Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 81 (2006)

Artikel: Growth exponent of generic groups
Autor: Ollivier, Yann
DOI: https://doi.org/10.5169/seals-1172

Comment. Math. Helv. 81 (2006), 569–593

Commentarii Mathematici Helvetici

Growth exponent of generic groups

Yann Ollivier

Abstract. In [GrH97], Grigorchuk and de la Harpe ask for conditions under which some group presentations have growth rate close to that of the free group with the same number of generators. We prove that this property holds for a generic group (in the density model of random groups). Namely, for every positive ε, the property of having growth exponent at least $1-\varepsilon$ (in base $2m-1$ where m is the number of generators) is generic in this model. In particular this extends a theorem of Shukhov [Shu99].

More generally, we prove that the growth exponent does not change much through a random quotient of a torsion-free hyperbolic group.

Mathematics Subject Classification (2000). 20P05, 20F69, 20F06.

Keywords. Random groups, growth, hyperbolic groups.

Introduction

The growth exponent is a very natural quantity associated to a group presentation, measuring the rate of growth of the balls in the group with respect to some given set of generators. Namely, let $G = \langle a_1, \dots, a_m \mid R \rangle$ be a finitely generated group. For $\ell \geqslant 0$ let $B_\ell \subset G$ be the set of elements of norm at most ℓ with respect to this generating set. The *growth exponent* of G (sometimes called *entropy*) with respect to this set of generators is

$$g = \lim_{\ell \to \infty} \frac{1}{\ell} \log_{2m-1} |B_\ell|.$$

The maximal value of g is 1, which is achieved if and only if G is the free group F_m on the m generators $a_1, \dots, a_m$. The limit in the definition exists thanks to the submultiplicativity property $|B_{\ell+\ell'}| \leqslant |B_\ell||B_{\ell'}|$. By standard properties of subadditive (or submultiplicative) sequences, this implies in particular that for any ℓ we have $|B_\ell| \geqslant (2m-1)^{g\ell}$.

Growth exponents of groups, first introduced by Milnor, are related to many other properties, for example in Riemannian geometry, dynamical systems and of course combinatorial group theory. We refer to [GrH97], [Har00] (chapters VI and VII), or [Ver00] for some surveys and applications.

The authors of [GrH97] ask for conditions under which some families of groups (namely one-relators groups) have growth exponents getting arbitrarily close to the maximal value 1. Shukhov gave an example of such a condition in [Shu99]: it is proven therein that if a group presentation has long relators satisfying the $C'(1/6)$ small cancellation condition, and if there are "not too many" relators (in a precise sense), then the growth exponent of the group so presented is arbitrarily close to 1.

We prove that having growth exponent at least $1 - \varepsilon$ is a *generic* property in the density model of random groups.

For a general discussion and extensive bibliography on random groups and the various models we refer to [Oll05b] or [Gh03]. The density model was introduced by Gromov in [Gro93]. We recall the precise definition in Section 1.1 below; basically, depending on a density parameter $d \geqslant 0$, it consists in taking a group presentation with m fixed generators and $(2m-1)^{d\ell}$ relators taken at random among all reduced words of length ℓ in the generators, and letting $\ell \to \infty$. The intuition is that at density d, any reduced word of length $d\ell$ will appear as a subword of some relator in the presentation.

This model allows a precise control of the quantity of relations put in the random group, which is examplified by the phase transition theorem proven in [Gro93]: below density $1/2$, random groups are very probably infinite and hyperbolic, and very probably trivial above density $1/2$ (see Theorem 5 below).

Keeping this in mind, our theorem reads:

Theorem 1. *Let $d < 1/2$ be a density parameter and let G be a random group on $m \geqslant 2$ generators at density d and at length ℓ.*

Then, for any $\varepsilon > 0$, the probability that the growth exponent of G is at least $1 - \varepsilon$ tends to 1 as $\ell \to \infty$.

When $d < 1/12$ this is a consequence of Shukhov's theorem: indeed for densities at most $1/12$, random groups satisfy the $C'(1/6)$ small cancellation condition. But for larger densities they do not any more, and so the theorem really provides a large class of new groups with large growth exponent.

Random groups at length ℓ look like free groups at scales lower than ℓ (more precisely, the length of the shortest relation in a random group is ℓ if $d < 1/4$ and $\ell(2 - 4d - \varepsilon)$ if $d \geqslant 1/4$), and so the cardinality of balls of course grows with exponent 1 at the beginning. However, growth is an asymptotic invariant, and the geometry of random groups at scale ℓ is highly non-trivial, so the theorem cannot be interpreted by simply saying that random groups look like free groups at small scales.

More generally, we show that for torsion-free hyperbolic groups, the growth exponent is stable in the following sense: if we randomly pick elements in the group and quotient by the normal subgroup they generate (the so-called quotient by *random elements* as opposed to the quotient by randomly picked words in the generators; see details below), then the growth exponent stays almost unchanged, unless we killed too many elements and get the trivial group. Note however that this exponent cannot stay exactly the same, as Arzhantseva and Lysenok proved in [AL02] that quotienting a hyperbolic group by an infinite normal subgroup decreases the growth exponent.

The study of random quotients of hyperbolic groups arises naturally from the knowledge that a random group (a random quotient of the free group) is hyperbolic: one can wonder whether a random quotient of a hyperbolic group stays hyperbolic. The answer from [Oll04] is yes (see Section 1.1 below for details) up to some critical density equal to $g/2$ where g is the growth exponent of the initial group; above this critical density the random quotient collapses. In this framework our second theorem reads:

Theorem 2. *Let G_0 be a non-elementary torsion-free hyperbolic group of growth exponent g. Let $d < g/2$. Let G be a quotient of G_0 by random elements at density d and at length ℓ.*

Then, for any $\varepsilon > 0$, with probability tending to 1 as $\ell \to \infty$, the growth exponent of G lies between $g - \varepsilon$ and g.

Of course, Theorem 1 is just Theorem 2 applied to a free group.

Remark 3. The proof of Theorem 2 only uses the two following facts: that the random quotient axioms of [Oll04] are satisfied, and that there is a local-to-global principle for growth in the random quotient. So in particular the result holds under slightly weaker conditions than torsion-freeness of G_0, as described in [Oll04] ("harmless torsion").

Locality of growth in hyperbolic groups. As one of our tools we use a result about locality of growth in hyperbolic groups (see the Appendix). Growth is an asymptotic invariant, and large relations in a group can change it noticeably. But in hyperbolic groups, if the hyperbolicity constant is known, it is only necessary to evaluate growth in some ball in the group to get that the growth of the group is not too far from this evaluation (see Proposition 17 in the Appendix).

In the case of random quotients by relators of length ℓ, this principle shows that it is necessary to check growth up to words of length at most $A\ell$ for some large constant A (which depends on density and actually tends to infinity when d is close to the critical density), so that geometry of the quotient matters up to scale ℓ (including the non-trivial geometry of the random quotient at this scale) but not at higher scales.

This result may have independent interest.

About the proofs, and about cogrowth. The proofs presented here make heavy use of the terminology and results from [Oll04]. We have included a reminder (Section 2.2) so that this paper is self-contained.

This paper comes along with a "twin" paper about *co*growth of random groups ([Oll05a]). Let us insist that, although the inspiration for these two papers is somewhat the same (use some locality principle and count van Kampen diagrams), the details do differ, except for the reminder from [Oll04] which is identical. Especially, the proof of the locality principle for growth and cogrowth is not at all the same. The counting of van Kampen diagrams begins similarly but soon diverges as we are not evaluating the same things eventually. And we do not work in the same variant of the density model: for growth we use the element variant, whereas for cogrowth we use the word variant (happily these two variants coincide in the case of a free group, that is, for "plain" random groups).

The result of [Oll05a] already implies some lower bound for the growth exponent of a random group, thanks to the formula $(2m-1)^{g/2} \geqslant (2m)^{1-\theta}$ where by definition $(2m)^{\theta-1}$ is the spectral radius of the simple random walk operator (see [GrH97]). However this bound is not sharp: for a random group it reads $(2m-1)^g \geqslant m^2/(2m-1)-\varepsilon$ whereas we prove here that $(2m-1)^g \geqslant 2m-1-\varepsilon$.

Acknowledgments. I would like to thank Étienne Ghys, Pierre de la Harpe, Pierre Pansu and an anonymous referee for helpful discussions and many comments on the text. Lots of the ideas presented here emerged during my very nice stay at the École normale supérieure de Lyon in Spring 2003, at the invitation of Damien Gaboriau and Étienne Ghys.

1. Definitions and notations

1.1. Random groups and density. The interest of random groups is twofold: first, to study which properties of groups are *generic*, i.e. shared by a large proportion of groups; second, to provide examples of new groups with given properties. This article falls under both approaches.

A random group is given by a random presentation, that is, the quotient of a free group $F_m = \langle a_1, \dots, a_m \rangle$ by (the normal closure of) a randomly chosen set $R \subset F_m$. Defining a random group is giving a law for the random set R.

More generally, a random quotient of a group G_0 is the quotient of G_0 by (the normal closure of) a randomly chosen subset $R \subset G_0$.

The philosophy of random groups was introduced by Gromov in [Gro87] through a statement that "almost every group is hyperbolic", the proof of which was later given by Ol'shanskiĭ ([Ols92]) and independently by Champetier ([Ch91, Ch95]). Gromov later defined the density model in [Gro93], in order to precisely control the quantity of relators put in a random group.

Since then random groups have gained broad interest and are connected to lots of topics in geometric or combinatorial group theory (such as the isomorphism problem, property T, Haagerup property, small cancellation, spectral gaps, the Baum–Connes conjecture…), especially since Gromov used them ([Gro03]) to build a counter-example to the Baum–Connes conjecture with coefficients (see also [HLS02]). We refer to [Oll05b] or [Gh03] for a general discussion on random groups and an extensive bibliography.

We now define the density model of random groups. In this model the random set of relations R depends on a density parameter d: the larger d, the larger R. This model exhibits a phase transition between infiniteness and triviality depending on the value of d; moreover, in the infinite phase some properties of the resulting group (such as the rank, property T or the Haagerup property) do differ depending on d, hence the interest of this model.

Definition 4 (Density model of quotient by random elements). Let G_0 be a group generated by the elements $a_1^{\pm 1}, \dots, a_m^{\pm 1}$ ($m \geqslant 2$). Let $B_\ell \subset G_0$ be the ball of radius ℓ in G_0 with respect to this generating set.

Let $d \geqslant 0$ be a density parameter.

Let R be a set of $(2m-1)^{d\ell}$ randomly chosen elements of B_ℓ, uniformly and independently picked in B_ℓ.

We call the group $G = G_0/\langle R\rangle$ a *quotient of* G_0 *by random elements*, at density d and at length ℓ.

In case G_0 is the free group F_m we simply call G a *random group* at density d and at length ℓ.

We sometimes also refer to this model as the *geodesic model* of random quotients.

In this definition, we can also replace B_ℓ by the sphere S_ℓ of elements of norm exactly ℓ, or by the annulus of elements of norm between ℓ and $\ell + C$ for some constant C: this does not affect our theorems. Compare Theorem 3 in [Oll04].

Another variant (the word variant) of random quotients consists in taking for R a set of reduced (or plain) random words in the generators $a_i^{\pm 1}$, which leads to a different probability distribution. Fortunately in the case of the free group, there is no difference between taking at random elements in B_ℓ or reduced words, so that the notions of random group and of a generic property of groups are well-defined anyway.

Quotienting by elements rather than words seems better suited to control the growth of the quotient (one works with elements of the group all the way long). However, the author believes that the same kind of proof would also work in the word model of random quotients, with a slightly more difficult argument.

The interest of the density model was established by the following theorem of Gromov, which shows a sharp phase transition between infinity and triviality of random groups.

Theorem 5 ([Gro93]). *Let $d < 1/2$. Then with probability tending to* 1 *as ℓ tends to infinity, random groups at density d are infinite hyperbolic.*

Let $d > 1/2$. Then with probability tending to 1 *as ℓ tends to infinity, random groups at density d are either $\{e\}$ or $\mathbb{Z}/2\mathbb{Z}$.*

(The occurrence of $\mathbb{Z}/2\mathbb{Z}$ is of course due to the case when ℓ is even and we take elements in the sphere S_ℓ; this disappears if one takes elements in B_ℓ, or of length between ℓ and $\ell + C$ with $C \geqslant 1$.)

Basically, $d\ell$ is to be interpreted as the "dimension" of the random set R (see the discussion in [Gro93]). As an illustration, if $L < 2d\ell$ then very probably there will be two relators in R sharing a common subword of length L. Indeed, the dimension of the pairs of relators in R is $2d\ell$, whereas sharing a common subword of length L amounts to L "equations", so the dimension of those pairs sharing a subword is $2d\ell - L$, which is positive if $L < 2d\ell$. This "shows" in particular that at density d, the small cancellation condition $C'(2d)$ is satisfied.

Since a random quotient of a free group is hyperbolic, one can wonder if a random quotient of a hyperbolic group is still hyperbolic. The answer is basically yes, and for the random elements variant, the critical density is in this case linked to the growth exponent of the initial group.

Theorem 6 ([Oll04], Theorem 3). *Let G_0 be a non-elementary, torsion-free hyperbolic group, generated by the elements $a_1^{\pm 1}, \dots, a_m^{\pm 1}$, with growth exponent g. Let $0 \leqslant d \leqslant g$ be a density parameter.*

If $d < g/2$, then a random quotient of G_0 by random elements at density d is infinite hyperbolic, with probability tending to 1 *as ℓ tends to infinity.*

If $d > g/2$, then a random quotient of G_0 by random elements at density d is either $\{e\}$ or $\mathbb{Z}/2\mathbb{Z}$, with probability tending to 1 *as ℓ tends to infinity.*

This is the context in which Theorem 2 is to be understood.

1.2. Hyperbolic groups and isoperimetry of van Kampen diagrams. Let G be a group given by the finite presentation $\langle a_1, \dots, a_m \mid R \rangle$. Let w be a word in the $a_i^{\pm 1}$'s. We denote by $|w|$ the number of letters of w, and by $\|w\|$ the distance from e to w in the Cayley graph of the presentation, that is, the minimal length of a word representing the same element of G as w.

Let λ be the maximal length of a relation in R.

We refer to [LS77] for the definition and basic properties of van Kampen diagrams. If D is a van Kampen diagram, we denote its number of faces by $|D|$ and its boundary length by $|\partial D|$.

It is well known (see for example [Sho91]) that G is hyperbolic if and only if there exists a constant $C_1 > 0$ such that for any word w representing the neutral

element of G, there exists a van Kampen diagram with boundary word w satisfying the isoperimetric inequality
$$|\partial D| \geqslant C_1 |D|.$$

We are going to use a slightly different way to write this inequality. Let D be a van Kampen diagram w.r.t. the presentation and define the *area* of D to be

$$\mathcal{A}(D) = \sum_{f \text{ face of } D} |\partial f|$$

which is also the number of external edges (not counting "filaments") plus twice the number of internal ones. Say a diagram is *minimal* if it has minimal area for a given boundary word.

It is immediate to see that if D satisfies $|\partial D| \geqslant C_1 |D|$, then we have $|\partial D| \geqslant C_1\, \mathcal{A}(D)/\lambda$ (recall λ is the maximal length of a relation in the presentation). Conversely, if $|\partial D| \geqslant C_2\, \mathcal{A}(D)$, then $|\partial D| \geqslant C_2 |D|$. So G is hyperbolic if and only if there exists a constant $C > 0$ such that every minimal van Kampen diagram satisfies the isoperimetric inequality
$$|\partial D| \geqslant C\, \mathcal{A}(D)$$
(where necessarily $C \leqslant 1$ unless G is free).

This inequality naturally arises in $C'(\alpha)$ small cancellation theory (with $C = 1 - 6\alpha$), in random groups at density d (with $C = \frac{1}{2} - d$, see [Oll-a]), in the assumptions of Champetier in [Ch93], in random quotients of hyperbolic groups (cf. [Oll04]) and in the (infinitely presented) limit groups constructed by Gromov in [Gro03]. Moreover there is a nice inequality between C and the hyperbolicity constant δ (Proposition 7 below).

The key feature of this formulation is that both $\mathcal{A}(D)$ and $|\partial D|$ scale the same way when the lengths of the relators change. This homogeneity property is crucial in our applications. So we think this is the right way to write the isoperimetric inequality when the lengths of the relators are very different.

Proposition 7. *Suppose that a hyperbolic group G given by some finite presentation satisfies the isoperimetric inequality*

$$|\partial D| \geqslant C\, \mathcal{A}(D)$$

for all minimal van Kampen diagrams D, for some constant $C > 0$.

Let λ be the maximal length of a relation in the presentation. Then the hyperbolicity constant δ of G satisfies
$$\delta \leqslant 12\lambda / C^2.$$

Proof. This is just a careful rewriting of classical proofs. Actually the proof of this is strictly included in [Sho91] (Theorem 2.5). Indeed, what the authors of [Sho91] prove is always of the form "the number of edges in D is at least something, so the number of faces of D is at most this thing divided by ρ" (in their notation ρ is the maximal length of a relation). Reasoning directly with the number of edges instead of the number of faces $|D|$ simplifies their arguments. But $\mathcal{A}(D)$ is simply twice the number of internal edges of D plus the number of boundary edges of D, so it is greater than the number of edges of D.

So simply by removing the seventh sentence in their proof of Lemma 2.6 (where the number of 2-cells of a diagram is evaluated by dividing the number of 1-cells by the maximal length of a relator ρ), we get a new Lemma 2.6 which reads (we stick to their notation in the framework of their proving Theorem 2.5)

Lemma 2.6 of [Sho91]. *If $\varepsilon > \rho$, then there is a constant C_1 depending solely on ε, such that the number of 1-cells in $N(\theta)$ is at least $\ell(\theta)\varepsilon/\rho - C_1$. Namely we can set $C_1 = \varepsilon(\varepsilon + \rho)/\rho$.*

Similarly, removing the last sentence of their proof of Lemma 2.7 we get a new version of it:

Lemma 2.7 of [Sho91]. *If $\varepsilon > \rho$, there is a constant C_2 depending solely on ε such that*

$$\mathcal{A}(D) > (\alpha + \beta + \gamma)\varepsilon/\rho - C_2 + 2r$$

where $\mathcal{A}(D)$ is the area of the diagram D. Namely we can set $C_2 = 3C_1 + 4\varepsilon + 2$.

We insist that those modified lemmas are obtained by *removing* some sentences in their proofs, and that there really is nothing to modify.

We still have to re-write the conclusion. In their notation α, β and γ are (up to 4ε) the lengths of the sides of some triangle which, by contradiction, is supposed not to be r-thin (we want to show that if r is large enough, then every triangle is r-thin).

The assumption $|\partial D| \geqslant C\,\mathcal{A}(D)$ reads

$$\mathcal{A}(D) \leqslant (\alpha + \beta + \gamma)/C + 12\varepsilon/C.$$

Combining this inequality and the result of Lemma 2.7, we have

$$(\alpha + \beta + \gamma)\varepsilon/\rho - C_2 + 2r \leqslant (\alpha + \beta + \gamma)/C + 12\varepsilon/C.$$

Now set $\varepsilon = \rho/C$. We thus obtain

$$2r \leqslant 12\rho/C^2 + C_2$$

where we recall that $C_2 = 3C_1+4\varepsilon+2 = 3\varepsilon(\varepsilon+\rho)/\rho+4\varepsilon+2 = \rho(3/C^2+7/C)+2$ with our choice of ε. Since $\rho \geqslant 1$ (unless G is free in which case there is nothing to prove) and necessarily $C \leqslant 1$ we have $7/C \leqslant 7/C^2$ and $2 \leqslant 2\rho/C^2$ and so finally

$$2r \leqslant 12\rho/C^2 + 12\rho/C^2$$

hence the conclusion, recalling that our δ and λ are [Sho91]'s r and ρ respectively. □

2. Growth of random quotients

We now turn to the main point of this paper, namely, evaluation of the growth exponent of a random quotient of a group.

2.1. Framework of the argument

Convention. Let G_0 be a non-elementary torsion-free hyperbolic group given by the finite presentation $G_0 = \langle a_1, \dots, a_m \mid Q \rangle$. Let $g > 0$ be the growth exponent of G_0 with respect to this generating set. Let B_ℓ be the set of elements of norm at most ℓ. Let λ be the maximal length of a relation in Q.

Let also R be a randomly chosen set of $(2m-1)^{d\ell}$ elements of the ball $B_\ell \subset G_0$, in accordance with the model of random quotients we retained (Definition 4). Set $G = G_0/\langle R \rangle$, the random quotient we are interested in. We will call the relators in R "new relators" and those in Q "old relators".

In the sequel, the phrase "with overwhelming probability" will mean "with probability exponentially tending to 1 as $\ell \to \infty$ (depending on everything)".

Fix some $\varepsilon > 0$. We want to show that the growth exponent of G is at least $g(1-\varepsilon)$, with overwhelming probability.

We can suppose that the length ℓ is taken large enough so that, for $L \geqslant \ell$, we have $(2m-1)^{gL} \leqslant |B_L| \leqslant (2m-1)^{g(1+\varepsilon)L}$.

Let $\mathcal{B}_L$ be the ball of radius L in G. We trivially have $|\mathcal{B}_L| \leqslant |B_L|$.

We will prove a lower bound for the cardinality of $\mathcal{B}_L$ for some well chosen L, and then use Proposition 17. In order to apply this proposition, we first need an estimate of the hyperbolicity constant of G.

Proposition 8. *With overwhelming probability, minimal van Kampen diagrams of G satisfy the isoperimetric inequality*

$$|\partial D| \geqslant C\,\mathcal{A}(D)$$

where $C > 0$ is a constant depending on G_0 and the density d but not on ℓ. In particular, the hyperbolicity constant δ of G is at most $12\ell/C^2$.

Proof. This is a rephrasing of Proposition 32 (p. 640) of [Oll04]: With overwhelming probability, minimal van Kampen diagrams D of the random quotient G satisfy the isoperimetric inequality

$$|\partial D| \geqslant \alpha_1 \ell |D''| + \alpha_2 |D'|$$

where α_1, α_2 are positive constants depending on G_0 and the density parameter d (but not on ℓ), and $|D''|$, $|D'|$ are respectively the number of faces of D bearing new relators (from R) and old relators (from Q). Since new relators have length at most ℓ and old relators have length at most λ, by definition we have $\mathcal{A}(D) \leqslant \ell|D''| + \lambda|D'|$ and so setting $C = \min(\alpha_1, \alpha_2/\lambda)$ yields

$$|\partial D| \geqslant C\,\mathcal{A}(D).$$

The estimate of the hyperbolicity constant follows by Proposition 7. □

In particular, in order to apply Proposition 17 it is necessary to control the cardinality of balls of radius roughly $\ell/C^2 + 1/g$. More precisely, let $A \geqslant 500$ be such that $40/A \leqslant \varepsilon/2$. Set $L_0 = 24\ell/C^2 + 4/g$ and $L = AL_0$. We already trivially know that $|\mathcal{B}_{L_0}| \leqslant (2m-1)^{g(1+\varepsilon)L_0}$. We will now show that, with overwhelming probability, we have $|\mathcal{B}_L| \geqslant (2m-1)^{g(1-\varepsilon/2)L}$. Once this is done we can conclude by Proposition 17.

The strategy to evaluate the growth of the quotient G of G_0 will be the following: There are at least $(2m-1)^{gL}$ elements in B_L. Some of these elements are identified in G. Let N be the number of equalities of the form $x = y$, for $x, y \in B_L$, which hold in G but did not hold in G_0. Each such equality decreases the number of elements of $\mathcal{B}_L$ by at most 1. Hence, the number of elements of norm at most L in G is at least $(2m-1)^{gL} - N$. So if we can show for example that $N \leqslant \frac{1}{2}(2m-1)^{gL}$, we will have a lower bound for the size of balls in G.

So we now turn to counting the number of equalities $x = y$ holding in G but not in G_0, with $x, y \in B_L$. Each such equality defines a (minimal) van Kampen diagram with boundary word xy^{-1}, of boundary length at most $2L$. We will need the properties of van Kampen diagrams of G proven in [Oll04].

So, for the ε and A fixed above, let $A' = 2L/\ell$ and let D be a minimal van Kampen diagram of G, of boundary length at most $A'\ell$. By the isoperimetric inequality $|\partial D| \geqslant C\mathcal{A}(D)$, we know that the number $|D''|$ of faces of D bearing a new relator of R is at most A'/C. So for all the sequel set

$$K = A'/C$$

which is the maximal number of new relators in the diagrams we have to consider (which will also have area at most $K\ell$). Most importantly, this K does not depend on ℓ.

2.2. A review of [Oll04]. In this context, it is proven in [Oll04] that the van Kampen diagram D can be seen as a "van Kampen diagram at scale ℓ with respect to the new relators, with equalities modulo G_0". More precisely, this can be stated as follows: (we refer to [Oll04] for the definition of "strongly reduced" diagrams; the only thing to know here is that for any word equal to e in G, there exists a strongly reduced van Kampen diagram with this word as its boundary word).

Proposition 9 ([Oll04], Section 6.6). *Let $G_0 = \langle S \mid Q \rangle$ be a non-elementary hyperbolic group, let R be a set of words of length ℓ, and consider the group $G = G_0/\langle R \rangle = \langle S \mid Q \cup R \rangle$.*

Let $K \geqslant 1$ be an arbitrarily large integer and let $\varepsilon_1, \varepsilon_2 > 0$ be arbitrarily small numbers. Take ℓ large enough depending on $G_0, K, \varepsilon_1, \varepsilon_2$.

Let D be a van Kampen diagram with respect to the presentation $\langle S \mid Q \cup R \rangle$, which is strongly reduced, of area at most $K\ell$. Let also D' be the subdiagram of D which is the union of the 1-skeleton of D and of those faces of D bearing relators in Q (so D' is a possibly non-simply connected van Kampen diagram with respect to G_0), and suppose that D' is minimal.

We will call worth-considering *such a van Kampen diagram.*

Let $w_1, \dots, w_p$ be the boundary (cyclic) words of D', so that each w_i is either the boundary word of D or a relator in R.

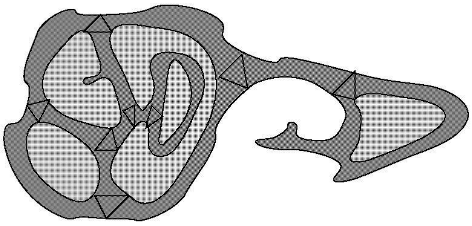
Then there exists an integer $k \leqslant 3K/\varepsilon_2$ and words $x_2, \dots, x_{2k+1}$ such that:

- *Each x_i is a subword of some cyclic word w_j.*
- *As subwords of the w_j's, the x_i's are disjoint and their union exhausts a proportion at least $1 - \varepsilon_1$ of the total length of the w_j's.*
- *For each $i \leqslant k$, there exists words δ_1, δ_2 of length at most $\varepsilon_2(|x_{2i}| + |x_{2i+1}|)$ such that $x_{2i}\delta_1 x_{2i+1}\delta_2 = e$ in G_0.*
- *If two words x_{2i}, x_{2i+1} are subwords of the boundary words of two faces of D bearing the same relator $r^{\pm 1} \in R$, then, as subwords of r, x_{2i} and x_{2i+1} are either disjoint or equal with opposite orientations (so that the above equality reads $x\delta_1 x^{-1}\delta_2 = e$).*

The pairs (x_{2i}, x_{2i+1}) are called translators. *Translators are called* internal, internal-boundary *or* boundary-boundary *according to whether x_{2i} and x_{2i+1} is a subword of some w_j which is a relator in R or the boundary word of D.*

(There are slight differences between the presentation here and that in [Oll04]. Therein, boundary-boundary translators did not have to be considered: they were eliminated earlier in the process, before Section 6.6, because they have a positive contribution to boundary length, hence always improve isoperimetry and do not deserve consideration in order to prove hyperbolicity. Moreover, in [Oll04] we further distinguished "commutation translators" for the kind of internal translator with $x_{2i} = x_{2i+1}^{-1}$, which we need not do here.)

Translators appear as dark strips on the following figure:



Remark 10. Since there are at most $3K/\varepsilon_2$ translators, the total length of the translators (x_{2i}, x_{2i+1}) for which $|x_{2i}| + |x_{2i+1}| \leqslant \varepsilon_3 \ell$ is at most $3K\ell\varepsilon_3/\varepsilon_2$, which makes a proportion at most $3\varepsilon_3/\varepsilon_2$ of the total length. So, setting $\varepsilon_3 = \varepsilon_1\varepsilon_2/3$ and replacing ε_1 with $\varepsilon_1/2$, we can suppose that the union of the translators exhausts a proportion at least $1 - \varepsilon_1$ of the total length of the diagram, and that each translator (x_{2i}, x_{2i+1}) satisfies $|x_{2i}| + |x_{2i+1}| \geqslant \varepsilon_1\varepsilon_2\ell/6$.

Remark 11. The number of ways to partition the words w_i into translators is at most $(2K\ell)^{12K/\varepsilon_2}$, because each w_i can be determined by its starting- and endpoint, which can be given as numbers between 1 and $2K\ell$ which is an upper bound for the cumulated length of the w_i's (since the area of D is at most $K\ell$). For fixed K and ε_2 this grows subexponentially in ℓ.

Remark 12. Knowing the words x_i, the number of possibilities for the boundary word of the diagram is at most $(6K/\varepsilon_2)!$ (choose which subwords x_i make the boundary word of the diagram, in which order), which does not depend on ℓ for fixed K and ε_2.

We need another notion from [Oll04], namely, that of *apparent length* of an element in G_0. Apparent length is defined in [Oll04] in a more general setting, with respect to a family of measures on the group depending on the precise model of random quotient at play. Here these are simply the uniform measures on the balls B_ℓ. So we only give here what the definition amounts to in our context. In fact we will not use here the full strength of this notion, but we still need to define it in order to state results from [Oll04].

Recall that in the geodesic model of random quotients, the axioms of [Oll04] are satisfied with $\beta = g/2$ and $\kappa_2 = 1$, by Proposition 20 of [Oll04].

Definition 13 ([Oll04], p. 652). Let $x \in G_0$. Let $\varepsilon_2 > 0$. Let L be an integer. Let $p_L(xuyv = e)$ be the probability that, for a random element $y \in B_L$, there exist elements $u, v \in G_0$ of norm at most $\varepsilon_2(\|x\| + L)$ such that $xuyv = e$ in G_0.

The *apparent length* of x at test-length L is

$$\mathbb{L}_L(x) = -\tfrac{2}{g} \log_{2m-1} p_L(xuyv = e) - L.$$

The *apparent length* of x is

$$\mathbb{L}(x) = \min\left(\|x\|,\ \min_{0\leqslant L\leqslant K\ell} \mathbb{L}_L(x)\right)$$

where we recall ℓ is the length of the relators in a random presentation.

We further need the notion of a *decorated abstract van Kampen diagram* (which was implicitly present in the free case when we mentioned the probability that some diagram "is fulfilled by random relators"), which is inspired by Proposition 9: it carries the combinatorial information about how the relators and boundary word of a diagram were cut into subwords in order to make the translators.

Definition 14 (Decorated abstract van Kampen diagram). Let $K \geqslant 1$ be an arbitrarily large integer and let $\varepsilon_1, \varepsilon_2 > 0$ be arbitrarily small numbers. Let I_ℓ be the cyclically ordered set of ℓ elements.

A *decorated abstract van Kampen diagram* $\mathcal{D}$ is the following data:

- An integer $|\mathcal{D}| \leqslant K$ called its *number of faces*.
- An integer $|\partial\mathcal{D}| \leqslant K\ell$ called its *boundary length*.
- An integer $n \leqslant |\mathcal{D}|$ called its *number of distinct relators*.
- An application $r^{\mathcal{D}}$ from $\{1,\dots,|\mathcal{D}|\}$ to $\{1,\dots,n\}$; if $r^{\mathcal{D}}(i) = r^{\mathcal{D}}(j)$ we will say that *faces i and j bear the same relator*.
- An integer $k \leqslant 3K/\varepsilon_2$ called the *number of translators* of $\mathcal{D}$.
- For each integer $2 \leqslant i \leqslant 2k+1$, a set of the form $\{j_i\} \times I'_i$ where either j_i is an integer between 1 and $|\mathcal{D}|$ and I'_i is an oriented cyclic subinterval of I_ℓ, or $j_i = |\mathcal{D}|+1$ and I'_i is a subinterval of $I_{|\partial\mathcal{D}|}$; this is called an *(internal) subword of the j_i-th face* in the first case, or a *boundary subword* in the second case.
- For each integer $1 \leqslant i \leqslant k$ such that $j_{2i} \leqslant |\mathcal{D}|$, an integer between 0 and 4ℓ called the *apparent length of the $2i$-th subword.*

such that

- The sets $\{j_i\} \times I'_i$ are all disjoint and the cardinal of their union is at least $(1-\varepsilon_1)\,(|\mathcal{D}|\ell + |\partial\mathcal{D}|)$.
- For all $1 \leqslant i \leqslant k$ we have $j_{2i} \leqslant j_{2i+1}$ (this can be ensured by maybe swapping them).
- If two faces j_{2i} and j_{2i+1} bear the same relator, then either I'_{2i} and I'_{2i+1} are disjoint or are equal with opposite orientations.

This way, Proposition 9 ensures that any worth-considering van Kampen diagram D with respect to $G_0/\langle R\rangle$ defines a decorated abstract van Kampen diagram $\mathcal{D}$ in the way suggested by terminology (up to rounding the apparent lengths to the nearest integer; we neglect this problem). We will say that $\mathcal{D}$ is *associated to* D. Remark 11 tells that the number of decorated abstract van Kampen diagrams grows subexponentially with ℓ (for fixed K).

Given a decorated abstract van Kampen diagram $\mathcal{D}$ and n given relators $r_1, \dots, r_n$, we say that these relators *fulfill* $\mathcal{D}$ if there exists a worth-considering van Kampen diagram D with respect to $G_0/\langle r_1, \dots, r_n\rangle$, such that the associated decorated abstract van Kampen diagram is $\mathcal{D}$. Intuitively speaking, the relators $r_1, \dots, r_n$ can be "glued modulo G_0 in the way described by $\mathcal{D}$".

So we want to study which diagrams can probably be fulfilled by random relators in R. The main conclusion from [Oll04] is that these are those with large boundary length, hence hyperbolicity of the quotient $G_0/\langle R\rangle$. Here for growth we are rather interested in the number of different elements of G_0 that can appear as boundary words of fulfillable abstract diagrams with given boundary length (recall that our goal is to evaluate the number of equalities $x = y$ holding in G but not in G_0, with x and y elements of norm at most L).

2.3. Evaluation of growth. We now turn back to random quotients: R is a set of $(2m-1)^{d\ell}$ randomly chosen elements of B_ℓ. Recall we set $L = A'\ell/2$ for some value of A' ensuring that if we know that $|\mathcal{B}_L| \geqslant (2m-1)^{g(1-\varepsilon/2)L}$ then we know that the growth exponent of $G = G_0/\langle R\rangle$ is at least $g(1-\varepsilon)$.

We want to get an upper bound for the number N of pairs $x, y \in B_L$ such that $x = y$ in G but $x \neq y$ in G_0. For any such pair there is a worth-considering van Kampen diagram D with boundary word xy^{-1}, of boundary length at most $A'\ell$, with at most $K = A'/C$ new relators, and at least one new relator (otherwise the equality $x = y$ would already occur in G_0). Let $\mathcal{D}$ be the decorated abstract van Kampen diagram associated to D. Note that we have to count the number of different pairs $x, y \in B_L$ and *not* the number of different boundary words of van Kampen diagrams: since each x and y may have numerous different representations as a word, the latter is higher than the former.

We will show that, with overwhelming probability, we have $N \leqslant \frac{1}{2}(2m-1)^{gL}$.

The up to now free parameters ε_1 and ε_2 (in the definitions of decorated abstract van Kampen diagrams and of apparent length) will be fixed in the course of the proof, depending on G_0, g and d but not on ℓ. The length ℓ upon which our argument works will be set depending on everything including ε_1 and ε_2.

Further notations. Let n be the number of distinct relators in $\mathcal{D}$. We only have to consider van Kampen diagrams in G which were not already van Kampen diagrams in G_0, so that there is at least one new relator i.e. $n \geqslant 1$. For $1 \leqslant a \leqslant n$, let m_a be the number of times the a-th relator appears in $\mathcal{D}$. Up to reordering, we can suppose that the m_a's are non-increasing. Also to avoid trivialities take n minimal so that $m_n \geqslant 1$.

Let also P_a be the probability that, if a words $r_1, \dots, r_a$ of length ℓ are picked at random, there exist $n-a$ words $r_{a+1}, \dots, r_n$ of length ℓ such that the relators $r_1, \dots, r_n$ fulfill $\mathcal{D}$. The P_a 's are of course a non-increasing sequence of probabilities. In particular, P_n is the probability that a random n-tuple of relators fulfills $\mathcal{D}$.

Back to our set R of $(2m-1)^{d\ell}$ randomly chosen relators. Let P^a be the probability that there exist a relators $r_1, \dots, r_a$ in R, such that there exist words $r_{a+1}, \dots, r_n$ of length ℓ such that the relators $r_1, \dots, r_n$ fulfill $\mathcal{D}$. Again the P^a 's are a non-increasing sequence of probabilities and of course we have

$$P^a \leqslant (2m-1)^{ad\ell} P_a$$

since the $(2m-1)^{ad\ell}$ factor accounts for the choice of the a-tuple of relators in R.

The probability that there exists a van Kampen diagram D with respect to the random presentation R, such that $\mathcal{D}$ is associated to D, is by definition less than P^a for any a. In particular, if for some $\mathcal{D}$ we have $P^a \leqslant (2m-1)^{-\varepsilon'\ell}$, then with overwhelming probability, $\mathcal{D}$ is not associated to any van Kampen diagram of the random presentation. Since, by Remark 11, the number of possibilities for $\mathcal{D}$ grows subexponentially with ℓ, we can sum this over $\mathcal{D}$ and conclude that for any $\varepsilon' > 0$, with overwhelming probability (depending on ε'), all decorated abstract van Kampen diagrams $\mathcal{D}$ associated to some van Kampen diagram of the random presentation satisfy $P^a \geqslant (2m-1)^{-\varepsilon'\ell}$ and in particular

$$P_a \geqslant (2m-1)^{-ad\ell-\varepsilon'\ell}$$

which we assume from now on.

We need to define one further quantity. Keep the notations of Definition 14. Let $1 \leqslant a \leqslant n$ and let $1 \leqslant i \leqslant k$ where k is the number of translators of $\mathcal{D}$. Say that the i-th translator is half finished at time a if $r^{\mathcal{D}}(j_{2i}) \leqslant a$ and $r^{\mathcal{D}}(j_{2i+1}) > a$, that is, if one side of the translator is a subword of a relator $r_{a'}$ with $a' \leqslant a$ and the other of $r_{a''}$ with $a'' > a$. Now let A_a be the sum of the apparent lengths of all translators which are half finished at time a. In particular, A_n is the sum of the apparent lengths of all subwords $2i$ such that $2i$ is an internal subword and $2i+1$ is a boundary subword of $\mathcal{D}$.

Proof of Theorem 2. We first give some intermediate results.

Proposition 15. *With overwhelming probability, we can suppose that any decorated abstract van Kampen diagram $\mathcal{D}$ satisfies*

$$A_n(\mathcal{D}) \geqslant \ell\alpha/g + \tfrac{2}{g}(d'_n(\mathcal{D}) + nd\ell)$$

where $\alpha = g/2 - d > 0$ and $d'_a(\mathcal{D}) = \log_{2m-1} P_a(\mathcal{D})$.

Proof. In our context, equation ($\star$) (p. 659) of [Oll04] reads

$$A_a - A_{a-1} \geqslant m_a \left(\ell(1-\varepsilon'') + \frac{\log_{2m-1} P_a - \log_{2m-1} P_{a-1}}{\beta} \right)$$

where ε'' tends to 0 when our free parameters $\varepsilon_1, \varepsilon_2$ tend to 0 (and ε'' also absorbs the $o(\ell)$ term in [Oll04]). Also recall that in the model of random quotient by random elements of balls we have

$$\beta = g/2$$

by Proposition 20 (p. 628) of [Oll04].

Summing over a we get, using $\sum m_a = |\mathcal{D}|$, that

$$\begin{aligned} A_n &\geqslant \left(\sum m_a\right)\ell(1-\varepsilon'') + \frac{2}{g}\sum m_a(d'_a - d'_{a-1}) \\ &= |\mathcal{D}|\ell(1-\varepsilon'') + \frac{2}{g}\sum d'_a(m_a - m_{a+1}). \end{aligned}$$

Now recall we saw above that for any $\varepsilon' > 0$, taking ℓ large enough we can suppose that $P_a \geqslant (2m-1)^{-ad\ell - \varepsilon'\ell}$, that is, $d'_a + ad\ell + \varepsilon'\ell \geqslant 0$. Hence

$$\begin{aligned} A_n &\geqslant |\mathcal{D}|\ell(1-\varepsilon'') + \frac{2}{g}\sum(d'_a + ad\ell + \varepsilon'\ell)(m_a - m_{a+1}) \\ &\quad - \frac{2}{g}\sum(ad\ell + \varepsilon'\ell)(m_a - m_{a+1}) \\ &= |\mathcal{D}|\ell(1-\varepsilon'') + \frac{2}{g}\sum(d'_a + ad\ell + \varepsilon'\ell)(m_a - m_{a+1}) - \frac{d\ell}{g/2}\sum m_a - \frac{\varepsilon'\ell}{g/2}m_1 \\ &\geqslant |\mathcal{D}|\ell(1-\varepsilon'') + \frac{d'_n + nd\ell + \varepsilon'\ell}{g/2}m_n - \frac{d\ell + \varepsilon'\ell}{g/2}\sum m_a \end{aligned}$$

where the last inequality follows from the fact that we chose the order of the relators so that $m_a - m_{a+1} \geqslant 0$.

So using $m_n \geqslant 1$ we finally get

$$A_n \geqslant |\mathcal{D}|\ell\left(1 - \varepsilon'' - \frac{d+\varepsilon'}{g/2}\right) + \frac{d'_n + nd\ell}{g/2}.$$

Set $\alpha = g/2 - d > 0$ so that this rewrites

$$A_n \geqslant \frac{2}{g}\left(|\mathcal{D}|\ell(\alpha - \varepsilon' - \varepsilon'' g/2) + d'_n + nd\ell\right).$$

Suppose the free parameters ε_1, ε_2 and ε' are chosen small enough so that $\varepsilon' + \varepsilon'' g/2 \leqslant \alpha/2$ (recall that ε'' is a function of ε_1, ε_2 and K, tending to 0 when ε_1 and ε_2 tend to 0). Since $|\mathcal{D}| \geqslant 1$ (because we are counting diagrams expressing equalities not holding in G_0) we get $A_n \geqslant \ell\alpha/g + \frac{2}{g}(d'_n + nd\ell)$. □

Let us translate back this inequality into a control on the numbers of n-tuples of relators fulfilling $\mathcal{D}$.

Proposition 16. *With overwhelming probability, we can suppose that for any decorated abstract van Kampen diagram $\mathcal{D}$, the number of n-tuples of relators in R fulfilling $\mathcal{D}$ is at most*

$$(2m-1)^{-\alpha\ell/2+gA_n(\mathcal{D})/2+\varepsilon'\ell}.$$

Proof. Recall that, by definition, d'_n is the log-probability that n random relators $r_1, \dots, r_n$ fulfill $\mathcal{D}$. As there are $(2m-1)^{nd\ell}$ n-tuples of random relators in R (by definition of the density model), by linearity of expectation the expected number of n-tuples of relators in R fulfilling $\mathcal{D}$ is $(2m-1)^{nd\ell+d'_n}$.

By the Markov inequality, for given $\mathcal{D}$ the probability to pick a random set R such that the number of n-tuples of relators of R fulfilling $\mathcal{D}$ is greater than $(2m-1)^{nd\ell+d'_n+\varepsilon'\ell}$, is less than $(2m-1)^{-\varepsilon'\ell}$. Using Proposition 15, the result then follows for fixed $\mathcal{D}$. But by Remark 11 the number of possibilities for $\mathcal{D}$ is subexponential in ℓ, hence the conclusion. □

Let us now turn back to the evaluation of the number of elements x, y in $B_L \subset G_0$ forming a van Kampen diagram D with boundary word xy^{-1}. For each such pair x, y fix some geodesic writing of x and y as words. We will first suppose that the abstract diagram $\mathcal{D}$ associated to D is fixed and evaluate the number of possible pairs x, y in function of $\mathcal{D}$, and then, sum over the possible abstract diagrams $\mathcal{D}$.

So suppose $\mathcal{D}$ is fixed. Recall Proposition 9: the boundary word of D is determined by giving two words for each boundary-boundary translator, and one word for each internal-boundary translator, this last one being subject to the apparent length condition imposed in the definition of $\mathcal{D}$. By Remark 12, the number of ways to combine these subwords into a boundary word for D is controlled by K and ε_2 (independently of ℓ).

In all the sequel, in order to avoid heavy notations, the notation $\varepsilon^\star$ will denote some function of ε', ε_1 and ε_2, varying from time to time, and increasing when needed. The important point is that $\varepsilon^\star$ tends to 0 when ε', ε_1, ε_2 do.

Let (x_{2i}, x_{2i+1}) be a translator in D. The definition of translators implies that there exist short words δ_1, δ_2, of length at most $\varepsilon_2(|x_{2i}| + |x_{2i+1}|)$, such that $x_{2i}\delta_1 x_{2i+1}\delta_2 = e$ in G_0. The words x_{2i} and x_{2i+1} are either subwords of the geodesic words x and y making the boundary of D, or subwords of relators in R; by definition of the geodesic model of random quotients, the relators are geodesic as well. So in either case x_{2i} and x_{2i+1} are geodesic[1]. Thus, the equality $x_{2i}\delta_1 x_{2i+1}\delta_2 = e$ implies

[1]Except maybe in the case when the translator straddles the end of x and the beginning of y or conversely, or when it straddles the beginning and end of a relator; these cases can be treated immediately by further subdividing the translator, so we ignore this problem.

that $\|x_{2i+1}\| \leqslant \|x_{2i}\|(1+\varepsilon^\star)$ and conversely. Also, by Remark 10, we can suppose that $\|x_{2i}\| + \|x_{2i+1}\| \geqslant \ell\varepsilon_1\varepsilon_2/6$, hence $\|x_{2i}\| \geqslant \ell\varepsilon_1\varepsilon_2(1-\varepsilon^\star)/12$.

By definition of the growth exponent, there is some length ℓ_0 depending only on G_0 such that if $\ell'_0 \geqslant \ell_0$, then the cardinal of $B_{\ell'_0}$ is at most $(2m-1)^{g(1+\varepsilon')\ell'_0}$. So, if ℓ is large enough (depending on G_0, ε_1, ε_2 and ε') to ensure that $\ell\varepsilon_1\varepsilon_2(1-\varepsilon^\star)/12 \geqslant \ell_0$, we can apply such an estimate to any x_{2i}.

To determine the number of possible pairs x, y, we have to determine the number of possibilities for each boundary-boundary or internal-boundary translator (x_{2i}, x_{2i+1}) (since by definition internal translators do not contribute to the boundary).

First suppose that (x_{2i}, x_{2i+1}) is a boundary-boundary translator. Knowing the constraint $x_{2i}\delta_1 x_{2i+1}\delta_2 = e$, if x_{2i} and $\delta_{1,2}$ are given then x_{2i+1} is determined (as an element of G_0). Now the number of possibilities for δ_1 and δ_2 is at most $(2m-1)^{2\varepsilon_2(\|x_{2i}\|+\|x_{2i+1}\|)}$. Furthermore, the number of possibilities for x_{2i} is at most $(2m-1)^{g(1+\varepsilon')\|x_{2i}\|}$ which, since $\|x_{2i}\| \leqslant \frac{1}{2}(\|x_{2i}\|+\|x_{2i+1}\|)(1+\varepsilon^\star)$, is at most $(2m-1)^{\frac{g}{2}(\|x_{2i}\|+\|x_{2i+1}\|)(1+\varepsilon^\star)}$. So the total number of possibilities for a boundary-boundary translator (x_{2i}, x_{2i+1}) is at most

$$(2m-1)^{\frac{g}{2}(\|x_{2i}\|+\|x_{2i+1}\|)(1+\varepsilon^\star)}$$

where of course the feature to remember is that the exponent is basically $g/2$ times the total length $\|x_{2i}\| + \|x_{2i+1}\|$ of the translator.

Now suppose that (x_{2i}, x_{2i+1}) is an internal-boundary translator. The word x_{2i} is by definition a subword of some relator $r_i \in R$. So if a set of relators fulfilling $\mathcal{D}$ is fixed then x_{2i} is determined (we will multiply later by the number of possibilities for the relators, using Proposition 16). As above, the number of possibilities for δ_1 and δ_2 is at most $(2m-1)^{\varepsilon^\star\|x_{2i}\|}$. Once x_{2i}, δ_1 and δ_2 are given, then x_{2i+1} is determined (as an element of G_0). So, if a set of relators fulfilling $\mathcal{D}$ is fixed, then the number of possibilities for x_{2i+1} is at most $(2m-1)^{\varepsilon^\star\|x_{2i}\|}$, which reflects the fact that the set of relators essentially determines the internal-boundary translators.

Let A'_n be the sum of $\|x_{2i+1}\|$ for all internal-boundary translators (x_{2i}, x_{2i+1}). Let B be the sum of $\|x_{2i}\| + \|x_{2i+1}\|$ for all boundary-boundary translators. By definition we have $|\partial\mathcal{D}| = A'_n + B$ maybe up to $\varepsilon_1 K\ell$.

So if a set of relators fulfilling $\mathcal{D}$ is fixed, then the total number of possibilities for the boundary of D is at most

$$(2m-1)^{\frac{g}{2}B(1+\varepsilon^\star)+\varepsilon^\star A'_n}$$

which, since both B and A'_n are at most $K\ell$, is at most

$$(2m-1)^{gB/2+K\ell\varepsilon^\star}$$

(note that A'_n does not come into play, since once the relators fulfilling $\mathcal{D}$ are given, the internal-boundary translators are essentially determined).

The number of possibilities for an n-tuple of relators fulfilling $\mathcal{D}$ is given by Proposition 16: it is at most $(2m-1)^{-\alpha\ell/2+gA_n/2+\varepsilon^\star\ell}$ (recall $\alpha = g/2 - d$), so that the total number of possibilities for the boundary of D is at most

$$(2m-1)^{-\alpha\ell/2+(B+A_n)g/2+K\ell\varepsilon^\star}.$$

Recall that A_n is the sum of $\mathbb{L}(x_{2i})$ for all internal-boundary translators (x_{2i}, x_{2i+1}). By definition of apparent length we have $\mathbb{L}(x_{2i}) \leqslant \|x_{2i}\|$. Since in an internal-boundary translator (x_{2i}, x_{2i+1}) we have $\|x_{2i}\| \leqslant \|x_{2i+1}\|(1+\varepsilon^\star)$, we get, after summing on all internal-boundary translators, that $A_n \leqslant A'_n + K\ell\varepsilon^\star$. In particular, the above is at most

$$(2m-1)^{-\alpha\ell/2+(B+A'_n)g/2+K\ell\varepsilon^\star}.$$

Now recall that by definition we have $|\partial\mathcal{D}| = B + A'_n$ maybe up to $\varepsilon_1 K\ell$ so that the above is in turn at most

$$(2m-1)^{-\alpha\ell/2+|\partial\mathcal{D}|g/2+K\varepsilon^\star\ell}.$$

This was for one decorated abstract van Kampen diagram $\mathcal{D}$. But by Remark 11, the number of such diagrams is subexponential in ℓ (for fixed K and ε_2), and so, up to increasing $\varepsilon^\star$, this estimate holds for all diagrams simultaneously.

2.4. Conclusion. Remember the discussion in the beginning of Section 2. We wanted to show that the cardinal $|\mathcal{B}_L|$ of the ball of radius L in G was at least $(2m-1)^{gL(1-\varepsilon/2)}$ for some ε chosen at the beginning of our work.

We just proved that the number N of pairs of elements x, y in B_L such that there exists a van Kampen diagram expressing the equality $x = y$ in G, but such that $x \neq y$ in G_0 (which was expressed in the above argument by using that D had at least one new relator) is at most

$$(2m-1)^{-\alpha\ell/2+(\|x\|+\|y\|)g/2+K\varepsilon^\star\ell}$$

where $\alpha = g/2 - d > 0$.

Now fix the free parameters $\varepsilon', \varepsilon_1, \varepsilon_2$ so that $K\varepsilon^\star \leqslant \alpha/4$ (this depends on K and G_0 but not on ℓ; K itself depends only on G_0). Choose ℓ large enough so that all the estimates used above (implying every other variable) hold. Also choose ℓ large enough (depending on d) so that $(2m-1)^{-\alpha\ell/4} \leqslant 1/2$. We get

$$N \leqslant \tfrac{1}{2}(2m-1)^{(\|x\|+\|y\|)g/2} \leqslant \tfrac{1}{2}(2m-1)^{gL}$$

since by assumption $\|x\|$ and $\|y\|$ are at most L. But on the other hand we have $|B_L| \geqslant (2m-1)^{gL}$ and so

$$|\mathcal{B}_L| \geqslant |B_L| - N \geqslant \tfrac{1}{2}(2m-1)^{gL} \geqslant (2m-1)^{gL(1-\varepsilon/2)}$$

as soon as ℓ is large enough (since L grows like ℓ), which ends the proof.

Appendix. Locality of growth in hyperbolic groups

The goal of this section is to show that, in a hyperbolic group, if we know an estimate of the growth exponent in some finite ball of the group, then this provides an estimate of the growth exponent of the group (whose quality depends on the radius of the given finite ball).

Let $G = \langle a_1, \dots, a_m \mid R \rangle$ be a δ-hyperbolic group generated by the elements $a_i^{\pm 1}$, with $m \geqslant 2$. For $x \in G$ let $\|x\|$ be the norm of x with respect to this generating set. Let B_ℓ be the set of elements of norm at most ℓ.

Proposition 17. *Suppose that for some $g > 0$, for some $\ell_0 \geqslant 2\delta + 4/g$ and $\ell_1 \geqslant A\ell_0$, with $A \geqslant 500$, we have*

$$|B_{\ell_0}| \leqslant (2m-1)^{1.1g\ell_0}$$

and

$$|B_{\ell_1}| \geqslant (2m-1)^{g\ell_1}.$$

Then the growth exponent of G is at least $g(1 - 40/A)$.

Note that the occurrence of $1/g$ in the scale upon which the proposition is true is natural: indeed, an assumption such as $|B_\ell| \geqslant (2m-1)^{g\ell}$ for $\ell < 1/g$ is not very strong... The growth g can be thought of as the inverse of a length, so this result is homogeneous.

Corollary 18. *The growth exponent of a presentation of a hyperbolic group is computable. That is, there exists an algorithm which, for any input made of a finite presentation of a hyperbolic group and an $\varepsilon > 0$, outputs a number g together with a proof that the growth exponent of the given presentation lies between $g - \varepsilon$ and $g + \varepsilon$.*

This corollary was already known: indeed, once δ is known one can compute (see [GhH90]) a finite automaton accepting some normal geodesic form of all elements in the group, and this in turn implies that the growth series is a rational function with explicitly computable coefficients; now the growth exponent is linked to the radius of convergence of this series, which is computable in the case of a rational function. Whereas in this approach, the exact value of the growth exponent is determined very indirectly by the full algebraic structure of some finite ball, our approach directly relates an approximate value of the growth exponent to that observed in this finite ball.

Proof. Indeed, recall from [Pap96] (after [Gro87]) that the hyperbolicity constant δ of a presentation of a hyperbolic group is computable. Thanks to the isoperimetric inequality, the word problem in a hyperbolic group is solvable, so that for any ℓ an exact computation of the cardinal of B_ℓ is possible. Setting $g_\ell = \frac{1}{\ell}\log_{2m-1}|B_\ell|$, we know that g_ℓ will converge to some (unknown) positive value, so that g_ℓ and $g_{A\ell}$ will become arbitrarily close, and since g_ℓ is bounded from below sooner or later we will have $\ell \geqslant 2\delta + 4/g_{A\ell}$, in which case we can apply the proposition to ℓ and $A\ell$. □

Proof of the proposition. Let (,) denote the Gromov product in G, with origin at e, that is

$$(x, y) = \frac{1}{2}(\|x\| + \|y\| - \|x - y\|)$$

for $x, y \in G$, where, following [GhH90], we write $\|x - y\|$ for $\|x^{-1}y\| = \|y^{-1}x\|$. Since triangles are δ-thin, we have ([GhH90], Proposition 2.21) for any three points x, y, z in G

$$(x, z) \geqslant \min\big((x, y), (y, z)\big) - 2\delta.$$

Let S_ℓ denote the set of elements of norm ℓ in the hyperbolic group G. Consider also, for homogeneity reasons, the annulus $S_{\ell,a} = B_\ell \setminus B_{\ell-a}$.

Proposition 19. *Let $g \in B_\ell$ and let $a \geqslant 0$. The number of elements g' in S_ℓ or B_ℓ such that $(g, g') \geqslant a$ is at most $|B_{\ell-a+2\delta}|$.*

Proof. Suppose that $(g, g') \geqslant a$. Let x be the point at distance a from e on some geodesic joining e to g. By construction we have $(g, x) = a$. But

$$(g', x) \geqslant \min\big((g', g), (g, x)\big) - 2\delta \geqslant a - 2\delta$$

and unwinding the definition of (g', x) yields

$$\|g' - x\| \leqslant \|g'\| + \|x\| - 2a + 2\delta \leqslant \ell - a + 2\delta.$$

So g' lies at distance at most $\ell - a + 2\delta$ from x, hence the number of possibilities for g' is at most $|B_{\ell-a+2\delta}|$. (This is most clear on a picture.) □

We know show that, if we multiply two elements of the sphere S_ℓ then we often get an element of norm close to 2ℓ.

Corollary 20. *Let $g \in S_{\ell,a}$. The number of elements g' in $S_{\ell,a}$ such that $\|gg'\| \geqslant 2\ell - 4a$ is at least $|S_{\ell,a}| - |B_{\ell-a+2\delta}|$.*

Proof. We have $\|gg'\| = \|g\| + \|g'\| - 2(g^{-1}, g')$. So if $\|g\| \geqslant \ell - a$, $\|g'\| \geqslant \ell - a$ and $(g^{-1}, g') \leqslant a$, then $\|gg'\| \geqslant 2\ell - 4a$.

But by the last proposition, the number of "bad" elements g' such that $(g^{-1}, g') \geqslant a$ is at most $|B_{\ell-a+2\delta}|$. □

So multiplying long elements often gives twice as long elements. We now show that this procedure does not build too often the same new element.

Proposition 21. *Let $x \in S_{2\ell,4a}$. The number of pairs (g, g') in $S_{\ell,a} \times S_{\ell,a}$ such that $x = gg'$ is at most $|B_{6a+2\delta}|$.*

Proof. Choose a geodesic decomposition $x = hh'$ with $\|h\| = \|h'\| = \|x\|/2$. It is easy to see that if $x = gg'$ as above, then g is $6a + 2\delta$-close to h (and then g' is determined). □

Combining the last two results yields the following "almost supermultiplicative" estimate for the cardinals of balls (compare the trivial converse inequality $|B_{2\ell}| \leqslant |B_\ell|^2$).

Corollary 22.
$$|B_{2\ell}| \geqslant \frac{1}{|B_{6a+2\delta}|}\left(|B_\ell| - 2|B_{\ell-a+2\delta}|\right)^2 .$$

Proof. Indeed, the last two results imply that
$$|S_{2\ell,4a}| \geqslant \frac{1}{|B_{6a+2\delta}|}|S_{\ell,a}|(|S_{\ell,a}| - |B_{\ell-a+2\delta}|)$$
which implies the above by the trivial estimates $|B_{2\ell}| \geqslant |S_{2\ell,4a}|$ and $|S_{\ell,a}| \geqslant |B_\ell| - |B_{\ell-a+2\delta}|$. □

In order to apply this estimate, we need to know both that $|B_\ell|$ is large and that $|B_{\ell-a}|$ is not too large compared to $|B_\ell|$. Asymptotically one would expect $|B_{\ell-a}| \approx (2m-1)^{-ga}|B_\ell|$. The next lemma states that, under the assumptions of Proposition 17, we can almost realize this, up to changing ℓ by some controlled factor.

Lemma 23. *Suppose that for some g, for some ℓ_0 and $\ell_1 \geqslant 100\ell_0$ we have $|B_{\ell_0}| \leqslant (2m-1)^{1.2g\ell_0}$ and $|B_{\ell_1}| \geqslant (2m-1)^{g\ell_1}$. Let $a \leqslant \ell_0$. There exists $0.65\ell_1 \leqslant \ell \leqslant \ell_1$ such that*
$$|B_\ell| \geqslant (2m-1)^{g\ell}$$
and
$$|B_\ell| \geqslant (2m-1)^{ga/2}|B_{\ell-a}|.$$

Proof. First, note that by subadditivity, the inequality $|B_{\ell_0}| \leqslant (2m-1)^{1.2g\ell_0}$ implies that for any ℓ, writing $\ell = k\ell_0 - r$ ($k \in \mathbb{N}, 0 \leqslant r < \ell_0$) we have $|B_\ell| \leqslant (2m-1)^{1.2kg\ell_0}$. Especially for $\ell \geqslant 50\ell_0$ we have $1 \leqslant k\ell_0/\ell \leqslant 51/50$ and so in particular, if $\ell_1 \geqslant 100\ell_0$ then $|B_{0.65\ell_1}| \leqslant (2m-1)^{0.8g\ell_1}$ (indeed $0.65 \times 1.2 \times 51/50 \leqslant 0.8$).

Suppose that for all $0.65\ell_1 \leqslant \ell \leqslant \ell_1$ with $\ell = \ell_1 - ka$ ($k \in \mathbb{N}$) we have $|B_\ell| < (2m-1)^{ga/2}|B_{\ell-a}|$. Write $\ell_1 - 0.65\ell_1 = qa - r$ with $q \in \mathbb{N}$, $0 \leqslant r < a$. Then we get

$$\begin{aligned}|B_{\ell_1}| &< (2m-1)^{ga/2}|B_{\ell_1-a}| < (2m-1)^{ga}|B_{\ell_1-2a}| < \cdots\\ &< (2m-1)^{gqa/2}|B_{0.65\ell_1-r}| \leqslant (2m-1)^{g(\ell_1-0.65\ell_1)/2+ga/2}|B_{0.65\ell_1}|\\ &\leqslant (2m-1)^{g(0.35\ell_1)/2+g\ell_1/200+0.8g\ell_1} < (2m-1)^{0.98g\ell_1}\end{aligned}$$

contradicting the assumption.

So we can safely take the largest $\ell \leqslant \ell_1$ satisfying $|B_\ell| \geqslant (2m-1)^{ga/2}|B_{\ell-a}|$ and such that $\ell_1 - \ell$ is a multiple of a.

Since ℓ is largest, for $\ell \leqslant \ell' \leqslant \ell_1$ we have $|B_{\ell'}| \leqslant (2m-1)^{ga/2}|B_{\ell'-a}|$. We get, a-step by a-step, that $|B_{\ell_1}| \leqslant (2m-1)^{g(\ell_1-\ell)/2}|B_\ell|$. Using the assumption $|B_{\ell_1}| \geqslant (2m-1)^{g\ell_1}$ we now get $|B_\ell| \geqslant (2m-1)^{g\ell_1-g(\ell_1-\ell)/2} \geqslant (2m-1)^{g\ell}$ as needed. □

Now equipped with the lemma, we can apply Corollary 22 to show that if we know that B_ℓ is large for some ℓ, then we get a larger ℓ' such that $B_{\ell'}$ is large as well. We will then conclude by induction.

Lemma 24. *Suppose that for some g, for some $\ell_0 \geqslant 2\delta + 4/g$ and $\ell_1 \geqslant A\ell_0$ (with $A \geqslant 100$) we have $|B_{\ell_0}| \leqslant (2m-1)^{1.2g\ell_0}$ and $|B_{\ell_1}| \geqslant (2m-1)^{g\ell_1}$. Then there exists $\ell_2 \geqslant 1.3\ell_1$ such that*

$$|B_{\ell_2}| \geqslant (2m-1)^{g\ell_2(1-9/A)}.$$

Proof. Consider the ℓ provided by Lemma 23 where we take $a = \ell_0$. This provides an $\ell \geqslant 0.65\ell_1$ such that $|B_\ell| \geqslant (2m-1)^{g\ell}$ and $|B_\ell| \geqslant (2m-1)^{ga/2}|B_{\ell-a}|$.

So by Corollary 22 (applied to $2a$ instead of a) we have

$$|B_{2\ell}| \geqslant \frac{1}{|B_{12a+2\delta}|}|B_\ell|^2\left(1 - 2|B_{\ell-2a+2\delta}|/|B_\ell|\right)^2.$$

Since $a = \ell_0 \geqslant 2\delta$ we have $\ell - 2a + 2\delta \leqslant \ell - \ell_0$ and so

$$|B_{2\ell}| \geqslant \frac{1}{|B_{12\ell_0+2\delta}|}|B_\ell|^2\big(1 - 2(2m-1)^{-g\ell_0/2}\big)^2.$$

If $\ell_0 \geqslant 4/g$, since $2m-1 \geqslant 2$ we have $\big(1 - 2(2m-1)^{-g\ell_0/2}\big)^2 \geqslant 1/4$ and so

$$|B_{2\ell}| \geqslant \frac{1}{4|B_{12\ell_0+2\delta}|}|B_\ell|^2.$$

We have $|B_{12\ell_0+2\delta}| \leqslant |B_{13\ell_0}| \leqslant |B_{\ell_0}|^{13}$ by subadditivity. So by the assumptions

$$|B_{2\ell}| \geqslant \frac{1}{4|B_{\ell_0}|^{13}}|B_\ell|^2 \geqslant (2m-1)^{2g\ell-16g\ell_0-2} = (2m-1)^{2g\ell(1-8\ell_0/\ell-1/g\ell)}$$

which is at least $(2m-1)^{2g\ell(1-9/A)}$ since $8\ell_0/\ell \leqslant 8/A$ and $1/g\ell \leqslant 1/gA\ell_0 \leqslant 1/A$ since $\ell_0 \geqslant 4/g$.

So we can take $\ell_2 = 2\ell$, which is at least $1.3\ell_1$. □

Now the proposition is clear: start from ℓ_1 and construct by induction a sequence ℓ_i with $\ell_{i+1} \geqslant 1.3\ell_i$ using the lemma applied to ℓ_0 and ℓ_i; thus

$$|B_{\ell_i}| \geqslant (2m-1)^{g\ell_i \prod_{k=0}^{i-2}(1-9/(A\cdot 1.3^k))}$$

and note that the infinite product converges to a value greater than $1-40/A$. The only thing to check is that, in order to be allowed to apply the previous lemma to ℓ_0 and ℓ_i at each step, we must ensure that $1.1/(1-40/A) \leqslant 1.2$, which is guaranteed as soon as $A \geqslant 500$. □

References

[AL02] G. N. Arzhantseva, I. G. Lysenok, Growth tightness for word hyperbolic groups. *Math. Z.* **241** (2002), 597–611. Zbl 1045.20035 MR 1938706

[Ch91] C. Champetier, Propriétés génériques des groupes de présentation finie. Ph.D. Thesis, Université Lyon 1, 1991.

[Ch93] C. Champetier, Cocroissance des groupes à petite simplification. *Bull. London Math. Soc.* **25** (1993), 438–444. Zbl 0829.20046 MR 1233406

[Ch95] C. Champetier, Propriétés statistiques des groupes de présentation finie. *J. Adv. Math.* **116** (1995), 197–262. Zbl 0847.20030 MR 1363765

[Gh03] É. Ghys, Groupes aléatoires. In *Séminaire Bourbaki*, Volume 2002/2003, Exposés 909-923, Soc. Math. de France, Paris 2004; *Astérisque* **294** (2004), 173–204. Zbl 02123627 MR 2111644

[GhH90] É. Ghys, P. de la Harpe, *Sur les groupes hyperboliques d'après Mikhael Gromov*. Progr. Math. 83, Birkhäuser, Boston, MA, 1990. Zbl 0731.20025 MR 1086648

[GrH97] R. I. Grigorchuk, P. de la Harpe, On problems related to growth, entropy, and spectrum in group theory. *Dynam. Control Systems* **3** (1997), 51–89. Zbl 0949.20033 MR 1436550

[Gro87] M. Gromov, Hyperbolic Groups. In *Essays in group theory* (ed. by S. M. Gersten), Math. Sci. Res. Inst. Publ. 8, Springer-Verlag, New York 1987, 75–263. Zbl 0634.20015 MR 0919829

[Gro93] M. Gromov, Asymptotic Invariants of Infinite Groups. In *Geometric group theory, Vol.* 2 (ed. by G. Niblo, M. Roller), London Math. Soc. Lecture Note Ser. 182, Cambridge University Press, Cambridge 1993, 1–295. Zbl 0841.20039 MR 1253544

[Gro03] M. Gromov, Random Walk in Random Groups. *Geom. Funct. Anal.* **13** (2003), 73–146. Zbl 01971826 MR 1978492

[Har00] P. de la Harpe, *Topics in geometric group theory*. Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000. Zbl 0965.20025 MR 1786869

[HLS02] N. Higson, V. Lafforgue, G. Skandalis, Counterexamples to the Baum-Connes conjecture. *Geom. Funct. Anal.* **12** (2002), 330–354. Zbl 1014.46043 MR 1911663

[LS77] R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory*. Ergeb. Math. Grenzgeb. 89, Springer-Verlag, Berlin, New York 1977. Zbl 0368.20023 MR 0577064

[Oll04] Y. Ollivier, Sharp phase transition theorems for hyperbolicity of random groups. *Geom. Funct. Anal.* **14** (2004), 595–679. Zbl 1064.20045 MR 2100673

[Oll05a] Y. Ollivier, Cogrowth and spectral gap of generic groups. *Ann. Inst. Fourier (Grenoble)* **55** (2005), 289–317. Zbl 02162474 MR 2141699

[Oll05b] Y. Ollivier, *A January 2005 Invitation to Random Groups*. Ensaios Matemáticos 10, Sociedade Brasileira de Matemática, Rio de Janeiro 2005.

[Oll-a] Y. Ollivier, Some small cancellation properties of random groups. To appear in *Internat. J. Algebra Comput.*; ArXiV math.GR/0409226.

[Ols92] A. Yu. Ol'shanskiĭ, Almost Every Group is Hyperbolic. *Internat. J. Algebra Comput.* **2** (1992), 1–17. Zbl 0779.20016 MR 1167524

[Pap96] P. Papasoglu, An Algorithm Detecting Hyperbolicity. In *Geometric and Computational Perspectives on Infinite Groups* (ed. by G. Baumslag et al.), DIMACS Ser. Discrete Math. Theor. Comput. Sci. 25 (1996), 193–200. Zbl 0857.20017 MR 1364185

[Sho91] H. Short (ed.) et al., Notes on word hyperbolic groups. In *Group theory from a Geometrical Viewpoint* (ed. by É. Ghys, A. Haefliger, A. Verjovsky), World Scientific, River Edge, NJ, 1991, 3–63. Zbl 0849.20023 MR 1170363

[Shu99] A. G. Shukhov, On the dependence of the growth exponent on the length of the defining relation. *Math. Notes* **65** (1999), 510–515. Zbl 0979.20033 MR 1715061

[Ver00] A. M. Vershik, Dynamic theory of growth in groups: entropy, boundaries, examples. *Russian Math. Surveys* **55** (2000), 667–733. Zbl 0991.37005 MR 1786730

Received September 16, 2004; revised February 1, 2005

Yann Ollivier, CNRS, UMPA, École normale supérieure de Lyon, 46, allée d'Italie, 69007 Lyon, France

E-mail: yann.ollivier@umpa.ens-lyon.fr

Leere Seite
Blank page
Page vide