(b) Try to generalize this approach to the other pairs of groups with the same generating function provided by Examples 4 and 5.

Example 9 Let G be a semidirect product of H and K. We recall that means that $G = HK$, where $H \cap K = 1$ and $H \triangleleft G$, but K need not be normal in G. To know the structure of G we have to know not only the structure of H and K, but also the action of K on H, i.e. we have to know for each $x \in K$ the automorphism σ_x of H defined by $\sigma_x : z \to z^x$ $(z \in H)$. The map $x \to \sigma_x$ is a homomorphism of K to $\mathrm{Aut}(H)$. If this homomorphism is trivial, we recapture the direct product, but sometimes the semidirect product is isomorphic to the direct one even if the above homomorphism is non-trivial, e.g. if $K = H$, acting on itself by inner automorphisms. Returning to the general case, each element of G can be written uniquely as xz, with $x \in K$ and $z \in H$. Given sets of generators for H and K, again their union is a set of generators for G. However, writing x and z in terms of these generators does not necessarily yield a shortest possible word for this product, even if the expressions for x and z are the shortest possible. This is so because the word $z^{x^{-1}}x$ may be shorter than the word xz, which is equal to it, when we write $z^{x^{-1}}$ in terms of the generators of H. However, this phenomenon cannot occur if the automorphisms σ_x preserve the length of words in H, equivalently if these automorphisms permute the generators of H and their inverses (the elements of length 1) among themselves. In that case we do get the shortest expression for xz by using the shortest ones for x and z, and therefore the growth function is the same as for the direct product of H and K.

Note that that yields another source for finding different groups with the same growth function. As an illustration, consider the infinite dihedral group. It can be considered as a semidirect product $\mathbb{Z}$ by C_2, the latter group acting on $\mathbb{Z}$ by inversion. Thus it has the same growth function as the direct product $\mathbb{Z} \times C_2$. On the other hand, we know already that, with a different choice of generators, it has the same growth function as $\mathbb{Z}$ (see Example 4).

Note also that the union of the sets of generators of H and K does not always yield the most natural set of generators for G. For example, the direct product of two cyclic groups of finite, relatively prime orders is itself cyclic. There are even examples of non-trivial, finitely generated groups which are isomorphic to their direct products with themselves [TJ 74]. An interesting example is obtained by considering sets of generators X and Y for groups H and K, and taking for the direct product $G = H \times K$ the set of generators consisting of $X \cup Y$ and of the set of products $\{xy \mid x \in X, y \in Y\}$. It is easy to see that the length of an element (h, k) relative to this set of generators is $\max(l_X(h), l_Y(k))$, implying $s_G(n) = s_H(n)s_K(n)$.

Exercise 1.5 Prove that, no matter which sets of generators we choose for $\mathbb{Z}$ and for $\mathbb{Z} \times C_2$, the two groups do not have the same growth function.

Example 10 Let $G = C_2 * C_3$, say $G = \langle x, y | x^2 = y^3 = 1\rangle$. It is well known that $G \cong \mathrm{PSL}(2, \mathbb{Z})$ (for a simple proof of that, see, e.g., appendix B of [Ku 56], or Section II.28 of [Hr 00]). If some word $w \in G$ ends with x, then we get a longer word by multiplying by either y or y^{-1}. But if w ends with y, then multiplying by x yields a longer word, multiplying by y^{-1} yields a shorter word, and multiplying by y yields a word ending in $y^2 = y^{-1}$, so $l(wy) = l(w)$. The same happens if w ends in y^{-1}. Now let us perform two consecutive multiplications, and check when the length increases both times. If w ends in x, we have first to multiply by y or y^{-1}, and then by x, while if w ends in y or y^{-1}, we have to multiply first by x and then by y or by y^{-1}. In either case there are two possibilities, which means that $a_G(n+2) = 2a_G(n)$. Starting from the values $a(1) = 3$ and $a(2) = 4$, we obtain $a(2n+1) = 3 \cdot 2^n$ and $a(2n) = 4 \cdot 2^{n-1} = 2^{n+1}$.

For a general free product we have

Proposition 1.5 *If $G = H * K$, and G, H, K have generating growth functions $A(X), B(X), C(X)$ respectively, then*

$$\frac{1}{A} - 1 = \left(\frac{1}{B} - 1\right) + \left(\frac{1}{C} - 1\right).$$

Proof Let $G = H*K$. Write a typical element as $x = u_1v_1u_2 \cdots v_r$, with $u_i \in H, v_i \in K$. Here all factors are different from the identity element, except possibly for u_1 or v_r. The number of elements of the above form of length n is $\sum a_H(s_1)a_K(t_1)a_H(s_2) \cdots a_K(t_r)$, where the sum is subject to the constraints $\sum s_i + \sum t_i = n$ and $s_i \geq 1$ for $i > 1$ and $t_i \geq 1$ for $i < r$. This is the coefficient of X^n in $B(X)C(X)((B(X) - 1)(C(X) - 1))^{r-1}$. Summing over r, we obtain

$$A(X) = \frac{B(X)C(X)}{1 - (B(X) - 1)(C(X) - 1)} = \frac{B(X)C(X)}{B(X) + C(X) - B(X)C(X)}.$$

Taking inverses we get the formula in the statement of the proposition.
QED

Again, this proposition enables an alternative approach to examples **3,4,5,** and **10.** Also, as in the case of direct products, it gives us another way of producing any number of groups with the same growth function. Unlike the case of direct products, free decompositions have strong uniqueness properties. Any finitely generated group is the free product of finitely many freely indecomposable groups, and the indecomposable factors are uniquely determined, up to isomorphism [Ku 56, section 35].

The above examples may give the impression that calculating the growth function of a group is a straightforward matter. This is not at all the case. Indeed, for most groups that calculation is impossible. The word "impossible" is used here in a very precise sense. We recall that mathematicians often equate the number theoretical functions that "can be calculated" with the so-called *recursive functions*. Unlike the phrase in inverted commas, the notion of a recursive function can be defined precisely, and the assumption that these functions are exactly the *computable* ones is known as Church's Thesis (after Alonzo Church, 1903-1995). Thus our claim that often the growth function is impossible to calculate means that for many groups this function is not recursive. We will not, however, repeat the definition of a recursive function, but will continue to use the expression "can be calculated" in an intuitive, naive way.

Let us consider groups that are not only finitely generated, but also *finitely presented*. We recall that this means that our group G is given by finitely many generators, say $x_1, \dots, x_d$, and finitely many *relations* $w_1 = 1, \dots, w_r = 1$, where each w_j is a word in the x_i, and G is the most general group which can be generated by d elements satisfying these equalities. In more precise terms, we consider the w_j as elements of the free group F^d, and $G \cong F^d/N$, where N is the normal closure in F^d of $w_1, \dots, w_r$. The words w_j are called the *relators*, and the equalities $w_j = 1$ are called the *defining relations*, of G. If H is any group with d generators, which we also denote $x_1, \dots, x_d$, then H also is isomorphic to a factor group of F^d, say $H \cong F^d/K$. The defining relations of G hold in H, i.e. $w_1 = \cdots = w_r = 1$ is true in H, if and only if $w_j \in K$, which is the same as $N \leq K$, and then $H \cong (F^d/N)/(K/N) \cong G/L$, for some $L \lhd G$. In that sense G is the "most general" group satisfying its defining relations; any other group satisfying them is isomorphic to a factor group of G.

Recall also that we say that *the word problem is soluble in* G, if there exists an algorithm to decide if two words in the generators are equal (i.e. represent the same element) in G. Since $x = y$ is the same as $xy^{-1} = 1$, it suffices to determine when a word is equal to the identity. It is easy to enumerate all the elements of F^d, say by using a lexicographic order, and thus index all words in $x_1, \ldots, x_d$ by the natural numbers. Solving the word problem is then the same as being able to tell if a particular natural number is the index of a word that is equal to 1 in G. In other words, the characteristic function of the set of such indices should be computable, or, using Church's thesis, recursive. A set whose characteristic function is recursive is itself termed a *recursive set.*

There are many groups with insoluble word problems (see [Ro 95, Ch. 12]), so our claim about the frequent incomputability of growth functions is justified by:

Proposition 1.6 *Let G be a finitely presented group. The word problem is soluble in G if and only if the growth function of G is recursive.*

Proof If the word problem is soluble, we calculate $a_G(n)$ by listing all words of length n and checking which of them are equal to each other or to shorter words. For the converse, notice first that if N is, as above, the normal closure in F^d of the set of relators, then the elements of N are exactly all the products of conjugates of the relators and their inverses, and these products can be listed, say by ordering r-tuples in F^d by the sum of r and the lengths of the r words, ordering the finitely many tuples with a given sum arbitrarily, and for each r-tuple writing down all the products of conjugates by these r elements of relators and their inverses. That means that all the words that are 1 in G are being listed one by one, possibly with repetitions, so if a certain word w in F^d is the identity in G, we will find that out by carrying out this listing process till we see w. But if $w \neq 1$, it will never appear in our list; but at any given moment we do not know if w did not appear yet because it is not 1, or just because we did not wait long enough. Thus to solve the word problem we have to know which words are not the identity. Now suppose that we are able to compute $s_G(n)$, and that w has length n (in F^d). We start by writing down all words of length n at most. Then we carry out the above process of listing the words representing 1. This is the same as listing all equalities $u = v$ between two words. From time to time we find equalities between two words of length at most n, and this reduces the number of elements of length n in G, either by showing that a word of length n has actually a shorter length in G, or by showing that two such words represent the same element. We continue this till this number goes down to the computed value of $s(n)$. At this stage we know that we are not going to find any more equalities among words of length at most n, and in particular if our word w was not shown yet to be 1, it is actually not the identity. Thus the word problem is solved. QED

It is interesting that a similar result holds in a sort of dual situation. By a *recursive permutation* we understand a permutation of the natural numbers that is recursive as a function. These permutations form a group. Let G be a finitely generated subgroup of this group. We can list the set of pairs (w, n), where w is a word on the generators of G and n is a natural number, and since the generators are recursive, we can evaluate $w(n)$ for each such pair. If $w \neq 1$ in G, then after listing enough pairs, we will find one for which $w(n) \neq n$. That means that this time, we are going to know which words are not the identity, and to solve the word problem we have to be able to decide which words are trivial in G.

Proposition 1.7 *With the above notation, the word problem is soluble in G if and only if the growth function $a_G(n)$ is recursive.*

Proof If the word problem is soluble, the growth function is recursive, as in the previous proposition. For the reverse direction, given a word w of length n, we again list all words of length at most n, and as explained above, we test them for inequalities. At each stage of the testing we are going to discover that certain words of length at most n are not equal to each other, while about other words we will be uncertain yet. In any case, we obtain a lower bound for the number of elements of G of length at most n, and when this bound reaches $s(n)$, a computable number, we know that we have representative words for all elements of length at most n of G. We continue to test w until we find that it is different from $s(n) - 1$ of these representatives, and then we know that w is equal to the remaining representative. In particular we know if it is the identity or not. QED

This proposition has a converse, which actually yields a sort of characterization of groups with a soluble word problem.

Proposition 1.8 *A finitely generated group G has a soluble word problem if and only if it is isomorphic to a group generated by finitely many*