arXiv:2304.09144v1 [math.GR] 18 Apr 2023

无限群上的概率律

Gideon Amir、GUY BLACHAR、MARIA GERASIMOVA 和 GADY KOZMA

Abstract. We study the probability that certain laws are satisfied on infinite groups, focusing on elements sampled by random walks. For several group laws, including the metabelian one, we construct examples of infinite groups for which the law holds with high probability, but the group does not satisfy the law virtually. On the other hand, we show that if an infinite group satisfies the law $x^2 = 1$ with positive probability, then it is virtually abelian.

1. Introduction

有限群的交换概率 G，记作 $\mathbb{P}([x, y] = 1)$，是从 G 中随机选取的两个元素彼此交换的概率。以下是 Gustafson 的一个著名定理 [7]:

定理。如果 $\mathbb{P}([x, y] = 1) > \frac{5}{8}$ 那么 G 是阿贝尔。

我们将这种现象称为间隙：当把所有有限群的交换概率集合视为 $[0, 1]$，的子集时，在接近 1 的位置存在一个间隙。

More generally, for a finite group G and a word $1 \neq w = w(x_1, \ldots, x_d) \in \mathrm{F}_d$, we define the probability that w is satisfied on G as the probability that d independent uniformly chosen elements $g_1, \ldots, g_d$ of G satisfy $w(g_1, \ldots, g_d) = 1$:

$$\mathbb{P}\left(w = 1 \text{ on } G\right) = \frac{\left|\left\{(g_1, \ldots, g_d) \in G^d : w(g_1, \ldots, g_d) = 1\right\}\right|}{|G|^d}.$$

一个自然的问题是：对于给定的字 w，这些概率是否也呈现类似的行为。

It is also well known (and with the same proof as Gustafson's theorem) that for a fixed k, the k-step nilpotent law $[x_1, \ldots, x_k] = [[\cdots[[x_1, x_2], x_3]\cdots], x_k] = 1$ presents a gap.

Considering power laws $x^m = 1$, several results have been established. Laffey showed the existence of a gap for the laws $x^2 = 1$, $x^3 = 1$ [15], $x^4 = 1$ [17] and $x^p = 1$ for prime p on non-p-groups [16]. For general exponent m, a result of Mann and Martinez [22] proves the existence of a gap for $x^m = 1$ for all groups with a fixed number of generators. Another result in this direction is the recent work of Delizia, Jezernik, Moravec and Nicotera [2] that the metabelian law $[[x, y], [z, w]] = 1$ and the 2-Engel law $[[x, y], y] = 1$ satisfy a gap.

尽管所有已知情形确实都满足有限群的间隙，但一般情形仍是一个未解决的问题：

问题 1.1. 是否存在某个律对有限群满足间隙?

The commuting probability of a finite group does not only present a gap, but also reveals structural information about the group. A well-known theorem of Peter Neumman [24, Theorem 1] states:

2020 Mathematics Subject Classification. 20P05、20F69、20F65、60B15、20E22。

Theorem. *If G is a finite group for which $\mathbb{P}([x,y]=1)\geq\varepsilon>0$, then G is (ε-bounded)-by-abelian-by-(ε-bounded), i.e. G contains subgroups $H'\lhd H<G$ such that $[G:H]$ and $|H'|$ are bounded by a function of ε, and such that H/H' is abelian.*

我们称这种行为为正性，并称“交换律满足正性”（更正式的定义见下文定义2.4 ）。

An interesting phenmenon is that sometimes, if a law holds with probability at least ε, then *another* law holds virtually. We quote two results of this type. For the law $x^2=1$, a result of Mann [21] shows that if $\mathbb{P}\left(x^2=1 \text{ on } G\right)\geq\varepsilon>0$, then G is (ε-bounded)-by-abelian-by-(ε-bounded). The example of dihedral groups shows that it is not true that the group is (ε-bounded)-by-(satisfying $x^2=1$)-by-(ε-bounded).

For the 2-step nilpotent law $[[x_1,x_2],x_3]=1$, a result of Eberhard and Shumyatsky [3] shows that such groups are not (ε-bounded)-by-(2-step-nilpotent)-by-(ε-bounded), but are (ε-bounded)-by-(3-step-nilpotent)-by-(ε-bounded).

We remark that in the nilpotent case, this phenomenon is due to our requirement that the excess parts are bounded *only* by ε. If one allows them to depend also on the number of generators, the picture changes completely. Indeed, Shalev [27] showed that if G is d-generated, and $\mathbb{P}\left([x_1,\ldots,x_k]=1 \text{ on } G\right)\geq\varepsilon>0$, then G is (k-step-nilpotent)-by-((k,d,ε)-bounded).

同样，一般情形仍然未知：

问题 1.2. 如果某个律 w 在有限群 G 上成立的概率大于 ε，那么群 G 是否包含一个大的子群（其指数有界，且仅取决于 ε，还可能取决于 G 的生成元个数），并且该子群满足一个仅取决于 w 的律?

1.1. **Infinite groups.** One may ask for a generalization of these concepts to infinite groups. As we can no longer sample elements according to a uniform distribution, one needs to define how to measure the probability of satisfying a law on an infinite group. When the group is locally compact, for example, a natural choice for a measure is the Haar measure.

本文主要关注无限有限生成离散群的情形。遵循 [1], 的思路，我们使用一列定义在 G上的概率测度 $M=\{\mu_n\}$ ，并定义 G 满足律 w 关于 M的概率为

$$\mathbb{P}_M\left(w=1 \text{ on } G\right)=\limsup_{n\to\infty}\mu_n\left(\{(g_1,\ldots,g_d):w(g_1,\ldots,g_d)=1\}\right). \tag{1}$$

If G is finitely generated, natural choices for $\{\mu_n\}$ include taking a random walk measure on G, or a uniform measure on a sequence of balls centered at the identity and converging to G. We will omit M if it is the random walk measure with respect to some natural generators (this is the case we are most interested in).

在 Ant´olin-Martino-Ventura [1] 以及后来 Tointon [28], 的工作中，研究了交换概率。这些工作证明了与有限情形类似的结果：

定理（Tointon [28, 定理 1.9]）。

(1) If $\mathbb{P}\left([x,y]=1 \text{ on } G\right)>\frac{5}{8}$, then G is abelian. (In other words, the commutator word satisfies a gap also for infinite finitely generated groups.)

(2) If $\mathbb{P}\left([x,y]=1 \text{ on } G\right)>0$, then G is virtually abelian.

(The results of [1] and [28] are more general than for random walks, we quoted only the random walk results for simplicity). Similar results are proved for the nilpotent case in [23].

In this paper we consider other examples of laws. Our goal is to answer the two questions above for various laws. Namely, do these laws satisfy a gap for infinite finitely generated groups? If the probability that a law is satisfied on a group is positive, does the group virtually satisfy the same law, or perhaps another one? We start with sketching an example showing that very different behaviour may occur in the infinite case.

1.2. **A lamplighter example.** Consider the group $G \coloneqq \mathrm{F}_2 \wr \mathbb{Z}^5$ i.e. a lamplighter with the base group being $\mathbb{Z}^5$ and the lamps being free groups with 2 generators (exact definitions will be given in Subsection 2.3). We will use this group to show that the metabelian law $[[x,y],[z,w]] = 1$ has no gap for infinite groups. It is easy to see that G does not satisfy the metabelian law virtually (thus we get that the metabelian law satisfies neither a gap nor a positivity result with the same example).

Consider first a single commutator, $[x,y]$. The walker (i.e. the $\mathbb{Z}^5$ projection) is at the identity. The lamps can be found on a random subset of places visited by the following process: do a random walk on n steps. Then do another random walk on n steps. Then repeat the first walker in reverse, and then the second.

The other commutator, $[z,w]$ gives a second, independent, subset of a random loop. The crucial property of $\mathbb{Z}^5$ that we exploit is that two such loops do not intersect (except at the identity) with positive probability (independent of the length of the loops). We conclude that with positive probability the lamps positions of $[x,y]$ and $[z,w]$ are disjoint. This, of course, means that these elements commute. This shows that the metabelian law does not satisfy positivity for infinite groups.

All this was using the natural generators of G. To get a no gap result we modify the generators as follows. Denote the generators of F_2 by a and b. Then the walker is allowed to act on the a lamp in its current position, but the b lamp is acted upon in a different position (shifted with respect to its current position by a fixed, large offset). See Figure 1. This modification means that even when the loops performed by the walkers intersect, with high probability you will only have lamps of one type in the intersection (at each site, either both acted with an a or both acted with a b). This modification means that by changing the generators (their number remains 160) one may make $\mathbb{P}([[x,y],[z,w]] = 1 \text{ on } G)$ arbitrarily close to 1. This shows that the metabelian law does not even satisfy a gap. Full details of the proof can be found in §6.

It is interesting to note how residual finiteness enters into the picture. Recall that the metabelian law *does* satisfy a gap for finite groups [2]. This means (see §3) that it satisfies a gap for residually finite groups. Thus we get a new manifestation of the fact that a lamplighter with non-commutative lamps is not residually finite (this fact is far from new, see [5]).

By varying the base group one may get additional examples of laws with no gap. In §11 we take the base group to be an infinite Burnside group to get that the law $[x^k, y^k]$ (with some restrictions on k) does not satisfy a gap. In §7 we take as the base group a certain generalization of the infinite dihedral group in order to handle laws like $[x^k,[y,z]]$ (exact definition of what does "like" means will be found there).

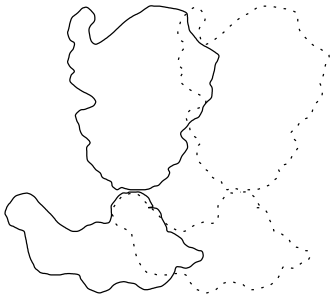

FIGURE 1. 实线表示沉积了 a 的位置，虚线表示沉积了 b 的位置。证明之所以成立，是因为上方的实线回路与下方的虚线回路不相交，反之亦然。

1.3. **Power laws.** We present two results about power laws. The first is about the law x^2. We have already mentioned the result of Mann that if $\mathbb{P}(x^2 = 1) \geq \varepsilon$ on a finite group G then G is (ε-bounded)-by-abelian-by-(ε-bounded). This example prompted Leemann and de la Salle [18] to conjecture that if an infinite group G satisfies $x^2 = 1$ with positive probability, it is virtually abelian. We prove this conjecture in Theorem 5.1.

The infinite dihedral group satisfies the law $x^2 = 1$ with probability $1/2$ but does not satisfy this law virtually. In Proposition 5.13 we show a generalization of this fact to any power. The example is the semi-direct product $\mathbb{Z}^{m-1} \rtimes \mathbb{Z}/m\mathbb{Z}$ where the action of $\mathbb{Z}/m\mathbb{Z}$ is given by powers of the companion matrix of $1 + \cdots + x^m$.

从正性结果转向间隙，我们介绍一个关于该主题的结果。我们证明，将（ $x^3 = 1$ 中的上极限替换为下极限后，该律1）满足一个间隙（定理 5.6）。幂大于 3 的情形仍然是开放问题。

1.4. 其他结果。 对于 剩余有限 群的情形，我们在 §3中证明，（在某些条件下），正性问题和间隙问题的答案与有限情形相同。

在 §4 中，我们证明，对于形如 $w' = [w(x_1, \ldots, x_n)\ x_{n+1}]$的分布，若对其中一个问题，$w$ 的答案为肯定，则 w' 对同一问题的答案也为肯定，从而推广了 k步幂零律的情形。

We focused so far on probabilities with respect to random walk, but it seems quite natural to also consider probabilities taken uniformly on balls in the Cayley graph of G. We believe that these measures are less natural, and we demonstrate that with one result. In §12 we show that many laws cannot satisfy a gap result with respect to uniform elements of balls. The example is simply the product with a finite group which does not satisfy the law.

1.5. **A lemma on random walks.** We end this introduction mentioning one lemma for readers interested in random walks on groups. A well-known open problem in this area is whether random walk on any transient group spends on more than r^2 time in a ball of radius r, with the best result known to us being that of Lyons, Peres, Sun and Zheng [20]. We use the techniques of [20] for the *path of a word*, namely for the elements of a group visited by $w(R^{(1)}, \ldots, R^{(d)})$, where w is

some word in d letters and $R^{(1)}, \dots, R^{(d)}$ are k independent random walks. See the exact statement in §10.

1.6. 致谢。 我们感谢 Mikael de la Salle 对定理 5.1的证明提出的重要建议。我们感谢 Yehuda Shalom 提供的一些有用参考文献，以及 Denis Osin 和 Andreas Thom 的评论和备注。

During this research G.A. and G.B. were supported by Israeli Science Foundation grant #957/20. G.B. was also supported by the Bar-Ilan President's Doctoral Fellowships of Excellence. G.K. was supported by the Israel Science Foundation and by the Jesselson Foundation. M.G. was supported by the DFG – Project-ID 427320536 – SFB 1442, and under Germany's Excellence Strategy EXC 2044 390685587, Mathematics Münster: Dynamics–Geometry–Structure.

2. Preliminaries

2.1. **The probability of satisfying a law.** By a **word** we mean a nontrivial element of the free group F_d. Let $x_1, \dots, x_d$ denote the standard generators of F_d. Any word $w \in \mathrm{F}_d$ defines the **word map** on any group G, which we also denote $w\colon G^d \to G$, defined as follows: for $g_1, \dots, g_d$, the value of $w(g_1, \dots, g_d)$ is given by substituting $g_1, \dots, g_d$ for $x_1, \dots, x_d$. We interpret any word as a law on groups by considering the equation $w(x_1, \dots x_d) = 1$ (where 1 is the identity element of G).

对于群 G 上的测度 μ，也用 μ 表示在 G^d 上诱导的测度 $\mu \times \cdots \times \mu$。我们采用 [23] 中介绍的思路：

定义 2.1. 设 G 为一个群，$w \in \mathrm{F}_d$ 为一个字。

(1) 设 μ 是 G 上的概率测度。我们定义 G 关于 μ 满足 w 的概率为

$$\mathbb{P}_\mu\left(w = 1 \text{ on } G\right) = \mu\left(\left\{(g_1, \dots, g_d) \in G^d : w(g_1, \dots, g_d) = 1\right\}\right).$$

(2) 设 $M = \{\mu_n\}$ 是 G 上的一个概率测度序列。我们定义 G 满足 w 关于 M 的概率为

$$\mathbb{P}_M\left(w = 1 \text{ on } G\right) = \limsup_{n\to\infty} \mathbb{P}_{\mu_n}\left(w = 1 \text{ on } G\right).$$

设 G 是一个有限生成群。下面介绍几种定义在 G上的概率测度序列，我们将在全文中对其进行研究。

Our main interest will be **random walk measures**. These are sequences of the form $M = \{\mu_n = \mu^{*n}\}$, where μ is a finitely supported generating probability measure on a group G with $\mu(1) > 0$. In other words, μ_n is the probability measure induced by a random walk with step distribution μ after n steps. It will occasionally be important to consider random walks also as a stochastic process (i.e. a measure on paths in the group) and then we will always use a right random walk, i.e. $R_{n+1} = R_n x_n$ where the x are i.i.d. with law μ.

另一类值得关注的序列在[28] 中如下给出：

Definition 2.2. *We say that a sequence of probability measures $M = \{\mu_n\}$ on G **measures index uniformly**, if $\mu_n(xH) \to 1/[G : H]$ uniformly over all $x \in G$ and all subgroups $H \leq G$. Similarly, for a sequence of random variables taking value in G we say that they measure index uniformly if their laws measure index uniformly.*

For example, (lazy) random walk measures satisfy this property [28, Theorems 1.11 and 1.12].

An additional way to define a sequence of measures on a group is by taking the uniform measures on balls centered at the identity. Formally, we take a finite symmetric generating set S of G which contains the identity, and let μ_n be the uniform measure on S^n (i.e. the ball of radius n around the identity in the Cayley graph). While such sequences of measures usually do not measure index uniformly (for instance, see [28, Remark after Theorem 1.12]), they are of interest on their own. We discuss these measures in §12.

2.2. 间隙与正性。本文讨论分布的两个性质。第一个涉及分布得到满足的概率值:

定义 2.3。固定一个测度序列族 $\mathcal{M}$，并令 $w \in \mathbb{F}_d$ 为一个字。

(1) *We say that w satisfies a **gap** with respect to $\mathcal{M}$, if there is a function $\phi\colon \mathbb{N} \to (0,1)$ such that for any r-generated group G and sequences of measures $M \in \mathcal{M}$ on G, if $\mathbb{P}_M(w = 1 \text{ on } G) > 1 - \phi(r)$, then G satisfies w. In this case we also say that w satisfies a ϕ-**gap**.*
(2) *If w satisfies a gap with respect to a constant function $\phi(r) = \varepsilon$, we say that w satisfies a **strong gap** (or an ε-**gap**) with respect to $\mathcal{M}$. In this case, the probability that w is satisfied cannot lie in the interval $(1-\varepsilon, 1)$.*

我们注意到，这一定义可能取决于所考虑的概率测度族。除非特别说明，我们将假设 $\mathcal{M}$ 是随机游走测度族。

Summarizing the results mentioned in the introduction in this language, for finite groups it is known the the laws $[x,y] = 1$, $x^2 = 1$, $x^3 = 1$, $x^4 = 1$, $[x,y,y] = 1$ and $[[x,y],[z,w]] = 1$ satisfy a strong gap, while $x^n = 1$ satisfies a weak gap. For finitely generated groups, it is known that $[x,y] = 1$ and $[x_1, \dots, x_k] = 1$ satisfy a strong gap.

我们接下来讨论要研究的群恒等式的第二个性质。若一个群有一个满足 w 的有限指数子群，我们就说它几乎满足群恒等式 w。如果一个群几乎满足某个群恒等式，那么它满足该群恒等式的概率为正。这引出了以下结论:

定义 2.4. 固定一个测度序列族 $\mathcal{M}$，并令 $w \in \mathbb{F}_d$ 为一个字。

(1) *We say that w satisfies a **positivity property** with respect to $\mathcal{M}$, if there is a function $\psi\colon (0,1)\times\mathbb{N} \to \mathbb{N}$ such that the following holds: for any $\varepsilon \in (0,1)$, any r-generated group G and any $M \in \mathcal{M}$ on G, if $\mathbb{P}_M(w = 1 \text{ on } G) \geq \varepsilon$, then G has a subgroup of index $\leq \psi(\varepsilon, r)$ which satisfies w.*
(2) *We say that w satisfies a **strong positivity property** with respect to $\mathcal{M}$, if it has a positivity property with respect to a function $\psi(\varepsilon, r)$ which depends only on ε.*

例如，Tointon [28, 定理 1.9] 证明了交换律满足强正性。

Remark. If G virtually satisfies a law, it must completely satisfy some other law. In particular, if G contains a non-abelian free subgroup, it cannot virtually satisfy any law.

Indeed, let $\Lambda \leq G$ be a finite index subgroup that satisfies a law w. There exists a normal subgroup $N \lhd G$ with $N \leq \Lambda$ and $[G : N] = k < \infty$. Therefore $g^k \in N \leq \Lambda$ for all $g \in G$, so G satisfies the law $w(x_1^k, \ldots, x_d^k) = 1$.

备注 2.5. 如果 G 几乎满足群恒等式，那么 G 的每个 H 也几乎满足该群恒等式。事实上，设 Λ 是满足该群恒等式的 G 的有限指数子群，则 $\Lambda \cap H$ 是 H 中的有限指数子群，也满足该群恒等式。

2.3. 绕积。本文将使用的一种主要构造是两个群的缠绕积。这里回顾缠绕积的定义及其关于群分布的一条基本性质。

Let G, H be two groups. The **wreath product** (or **lamplighter group**) $H \wr G$ is the semidirect product $\left(\bigoplus_{g\in G} H\right) \rtimes G$, where G acts on $\bigoplus_{g\in G} H$ by permuting the indices, i.e.

$$g \cdot (h_a)_{a\in G} = (h_{g^{-1}a})_{a\in G}.$$

The group G is called the **base group** of $H \wr G$, and H is called the **lamp group** of $H \wr G$. Each element of $H \wr G$ can be written in the form (L, g), where $g \in G$ is the **lamplighter position**, and $L \in \bigoplus_{g\in G} H$ is the **lamp configuration**. For an element (L, g) we define its **support** $\mathrm{supp}(L, g) = \{a \in G : L(a) \neq 1\}$.

我们作如下观察：

命题 2.6. 如果 H 不满足律 $w \in \mathbf{F}_d$，那么对于任意无限群 G，灯笼群 $H \wr G$ 几乎不满足律 w。

Proof. Let us take $\bigoplus_{g\in G} H$, which we identify with the subgroup of all elements with trivial lamplighter position. Assume by contradiction that there exists a finite index subgroup $\Lambda < H \wr G$ that satisfies the law $w = w(x_1, \ldots, x_d)$. Then note that $\Lambda \cap \bigoplus_{g\in G} H$ is a finite index subgroup in $\bigoplus_{g\in G} H$. Let us take representatives $t_1, \ldots, t_n$ of the left cosets of $\bigoplus_{g\in G} H/(\Lambda \cap \bigoplus_{g\in G} H)$. We take the set $A = \cup_{i=1}^n \mathrm{supp}(t_i) \subset G$ and consider $g_0 \in G \setminus A$. Let us consider $h_1, \ldots h_d \in H$ such that $w(h_1, \ldots, h_d) \neq 1$, and take $y_1, \ldots, y_d \in \bigoplus_{g\in G} H$ such that $y_i(g_0) = h_i$ for $i = 1, \ldots, d$. Then for any $i = 1, \ldots, d$ there exists $j \in \{1, \ldots, n\}$ such that $z_i := t_j^{-1} y_i \in \Lambda \cap \bigoplus_{g\in G} H$, so $z_i(g_0) = h_i$. Therefore, since $w(z_1, \ldots, z_d)(g_0) = w(h_1, \ldots, h_d)$, we get that $w(z_1, \ldots, z_d) \neq 1$. A contradiction. □

2.4. **Notation.** A "word" is a sequence w of letters in some alphabet. We denote by $|w|$ the number of letters in w. Let G and H be groups and let $g \in G$ and $h \in H$. Then the notation $h\delta_g$ refers to the element of $\bigoplus_{g\in G} H$ which takes value h at g and takes the unit of H at any $g' \neq g$.

We use the following standard group notation. We use $C_G(x)$ for the centralizer of x in G, namely, $\{y \in G : [x, y] = 1\}$. We use $C_G(H) = \bigcap_{h\in H} C_G(h)$. We use $Z(G)$ for the center of G, namely, $\{g \in G : C_G(g) = G\}$.

We use c and C to denote constants that depend only on the law in question, and, for infinite groups, on the walk. Their value may change from line to line, and even within the same line. We use c for constants which are "sufficiently small" and C for constants which are "sufficiently large". When we want to specify specific constants we will use c', c'', etc. These change value only from lemma to lemma.

3. Residually finite groups

In this section we study the questions of gap and positivity for laws on residually finite groups. We show that, when working with sequences of probability measures that measure index uniformly, these questions are equivalent to the same questions on finite groups.

Let G be a group, and let $N \lhd G$ be a normal subgroup. Any probability measure μ on G induces a probability measure $\overline{\mu}$ on G/N by taking the pushforward of μ with respect to the natural projection $G \to G/N$. The following lemmas follow directly from the definition of measuring index uniformly and the pushforward measure:

引理 3.1. 设 G 是一个有限群，并设 $M = \{\mu_n\}$ 是 G 上一列一致地测量指数的概率测度。令 U_G 表示 G 上的均匀概率测度。那么 $\mu_n \to U_G$。

引理 3.2. 设 G 是一个群，$N \lhd G$ 是一个正规子群。设 $M = \{\mu_n\}$ 是 G 上的概率测度序列，且 $\overline{M} = \{\overline{\mu_n}\}$。设 w 是一个字。则

$$\mathbb{P}_M\left(w = 1 \text{ on } G\right) \leq \mathbb{P}_{\overline{M}}\left(w = 1 \text{ on } G/N\right).$$

Proof. For $g_1, \ldots, g_d \in G$, if $w(g_1, \ldots, g_d) = 1$ in G, then $w(g_1N, \ldots, g_dN) = 1$ in G/N, so the probability of satisfying w cannot decrease. □

现在我们可以结合上述引理来研究剩余有限群的一般情形。回顾一下，若 $N \lhd_f G$ 是 G 的一个有限指数正规子群，则 N。

命题 3.3. 设 G 是一个有限生成的残有限群，并设 M 是 G 上的一列概率测度，它们一致地测量指数。那么

$$\mathbb{P}_M\left(w = 1 \text{ on } G\right) = \inf\left\{\mathbb{P}\left(w = 1 \text{ on } G/N\right) : N \lhd_f G\right\}.$$

Proof. The left hand side is not bigger than the right hand side by Lemma 3.2. For the opposite direction, as G is finitely generated and residually finite, one can find a sequence of finite indexed normal subgroups $N_k \lhd_f G$ such that $N_{k+1} \subseteq N_k$ and $\bigcap_{k=1}^{\infty} N_k = 1$. Therefore

$$\left\{w = 1 \text{ on } G\right\} = \bigcap_{k=1}^{\infty} \left\{w = 1 \text{ on } G/N_k\right\},$$

因此，根据概率的连续性，我们有

$$\mathbb{P}_M\left(w = 1 \text{ on } G\right) = \lim_{k\to\infty} \mathbb{P}\left(w = 1 \text{ on } G/N_k\right) \geq \inf\left\{\mathbb{P}\left(w = 1 \text{ on } G/N\right) : N \lhd_f G\right\}.$$

□

定理 3.4. 设 $w \in \mathbf{F}_d$ 是一个字，并令 $\mathcal{M}$ 表示一个在指数上均匀测度的概率测度序列族。

(1) *If w satisfies a gap for all finite groups, then w satisfies a gap for all residually finite groups with respect to $\mathcal{M}$, with the same gap function $\varepsilon(r)$.*
(2) *If w satisfies a positivity result for all finite groups, then w satisfies a positivity result for all residually finite groups with respect to $\mathcal{M}$.*

由此可得，如果 w 对所有有限群都满足强间隙，那么它对残有限群也满足强间隙，因为强间隙只不过是间隙函数 $\varepsilon(r)$ 有下界的弱间隙。

证明。设 G 是一个由 r生成的残有限群，并设 $M = \{\mu_n\}$ 是 G 上的一列一致地测量指数的概率测度。

（1）这是命题的直接推论3.3。

(2) Assume that w satisfies a weak positivity property for all finite groups. That is, there is a function $\psi\colon (0,1)\times\mathbb{N}\to\mathbb{N}$ such that for any $\varepsilon\in(0,1)$ and any finite r-generated group Λ, if $\mathbb{P}(w=1 \text{ on } \Lambda)\geq\varepsilon$ then Λ has a subgroup of index $\leq\psi(\varepsilon,r)$ satisfying w.

If $\mathbb{P}_M(w=1 \text{ on } G)\geq\varepsilon$, the same holds for G/N for any finite indexed normal subgroup $N\lhd G$. Therefore, for any such N, the group G/N contains a subgroup of index $\leq\psi(\varepsilon,r)$ which satisfies w, so there is a subgroup $N\leq H\leq G$ such that $[G:H]\leq\psi(\varepsilon,r)$ and $w(H,\dots,H)\subseteq N$.

Let $\mathcal{T}$ denote the set of subgroups of G of index $\leq\psi(\varepsilon,r)$. As G is finitely generated, it has finitely many such subgroups and their number only depends on r and $\psi(\varepsilon,r)$ (see, e.g., [19, Corollary 1.1.2]). Hence $K=\bigcap_{H\in\mathcal{T}}H$ is a finite index subgroup of G, and its index is bounded by a function of ε and r. Note that $w(K,\dots,K)\subseteq\bigcap_{N\lhd_f G}N=\{e\}$, so K satisfies w, as required. □

4. Derived laws

Fix a word $w=w(x_1,\dots,x_d)\in\mathrm{F}_d$. We define the **derived word of** w to be $w'=[w(x_1,\dots,x_d)\ x_{d+1}]\in\mathrm{F}_{d+1}$. In this section we show that if w satisfies a gap or positivity result, then so does w'. This is a result with similar flavor to results in [27]. We now state our main theorem:

定理 4.1。设 $w\in\mathrm{F}_d$ 是一个字，并考虑 $w'\in\mathrm{F}_{d+1}$。设 $\mathcal{M}$ 是在指数上均匀测度的概率测度序列族。那么：

(1) 如果 w 相对于 $\mathcal{M}$满足间隙条件，那么 w' 相对于 $\mathcal{M}$满足间隙条件；(2) 如果 w 相对于 $\mathcal{M}$满足正性结果，那么 w' 相对于 $\mathcal{M}$满足正性结果。

我们的策略类似于 [14, 命题 2.3] 和 [27, 命题 1.8]的证明。我们首先证明[28, 命题 2.1]的一个版本：

引理 4.2. 设 G 是一个群，且 x_n 和 y_n 是取值于 G 的两个随机变量序列。假设 y_n 一致地测量指数，并且

$$\limsup_{n\to\infty}\mathbb{P}([x_n,y_n]=1)>\varepsilon.$$

那么，对于任意 $\delta>0$,

$$\limsup_{n\to\infty}\mathbb{P}([G:C_G(x_n)]<1/\delta)>\frac{\varepsilon-\delta}{1-\delta}.$$

通常， $C_G(x)$ 是 G 中 x 的中心化子。

证明。根据定义，存在一个非负整数序列 $\{n_k\}$，使得$\mathbb{P}([x_{n_k},y_{n_k}]=1)>\varepsilon$，即 $\mathbb{P}[y_{n_k}\in C_G(x_{n_k})]>\varepsilon$。设

$$A=\{x\in G:[G:C_G(x)]<1/\delta\}.$$

Then

$$\begin{aligned}\varepsilon &< \mathbb{P}(x_{n_k} \in A) + \mathbb{E}[y_{n_k} \in C_G(x_{n_k}) \mid x \notin A] \cdot \mathbb{P}(x_{n_k} \notin A) \leq \\ &\leq \mathbb{P}(x_{n_k} \in A) + \left(\frac{1}{[G : C_G(x)]} + o(1)\right)(1 - \mathbb{P}(x_{n_k} \in A)) \leq \\ &\leq \mathbb{P}(x_{n_k} \in A) + \delta(1 - \mathbb{P}(x_{n_k} \in A)) + o(1)\end{aligned}$$

其中第二个不等式利用了 y_n 一致地测量指数这一事实。结论成立。□

定理证明 *4.1*。

(1) Suppose that w satisfies a gap with respect to a function ϕ. We may assume that $\phi(r) > \frac{1}{2}$ for all r. Let G be an r-generated group, and let $x_1, \ldots, x_{d+1}$ be sequences of random variables measuring index uniformly on G such that

$$\limsup_{n\to\infty} \mathbb{P}\left([w(x_1, \ldots, x_d), x_{d+1}] = 1 \text{ on } G\right) = \varepsilon > \frac{\phi(r) + 1}{2}$$

(each x_i is a sequence of variables depending on n, but we suppress the dependence on n in the notation). We apply Lemma 4.2 with $x_{\text{Lemma 4.2}} = w(x_1, \ldots, x_d)$, $y_{\text{Lemma 4.2}} = x_{d+1}$ and $\delta = \frac{1}{2}$. Note that it is important here that in Lemma 4.2 only y needs to measure index uniformly, and x does not need to do that. We get

$$\limsup_{n\to\infty} \mathbb{P}\left([G : C_G(w(x_1, \ldots, x_d))] < 2\right) > \frac{\varepsilon - \frac{1}{2}}{1 - \frac{1}{2}} > \phi(r).$$

当然，如果 $[G: C_G(w(x_1, \ldots, x_d)] < 2$，那么实际上 $w(x_1, \ldots, x_d)$ 是 $\in Z(G)$，即 G 的中心。

Consider the r-generated group $\overline{G} = G/Z(G)$. Using the induced sequences of random variables $\overline{x_i}$, we have $\mathbb{P}\left(w(\overline{x_1}, \ldots, \overline{x_d}) = 1 \text{ on } \overline{G}\right) > \phi(r)$; therefore $\overline{G}$ satisfies w. But then $w(x_1, \ldots, x_n) \in Z(G)$ for all $x_1, \ldots, x_n \in G$, so G satisfies w'.

从证明中我们还可以看出，如果 w 满足强间隙，即 ϕ 是常数，那么 w' 也满足强间隙。

(2) Assume that w satisfies a positivity property with respect to a function $\psi\colon (0,1) \times \mathbb{N} \to \mathbb{N}$. Let $\varepsilon > 0$, let G be an r-generated group and let $x_1, \ldots, x_{d+1}$ be random variables on G measuring index uniformly such that

$$\mathbb{P}\left(w'(x_1, \ldots, x_{d+1}) = 1 \text{ on } G\right) > \varepsilon.$$

使用引理 4.2 如同上一部分一样，我们得到

$$\limsup_{n\to\infty} \mathbb{P}\left([G : C_G(w(x_1, \ldots, x_d))] < \frac{2}{\varepsilon}\right) > \frac{\varepsilon - \frac{\varepsilon}{2}}{1 - \frac{\varepsilon}{2}} = \frac{\varepsilon}{2 - \varepsilon}.$$

令 N 表示 G 中所有指数至多为 $\frac{2}{\varepsilon}$ 的子群的交集。这是 G 的一个正规子群，其指数由 r 和 $\frac{2}{\varepsilon}$ 的函数所界定。于是我们有

$$\limsup_{n\to\infty} \mathbb{P}\left(w(x_1, \ldots, x_d) \in C_G(N)\right) > \frac{\varepsilon}{2 - \varepsilon}.$$

Consider the group $\overline{G} = G/C_G(N)$. By the above,

$$\limsup_{n\to\infty} \mathbb{P}\left(w(x_1, \ldots, x_d)C_G(N) = C_G(N)\right) > \frac{\varepsilon}{2 - \varepsilon}.$$

Therefore $G/C_G(N)$ contains a subgroup $H/C_G(N)$ of index bounded by $\psi(\frac{\varepsilon}{2-\varepsilon}, r)$ that satisfies w. We therefore conclude that $H \cap N$ satisfies w', and its index is bounded as a function of ε and r. □

5. Power laws

5.1. $x^2 = 1$ 的正性。在本节中我们证明

定理 5.1. 设 G 是一个有限生成群。如果

$$\mathbb{P}\left(x^2 = 1 \text{ on } G\right) > 0$$

关于某种随机游走，则 G 几乎阿贝尔。

请回忆，我们一直假设所有随机游走都是惰性的，即以正概率在一步中停留在原地。这一事实并非关键（不作此假设时，定理基本上仍可用相同的证明得出），但这样做很方便，因为它意味着随机游走测度一致地测量指数。

在本小节余下部分，我们证明上述定理。设 G 是一个有限生成群，且 R_n 是 G 上的一个（惰性）随机游走，使得

$$\limsup_{n\to\infty} \mathbb{P}(R_n^2 = 1) = \alpha > 0.$$

取一个序列 $\{m_k\}$ 使得 $\mathbb{P}(R_{m_k}^2 = 1) \geq \frac{\alpha}{2}$ 对所有 k成立。

引理 5.2. 存在 k_0，使得对于任意 $k \geq k_0$,

$$\limsup_{s\to\infty} \mathbb{P}(R_{m_k}^2 = 1, R_{m_k+s}^2 = 1) > \frac{\alpha^2}{16}.$$

证明。反设不存在这样的 k_0，也就是说，存在 k 的无穷多个取值，使得

$$\limsup_{s\to\infty} \mathbb{P}(R_{m_k}^2 = 1, R_{m_k+s}^2 = 1) \leq \frac{\alpha^2}{16}. \tag{2}$$

写出 $M = \lceil \frac{4}{\alpha} \rceil$。我们按如下方式构造一个序列 $\{k_i'\}_{i=1}^M$。设 k_1' 为满足（2）的最小指数。设 k_2' 为满足（2）且使得

$$\mathbb{P}(R_{m_{k_1'}}^2 = 1, R_{m_{k_2'}}^2 = 1) < \frac{\alpha}{4}$$

（其存在是因为 $\frac{\alpha}{4} > \frac{\alpha^2}{16}$）。令 k_3' 为满足（2）且使得

$$\mathbb{P}(R_{m_{k_j'}}^2 = 1, R_{m_{k_3'}}^2 = 1) < \frac{\alpha}{8} \text{ for } j = 1, 2.$$

我们继续通过归纳定义 $\{k_i'\}$ 对于 $1 \leq i \leq M$，其中 k_i' 选为满足（2）的第一个指数，使得

$$\mathbb{P}(R_{m_{k_j'}}^2 = 1, R_{m_{k_i'}}^2 = 1) < \frac{\alpha}{4(i-1)} \text{ for } j = 1, \ldots, i-1.$$

这样的指标确实存在，因为对于任意 $i \leq M$，都有 $4^{\frac{\alpha}{(i-1)}} > \frac{\alpha^2}{16}$。

由于对于任意 $1 \leq i \leq M$，$\geq \frac{\alpha}{2}$ 都是 $\mathbb{P}(R_{m_{k_i'}}^2 = 1)$，因此可得

$$\mathbb{P}(R_{m_{k_i'}}^2 = 1, R_{m_{k_1'}}^2 \neq 1, \ldots, R_{m_{k_{i-1}'}}^2 \neq 1) > \frac{\alpha}{2} - (i-1) \cdot \frac{\alpha}{4(i-1)} = \frac{\alpha}{4}.$$

但这是一个概率大于 $\frac{\alpha}{4}$ 的 $M = \lceil \frac{4}{\alpha} \rceil$ 两两不相交事件序列，这就产生了矛盾。□

写入 $\beta = \frac{\alpha^2}{16}$。

引理 5.3。

$$\limsup_{n\to\infty} \mathbb{P}\left([G : C_G(R_n)] \le \frac{2}{\beta^2}\right) \ge \frac{\beta^2}{2}.$$

通常， $C_G(R_n)$ 是 G 中 R_n 的中心化子。

证明。固定一个 n 使得

$$\limsup_{s\to\infty} \mathbb{P}(R_n^2 = 1, R_{n+s}^2 = 1) > \beta > 0. \tag{3}$$

由前一个引理可知，这样的 n 有无穷多个。因此存在一个序列$s_1 < s_2 < \cdots$使得

$$\mathbb{P}(R_n^2 = 1, R_{n+s_i}^2 = 1) \ge \beta.$$

写作 $u = R_n^{-1} R_{n+s_i}$，它与 R_{s_i} 具有相同的分布，且与 R_n 独立。注意，方程 $R_n^2 = R_{n+s_i}^2 = 1$ 意味着 $u^{-1} = R_n u R_n^{-1}$，因此

$$\mathbb{P}(u^{-1} = R_n u R_n^{-1}) \ge \beta.$$

如果 R_n' 是一个与 R_n 分布相同的独立副本，我们有

$$\mathbb{P}(u^{-1} = R_n u R_n^{-1} = R_n' u (R_n')^{-1}) \ge \beta^2,$$

so

$$\mathbb{P}([(R_n')^{-1} R_n, u] = 1) \ge \beta^2.$$

由于 $(R_n')^{-1} R_n$ 与 R_{2n} 具有相同的分布，且二者都独立于 u,

$$\mathbb{P}([R_{2n}, u] = 1) \ge \beta^2.$$

因此可得（类似于引理 4.2），

$$\mathbb{P}\left(\mathbb{P}\left([R_{2n}, u] = 1 : R_{2n}\right) \ge \frac{1}{2}\beta^2\right) \ge \frac{1}{2}\beta^2.$$

由于 u 服从长度为 s_i 的随机游走，且与 R_{2n}独立，令 i趋于无穷可得

$$\mathbb{P}\left([G : C_G(R_{2n})] \le \frac{2}{\beta^2}\right) \ge \frac{1}{2}\beta^2.$$

根据引理 5.2 存在无穷多个 n 使得（3）成立。这就证明了该引理。 □

现在我们可以证明该定理了。

定理证明 *5.1*。 由于 G 是有限生成的，因此它的任意有限指数子群都只有有限多个。因此，记

$$Q = \bigcap_{H \le G, [G:H] \le 2/\beta^2} H,$$

我们有 $[G : Q] < \infty$。

Now,

$$\mathbb{P}(R_{2n} \in C_G(Q)) = \mathbb{P}([R_{2n}, Q] = 1) \ge \frac{1}{2}\beta^2,$$

因此 $[G : C_G(Q)] \le \frac{2}{\beta^2} < \infty$。因此， $Q \cap C_G(Q)$ 是 G 的一个有限指数阿贝尔子群，符合要求。□

我们立即得到上述定理的一个推论。

Corollary 5.4. *(1) The law $x^2 = 1$ satisfies a gap.*
(2) The value of $\limsup_{n\to\infty} \mathbb{P}(R_n^2 = 1)$ does not depend on the random walk's step distribution μ, and it is a limit rather than a $\limsup$.

证明。我们首先证明 $x^2 = 1$ 存在间隙。根据定理 5.1，任何以正概率满足 $x^2 = 1$ 的群都是几乎阿贝尔的，因此是剩余有限的。所以该间隙由有限情形中的间隙推出。

For the second part, if $\limsup_{n\to\infty} \mathbb{P}(R_n^2 = 1) > 0$ for some random walk R_n on G, Theorem 5.1 shows that G is virtually abelian. In particular, G is virtually nilpotent, so the corollary follows from [23, Corollary 1.14]. □

定理的证明 4.1(2) 可以推广以证明以下结论：

命题 5.5. 如果一个群 G 在概率意义下满足 $[x^2, y]$，则 G 几乎是二步幂零。

所需的修改很简单，细节从略。

5.2. $x^3 = 1$ 的强间隙。本小节旨在证明以下结果：

定理 5.6。考虑一个有限生成群 G，其具有包含单位元的有限对称生成集 S，并令 R_n 为 G 上的随机游走。那么存在 $\varepsilon > 0$，使得如果

$$\liminf_{n\to\infty} \mathbb{P}\left(R_n^3 = 1\right) > 1 - \varepsilon$$

那么，$x^3 = 1$ 在 G 中成立（因此 G 是有限的）。

我们的证明还找到了一个显式值 ε，使上述定理成立。然而，我们认为这个 ε 并非最优，并且该定理可以针对 limsup 而非 liminf 得到证明。

We prove this result in several steps. Let G be a group, and let $x, y, z, w \in G$. A product of $x^{\pm 1}, y^{\pm 1}, z^{\pm 1}, w^{\pm 1}$ is called **simple** if any letter appears at most once (thus there are only finitely many simple products of any four elements). We say that x, y, z, w are **good** if any simple product of them has order 3. For example, if x, y, z, w are good then $(z^{-1}xw)^3 = 1$ and $(yx^{-1}w^{-1}z)^3 = 1$, but not necessarily $(xyx^{-1}z)^3 = 1$.

Note that the assumption of the theorem suggest that if x, y, z, w are independent random walks with respect to S, then x, y, z, w are good with high probability. Indeed, any simple product of x, y, z, w is also distributed like a random walk with respect to S (with a different number of steps), and therefore has order 3 with high probability.

Our method of proof is as follows. We prove that if x, y, z, w are good, then $[x, y, z, w] = 1$ (we originally verified this with a GAP program, but here we give a human proof of this fact). Therefore, if $\mathbb{P}\left(R_n^3 = 1\right) > 1 - \varepsilon$ for small enough ε, the group G is nilpotent with positive probability. Therefore, G is virtually nilpotent, so it is residually finite, and as $x^3 = 1$ has a gap on finite groups we are finished.

Recall the following standard notation. For any $a, b \in G$ write $a^b = bab^{-1}$, and for any $a_1, \ldots, a_n \in G$ we defined inductively $[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$.

引理 5.7. 如果 $b^3 = (ab)^3 = (ab^{-1})^3 = 1$，那么 $[a^b, a] = 1$。

证明。这由该单位元直接推出。

$$[a^b, a] = \left(\left(ab^{-1}\right)^b\right)^3 \left(b^2a^{-1}\right)^3 \left(\left(b^{-1}\right)^a\right)^3$$

在任何群中都成立。 □

引理 5.8。如果 $[a^b, a] = 1$ 和 $a^3 = 1$，那么 $[a, b]^3 = 1$、$[b, a, a] = 1$ 和 $[a, b]^{-1} = [a^{-1}, b]$。

证明。注意，$[b, a] = a^b a^{-1}$，所以

$$[a, b]^3 = \left(a^b a^{-1}\right)^3 = (a^b)^3 a^{-3} = 1 \tag{4}$$

$$[b, a, a] = [[b, a], a] = [a^b a^{-1}, a] = 1$$

$$[a, b]^{-1} = bab^{-1}a^{-1} = a^b a^{-1} = a^{-1}a^b = a^{-1}bab^{-1} = [a^{-1}, b]. \tag{5}$$

因此，引理得证。 □

Lemma 5.9. *If* $[a^b, a] = [a^c, a] = [a^b, a^c] = [b^a, b] = [(bc)^a, bc] = [c^b, c] = [c^{ba}, c] = 1$, *then* $[a, b, c]^{-1} = [a, c, b]$.

证明。在任意群中

$$[a, bc] = [a, b][a, c]^b \text{ and } [ab, c] = [b, c]^a[a, c], \tag{6}$$

so

$$[a, bc, c] = [[a, b][a, c]^b, c] = [[a, c]^b, c]^{[a,b]}[a, b, c].$$

注意，$[a, c]^b = (c^a c^{-1})^b = c^a(c^{-1})^b$，因此根据假设 $[[a, c]^b, c] = 1$，从而

$$[a, bc, c] = [a, b, c].$$

以类似的方式，

$$[a, bc, b] = [[a, b][a, c]^b, b] = [[a, c]^b, b]^{[a,b]}[a, b, b] \overset{(*)}{=} [[a, c]^b, b]^{[a,b]} = [[a, c]^{[a,b]b}, b^{[a,b]}].$$

As $[b^a, b] = 1$, the elements b and $[a, b]$ commute, which gives $(*)$ and also $b^{[a,b]} = b$. In addition, $[a, b] = a(a^{-1})^b$ and $[a, c] = a(a^{-1})^c$, so our assumptions imply that $[a, b]$ and $[a, c]$ commute. This proves that

$$[a, bc, b] = [[a, c]^b, b] = [a, c, b]^b.$$

最后，由于 $[(bc)^a, bc] = 1$，再次使用 (6)，

$$1 = [[a, bc], bc] = [[a, bc], b][[a, bc], c]^b = [a, c, b]^b[a, b, c]^b,$$

证明了 $[a, c, b] = [a, b, c]^{-1}$，如所需。 □

引理 5.10。如果 $[a, c, b]^{-1} = [a, b, c]$ 和 $[[a, c]^b, [a, c]] = 1$，那么 $[a, b, c] = [c, a, b]$。

Proof. Since $[[a, c]^b, [a, c]] = 1$, we have $[a, c, b]^{-1} = [[a, c], b]^{-1} \overset{(5)}{=} [[a, c]^{-1}, b] = [c, a, b]$, so $[c, a, b] = [a, c, b]^{-1} = [a, b, c]$. □

我们希望能够应用上述引理，其中 a、b、c 是字母、交换子，或字母与交换子的乘积。因此，我们需要以下引理：

Lemma 5.11. *If* $a^3 = (abc)^3 = (ac)^3 = (acb^{-1})^3 = (ac^{-1})^3 = [b^a, b] = [b^c, b] = [c^b, c] = [c^a, c^b] = 1$, *then* $(a[b, c])^3 = 1$.

证明。由 $[b^c, b] = [c^b, c] = 1$，我们有

$$[b,c] \overset{(5)}{=} [b^{-1},c]^{-1} = [c,b^{-1}] \overset{(5)}{=} [c^{-1},b^{-1}]^{-1} = [b^{-1},c^{-1}]. \tag{7}$$

此外，由于 $(abc)^3 = (ac)^3 = (acb^{-1})^3 = (ac^{-1})^3 = 1$，我们有

$$bcabc = a^{-1}c^{-1}b^{-1}a^{-1} \tag{8}$$

$$c^{-1}a^{-1}c^{-1} = aca \tag{9}$$

$$b^{-1}acb^{-1}a = c^{-1}a^{-1}bc^{-1} \tag{10}$$

$$ac^{-1}ac^{-1} = ca^{-1} \tag{11}$$

因此

$$\begin{aligned}
a[b,c]a[b,c] &\overset{(7)}{=} a[b^{-1},c^{-1}]a[b,c] = ab^{-1}c^{-1}bcabcb^{-1}c^{-1} = ab^{-1}c^{-1}(bcabc)b^{-1}c^{-1} = \\
&\overset{(8)}{=} ab^{-1}c^{-1}(a^{-1}c^{-1}b^{-1}a^{-1})b^{-1}c^{-1} = ab^{-1}(c^{-1}a^{-1}c^{-1})b^{-1}a^{-1}b^{-1}c^{-1} = \\
&\overset{(9)}{=} ab^{-1}(aca)b^{-1}a^{-1}b^{-1}c^{-1} = ab^{-1}ac((ab^{-1}a^{-1})b^{-1})c^{-1} = \\
&\overset{[b^a,b]=1}{=} ab^{-1}ac(b^{-1}(ab^{-1}a^{-1}))c^{-1} = a(b^{-1}acb^{-1}a)b^{-1}a^{-1}c^{-1} = \\
&\overset{(10)}{=} a(c^{-1}a^{-1}bc^{-1})b^{-1}a^{-1}c^{-1} = (ac^{-1}a^{-1})(bc^{-1}b^{-1})a^{-1}c^{-1} = \\
&\overset{[c^a,c^b]=1}{=} (bc^{-1}b^{-1})(ac^{-1}a^{-1})a^{-1}c^{-1} = bc^{-1}b^{-1}ac^{-1}a^{-2}c^{-1} = \\
&= bc^{-1}b^{-1}(ac^{-1}ac^{-1}) \overset{(11)}{=} bc^{-1}b^{-1}ca^{-1} = [b,c^{-1}]a^{-1} = \\
&= [c^{-1},b]^{-1}a^{-1} = [c,b]a^{-1} = (a[b,c])^{-1},
\end{aligned}$$

因此 $(a[b,c])^3 = 1$。 □

最后，我们可以证明如下：

命题 5.12. 假设 x、y、z、$w \in G$ 都是良好的。那么 $[x,y,z,w] = 1$。

证明。 我们的第一步是三次应用引理 5.7、方程（4）和引理 5.11。具体细节如下。

We first apply Lemma 5.7 to get that $[x^y, x] = 1$ and similarly for all other disjoint simple products of letters from $\{x, y, z, w, x^{-1}, y^{-1}, z^{-1}, w^{-1}\}$, for example $[(zy)^{xw^{-1}}, zy] = 1$ (recall that x, y, z, w are good, namely any simple product is or order 3). In particular we get $[x^{z^{-1}y}, x] = 1$ which implies $[x^y, x^z] = 1$ (again, for any 3 disjoint simple products).

These facts allow us to apply (4) to get $[x,y]^3 = 1$ and Lemma 5.11 to get $(x[y,z])^3 = 1$, again for any 2 and 3 disjoint simple products. These estimates we can feed back into Lemma 5.7 to get $[[x,y]^z, [x,y]] = [[x,y]^{zw}, [x,y]] = [x^{[y,z]}, x] = [x^{y[z,w]}, x] = 1$ (for the last case we use that if $(y^{-1}x[w,z])^3 = 1$ then one can conjugate with y and get that $(x[w,z]y^{-1})^3 = 1$). Again we conclude from $[x^{y^{-1}[z,w]}, x] = 1$ that $[x^{[z,w]}, x^y] = 1$.

We continue using (4) to get $[[x,y],z]^3 = 1$ and Lemma 5.11 to get $(w[[x,y],z])^3 = 1$. A final round through Lemma 5.7 and (4) gives $[[[x,y],z],w]^3 = 1$.

因此，只要 5.9 引理和 5.10 引理适用，则 a、b、c 是 x、y、z、w 的字母或交换子，且不含共同字母，并且至多有一个交换子

（可能迭代的）出现。一方面，

$$[[x,y],[z,w]] \overset{5.10}{=} [[[z,w],x],y] = [[z,w,x],y] \overset{5.10}{=} [x,z,w,y] = \\ \overset{5.9}{=} [x,z,y,w]^{-1} \overset{5.9}{=} [[x,y,z]^{-1},w]^{-1} \overset{(5)}{=} [x,y,z,w].$$

On the other hand, $[[z,w],[x,y]] = [[x,y],z,w] = [x,y,z,w]$, so $[x,y,z,w]^{-1} = [x,y,z,w]$, which can be written as $[x,y,z,w]^2 = 1$. As $[x,y,z,w]^3 = 1$, it follows that $[x,y,z,w] = 1$. □

现在我们可以完成该定理的证明。

Proof of Theorem 5.6. Assume that $\liminf_{n\to\infty} \mathbb{P}\left(R_n^3 = 1\right) > 1-\varepsilon$. Take four independent random walks X_n, Y_n, Z_n, W_n with respect to S. As previously explained, any simple product of X_n, Y_n, Z_n, W_n is also distributed as a random walk on G with respect to S, so it is of order 3 with high probability. Therefore, the elements X_n, Y_n, Z_n, W_n are good with high probability (that depends only on ε).

If X_n, Y_n, Z_n, W_n are good, by Proposition 5.12 it follows that $[X_n, Y_n, Z_n, W_n] = 1$. Therefore, if ε is small enough, $\liminf_{n\to\infty} \mathbb{P}\left([X_n, Y_n, Z_n, W_n] = 1\right) > 0$, so by [23, Theorem 1.5] the group G is virtually nilpotent. By [10, Theorem 3.25], any nilpotent groups is residually finite, so G is also residually finite. As the law $x^3 = 1$ has a gap for finite groups [15], if ε is small enough than G must satisfy $x^3 = 1$, and we are done. □

5.3. $x^m = 1$ 的非正性结果。现在我们证明，律 $x^m = 1$ 不满足正性性质。我们使用一个与 [16] 中出现的 Frobenius 群示例类似的例子。

Let us choose a matrix $A \in \mathrm{Mat}_{m-1}(\mathbb{Z})$ such that $A^m = I$ and $\det(A - I) \neq 0$. Then we have $(A - I)(A^{m-1} + \cdots + A + I) = 0$ and since $\det(A - I) \neq 0$ we have $A^{m-1} + \cdots + A + I = 0$. For example, one can take the companion matrix of $1 + x + \cdots + x^{m-1}$, namely the matrix $A = (a_{ij})_{i,j=1\cdots m-1}$ with

$$a_{ij} = \begin{cases} 1, & \text{if } i = j+1, \\ -1, & \text{if } j = m-1, \\ 0, & \text{otherwise.} \end{cases}$$

考虑半直积 $G = \mathbb{Z}^{m-1} \rtimes_A \mathbb{Z}/m\mathbb{Z}$，即$\mathbb{Z}/m\mathbb{Z}$ 的作用由 A的幂给出。

Proposition 5.13. *Let $G = \mathbb{Z}^{m-1} \rtimes_A \mathbb{Z}/m\mathbb{Z}$, and let R_n be a (lazy) random walk on G. Then $x^m = 1$ with probability at least $\frac{\phi(m)}{n}$ with respect to the random walk R_n, where $\phi(m)$ is the Euler's totient function, but G does not satisfy $x^m = 1$ virtually.*

证明。令我们取 $(v,k) \in \mathbb{Z}^{m-1} \rtimes_A \mathbb{Z}/m\mathbb{Z}$。那么我们有

$$(v,k)^m = ((A^{k(m-1)} + \cdots + A^{2k} + A^k + I)v, mk) \\ = ((A^{k(m-1)} + \cdots + A^{2k} + A^k + I)v, 0).$$

如果 k 和 m 互素，那么上面的公式可以简化为：得到

$$(v,k)^m = ((A^{m-1} + \cdots + A + I)v, 0) = (0,0).$$

Let $X_k = \{(v,k), \text{ where } v \in \mathbb{Z}^{m-1}\} \subset G$. We note that $\mathbb{P}(R_n \in X_k) \to \frac{1}{m}$ as $n \to \infty$. Then $\mathbb{P}(R_n^m = 1) \geq \mathbb{P}(R_n \in \cup_{\gcd(k,m)=1} X_k) \to \frac{\phi(m)}{m}$, where $\gcd(k,m)$ is the greatest common divisor and this proves the first claim.

Now we show that G does not contain a torsion finite index subgroup of exponent n. First note that X_0 is a subgroup of G of index m such that for any $x \in X_0 \setminus \{0\}$ we have $x^m \neq 1$, so X_0 does not satisfy the law $x^m = 1$ virtually. Therefore, by Remark 2.5, the group G does not satisfy the law virtually. □

Remark 5.14. Let us note that we can get a higher probability by considering the group $G = \mathbb{Z}^{p-1} \rtimes_A \mathbb{Z}/p\mathbb{Z}$, where p the largest prime factor of m. G satisfies $x^p = 1$ and hence $x^m = 1$ with probability at least $1 - \frac{1}{p} = \frac{\varphi(p)}{p} \geq \frac{\varphi(m)}{m}$. It follows from the proof that G does not satisfy the law $x^m = 1$ virtually,

6. 平衡律的交换子

In the coming sections, we will be interested in laws of the form $[w_1, w_2]$. We will usually assume that w_1, w_2 are laws on disjoint letters. We will show that in many cases, such laws do not satisfy a gap result, and also do not satisfy a positivity result.

In fact, our results are somewhat stronger. We will show that for such laws, we can find a group Γ, which contains a non-abelian free group as a subgroup, and satisfies the following: one can find generating sets S of Γ so that the probabilty that Γ satisfies $[w_1, w_2]$ with respect to an S-random walk can be arbitrarily close to 1.

我们作如下区分：若一个律的阿贝尔化是平凡的，就称它为平衡的。我们将根据内层的律是否平衡，分别讨论律的交换子。

Remark 6.1. If G has an element of infinite order and w is a non-balanced law, then G cannot satisfy w virtually. Indeed, let $H_0 \cong \mathbb{Z}$ be a subgroup generated by an element of infinite order and Λ be a finite index subgroup of G, then $\Lambda \cap H_0$ is a non-trivial finite index subgroup of H_0. Let $w = w(x_1, \dots x_n)$ be a non-balanced law and the total degree of some variable x_k is not zero. Let us fix some $a \neq 1$ in $\Lambda \cap H_0$. For $x_i = 1$ for $i \neq k$ and $x_k = a$ we have $w(x_1, \dots x_n) \neq 1$, so any finite index subgroup Λ does not satisfy w and G does not satisfy w virtually.

In this section we discuss the case of a commutator of two balanced laws. We first present the proof for the metabelian law $[[x,y],[z,w]] = 1$; we then generalize it to an arbitrary commutator law $[w_1, w_2] = 1$ (where w_1, w_2 are balanced).

6.1. 随机游走的词路径。

Definition 6.2. *For a word $w \in \mathrm{F}_d$ and random walks $R_n^{(1)}, \dots, R_n^{(d)}$, we write $\gamma = \gamma(w; R_n^{(1)}, \dots, R_n^{(d)})$ to be the path defined by w when substituting the random walks $R_n^{(1)}, \dots, R_n^{(d)}$. Namely, if $w = a_1^{\varepsilon_1} \cdots a_\ell^{\varepsilon_\iota}$ where $a_j \in \{1, \dots, d\}$ and $\varepsilon_j \in \{\pm 1\}$. Then $\gamma = (\gamma_0, \dots, \gamma_{\ell n})$ with*

$$\gamma_{jn+k} = \begin{cases} \left(R_n^{(a_1)}\right)^{\varepsilon_1} \cdots \left(R_n^{(a_j)}\right)^{\varepsilon_{j+}} R_k^{(a_{j+1})} & \varepsilon_{j+1} = 1 \\ \left(R_n^{(a_1)}\right)^{\varepsilon_1} \cdots \left(R_n^{(a_j)}\right)^{\varepsilon_j} \left(R_n^{(a_{j+1})}\right)^{-1} R_{n-k}^{(a_{j+1})} & \varepsilon_{j+1} = -1. \end{cases} \tag{12}$$

对所有 $j \in \{0, \dots, \ell-1\}$和 $k \in \{1, \dots, n\}$，且 γ_0为群单位元。

In words, the path is constructed by first following $(R_n^{(i_1)})^{\varepsilon_1}$, then following the steps of $(R_n^{(i_2)})^{\varepsilon_2}$ and so on. In particular, it is indeed a path in the Cayley graph, i.e. γ_i and γ_{i+1} are always neighbors.

6.2. **The metabelian law.** We turn to studying the law $[[x,y],[z,w]]=1$. Our aim is to show that this law does not satisfy a general gap result as well as any positivity result. We do this by studying the wreath product $H\wr\mathbb{Z}^5$ for a non-abelian group H, and proving the following theorem:

Theorem 6.3. *Let H be a non-abelian group generated by two elements a,b, and consider the wreath product $\Gamma=H\wr\mathbb{Z}^5$. Then for any $\varepsilon>0$ there exists a symmetric generating set S of Γ of size 160 such that, if X_n,Y_n,Z_n,W_n are independent simple random walks on Γ where each step is uniform on S,*

$$\liminf_{n\to\infty}\mathbb{P}\left([[X_n,Y_n],[Z_n,W_n]]=1\right)\geq 1-\varepsilon.$$

换句话说， Γ 以概率 $\geq 1-\varepsilon$ 满足亚交换律，其中概率是相对于由 S诱导的简单随机游走而言的。

In fact, the generating set can be taken as follows: Let $\pm e_i$ denote the 10 standard generators of $\mathbb{Z}^5$. We then take $S=\{s_1ms_2 : s_1,s_2\in\{(a^{\pm1}\delta_{\underline{0}},\underline{0}),(b^{\pm1}\delta_{ke_1},\underline{0})\},m\in\{(\underline{\mathrm{id}_H},\pm e_i)\}\}$ for a large enough k.

备注。（1）对于采用以下 14 个生成元的随机游走，同一定理也成立： $\pm e_i$、$(a^{\pm1}\delta_{\underline{0}},0)$ 和 $(b^{\pm1}\delta_{ke_1},0)$。不过，为了简化证明，我们采用更大的生成集。

(2) 当 H 由多于 2 个元素生成时，类似的结果也成立。在这种情况下，需要为 H选择一个有限生成集 S，并对 $H\wr\mathbb{Z}^5$ 的生成集中的每个生成元，将其置于远离其他生成元的位置。

(3) One can use this result to find a sequence of probability measures $M=\{\mu_n\}$ that measures index uniformly, such that $\mathbb{P}_M\left([[x,y],[z,w]]=1 \text{ on } \Gamma\right)=1$. To do this, for each n one takes a generating set $S^{(n)}$ of Γ such that one has $\mathbb{P}_{S^{(n)}}\left([[x,y],[z,w]]=1 \text{ on } G\right)>1-\frac{1}{n}$. For each n, take μ_n to be the distribution of a random walk with step distribution uniform on $S^{(n)}$, after many steps. By taking this number of steps to be large enough, one can make sure that the supports of μ_n cover all of G, M measures index uniformly, and $\mathbb{P}_M\left([[x,y],[z,w]]=1 \text{ on } \Gamma\right)=1$.

Before proving the theorem, let us mention its implications. Taking $H=\mathrm{F}_2$ to be the free group on 2 generators, we get that the group $F_2\wr\mathbb{Z}^5$ satisfies the metabelian law with probability arbitrarily close to 1. Because of its free subgroups it does not satisfy any law, and hence does not satisfy and law virtually. Thus the metabelian law does not satisfy neither gap nor positivity.

我们转向定理的证明6.3。我们需要以下关于缠绕积中交换子的观察：

Fact 6.4. *Let $L_1,L_2\in\bigoplus_{g\in G}H$. If for any $x\in G$ we have $[L_1(x)\ L_2(x)]=\mathrm{id}_H$, then in the wreath product $H\wr G$ we have $[(L_1,\mathrm{id}_G),(L_2,\mathrm{id}_G)]=\mathrm{id}_{H\wr G}$.*

我们还需要关于 $\mathbb{Z}^5$中随机路径交点的若干估计，以下两个引理给出了这些估计。在 $\mathbb{Z}^5$ 上的所有随机游走均相对于标准生成集进行。

引理 6.5。设 $\gamma = (X_n)_{n=0}^{\infty}$ 和 $\gamma' = (Y_n)_{n=0}^{\infty}$ 是 $\mathbb{Z}^5$ 上分别从 x_0 和 y_0 出发的两条独立简单随机游走路径。则存在一个常数$C > 0$ 使得

$$\mathbb{P}(\gamma \cap \gamma' \neq \varnothing) < C \cdot d(x_0, y_0)^{-\frac{1}{2}}.$$

下文中，$\gamma \cap \gamma'$ 表示出现在两条路径中的顶点集合。

证明。设 $r = d(x_0, y_0)$，并将路径之间的交点数记为 $K = |\gamma \cap \gamma'|$。然后

$$\mathbb{P}(\gamma \cap \gamma' \neq \varnothing) = \mathbb{P}(K \geq 1) \leq \mathbb{E}[K] \leq \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \mathbb{P}(X_n = Y_m) = \sum_{m+n \geq r} \mathbb{P}(X_n = Y_m).$$

设 S_n 是 $\mathbb{Z}^5$ 上的简单随机游走。那么 $Y_m - X_n - (y_0 - x_0)$ 与 S_{n+m} 具有相同的分布。众所周知，对于所有 $x \in \mathbb{Z}^5$，$\mathbb{P}(S_n = x) \leq Cn^{-5/2}$ 】【。

$$\mathbb{P}(\gamma \cap \gamma' \neq \varnothing) \leq \sum_{n+m \geq r} \mathbb{P}(S_{n+m} = x_0 - y_0) \leq \sum_{n+m \geq r} C \frac{1}{(n+m)^{\frac{5}{2}}} \leq C' r^{-\frac{1}{2}}$$

如所要求。 □

我们备注，正确的渐近行为是 $\mathbb{P}(\gamma \cap \gamma' \neq \varnothing) \approx d(x_0, y_0)^{-1}$，但我们不需要这种额外的精确性，因此不会证明它。

Lemma 6.6. *Let $\{X_i, Y_i, Z_i, W_i\}_{i=1}^{n}$ be four simple random walks on $\mathbb{Z}^5$. Consider each of the random walks as a path in $\mathbb{Z}^5$, and denote by γ, γ' the paths (of length $4n$) described by the commutators $[X_n, Y_n], [Z_n, W_n]$ respectively. Denote by $\gamma' + v$ the translation of γ' by the vector v.*

那么，对于任意 $\varepsilon > 0$，都存在一个与 n 无关的 k_0，使得对于 $k \geq k_0$，我们有

$$\mathbb{P}(\gamma \cap (\gamma' + ke_1) \neq \varnothing) < \varepsilon.$$

Proof. Notice that each of the commutator paths is a loop starting at the origin that can be divided into two simple random walk paths of length $2n$ each: for instance, γ can be divided into $X_n Y_n$ and $\overleftarrow{Y_n}\overleftarrow{X_n}$. The arrow indicates that the path is traversed in the opposite direction, though this will not matter to us. Therefore by symmetry

$$\begin{aligned}\mathbb{P}(\gamma \cap (\gamma' + ke_1) \neq \varnothing) \leq\ & \mathbb{P}(X_n Y_n \cap (Z_n W_n + ke_1) \neq \varnothing) + \\ & + \mathbb{P}(\overleftarrow{Y_n}\overleftarrow{X_n} \cap (Z_n W_n + ke_1) \neq \varnothing) + \\ & + \mathbb{P}(X_n Y_n \cap (\overleftarrow{W_n}\overleftarrow{Z_n} + ke_1) \neq \varnothing) + \\ & + \mathbb{P}(\overleftarrow{Y_n}\overleftarrow{X_n} \cap (\overleftarrow{W_n}\overleftarrow{Z_n} + ke_1) \neq \varnothing).\end{aligned}$$

每个术语都可以由 $\mathbb{Z}^5$ 起始距离为 k 的两个无限简单随机游走的相交概率作为上界。根据引理6.5，该概率有上界 $Ck^{-\frac{1}{2}}$，因此引理得证。□

现在我们已经可以证明主要定理了。

定理的证明 *6.3*。固定某个 $k \geq 0$。回忆一下，生成集 S 由标准生成元 $\pm e_i$ 组成，它们属于 $\mathbb{Z}^5$，$(a^{\pm 1}\delta_0, \pm e_i)$ 和 $(b^{\pm 1}\delta_{ke_1}, \pm e_i)$。设

X_n, Y_n, Z_n, W_n 是相互独立的简单随机游走，其步分布在 S上均匀。

Consider the commutator paths γ and γ' of $[X_n, Y_n]$ and $[Z_n, W_n]$ respectively as in Lemma 6.6, and write $[X_n, Y_n] = (L_1, \underline{0})$ and $[Z_n, W_n] = (L_2, \underline{0})$. Notice that for $x \in \mathbb{Z}^5$, $L_1(x) = \mathrm{id}$ for $x \notin \gamma \cup (ke_1 + \gamma)$, $L_1(x) \in A := \{a^n\}_{n=-\infty}^{\infty}$ for $x \in \gamma \setminus (ke_1 + \gamma)$ and $L_1(x) \in B := \{b^n\}_{n=-\infty}^{\infty}$ for $x \in (ke_1 + \gamma) \setminus \gamma$.

Fix $\varepsilon > 0$. By Lemma 6.6 we can choose k large enough so that with probability $\geq 1 - \varepsilon$ the commutator loops satisfy $\gamma \cap (ke_1 + \gamma') = \varnothing$ and $(\gamma + ke_1) \cap \gamma' = \varnothing$. Under this event, any $x \in \mathbb{Z}^5$ falls into at least one of the following cases:

(1) $x \notin \gamma \cup (ke_1 + \gamma)$. In this case $L_1(x) = \mathrm{id}_H$ hence $[L_1(x)\ L_2(x)] = \mathrm{id}_H$.
(2) $x \notin \gamma' \cup (ke_1 + \gamma')$. In this case $L_2(x) = \mathrm{id}_H$ hence $[L_1(x)\ L_2(x)] = \mathrm{id}_H$.
(3) $x \in (\gamma \cap \gamma') \setminus ((ke_1 + \gamma) \cup (ke_1 + \gamma'))$. In this case $L_1(x)\ L_2(x) \in A$ and thus $[L_1(x)\ L_2(x)] = \mathrm{id}_H$.
(4) $x \in ((ke_1 + \gamma) \cap (ke_1 + \gamma')) \setminus (\gamma \cup \gamma')$. In this case $L_1(x)\ L_2(x) \in B$ and thus $[L_1(x)\ L_2(x)] = \mathrm{id}_H$.

现在由事实6.4可知 $[[X_n, Y_n], [Z_n, W_n]]$ 是平凡的。因此

$$\mathbb{P}\left([[X_n, Y_n], [Z_n, W_n]] = 1\right) \geq \mathbb{P}\left(\gamma \cap (ke_1 + \gamma') = (\gamma + ke_1) \cap \gamma' = \varnothing\right) \geq 1 - \varepsilon$$

正如所要求的。 □

6.3. 一般情形。前一定理的思路可以推广，从而得到以下结果：

Theorem 6.7. *Let $w_1 \in \mathrm{F}_d$ and $w_2 \in \mathrm{F}_{d'}$ be two balanced laws such that $[w_1, w_2]$ is not trivial. Let H be a non-abelian group generated by two elements a, b, and consider the wreath product $\Gamma = H \wr \mathbb{Z}^5$. Then for any $\varepsilon > 0$ there exists a symmetric generating set S of Γ of size 160 such that, if $R_n^{(1)}, \ldots, R_n^{(d)}, S_n^{(1)}, \ldots, S_n^{(d')}$ are independent simple random walks on Γ where each step is uniform on S,*

$$\liminf_{n\to\infty} \mathbb{P}\left([w_1(R_n^{(1)}, \ldots, R_n^{(d)}), w_2(S_n^{(1)}, \ldots, S_n^{(d')})] = 1\right) \geq 1 - \varepsilon.$$

事实上，生成集 S 可以如定理 *6.3* 中所示选取。

特别地，对于任意两个平衡律 w_1 和 w_2，律 $[w_1, w_2]$ 不满足间隙或正性结果。

该定理的证明将类似于定理 6.3的证明。我们再次考虑群 $\Gamma = H \wr \mathbb{Z}^5$，其生成集与上文相同。

我们首先给出一个类似于引理 6.5 的结果，讨论此类路径的交点。注意，这些已不再是随机游走路径，但仍可分解为随机游走线段。

Lemma 6.8. *Let $R_n^{(1)}, \ldots, R_n^{(d)}$ and $S_n^{(1)}, \ldots, S_n^{(d')}$ be $d + d'$ independent random walks on $\mathbb{Z}^5$ of length n. Set $\gamma = \gamma(w_1, R_n^{(1)}, \ldots, R_n^{(d)})$ and $\gamma' = \gamma(w_2, S_n^{(1)}, \ldots, S_n^{(d')})$ to be the corresponding paths. Then for any $\varepsilon > 0$ there exists k_0, independent of n, such that for $k \geq k_0$ we have*

$$\mathbb{P}\left(\gamma \cap (\gamma' + ke_1) \neq \varnothing\right) < \varepsilon.$$

证明。记 γ_i 和 γ_i' 为 i中第 γ 以及 γ'中的第 i6.5：记 $K = |\gamma \cap (\gamma' + ke_1)|$ 为这些路径之间的交点数。

Then

$$\mathbb{P}\left(\gamma \cap (\gamma' + ke_1) \neq \varnothing\right) = \mathbb{P}(K \geq 1) \leq \mathbb{E}[K] \leq \sum_{i=0}^{|\gamma|} \sum_{i'=0}^{|\gamma'|} \mathbb{P}(\gamma_i = \gamma'_{i'} + ke_1) =$$

$$= \sum_{i=0}^{|\gamma|} \sum_{i'=0}^{|\gamma'|} \mathbb{P}(\gamma_i - \gamma'_{i'} = ke_1). \tag{13}$$

Examining the definition of γ (12) we see that γ_i is the sum of several copies of various $R_n^{(j)}$, some with positive sign and some with negative sign, as well as one copy of $R_k^{(j_0)}$ for some j_0 (coming from the random walk path on which the i'th step lies). We wish to write γ as a combination of *independent* random walks, so we write $R_n^{(j_0)} = R_k^{(j_0)} + (R_n^{(j_0)} - R_k^{(j_0)})$ and note that $R_n^{(j_0)} - R_k^{(j_0)}$ is itself a random walk, and is independent of $R_k^{(j_0)}$ (and, of course, of the other $R_n^{(j)}$). We have thus arrived at a representation

$$\gamma_i = \sum_{j=1}^{d+1} b_j X_{m_j}^{(j)}$$

其中 $b_j \in \mathbb{Z}$和 $m_j = n$ 除可能有两个 j值外，均为独立随机游走。此外，每个不同于 n 的 m_j 值至多对应 $2|w|$个不同的 i值，并且每个 $|b_j| \leq |w_1|$。

对 γ' 重复此计算，我们可以写出

$$\gamma_i - \gamma'_{i'} = \sum_{j=1}^{d+d'+2} b_j X_{m_j}^{(j)}.$$

Rearrange the nonzero terms $X^{(j)}$ so that $m_1 \geq m_2 \geq \cdots$. Let $l = \max\{|w_1|, |w_2|\}$. As $|b_j| \leq l$ for all j, we get that if $m_1 < \frac{k}{l(d+d'+2)} = c'k$, then $|\gamma_i - \gamma'_{i'}| < k$, and cannot be equal to ke_1. Note that after rearranging, the number of (i, i') for which $m_1 = M$ is at most $2Ml^2$, for any $M < n$. For $M = n$ it will be enough to use the trivial bound that the number of couples (i, i') with $m_1 = n$ is smaller than the total number of couples, $|w_1||w_2|n^2$.

对 $X_{m_2}^{(2)}$、…、$X^{(d+d'+2)}{}_{m_{d+d'+2}}$ 的取值进行条件化。我们得到

$$\mathbb{P}(\gamma_i - \gamma'_{i'} = ke_1) \leq \max_{v \in \mathbb{Z}^d} \mathbb{P}\left(\gamma_i - \gamma'_{i'} = ke_1 \,\middle|\, \sum_{j=2}^{d+d'+2} b_j X_{m_j}^{(j)} = v\right)$$

$$= \max_{v \in \mathbb{Z}^d} \mathbb{P}\left(b_1 X_{m_1}^{(1)} = ke_1 - v\right) \leq C m_1^{-5/2}.$$

利用上文说明的 m_1 可能取值的重数，以及若 $m_1 < c'k$ 则该概率为零这一事实，可以估算（13）中的和，

$$\sum_{i=0}^{|\gamma|} \sum_{i'=0}^{|\gamma'|} \mathbb{P}(\gamma_i - \gamma'_{i'} = ke_1) = \sum_{M=c'k}^{n} \sum_{(i,i'):m_1=M} \mathbb{P}(\gamma_i - \gamma'_{i'} = ke_1)$$

$$\leq \sum_{M=c'k}^{n-1} 2Ml^2 \cdot CM^{-5/2} + l^2 n^2 \cdot Cn^{-5/2} \leq Ck^{-1/2}$$

（最后一个常数可能依赖于 w_1 和 w_2）。由（13）可证得该引理。 □

现在我们可以证明这个定理。

Proof of Theorem 6.7. This is essentially the same proof as Theorem 6.3. Since tha base group $\mathbb{Z}^5$ is abelian and the laws w_1, w_2 are balanced, each one of them defines a loop. By Lemma 6.8, the probability that the w_1-loop and the translation of the w_2-loop are disjoint (and vice versa) can be made arbitrarily close to 1 by choosing k large enough. The rest of the proof remains verbatim as the proof of the metabelian case. □

7. Commutators of a power and a balanced law

设我们取一个循环置换的矩阵 $A_0 = (a_{ij})_{1 \le i,j \le m}$，也就是说

$$a_{ij} = \begin{cases} 1 & \text{if} \quad j - i \equiv 1 \pmod m, \\ 0 & \text{otherwise.} \end{cases}$$

对于任意整除 m 的 d，考虑由以下内容定义的子空间 $V_d \subset \mathbb{C}^m$

$$V_d = \left\{ (x_1, \cdots x_m) \in \mathbb{C}^m : \forall 1 \le i \le \frac{m}{d} : \quad x_i + x_{i+\frac{m}{d}} + \cdots + x_{i+\frac{(d-1)m}{d}} = 0 \right\}.$$

We have $\dim V_d = m - \frac{m}{d}$, and each V_d is A_0-invariant. Let us fix a primitive m-th root of unity ξ. The vectors $v_k := (1, \xi^k, \xi^{2k}, \cdots, \xi^{(m-1)k})$ are eigenvectors of A_0, i.e. $A_0 v_k = \xi^k v_k$. Note also that $v_k \in V_d$ if and only if d does not divide k, so the number of such v_k is exactly $m - \frac{m}{d}$, and they form a basis of V_d.

Let us define the space $V = \cap_{1 \ne d | m} V_d$. By the construction, V has the basis $\{v_k\}_{\gcd(k,m)=1}$, hence $\dim V = \varphi(m)$, where φ is the Euler's totient function, and the eigenvalues of $A_0|_V$ are exactly the primitive m-th roots of unity ξ^k with $\gcd(k, m) = 1$. The space V is defined by rational equations, so $V \cap \mathbb{Z}^m \cong \mathbb{Z}^{\varphi(m)}$. Moreover, $A_0 \cdot V = V$ and $A_0 \cdot \mathbb{Z}^m = \mathbb{Z}^m$, hence $A_0 \cdot (V \cap \mathbb{Z}^m) = V \cap \mathbb{Z}^m$.

Fix a $\mathbb{Z}$-basis e_i, $i = 1, \ldots, \varphi(m)$ of $V \cap \mathbb{Z}^m$. For convenience, we identify $V \cap \mathbb{Z}^m$ with $\mathbb{Z}^{\varphi(m)}$, by identifying the $\mathbb{Z}$-basis e_i with the standard generators of $\mathbb{Z}^{\varphi(m)}$. Let A be the matrix of $A_0|_V$ in the basis $\{e_i\}$. Observe that since $A_0^m = 1$, we have $A^m = 1$.

引理 7.1. 设 A 为上述定义的矩阵，且 $f(x) \in \mathbb{Q}[x]$。那么对于矩阵 $M = f(A)$，我们有 $M = 0$ 或 $\det(M) \ne 0$.

Proof. As A is diagonalizable with eigenvalues ξ^k for any $\gcd(k, m) = 1$, the matrix $f(A)$ is diagonalizable with eigenvalues $f(\xi^k)$ for such k. If $f(\xi^k) = 0$ for some k with $\gcd(k, m) = 1$, then f is divisible by the cyclotomic polynomial $\Phi_m(x)$, and thus $f(\xi^j) = 0$ for any j with $\gcd(m, j) = 0$, i.e. $M = f(A) = 0$. Otherwise, M has no zero eigenvalues, so $\det(M) \ne 0$. □

Let us consider the group $G_m = \mathbb{Z}^{\varphi(m)} \rtimes_A \mathbb{Z}/m\mathbb{Z}$, where the semidirect product is taken using the matrix A defined as above. Consider a simple random walk R_n on G_m corresponding to the generating set $(\pm e_i, k), (0, k)$ where $i = 1, \ldots, \varphi(m)$, $k = 0, \ldots, m - 1 \in \mathbb{Z}/m\mathbb{Z}$.

Theorem 7.2. *Let H be a non-abelian group generated by two elements a and b and consider the wreath product $\Gamma = H \wr G_m^5$. Then for any $\varepsilon > 0$ and any balanced law $w = w(y_1, \ldots, y_d)$ there exists a symmetric generating set S on Γ such that if*

X_n, $Y_{(1)n}$, .. ., $Y_{(d)n}$是相互独立的简单随机游走，其中每一步在 S上均匀分布，且 Γ

$$\liminf_{n\to\infty} \mathbb{P}\left([(X_n)^m, w(Y_n^{(1)}, \dots, Y_n^{(d)})] = 1\right) \geq \left(\frac{\varphi(m)}{m^{d+1}}\right)^5 - \varepsilon.$$

换句话说， Γ 以正概率满足关于由 S诱导的简单随机游走的律 $[x^m, w]$ 。

As before, the theorem holds one H is taken to be the free group on two generators, and in this case, since this group contains a free subgroup it cannot satisfy any law virtually, so we conclude that $[x^m, w(y_1, \dots, y_d)]$ does not satisfy positivity.

To prove this theorem we will use a strategy similar to the proof of Theorem 6.3. In particular, recall the definition of the path of a word (Definition 6.2). Let $R_n^{(1)}, \dots, R_n^{(d+1)}$ be independent random walks on G_m^5 and let γ and γ' be the paths of $\left(R_n^{(d+1)}\right)^m$ and $w(R_n^{(1)}, \dots, R_n^{(d)})$. Our goal is to prove that $\mathbb{P}(\gamma \cap \gamma' q \neq \varnothing)$ is small for an appropriate $q \in G_m^5$.

首先，我们希望简化该表述。我们将假设 $q = (q_0, .., q_0)$ 对于某个 $q_0 \in G_m$ ，然后

$$\mathbb{P}(\gamma \cap \gamma' q \neq \varnothing) \leq \sum_{\substack{k \leq mn \\ l \leq n|w|}} \mathbb{P}((\gamma'_{l,1})^{-1}\gamma_{k,1} = q_0)^5,$$

where γ'_l is the l-th step of γ', γ_k is the k-th step of x^m and also $\gamma'_{l,1}$ and $\gamma_{k,1}$ are the first "coordinates" of γ'_l and γ_k respectively. As in the proof of Lemma 6.8, we may write

$$(\gamma'_{l,1})^{-1}\gamma_{k,1} = \widehat{w}_{k,l}(R_r^{(1)}, R_{n-r}^{(2)}, R_{r'}^{(3)}, R_{n-r'}^{(4)}, R_n^{(5)}, \dots R_n^{(d+3)})$$

其中 $R_r^{(1)}$、$R_{n-r}^{(2)}$、$R_{r'}^{(3)}$、$R_{n-r'}^{(4)}$、$R_n^{(5)}$、$\dots R_n^{(d+3)}$ 是独立随机游走，且 r 取决于 k， r' 取决于 l。因此

$$\mathbb{P}(\gamma \cap \gamma' q \neq \varnothing) \leq \sum_{\substack{k \leq nm \\ l \leq n|w|}} \left(\mathbb{P}(\widehat{w}_{k,l}(R_r^{(1)}, R_{n-r}^{(2)}, R_{r'}^{(3)}, R_{n-r'}^{(4)}, R_n^{(5)}, \dots R_n^{(d+3)}) = q)\right)^5.$$

Therefore the proof of Theorem 7.2 boils down to getting an upper bound on the probability that a word evaluated at some random walks will hit a far-away point. This was done in §6 for abelian groups. Here G_m is not abelian, however we can exploit its structure to get a similar result.

引理 7.3. 对于任意固定的字 $\widehat{w} = \widehat{w}(z_1, .., z_u)$，存在一个有限集合 $B \subset \mathrm{Mat}_{\varphi(m)}(\mathbb{Z})$，使得对于任意 $(v_i, k_i) \in G_m$ ，我们都有

$$\widehat{w}((v_1, k_1), \dots, (v_u, k_u)) = \left(\sum_{i=1}^{u} b_i \cdot v_i, *\right)$$

对于某个 $b_i \in B$，其中 $*$ 是 $\mathbb{Z}/m\mathbb{Z}$ 的某个元素。

证明。 G_m 中的乘法和求逆由第一坐标乘以 A的幂给出。因此，我们可以将 B 取为所有长度不超过 $|\widehat{w}|$的 $\pm A^k$之和的集合。□

Let $q = (v_0, k_0) \in G_m$, and let $R^i_* = (v_i, k_i)$ be random walks on G_m. Write $B = B(\widehat{w})$ and $\widehat{w}_{k,l}(R^{(1)}_r, R^{(2)}_{n-r}, R^{(3)}_{r'}, R^{(4)}_{n-r'}, R^{(5)}_n, \dots, R^{(d+3)}_n) = \left(\sum_{i=1}^{d+3} b_i \cdot v_i, *\right)$ by the previous lemma. The b_i's only depend on $k_1, \dots, k_{d+3}$, but actually we do not need to calculate them. Instead we can use the fact that B is finite together with a union bound. Thus we need to bound the probabilities $\mathbb{P}\left(\sum_i b_i v_i = v_0\right)$.

引理 7.4。对于任意 $n > 0$ 和任意 $b \in B \setminus \{0\}$，如果 R_n 是 G_m 上的随机游走，并且如果 $R_n = (v, k)$ 那么

$$\mathbb{P}(b \cdot v = v_0) \le C n^{-\varphi(m)/2} e^{-c|v_0|^2/n}.$$

Proof. By Lemma 7.1 for $b \in B \setminus \{0\}$ we have $\det(b) \neq 0$. Now $\mathbb{P}(b \cdot v = v_0) = \mathbb{P}(v = b^{-1} \cdot v_0)$ and $|b^{-1} \cdot v_0| \ge c|v_0|$ with $c = 1/\max_{b \in B \setminus \{0\}} ||b||$. The lemma then follows from the usual heat kernel bound for random walks in $\mathbb{Z}^{\varphi(m)}$. □

引理 7.5。对于随机游走的任意固定长度 $R^{(i)}_*$ 和任意 $b_1, \dots, b_{d+3} \in B$，记为 $R^{(i)}_* = (v_i, k_i)$，我们有：

$$\mathbb{P}\left(\sum_i b_i \cdot v_i = v_0\right) \le C s^{-\varphi(m)/2} e^{-c|v_0|^2/s}.$$

其中 $s = \sum_{i:\ b_i \neq 0} \mathsf{len}(R^{(i)})$】【。

证明。直接计算表明，上述引理中的两个界分别带有 $n = n_1$ 和 $n = n_2$，它们的卷积是同类型的函数，带有 $n = n_1 + n_2$，常数可能不同。□

We now return to $\widehat{w}_{k,l} = \widehat{w}_{k,l}(R^{(1)}_r, R^{(2)}_{n-r}, R^{(3)}_{r'}, R^{(4)}_{n-r'}, R^{(5)}_n \dots, R^{(d+3)}_n)$. We wish to simply sum over the finite set of possibilities for the b_i, but we need to restrict the set slightly. We therefore note that b_1 and b_2 cannot both be zero. This is because $R^{(1)}_r$ and $R^{(2)}_{n-r}$ appear in $\widehat{w}_{k,l}$ together, except the very last letter in $\widehat{w}_{k,l}$ which is $R^{(1)}_r$. The same holds for b_3 and b_4. We get that $s \ge \min\{r, n-r\} + \min\{r', n-r'\}$. Denote this value by s'. Since $s^{-\frac{\varphi(m)}{2}} e^{\frac{-|v_0|^2}{s}}$ as a function of s takes a maximum value at $s = \frac{2|v_0|^2}{\varphi(m)}$, we get

$$s^{-\varphi(m)/2} e^{-|v_0|^2/s} \le \max_{s \ge s'} s^{-\varphi(m)/2} e^{-|v_0|^2/s} \le C \max\{s', |v_o|^2\}^{-\varphi(m)/2}.$$

这使得可以写出

$$\begin{aligned}\mathbb{P}(\widehat{w}_{k,l} = q) &\le \sum_{\substack{b_1,\dots,b_{d+3} \in B \\ b_1 \neq 0 \text{ or } b_2 \neq 0 \\ b_3 \neq 0 \text{ or } b_4 \neq 0}} \mathbb{P}\left(\sum_j b_j v_j = v_0\right) \\ &\le \sum_{b_1,\dots,b_{d+3} \in B} C \max\{s', |v_0|^2\}^{-5\varphi(m)/2} \le C \max\{s', |v_0|^2\}^{-5/2}\end{aligned}$$

for $q = (q_0, \dots, q_0)$ and $q_0 = (v_0, k_0)$. We sum these over k and l and use the fact that s' (which is a function of k and l) takes any value S no more than $4m|w|(S+1)$

次。因此

$$\sum_{k\le mn}\sum_{l\le n|w|}\mathbb{P}(\widehat{w}_{k,l}=q)\le\sum_{S=1}^{\infty}\sum_{(k,l):s'=S}C\max\{S,|v_0|^2\}^{-5/2}$$
$$\le\sum_{S=1}^{\infty}4m|w|(S+1)\cdot C\max\{S,|v_0|^2\}^{-5/2}\le\frac{C}{|v_0|}.$$

因此，我们证明了以下命题。

命题 7.6. 对于 $q=(q_0,..,q_0)$, $q_0\in G_m$, $q_0=(v_0,k_0)$, 我们有

$$\mathbb{P}(\gamma\cap\gamma' q\neq\varnothing)<C|v_0|^{-1}.$$

现在我们可以证明定理7.2

证明。设取 $q=(q_0,\dots q_0)\in G_m^5$, 其中 $q_0=(v_0,k_0)\in G_m$, 且 $|v_0|$足够大。我们将选择 $\Gamma=H\wr G_m$ 的以下生成集

$$\{s_1ms_2:s_1,s_2\in\{a^{\pm1}\delta_0,b^{\pm1}\delta_q\},m\in\{(\pm e_i,k)\}_{i,k}^5\}.$$

In the formula above, $a^{\pm1}\delta_0$ and $b^{\pm1}\delta_q$ are both elements of $\oplus_{G_m}H$ (which is embedded in Γ) while $(\pm e_i,k)$ are elements of G_m, and G_m^5 is also embedded in Γ (the parameter i takes values in $\{1,\dots,5\}$ and k in $\{1,\dots,m\}$). Note that the projection of the n-th step of the simple random walk on Γ corresponding to this generating set is the n-th step of the simple random walk that corresponds to S^5 of G_m^5.

We will use the same idea as in the previous section: $(X_n)^m$ and $w(Y_n^{(1)},\dots,Y_n^{(d)})$ commute if the corresponding paths γ and γ' in the base group are loops and $\gamma\cap\gamma' q=\varnothing$, $\gamma q\cap\gamma'=\varnothing$. Similar to the proof of Proposition 5.13 we get that γ is a loop with probability $\left(\frac{\varphi(m)}{m}\right)^5$, and γ' is a loop if all $Y_n^{(i)}\in H\wr\mathbb{Z}^{5\varphi(m)}<\Gamma$, which happens independently for each i with probability $\left(\frac{1}{m}\right)^5$. And finally, by Proposition 7.6 we have

$$\mathbb{P}(\gamma\cap\gamma' q\neq\varnothing)+\mathbb{P}(\gamma q\cap\gamma'\neq\varnothing)\le\varepsilon$$

因此，对于足够大的 $|q_0|$。

$$\liminf_{n\to\infty}\mathbb{P}\left([(X_n)^m,w(Y_n^{(1)},\dots,Y_n^{(d)})]=1\right)\ge\left(\frac{\varphi(m)}{m^{d+1}}\right)^5-\varepsilon.$$

如所要求。 □

备注。 该定理也可以作为引理 11.2 的推论来证明（代价是将幂 5 替换为 8），但由此带来的简化并不显著。

8. Commutators of a power and a non-balanced law

让我们考虑维数为 $2m-1$ 的一般 Heisenberg 群

$$H_{2m-1}=\left\{\left(\begin{array}{c|ccc|c}1&-&u^t&-&a\\\hline 0&1&&0&|\\\vdots&&\ddots&&v\\0&0&&1&|\\\hline 0&0&\cdots&0&1\end{array}\right):u,v\in\mathbb{Z}^{m-1},a\in\mathbb{Z}\right\}.$$

为方便起见，我们将 H_{2m-1} 的元素写成三元组 (u, a, v)，其中 $u, v \in \mathbb{Z}^{m-1}, a \in \mathbb{Z}$。那么乘法由公式给出。

$$(u_1, a_1, v_1) \cdot (u_2, a_2, v_2) = (u_1 + u_2, a_1 + a_2 + u_1^t v_2, v_1 + v_2).$$

取一个矩阵 A 如§7中所示。定义 $\mathbb{Z}/m\mathbb{Z}$ 在 H_{2m-1} 上的作用

$$1 * \left(\begin{array}{c|ccc|c} 1 & - & u & - & a \\ \hline 0 & 1 & & 0 & | \\ \vdots & & \ddots & & v \\ 0 & 0 & & 1 & | \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array}\right) = \left(\begin{array}{c|ccc|c} 1 & - & u^t A & - & a \\ \hline 0 & 1 & & 0 & | \\ \vdots & & \ddots & & A^{-1}v \\ 0 & 0 & & 1 & | \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array}\right)$$

这确实是 $\mathbb{Z}/m\mathbb{Z}$ 在 H_{2m-1} 上的作用，因为它保持乘法和 $A^m = 1$。

我们来考虑半直积 $H_{2m-1} \rtimes_A \mathbb{Z}/m\mathbb{Z}$。

Proposition 8.1. *Let $G = H_{2m-1} \rtimes_A \mathbb{Z}/m\mathbb{Z}$ and let μ be any finitely supported symmetric generating measure of G with $\mu(1) > 0$, and let R_n be a random walk with step distribution μ. Then for any law $w(x, y_1, \dots, y_d)$ with a total degree of some y_i not equal to zero we have $[x^m, w] = 1$ with probability at least $\frac{\phi(m)}{m}$ with respect to the random walk R_n, where $\phi(m)$ is the Euler's totient function, but G does not satisfy $[x^m, w] = 1$ virtually.*

注意，与我们关于交换子的其他结果不同，后者都要求两个字包含不同的字母，而在本结果中，字母 x 可能同时出现在两个项中。不过，不平衡的字母必须是 y_i 之一。

证明。令我们取 $x = ((u, a, v)\ k) \in G$。我们有 $x^m = ((u', a', v')\ km)$，其中

$$\begin{aligned} (u')^t &= u^t\big(I + A^k + \cdots + A^{k(m-1)}\big), \\ a' &= ma + u\big((m-1)I + (m-2)A^k + \cdots + A^{(m-2)k}\big)v, \\ v' &= \big(I + A^{-k} \cdots + A^{-k(m-1)}\big)v. \end{aligned}$$

If k and m are coprime, then $u' = v' = 0$, so x^m lies in the center of G and $[x^m, w] = 1$ for any $y_1, \dots y_l \in G$. Let $R_n^x, R_n^{y_1}, \dots, R_n^{y_d}$ be the set of independent random walks. Let $X_k = \{((u, a, v)\ k),$ where $(u, a, v) \in H\} \subset G$. We note that $\mathbb{P}(R_n^x \in X_k) \to \frac{1}{m}$ as $n \to \infty$. Then

$$\mathbb{P}([(R_n^x)^m, w(R_n^x, R_n^{y_1}, \dots, R_n^{y_d})] = 1) \geq \mathbb{P}(R_n^x \in \cup_{\gcd(k,m)=1} X_k) \to \frac{\phi(m)}{m},$$

其中 $\gcd(k, m)$ 是最大公约数，由此证明了第一个断言。

Now let us show that G does not contain a finite index subgroup which satisfies the given law. Let us assume that there is a finite index subgroup Λ of G such that for any $x, y_1 \dots y_d \in \Lambda$ one has $[x^m, w(y_1, \dots, y_d)] = 1$. Let $\{e_1, \dots, e_{m-1}\}$ be the standard generating set of $\mathbb{Z}^{m-1}$. Let us consider the subgroups $K_u < H < G$ and $K_v < H < G$ defined as follows:

$$\begin{aligned} K_u &= \{(u, a, v) \mid u = \lambda e_1, a = 0, v = 0, \lambda \in \mathbb{Z}\} \cong \mathbb{Z}, \\ K_v &= \{(u, a, v) \mid u = 0, a = 0, v = \lambda e_1, \lambda \in \mathbb{Z}\} \cong \mathbb{Z}. \end{aligned}$$

Note that $\Lambda \cap K_u$ and $\Lambda \cap K_v$ are finite index subgroups of K_u and K_v respectively, and hence are nontrivial. Let us take $g \in (\Lambda \cap K_u) \setminus \{0\}$ and $h \in (\Lambda \cap K_v) \setminus \{0\}$. Let us fix an index i such that $w(x, y_1, \dots y_d)$ has a total degree of y_i not equal to zero.

Then for $x = g, y_i = h$ and $y_j = 0$ for $j \neq i$ we have $x^m = (\lambda e_1, 0, 0)$, $w = (u, a, \mu e_1)$, where λ and μ are non-zero integers. Hence, $[x^m, w(x, y_1, \cdots, y_l)] = (0, \lambda\mu, 0) \neq 1$. Thus we get elements $x, y_1, \ldots, y_k \in \Lambda$ that do not satisfy $[x^m, w] = 1$. A contradiction. □

备注 8.2。 类似于备注 5.14，有时可以通过考虑 $G = H_{2p-1} \rtimes_A \mathbb{Z}/p\mathbb{Z}$ 来提高概率，其中 p 是 m的最大素因子。

9. Commutators of a law with itself

令 $w \in \mathbf{F}_d$ 为一个字，并考虑由 $[w, w] \in \mathbf{F}_{2d}$ 给出的律

$$[w, w](x_1, \ldots, x_d, y_1, \ldots, y_d) = [w(x_1, \ldots, x_d), w(y_1, \ldots, y_d)].$$

我们的目标是证明，如果 w 不满足间隙或正性结果，那么 $[w, w]$也不满足。 若 w 是平衡的，相关情形已在 §6中讨论，因此我们着重讨论 w 不是平衡的情形。

Proposition 9.1. *Let R_n be a random walk on $H \wr G$ with a step distribution μ. Let R'_n be a random walk on G with a step distribution $\pi_*(\mu)$ where π is a natural projection $\pi : H \wr G \to G$. If G satisfies a law w with probability $1 - \varepsilon$ with respect to R'_n, and H is any abelian group, then $H \wr G$ satisfies $[w, w]$ with probability at least $(1 - \varepsilon)^2$.*

证明。由于 H 是阿贝尔的，我们知道 $\bigoplus_{i=1}^{\infty} H$ 也是阿贝尔的，并且我们有

$$\begin{aligned}
&\mathbb{P}([w(R_n^{x_1}, \ldots R_n^{x_d}), w(R_n^{y_1}, \ldots, R_n^{y_d})] = 1) \geq \\
&\geq \mathbb{P}\left(w(R_n^{x_1}, \ldots R_n^{x_d}), w(R_n^{y_1}, \ldots, R_n^{y_d}) \in \ker \pi \cong \bigoplus_{i=1}^{\infty} H \right) = \\
&= (\mathbb{P}(w(\pi(R_n^{x_1}), \ldots \pi(R_n^{x_d})) = 1 \in G))^2.
\end{aligned}$$

因此， $H \wr G$ 满足律 $[w, w]$ 的概率至少为$(1 - \varepsilon)^2$。 □

命题9.2。假设无限的 G 几乎不满足律 $w = w(x_1, \ldots, x_r)$，且 H 是不满足 w 的群。那么 $H \wr G$ 几乎不满足$[w, w]$ 。

证明。设 Λ 是 $\Gamma = H \wr G$ 的有限指数子群。我们要证明 Λ 不满足律 $[w, w]$。

Let $\Gamma_0 = \{(\mathbf{1}, g) : g \in G\} \cong G$, i.e. all elements of Γ with trivial lamps. Since $[\Gamma_0 : \Gamma_0 \cap \Lambda] < \infty$ and $\Gamma_0 \cong G$, it has no subgroups of finite index which satisfy w, so there are elements $t_1, \ldots, t_r \in \Lambda \cap \Gamma_0$ such that $w(t_1, \ldots, t_r) = (\mathbf{1}, g_0) \neq 1$. Let $g_1, g_2, \cdots \in G$ such that

$$\left| g_j^{-1} g_i \right| \geq 2|g_0|$$

for all i, j. Consider the subgroup $\Gamma_1 = \{(L, e) : \mathrm{supp}(L) \subseteq \{g_1, g_2, \ldots\}\} \cong \bigoplus_{i=1}^{\infty} H$ which does not satisfy w virtually. Again we have $[\Gamma_1 : \Gamma_1 \cap \Lambda] < \infty$; therefore there are elements $x_1, \ldots, x_r \in \Gamma_1 \cap \Lambda$ such that $w(x_1, \ldots, x_r) = (L_0, e) \neq 1$. Finally, we have $w(t_1, \ldots, t_r) \cdot w(x_1, \ldots, x_r) = (L_1, g_0)$ and $w(x_1, \ldots, x_r) \cdot w(t_1, \ldots, t_r) = (L_0, g_0)$ where $\mathrm{supp}(L_1) \subseteq \{g_1 g_0, g_2 g_0, \ldots\}$ which does not intersect $\mathrm{supp}(L_0)$, so $L_1 \neq L_0$ and hence $[w(t_1, \ldots, t_r)\ w(x_1, \ldots, x_r)] \neq 1$. □

推论 9.3。

(1) 如果 w 不满足（强）间隙， $[w, w]$ 也不满足。(2) 如果 w 不满足（强）正性结果， $[w, w]$ 也不满足。

10. 球内随机游走路径的占用测度

The aim of this section is to provide upper bounds on the occupation measure of a path $\gamma(w; R_n^{(1)}, \dots, R_n^{(d)})$ in balls (of the Cayley graph of G). These results will be used in the following section, and were put in a separate section since they may be of independent interest.

我们先介绍两个引理，用于估计暂态群上的条件随机游走，最终目的是证明引理 10.3。

引理 10.1. 设 G 是一个具有超多项式增长的有限生成群，且 S 是其某个生成元集合。设 $\{R_t\}_{t\le n}$ 是关于 S 在群 G 上的随机游走。设 $r \in \mathbb{N}$。那么

$$\mathbb{E}\big(\max_{x\in G}\mathbb{E}\big(|\{t<n : R_t \in B(x,r)\}| \,\big|\, R_n\big)\big) \le Cr^3.$$

常数 C 可能取决于 G 和 S，但不取决于 r 和 n。

In words, the typical number of visits to a ball of radius r is not more than Cr^3, even when one conditions on R_n, the place where the random walk "ends", as long as R_n is typical. Let us remark that this does not hold for every value of R_n. For example, a random walk on the free group, conditioned on $R_n = 1$ i.e. on returning to the identity, visits the identity about $\sqrt{n}$ times.

It is reasonable to conjecture that the value r^3 can be replaced by r^2, as is conjectured (and still open) for the number of visits to $B(1,r)$ for an unconditioned random walk. On the unconditioned problem the best known to us is $r^{5/2}$, see [20]. For the purposes of this paper the exact value of the exponent is not important.

证明。记 M_n 为该引理中的期望，即。

$$M_n := \mathbb{E}(\max_{x\in G}\mathbb{E}(|\{t<n : R_t \in B(x,r)\}| \,|\, R_n)).$$

Examine for one x and one value of R_n the quantity $\mathbb{E}(|\{t<n : R_t \in B(x,r)\}| \,|\, R_n)$. We wish to write it as $A_1+A_2+A_3+A_4$, dividing according to time. For symmetry reasons we have to be slightly careful. Define $n_0 = 0$, $n_1 = \lceil n/4\rceil$, $n_2 = \lceil n/2\rceil$, $n_3 = n - \lceil n/4\rceil + 1$ and $n_4 = n+1$ and define

$$A_i := A_i(x) := \mathbb{E}\left[|\{t \in [n_{i-1}, n_i) : R_t \in B(x,r)\}| : R_n\right].$$

现在，对于任意四个非负数 A、B、C 和 D，我们有

$$A+B+C+D \le \max\{A+B+C, B+C+D\} + D\,\mathbb{I}\{A+B>0\} + A\,\mathbb{I}\{C+D>0\}. \quad (14)$$

我们将其应用于 $A_1(x), \dots, A_4(x)$，并对 x 取最大值。为简便起见，我们将 $A_{123}(x) = A_1(x) + A_2(x) + A_3(x)$ 记作 .....，对 $\{1,\dots,4\}$ 的其他子集也类似。我们得到

$$\begin{aligned}
\max_x\{A_{1234}(x)\} &\overset{(14)}{\le} \max_x\{\max\{A_{123}(x), A_{234}(x)\}+ \\
&\quad + A_4(x)\,\mathbb{I}\{A_{12}(x)>0\} + A_1(x)\,\mathbb{I}\{A_{34}(x)>0\}\}\} \\
&\le \max\{\max_x\{A_{123}(x)\}, \max_x\{A_{234}(x)\}+ \\
&\quad + \max_x\{A_4(x)\,\mathbb{I}\{A_{12}(x)>0\}\} \\
&\quad + \max_x\{A_1(x)\,\mathbb{I}\{A_{34}(x)>0\}\} =: I + II + III. \quad (15)
\end{aligned}$$

为了估计项 I，我们断言：

$$\max_x A_{123}(x) = \max_x A_{234}(x). \tag{16}$$

要看（16），注意到 A_{123} 只不过是

$$\mathbb{E}(|\{t \in [0, n_3 - 1] : R_t \in B(x, r)\}| \,|\, R_n)$$

and, similarly, A_{234} is for the interval $[\lceil n/4 \rceil, n]$. The time reversal of a random walk starting from 1 and conditioned to end at some y is random walk starting from y and conditioned to end at 1, so $A_{123}(x) = A_{234}(R_n^{-1}x)$. This shows (16).

现在固定一个 z 使得 $\mathbb{P}(R_n = z) > 0$，并令 S 为一个在 $S_n = z$条件下的长度为 n的随机游走。对于每个 x_0，我们可以写道

$$\begin{aligned}\mathbb{E}(|\{t \in [0, n_3 - 1] : S_t \in B(x_0, r)\}|) &= \mathbb{E}\big(\mathbb{E}\big(|\{t \in [0, n_3 - 1] : S_t \in B(x_0, r)\}| \,\big|\, S_{n_3}\big)\big) \\ &\le \mathbb{E}\big(\max_x \mathbb{E}\big(|\{t \in [0, n_3 - 1] : S_t \in B(x, r)\}| \,\big|\, S_{n_3}\big)\big).\end{aligned}$$

对 x_0 取最大值（注意右侧不依赖于 x_0），并对 z 积分，得到

$$\mathbb{E}(I) \le M_{n_3}. \tag{17}$$

这就完成了对 I的估计。

我们转而估计 II 和 III。它们本质上完全相同，因此为简洁起见，我们只证明 II。对于每个 x,

$$\begin{aligned}A_4(x) &\mathbb{1}\{A_{12}(x) > 0\} \\ &\le \mathbb{E}\big(|\{(t, s) : t \ge n_3, s < n_2, R_t, R_s \in B(x, r)\}| \,\big|\, R_n\big). \\ &\le \sum_{t=n_3}^{n_4} \sum_{s=0}^{n_2} \mathbb{P}(d(R_t, R_s) \le 2r \,\big|\, R_n).\end{aligned}$$

由于右侧不包含 x，它也对 II 构成界。对 R_n积分得到

$$\mathbb{E}(II) \le \sum_{t=n_3}^{n_4} \sum_{s=0}^{n_2} \mathbb{P}(d(R_t, R_s) \le 2r) \le Cn^2 \max_{m \ge n/4-1} \mathbb{P}(d(1, R_m) \le 2r). \tag{18}$$

为了估计右侧，我们使用 Lyons、Peres、Sun 和 Zheng 的结果。根据 [20, 推论 2.6], , 对于任意整数 m 和 r，以及任意两个 x、$y \in G$,

$$p_m(x, y) < C(m^{-10} r^{20} / |B(2r)| + e^{-cm/r^2})$$

（在 [20] 中还有一个额外参数 k，我们将其设为 20）。注意，正是在此处我们用到了 G 具有超多项式增长这一事实。将此估计代入（18）可得

$$\mathbb{E}(II) \le Cn^{-8} r^{20} + Cn^2 |B(2r)| e^{-cn/r^2}.$$

若对于某个足够大的 C'，$n > C' r^3$ 则 $\mathbb{E}(II) \le C/n$。

现在我们可以完成引理的证明。如果 $n \le C' r^3$，那么引理的结论显然成立。对于任意的 $n > C' r^3$，我们有

$$M_n \le \mathbb{E}(\max_x A_{1234}(x)) \overset{(15)}{\le} \mathbb{E}(I) + \mathbb{E}(II) + \mathbb{E}(III) \overset{(*)}{\le} M_{n_3} + C/n$$

where in $(*)$ we used (17) and the estimate of II above (which, as explained, applies verbatim to III). Recall that $n_3 = n - \lceil n/4 \rceil + 1$. The lemma now follows by a straightforward induction on n. □

引理 10.2。 引理 *10.1* 的结论对任何瞬态群都成立。

证明。 由于引理 10.1 证明了对于 G 具有超多项式增长的情形，我们只需处理 G 具有多项式增长的情形。然而，对于 G 具有增长 d的情形，我们有以下估计

$$p_n(1,y) \le Cn^{-d/2}e^{-c|y|^2/n}.$$

This is well known, but for completeness let us explain this estimate. By Gromov's theorem [4, 13] the group G is virtually nilpotent. It is not difficult to see that any nilpotent group is virtually torsion free [26, chapter II]. By Mal'cev's theorem [26, chapter II], a nilpotent torsion-free group is embedded as a cocompact lattice in a connected nilpotent Lie group. By the results of Guivarc'h [6] there is an integer d such that the Lie group has volume growth d. Since a Lie group is quasi-isometric to a cocompact lattice in it, and since our cocompact lattice is quasi-isometric to G, and since growth is preserved by quasi-isometries, we get that G satisfies that $cr^d \le |B(1,r)| \le Cr^d$. Finally the results of Hebisch and Saloff-Coste [9, theorems 2.1 and 4.1] give the estimate above.

在时间 t 位于 z 并在时间 $n>t$ 位于 y 的概率随后可由以下内容界定

$$Ct^{-d/2}(n-t)^{-d/2}e^{-c|z|^2/t-c|y-z|^2/(n-t)}.$$

对这一估计式关于 $t \le n$ 求和，得到

$$C\left(\min\{|z|,|y-z|\}\right)^{2-d} n^{-d/2}e^{-c|y|^2/n}$$

（使用 $d \ge 3$，这由我们关于该群是暂态的假设得出）。对 $z \in B(x,r)$ 求和得到 $r^2n^{-d/2}e^{-c|y|^2/n}$，且与 x 独立。因此

$$\max_x \mathbb{E}\big(|\{t<n : R_t \in B(x,r)\}| \,\big|\, R_n = y\big) \le \frac{Cr^2n^{-d/2}e^{-c|y|^2/n}}{\mathbb{P}(R_n=y)}.$$

对 R_n 取期望得到

$$\mathbb{E}\big(\max_x \mathbb{E}\big(|\{t<n : R_t \in B(x,r)\}| \,\big|\, R_n\big)\big) \le Cr^2n^{-d/2}\sum_y e^{-c|y|^2/n} \le Cr^2,$$

其中，在最后一个不等式中，我们用到了事实 $|B(1,r)| \le Cr^d$。这就证明了引理。□

Lemma 10.3. *Let G be a finitely generated group, let S be a set of generators, let w be a word and let γ be the path corresponding to w and random walks of length n with repsect to the generating set S. Let $x \in G$ and let $r \in \mathbb{N}$. Then*

$$\mathbb{E}(|\gamma \cap B(x,r)|) \le Cr^3.$$

（常数 C 可能取决于 w）。

Proof. The lemma holds trivially for G recurrent, since the only recurrent groups are those having volume growth 1 and 2. Assume therefore that G is transient. Let l be the length of w and let a_i be its letters, so $w = (a_1 \dots a_l)$. Let w_i be the word comprising of the first i letters of w, for $i \in \{0,\dots,l-1\}$. Let $R^{(1)},\dots,R^{(d)}$ be the

构造 γ 的随机游走。以 $R_n^{(1)},\dots,R_n^{(d)}$ 为条件。然后

$$\begin{aligned}
&\mathbb{E}\big(|\gamma\cap B(x,r)|\,\big|\,R_n^{(1)},\dots,R_n^{(d)}\big)\\
&\qquad\le\sum_{i=0}^{l-1}\mathbb{E}\big(|w_i(R_n^{(1)},\dots,R_n^{(d)})R^{(a_{i+1})}\cap B(x,r)|\,\big|\,R_n^{(1)},\dots,R_n^{(d)}\big)\\
&\qquad=\sum_{i=0}^{l-1}\mathbb{E}\big(|R^{(a_{i+1})}\cap B(w_i(R_n^{(1)},\dots,R_n^{(d)})^{-1}x,r)|\,\big|\,R_n^{(1)},\dots,R_n^{(d)}\big)\\
&\qquad\le\sum_{i=0}^{l-1}\max_{y\in G}\mathbb{E}\big(|R^{(a_{i+1})}\cap B(y,r)|\,\big|\,R_n^{(1)},\dots,R_n^{(d)}\big)\\
&\qquad=\sum_{i=0}^{l-1}\max_{y\in G}\mathbb{E}\big(|R^{(a_{i+1})}\cap B(y,r)|\,\big|\,R_n^{(a_{i+1})}\big).
\end{aligned}$$

对 $R_n^{(1)}$，.....，$R_n^{(d)}$取期望后，我们可利用引理10.2对每一项进行估计，得到

$$\mathbb{E}(|\gamma\cap B(x,r)|)\le Clr^3,$$

按需。 □

11. Commutators of a power law with itself

Definition 11.1. *Let w be a word on k letters, let G be finitely generated group and let S be a finite set of generators. Let γ_n be the path corresponding to the word w and $R^{(1)},\dots,R^{(d)}$, where $R^{(1)},\dots,R^{(d)}$ are independent random walks on G of length n.*

我们称 w 在 G 上是非 Peano 的，当且仅当 S 天天爱

$$\max_n\mathbb{P}(g\in\gamma_n)\le C\,|g|^{-4},$$

对于某个独立于 n 和 g 的 C（C 可能依赖于 G、S 和 w）。

We call this property non-Peano because such a path is far from visiting all of G. Clearly G must have at least 8 dimensional volume growth to be non-Peano for any w. But we do not believe this is enough. Presumably it is possible to construct artificial examples of a w and a "large" group G such that w is Peano on G, but we decided not to pursue this direction here.

引理 11.2. 设 G 是一个有限生成群，且 S 是一个有限生成元集。设 H 是一个二生成群。设 w_1 和 w_2 分别是定义在 d_1 个和 d_2 个字母上的两个分布，使得

$$\liminf_{n\to\infty}\mathbb{P}(w_i(R_n^{(1)},\dots,R_n^{(d_i)})=1)=p_i\qquad i\in\{1,2\}$$

对于某些 p_1 和 p_2（注意这里我们需要的是下极限，而不是通常使用的上极限）。还假设 w_1 和 w_2 在 G、S 上是非 Peano 的。那么对于每个 $\varepsilon>0$，都存在 $H\wr G$ 的生成元 S'，使得该律

$$[w_1,w_2]:=[w_1(R_n^{(1)},\dots,R_n^{(d_1)}),w_2(R_n^{(d_1+1)},\dots,R_n^{(d_1+d_2)})]$$

在 $H\wr G$ 上以至少 $p_1p_2-\varepsilon$ 的概率得到满足。

证明。设 $u \in G$ 为某个足够大的元素，稍后选择，使其仅取决于 ε。设 a 和 b 为 H 的生成元。我们将 $H \wr G$ 的修改版切换 - 移动 - 切换生成元定义为

$$S' = \{s_1 m s_2 : s_i \in \{a^{\pm 1}\delta_1, b^{\pm 1}\delta_u\}, m \in S\}$$

Let us estimate the probability that $[w_1, w_2]$ is satisfied under random walk. Write $w_i(\vec{R}^i) = (L_i, g_i)$ for $i = 1, 2$, where $g_i \in G$ and $L_i \in \bigoplus_{g\in G} H$. We use again Fact 6.4: $[w_1(\vec{R}^1)\ w_2(\vec{R}^2)] = 1$ in $H \wr G$ if $g_1 = g_2 = 1$ and $[L_1(g)\ L_2(g)] = 1$ for all $g \in G$.

Write D for the event that $g_1 = g_2 = 1$. Since G satisfies w_1 and w_2 with probabilities p_1 and p_2 respectively, and the events $g_1 = 1$ and $g_2 = 1$ are independent (recall that w_1 and w_2 are laws on independent random walks), $\mathbb{P}(D) \geq p_1 p_2$.

对于任意 $g \in G$，令 $A(g) = \{[L_1(g)\ L_2(g)] = 1\}$。则

$$\mathbb{P}\left([w_1(\vec{R}^1), w_2(\vec{R}^2)] = 1\right) \geq \mathbb{P}\left(D \cap \bigcap_{g\in G} A(g)\right) \geq \mathbb{P}(D) - \mathbb{P}\left(\bigcup_{g\in G} A(g)^c\right) \geq$$
$$\geq \mathbb{P}(D) - \sum_{g\in G} \mathbb{P}(A(g)^c). \tag{19}$$

For ease of notation, write $\gamma_i = \gamma(w_i; \vec{R}^i)$ to be the path defined by w_i under $\vec{R}$. Note that if $L_i(g) \notin \langle b\rangle$ we must have $g \in \gamma_i$, and if $L_i(g) \notin \langle a\rangle$ then $gu^{-1} \in \gamma_i$.

To estimate $\sum_{g\in G} \mathbb{P}(A(g)^c)$, first note that if $[L_1(g)\ L_2(g)] \neq 1$, then at least one of them used an a lamp, while the other used a b lamp (otherwise both lie in $\langle a\rangle$ or in $\langle b\rangle$, which are abelian subgroups). In particular, for any g we have

$$\mathbb{P}(A(g)^c) \leq \mathbb{P}(L_1(g) \notin \langle a\rangle, L_2(g) \notin \langle b\rangle) + \mathbb{P}(L_1(g) \notin \langle b\rangle, L_2(g) \notin \langle a\rangle) =$$
$$= \mathbb{P}\left(gu^{-1} \in \gamma_1, g \in \gamma_2\right) + \mathbb{P}\left(g \in \gamma_1, gu^{-1} \in \gamma_2\right).$$

由于对于每个 g，路径 γ_1 和 γ_2 都是独立的（回顾一下，记号 $[w_1, w_2]$ 表示这两个分布由不同且独立的随机游走生成），我们有

$$\mathbb{P}(A(g)^c) \leq \mathbb{P}\left(gu^{-1} \in \gamma_1\right)\mathbb{P}(g \in \gamma_2) + \mathbb{P}(g \in \gamma_1)\,\mathbb{P}\left(gu^{-1} \in \gamma_2\right),$$

因此

$$\sum_{g\in G} \mathbb{P}(A(g)^c) \leq \sum_{g\in G} \mathbb{P}\left(gu^{-1} \in \gamma_1\right)\mathbb{P}(g \in \gamma_2) + \sum_{g\in G} \mathbb{P}(g \in \gamma_1)\,\mathbb{P}\left(gu^{-1} \in \gamma_2\right).$$

Write $G = B_L(u, |u|/2) \cup V$ where B_L is the left ball around u, i.e. $B_L(u, |u|/2) = \{gu : |g| < |u|/2\}$, and where V is the remainder. We will estimate each part independently.

我们从 $B_L(u, |u|/2)$ 开始。对于任意 $g \in B_L(u, |u|/2)$，我们有 $d(g, 1) > |u|/2$。由于 w_i 是非 Peano，我们有

$$\mathbb{P}(g \in \gamma_i) \leq C\,|u|^{-4}.$$

接下来，根据引理 10.3,

$$\sum_{g\in B_L(u,|u|/2)} \mathbb{P}\left(gu^{-1} \in \gamma_i\right) = \mathbb{E}\left[|(B(1, |u|/2)) \cap \gamma_i|\right] \leq C\,|u|^3,$$

其中等式利用了当中心为单位元时，左球与右球相同这一事实。因此我们可以得出结论:

$$\sum_{g\in B_L(u,|u|/2)} \mathbb{P}\left(A(g)^c\right) \leq C\left|u\right|^{-1}.$$

To handle V we write $V=\bigcup_{r=0}^{\infty} V_r$, where $V_0 = V\cap B(1,|u|)$, and $V_r = V\cap \left(B(1,2^r|u|)\setminus B(1,2^{r-1}|u|)\right)$ for any $r\geq 1$. For any $g\in V_r$, since w_i is non-Peano,

$$\mathbb{P}\left(gu^{-1}\in\gamma_i\right) \leq C\left(2^r|u|\right)^{-4},$$

where we estimate that $|gu^{-1}| > c2^r|u|$ because $|g| > 2^{r-1}|u|$ for $r\geq 1$, and $g\notin B_L(u,|u|/2)$ for $r=0$. In addition, again with Lemma 10.3,

$$\sum_{g\in V_r} \mathbb{P}\left(g\in\gamma_i\right) \leq \mathbb{E}\left[|B(1,2^r|u|)\cap\gamma_i|\right] \leq C\left(2^r|u|\right)^3.$$

这证明我们可以再次得出结论

$$\sum_{g\in V_r} \mathbb{P}\left(A(g)^c\right) \leq C\left(2^r|u|\right)^{-1}.$$

总而言之,

$$\sum_{g\in G}\mathbb{P}\left(A(g)^c\right) = \sum_{g\in B_L(u,|u|/2)}\mathbb{P}\left(A(g)^c\right) + \sum_{r=0}^{\infty}\sum_{g\in V_r}\mathbb{P}\left(A(g)^c\right) \leq$$

$$\leq 2C\left|u\right|^{-1} + \sum_{r=0}^{\infty} C(2^r|u|)^{-1} \leq C\left|u\right|^{-1}.$$

我们可以选择 $|u|$ 足够大，使得 $C\left|u\right|^{-1}\leq\varepsilon$，从而有 $\mathbb{P}\left(\bigcap A(g)\right)\geq 1-\varepsilon$。因此

$$\mathbb{P}\left([w_1(\vec{R}^1),w_2(\vec{R}^2)]=1\right) \geq \mathbb{P}\left(D\cap\bigcap A(g)\right) \geq \mathbb{P}\left(D\right)+\mathbb{P}\left(\bigcap A(g)\right)-1 \geq p_1p_2-\varepsilon$$

如所需。 □

在继续讨论 Burnside 群之前，我们需要两个简单的引理。一个关于灯笼群中的路径，另一个关于线性代数。

Lemma 11.3. *Let B be a d-generated group and let $G=\mathbb{Z}/l\mathbb{Z}\wr B$ with the switch-move-switch generators, with respect to lazy simple random walk on $\mathbb{Z}/l\mathbb{Z}$ and the natural walk on B. Let γ be a geodesic path of length n in G and let β be its projection to B. Then*

$$|\{\beta_0,\ldots,\beta_n\}| \geq \frac{1}{l/2+2}|\gamma_n|.$$

（回顾一下，测地路径是其端点之间的最短路径）。

Proof. We will show that for any path γ there exists a path γ' with length $n'\leq n$ with the same projection to B and same endpoint, such that for all b, the projection β' of γ' visits b no more than $l/2+2$ times. This will show the lemma by contradiction since if not, then

$$n' \leq |\{\beta'_0,\ldots,\beta'_n\}|(l/2+2) = |\{\beta_0,\ldots,\beta_n\}|(l/2+2) < |\gamma_n| = |\gamma'_n|$$

这与将 $|\gamma_n|$ 定义为最短路径的长度相矛盾。

To construct γ' we first modify γ so that at every visit to every b it does a geodesic in $\mathbb{Z}/l\mathbb{Z}$ towards $\gamma_n(b)$ and when it reaches that value it no longer moves (recall that the walk on $\mathbb{Z}/l\mathbb{Z}$ is lazy). Since at every visit to b it can move the value by 2 (once when entering and once when exiting), and since the diameter of $\mathbb{Z}/l\mathbb{Z}$ is $\lfloor l/2 \rfloor$, we get that after $\lfloor l/4 \rfloor + 1$ visits to b, it has already taken the value $\gamma_n(b)$.

Next, since the set of sites visited by β is connected, one may find a spanning tree. A simple induction shows that any tree can be traversed so that each vertex is visited at least once and the overall number of is at most twice the size of the tree (e.g. doing Depth first search). Therefore to get the the desired position and configuration, we repeat this traversal $\lfloor l/4 \rfloor$ times to set all the lamps to the right configuration, then take a geodesic to the desired endpoint. □

Lemma 11.4. *Let A be an $m \times m'$ matrix with $\mathbb{Z}/l\mathbb{Z}$ entries, such that no row of A is identically zero. Assume that for some k we have that every row of A contains no more than k non-zero entries, and similarly for all columns of A. Let $X_1, \ldots, X_{m'}$ be independent (not necessarily identically distributed) random $\mathbb{Z}/l\mathbb{Z}$ variables with the property that X_i takes no specific value with probability bigger than $1-\varepsilon$ (with ε independent of i). Then for any $v \in (\mathbb{Z}/l\mathbb{Z})^m$*

$$\mathbb{P}(AX = v) \leq (1-\varepsilon)^{\lceil m/k^2 \rceil}.$$

证明。考虑 A 的第一行（将各行视为方程）。对该行中除一个以外的所有 X_i 的取值进行条件化，我们可以看到，要使该方程成立，最后一个变量必须取某个特定值，而该事件的概率至多为 $1-\varepsilon$。

Now, since the first row contains at most k non-zero entry, and since for any such entry that are at most k rows containing it, we see that at most k^2 rows of A have any joint variable with the first row. Discarding these rows, the next one is independent of the first. Since it, too, has probability $1-\varepsilon$ to be satisfied, the probability that both are satisfied is at most $(1-\varepsilon)^2$. Continuing this way, the lemma is proved. □

引理 11.5. 令 q 为一个足够大的合数。则存在一个群 G，对所有 $x \in G$ 满足 $x^q = 1$，以及 G 的一个有限生成元集 S，使得 x^q 对于 G, S 是非 Peano 的。

Proof. For any k_0 there exists q_0 such that if $q > q_0$ is composite then it is possible to write $q = kl$ with $k > k_0$ and with $l > 1$. By [11] for any $k \geq 2^{57}$ the free Burnside group B of exponent k on 2 generators is infinite (the formulation in [11] is "k larger than 2^{48} and either odd or divisible by 2^9" but this is the same. Indeed, if the Burnside group of a given exponent k is infinite then so is the Burnside group of every product of k). We take q_0 corresponding to $k_0 = 2^{57}$ in the above. Consider the group $G = \mathbb{Z}/l\mathbb{Z} \wr B$. Then it is easy to see that G is of exponent q. Indeed, for any $g = (\omega, b) \in G$, $g^k = (\xi, b^k) = (\xi, 1)$ for some $\xi : B \to \mathbb{Z}/l\mathbb{Z}$ and then

$$g^q = \left(g^k\right)^l = (\xi, 1)^l = (l\xi, 1) = (\vec{0}, 1)$$

其为 G中的单位元。我们取此 G，其对应于关于 $\mathbb{Z}/l\mathbb{Z}$ 上的懒随机游走和 B上的标准随机游走的标准切换-移动-切换生成元。

因此我们只需证明 x^q 是非 Peano 的，即对于所有 n，$\mathbb{P}(g \in \gamma) \leq C|g|^{-4}$，其中 γ 是 R^q 的路径，R 是长度为 n的随机游走。要证明这一点

condition on the path of R in B and call this path β (we apologise for the confusing use of the word "path" for both the path in B and in G — hopefully, if the reader keeps in mind that the path in B is denoted by β and the path in G is denoted by γ not too much confusion will arise). Denote $g =: (\omega, b)$ and consider one i such that $\beta_i = b$. By Lemma 11.3 we know that the set $M := \{\beta_0, \dots, \beta_i\}$ must have size at least $c|g|$ (here and below constants may depend on q, k and l), otherwise it is impossible for γ_i to be g and we may discard such i.

Write $i = an + r$ for $0 \le r < n$ (and $a \le q$), and write $R_n = R_r R'_{n-r}$, where $R_r = (\xi, g_0)$ and $R'_{n-r} = (\xi', g'_0)$ are independent random walks with r and $n-r$ steps respectively. As R_r and R'_{n-r} are independent, and after conditioning on the path β, the random variables $\{\xi(g)\}_{g\in G}$ and $\{\xi'(g)\}_{g\in G}$ are independent and non-degenerate.

As $\gamma_i = (R_r R'_{n-r})^a R_r$, for any $x \in B$ which is visited by the random walk R_n by time n, $\gamma_i(x)$ is a linear combination of the variables $\{\xi(g)\}_{g\in G}$ and $\{\xi'(g)\}_{g\in G}$. Each $\gamma_i(x)$ is a linear combination of at most $2q$ such variables, and each such variable appears in at most $2q$ combinations. Thus we are exactly in the situation of Lemma 11.4 and we may conclude that

$$\mathbb{P}(\gamma_i = g \,|\, \beta) \le (1-c)^{\lceil |M|/4q^2 \rceil}.$$

结合前面的观察，对于满足 $\beta_i = b$ 的 i，仍然有 $\mathbb{P}(\gamma_i = g \,|\, \beta) \le \exp(-c|g|)$。

Finally, to estimate the number of relevant i we note that B is transient and hence using Lemma 10.2 with $r = 1$ shows that, conditioning only on β_n and not on the whole of β, each piece of β visits b in expectation at most a constant number of times. Integrating this conditioning shows that

$$\mathbb{E}(|\{i : \beta_i = b\}|) \le Cq.$$

然后通过以下计算即可完成该引理。

$$\mathbb{P}(g \in \gamma) \le \sum_{i=0}^{qn} \mathbb{E}(\mathbb{P}(\gamma_i = g \,|\, \beta)) \le \sum_{i=0}^{qn} \mathbb{P}(\beta_i = b) \exp(-c|g|) \le Cq \exp(-c|g|),$$

这远强于我们为证明结论所需的八维估计。 □

备注。灯笼人群的基群为伯恩赛德群时，其本身也是伯恩赛德群的这一想法此前已被采用，参见 [25] 的附录及其中的参考文献。

定理 11.6. 对于充分大的合数 q，律 $[x^q, y^q]$ 对无限群既没有间隙也不具有正性。

这可由引理 11.2立即推出，只需考虑缠绕积$\Gamma = \mathrm{F}_2 \wr G$（引理 11.5中的群 G），并利用这样一个事实：由于 $\mathrm{F}_2 \wr G$ 含有自由子群，因此它不满足任何律（即使几乎如此）。

12. Uniform measures on balls

本节讨论通过在球上取均匀测度所诱导的测度。也就是说，我们选取一个包含 1 的有限对称生成集 S，并令 μ_n 表示 S^n 上的均匀测度。我们证明，在这种情况下，许多分布不存在强间隙。

定理 12.1。设 w 是一个非平凡的律，使得存在某个指数增长的群满足 w。那么 w 相对于由球上的均匀测度诱导的测度不存在强间隙。

Proof. Write $w = w(x_1, \dots, x_d)$, and let G be a group of exponential growth satisfying w. Take a finite symmetric generating set S of G containing 1, and let $\rho = \lim_{n\to\infty} \sqrt[n]{|S^n|} > 1$ be the growth exponent of G with respect to S. Also, let H be a finite group which does not satisfy w (it is easy to see that any non-trivial law is not satisfied by a sufficiently large symmetric group).

考虑群 $\Gamma = G \times H$，其生成集为 $T = (S \times \{1\}) \cup (\{1\} \times H)$，并令 μ_n 表示 T^n 上的均匀测度。那么，对于任意 $n \geq 1$ 和 $h \in H$，我们有

$$|\{(g,h) \in T^n \mid g \in G\}| = \begin{cases} |S^{n-1}|, & h \neq 1 \\ |S^n|, & h = 1. \end{cases}$$

Note that $w((g_1,h_1) \dots, (g_d,h_d)) = 1$ if and only if $w(h_1, \dots, h_d) = 1$ (because G satisfies w), and thus w holds if $h_1 = \cdots = h_d = 1$. Therefore, if (g_i, h_i) are distributed uniformly in a ball of radius n then

$$\begin{aligned} \mathbb{P}(w((g_1,h_1),\dots,(g_d,h_d)) = 1) &\geq \mathbb{P}(h_1 = \cdots = h_d = 1) = \\ &= \frac{|S^n|^d}{((|H|-1)|S^{n-1}| + |S^n|)^d} = \\ &= \frac{1}{\left((|H|-1)\frac{|S^{n-1}|}{|S^n|} + 1\right)^d}, \end{aligned}$$

这表明

$$\limsup_{n\to\infty} \mathbb{P}(w((g_1,h_1),\dots,(g_d,h_d)) = 1) \geq \frac{1}{((|H|-1)\rho^{-1}+1)^d}.$$

只要 m 足够大，就可以将 S 替换为 S^m，从而令 $\rho \to \infty$，并且上述概率趋于 1。然而，显然 Γ 不满足所要求的 w。□

备注。 任何满足定理假设的律12.1 也不满足强正性结果（相对于球上的均匀测度）。

Indeed, let w be such a law, and let G be a group of exponential growth satisfying w. Fix $\varepsilon > 0$. Following the proof of the theorem, for any k we may find a generating set of $G \times \mathrm{Sym}_k$ such that $\mathbb{P}(w = 1 \text{ on } G \times \mathrm{Sym}_k) \geq \varepsilon$ (with respect to balls in the appropriate Cayley graph of $G \times \mathrm{Sym}_k$). However, $G \times \mathrm{Sym}_k$ cannot have a subgroup satisfying w for which the index is bounded by a function of ε, since this is not true for Sym_k as k tends to ∞.

例 12.2。 我们给出两个满足定理 *12.1*的律的例子：

(1) *The law $x^n = 1$ for large enough n such that the Burnside group $B(d,n)$ is infinite (for some d).*
(2) *The metabelian law $[[x,y],[z,w]] = 1$ (for which we can take $G = \mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$).*

13. Open questions

我们以若干开放问题结束本文。对于有限群（或对于残有限群），间隙的存在性（问题 1.1）以及正性（问题 1.2）仍然是开放问题。

A particular case of interest is for power laws $x^m = 1$. When G is finite, it is known that there exists a gap for $\mathbb{P}(x^m = 1 \text{ on } G)$ depending on m and on the number of generators of G. However, the dependency on the number of generators is still, as far as we know, unknown:

问题 13.1。律 $x^m = 1$ 对有限群是否满足间隙结果，且不依赖于生成元的数量?

This question is open for both the finite case and the infinite case with respect to random walks (though we believe that the two cases might be very different). Note that for $m = 3$ and 4 Laffey gave a positive answer [15, 17]. Further, for $m = p$ a prime number, Laffey shows that any non-p-groups must have $\mathbb{P}(x^p = 1) \leq p/(p+1)$ [16]. For p-groups the situation is more complicated, and Khukhro gave an example of a 5-group where $1 > \mathbb{P}(x^5 = 1) \geq 24/25$ [12]. See [8] for a survey of this direction.

作为本文所给出的若干结果的推广，我们提出以下问题:

Question 13.2. Let $w_1 = w_1(x_1, \ldots, x_d) \in \mathrm{F}_d$ and $w_2 = w_2(y_1, \ldots, y_{d'}) \in \mathrm{F}_d$ be words. Does the law $[w_1, w_2]$ satisfy a gap or positivity result?

Recall that our results show that when w_1, w_2 are balanced, or when w_1, w_2 are the same word with disjoint variables, then $[w_1, w_2]$ does not satisfy a gap or a positivity result; also, if w_1 is a power law, then $[w_1, w_2]$ does not satisfy a positivity result.

我们的下一个问题是关于律的间隙和正性的某些“极端”情形。我们证明了，一个群上可以以任意接近 1 的概率满足某个律，而该群几乎不满足该律（或任何律）。人们可以提出以下问题:

Question 13.3. Let $w \in \mathrm{F}_d$ be a word, let G be a finitely generated group generated by S, and let $R_n^{(1)}, \ldots, R_n^{(d)}$ be independent random walks on G with respect to S. If $\lim_{n\to\infty} \mathbb{P}(w(R_n^{(1)}, \ldots, R_n^{(d)}) = 1) = 1$, is it true that $w = 1$ holds on G?

关于正性,

问题 13.4. 对于一个生成集，满足一条律的概率可以为 0，而对于另一个生成集为正吗?

最后，我们提出另一个问题，这个问题在性质上稍微更具技术性:

问题 13.5。满足 w 的概率的上极限 $\neq$ 下极限能否?

This can be arranged, for example, if the random walk is not lazy (consider for example the infinite Dihedral group $D_\infty = \langle a, b : a^2 = b^2 = 1 \rangle$, with respect to the generating set $S = \{a, b\}$, and the law $x^2 = 1$). However, when the random walk is lazy, it is unclear whether the probabilities converge or not. We conjecture that, in fact, an example where the probabilities do not converge can be constructed.

References

[1] Yago Antolín, Armando Martino, and Enric Ventura. Degree of commutativity of infinite groups. *Proceedings of the American Mathematical Society*, 145(2):479–485, 2017.

[2] Costantino Delizia, Urban Jezernik, Primož Moravec, and Chiara Nicotera. Gaps in probabilities of satisfying some commutator-like identities. *Israel Journal of Mathematics*, 237(1):115–140, 2020.

[3] Sean Eberhard and Pavel Shumyatsky. Probabilistically nilpotent groups of class two. *arXiv preprint arXiv:2108.02021*, 2021.

[4] Mikhael Gromov. Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.*, 53:53–73, 1981.

[5] Karl W. Gruenberg. Residual properties of infinite soluble groups. *Proc. London Math. Soc. (3)*, 7:29–62, 1957.

[6] Yves Guivarc'h. Croissance polynomiale et périodes des fonctions harmoniques. *Bull. Soc. Math. France*, 101:333–379, 1973.

[7] William H. Gustafson. What is the probability that two group elements commute? *The American mathematical monthly*, 80(9):1031–1034, 1973.

[8] George Havas and Michael Vaughan-Lee. On counterexamples to the Hughes conjecture. *J. Algebra*, 322(3):791–801, 2009.

[9] W. Hebisch and L. Saloff-Coste. Gaussian estimates for Markov chains and random walks on groups. *Ann. Probab.*, 21(2):673–709, 1993.

[10] Kurt A. Hirsch. On infinite soluble groups (III). *Proceedings of the London Mathematical Society*, 2(1):184–194, 1946.

[11] Sergei V. Ivanov. The free Burnside groups of sufficiently large exponents. *Internat. J. Algebra Comput.*, 4(1-2):ii+308, 1994.

[12] Evgeniĭ I. Khukhro. On the connection between the Hughes conjecture and the relations in finite groups of prime period. *Mat. Sb. (N.S.)*, 116(158)(2):253–264, 1981.

[13] Bruce Kleiner. A new proof of Gromov's theorem on groups of polynomial growth. *J. Amer. Math. Soc.*, 23(3):815–829, 2010.

[14] Zoltan A. Kocsis. Degree of satisfiability of some special equations. *arXiv preprint arXiv:2002.01773*, 2020.

[15] Thomas J. Laffey. The number of solutions of $x^3 = 1$ in a 3-group. *Mathematische Zeitschrift*, 149(1):43–45, 1976.

[16] Thomas J. Laffey. The number of solutions of $x^p = 1$ in a finite group. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 80, pages 229–231. Cambridge University Press, 1976.

[17] Thomas J. Laffey. The number of solutions of $x^4 = 1$ in a 3-group. *Proc. Roy. Irish Acad. Sect. A*, 79(4):29–36, 1979.

[18] Paul-Henry Leemann and Mikael de la Salle. Cayley graphs with few automorphisms: the case of infinite groups. *arXiv preprint arXiv:2010.06020*, 2020.

[19] Alexander Lubotzky and Dan Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.

[20] Russell Lyons, Yuval Peres, Xin Sun, and Tianyi Zheng. Occupation measure of random walks and wired spanning forests in balls of Cayley graphs. *Ann. Fac. Sci. Toulouse Math. (6)*, 29(1):97–109, 2020.

[21] Avinoam Mann. Finite groups containing many involutions. *Proceedings of the American Mathematical Society*, pages 383–385, 1994.

[22] Avinoam Mann and Consuelo Martinez. The exponent of finite groups. *Archiv der Mathematik*, 67(1):8–10, 1996.

[23] Armando Martino, Matthew C. H. Tointon, Motiejus Valiunas, and Enric Ventura. Probabilistic nilpotence in infinite groups. *Israel Journal of Mathematics*, 244(2):539–588, 2021.

[24] Peter M. Neumann. Two combinatorial problems in group theory. *Bulletin of the London Mathematical Society*, 21(5):456–458, 1989.

[25] Damian Osajda. Group cubization. *Duke Math. J.*, 167(6):1049–1055, 2018. With an appendix by Mikaël Pichot.

[26] M. S. Raghunathan. *Discrete subgroups of Lie groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68. Springer-Verlag, New York-Heidelberg, 1972.

[27] Aner Shalev. Probabilistically nilpotent groups. *Proceedings of the American Mathematical Society*, 146(4):1529–1536, 2018.
[28] Matthew C. H. Tointon. Commuting probabilities of infinite groups. *Journal of the London Mathematical Society*, 101(3):1280–1297, 2020.

Email address: gidi.amir@gmail.com

Bar-Ilan University, Ramat Gan 52900, Israel

Email address: guy.blachar@gmail.com

Bar-Ilan University, Ramat Gan 52900, Israel

Email address: mari9gerasimova@mail.ru

Westälische Wilhelms-Universität Münster, 48149 Münster, Germany

Email address: gady.kozma@weizmann.ac.il

The Weizmann Institute of Science, Rehovot 76100, Israel