Full Length Article

A metric characterization of freeness

L. Cadilhac [a],[*], B. Collins [b]

[a] *Laboratoire de Mathématiques d'Orsay, Univ. Paris-Sud, CNRS, Université Paris-Saclay, 91405 Orsay, France*
[b] *Department of Mathematics, Kyoto University, Kitashirakawa Oiwake-cho, Sakyo-ku, 606-8502, Japan*

A R T I C L E   I N F O

A B S T R A C T

Let $\mathcal{M}$ be a finite von Neumann algebra and $u_1, \ldots, u_N$ be unitaries in $\mathcal{M}$. We show that $u_1, \ldots, u_N$ freely generate $L(\mathbb{F}_N)$ if and only if

$$\left\| \sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}} \right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}} = 2\sqrt{2N-1}.$$

1. Introduction

The von Neumann conjecture formulated by Day in 1957 says that a group is not amenable if and only if it contains a non-amenable free group. It was first disproved by A. Ol'shanskii in 1980 [9], and since then, the family of counterexamples has been expanded. A similar question can be asked at the level of von Neumann algebras: if a finite factor is not amenable, does it necessarily contain a free group factor? Little is known in that direction except for a breakthrough of Gaboriau and Lyons [4], who show that

* Corresponding author.
E-mail addresses: leonard.cadilhac@u-psud.fr (L. Cadilhac), collins@math.kyoto-u.ac.jp (B. Collins).

for certain wreath product groups G (which may not contain $\mathbb{F}_2$), $L(\mathbb{F}_2) \subset L(G)$. Note that the authors of [4] are, in fact, mainly interested in a version of the von Neumann conjecture for measure-preserving actions for which they provide a positive answer.

A difficulty in tackling this problem is that there are no known abstract properties of $\mathcal{M}$ which would characterize the fact that $L(\mathbb{F}_2)$ embeds in $\mathcal{M}$. This remark first motivated us to write this note on a metric characterization of freeness. Although it is not clear that the results obtained (see Corollary 1.2) can be used in the study of the von Neumann conjecture, we believe that they are of independent interest.

Indeed, they generalize at the operator level a well-known result of Kesten [6] who showed that given $g_1, \ldots, g_N$ in a countable group G, the freeness of the g_i's is characterized by the norm of the Markov operator associated to a random walk on G supported by the g_i's and their inverses. Let us denote by $\lambda : G \to L(G)$ the left-regular representation. From a von Neumann algebraic point of view, Kesten's result can be reformulated as follows:

$$g_1, \ldots, g_N \text{ are free in } G \iff \left\| \sum_{i=1}^{N} \lambda(g_i) + \lambda(g_i)^* \right\|_{L(G)} = 2\sqrt{2N - 1}. \qquad (1.1)$$

We extend this result by replacing the $\lambda(g_i)$'s with any finite family of unitary operators in a finite von Neumann algebra $\mathcal{M}$. The notion of freeness and Haar unitaries (unitaries with null moments) will be considered with respect to a fixed normal faithful tracial state τ. We obtain the following:

Theorem 1.1. *Let $N \in \mathbb{N}$, $N > 1$. Let $u_1, \ldots, u_N$ be unitaries in $\mathcal{M}$. Then, the following assertions are equivalent:*

(1) the operators $u_1, \ldots, u_N$ are free Haar unitaries,
(2) the following equality holds:

$$\left\| \sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}} \right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}} = 2\sqrt{2N - 1}.$$

Note that $(1) \Rightarrow (2)$ is a consequence of (1.1). Let us also mention that the inequality

$$\left\| \sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}} \right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}} \geq 2\sqrt{2N - 1},$$

is verified for any family of unitaries. This affirmation will become obvious when we reformulate the problem in terms of moments; it also appears in a paper of Pisier [10]. This leads to the following corollary:

Corollary 1.2. *Let $\mathcal{M}$ be a finite von Neumann algebra. Then the following are equivalent:*

(1) $L(\mathbb{F}_2)$ *embeds in* $\mathcal{M}$,

(2) $\inf_{u_1, u_2 \in \mathcal{U}(\mathcal{M})} \| u_1 \otimes \bar{u}_1{}^* + u_1^* \otimes \bar{u}_1 + u_2 \otimes \bar{u}_2{}^* + u_2^* \otimes \bar{u}_2 \|_{\mathcal{M} \otimes \mathcal{M}} = \sqrt{3}$, *and this infimum is achieved.*

Let us make a few remarks in relation to this result. Firstly, amenability can also be characterized by considering the same quantity. Indeed, in the spirit of Connes' [3, Theorem 5.1], we know that a factor $\mathcal{N}$ is hyperfinite if and only if for every finite family of unitaries $u_1, \ldots, u_n$ in $\mathcal{N}$,

$$\left\| \sum_{i=1}^{n} u_i \otimes (u_i^*)^{\mathrm{op}} \right\|_{\mathcal{N} \otimes^{\min} \mathcal{N}^{\mathrm{op}}} = n.$$

In this sense, it is at the extreme opposite of freeness. Secondly, it is worth pointing out that the problem considered in this manuscript complements results of [7], and also of [5,2], who consider generators of a group instead of general unitaries. Thirdly, in view of the above papers, it is natural to wonder what are the possible values of

$$\left\| \sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}} \right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}}$$

when the unitaries range on all possible choices in any tracial von Neumann algebra. This is clearly a subset of the interval $[2\sqrt{2N-1}, 2N]$, and it can easily be seen that this is the whole interval. Although many other approaches seem to be possible, let us just outline one way to prove this assertion: take N free unitary Brownian motions $\{ t \mapsto u_i(t), i \in \{1, \ldots, N\} \}$ as defined in [11]. Using explicit descriptions of the free unitary Brownian motion (see [1]) one can show that it is norm continuous, converges to free Haar unitaries, and that this convergence holds in norm for $t \mapsto \sum_{i=1}^{N} u_i(t) \otimes (u_i^{\mathrm{op}}(t))^* + u_i^*(t) \otimes u_i^{\mathrm{op}}(t)$, therefore its norm is a continuous function taking value $2N$ at $t = 0$ and tending to $2\sqrt{2N-1}$. It follows that the whole range $[2\sqrt{2N-1}, 2N]$ is attained. Finally, it was brought to our attention by Franz Lehner that the traciality condition in Theorem 1.1 is necessary, as illustrated by a counterexample appearing in his Ph.D. thesis [8, p.51].

In section 2, we introduce our combinatorial approach to Theorem 1.1. Section 3 contains the core technicalities: we use free group combinatorics to obtain a suitable lower bound on positive characters of $\mathbb{F}_N$, which allows us to conclude in Section 4.

2. A combinatorial approach

2.1. Reformulation of Theorem 1.1

Let $N \in \mathbb{N}$. Let φ be a positive definite function on the free group $\mathbb{F}_N$. We extend φ linearly to $\mathbb{C}[\mathbb{F}_N]$ and keep the same notation, *i.e.* for any finitely supported family $(a_g)_{g \in \mathbb{F}_N} \in \mathbb{C}$,

$$\varphi\left(\sum_{g \in \mathbb{F}_N} a_g \cdot g\right) = \sum_{g \in \mathbb{F}_N} a_g \cdot \varphi(g).$$

Let $s_1, \ldots, s_N \in \mathbb{F}_N$ be free generators of $\mathbb{F}_N$ and set

$$a := \sum_{i=1}^{N} s_i + s_i^{-1} \in \mathbb{C}[\mathbb{F}_N].$$

We aim to prove the following:

Theorem 2.1. *Assume that:*

- φ *is constant on the conjugacy classes of* $\mathbb{F}_N$ *(it is a character),*
- $\varphi(e) = 1$,
- $\exists g \in \mathbb{F}_N, g \neq e, \varphi(g) \neq 0$,
- $\forall g \in \mathbb{F}_N, \varphi(g) \geq 0$.

Then,

$$\lim_{n \to \infty} \varphi(a^{2n})^{\frac{1}{2n}} > 2\sqrt{2N - 1}.$$

Lemma 2.2. *Theorem 2.1 implies Theorem 1.1.*

Proof. Consider the representation π of $\mathbb{F}_N$ determined by $\pi(s_i) = u_i \otimes (u_i^{\mathrm{op}})^*$ in $\mathcal{U}(\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}})$ for any $i \in \{1, \ldots, N\}$. Define $\varphi := (\tau \otimes \tau^{\mathrm{op}}) \circ \pi$. Note that φ is a positive character on $\mathbb{F}_N$ and that

$$\left\|\sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}}\right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}} = \lim_{n \to \infty} \left\|\sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}}\right\|_{2n}$$

$$= \lim_{n \to \infty} \varphi(a^{2n})^{\frac{1}{2n}}.$$

Assume that the u_i's are not free Haar unitaries. This means that there exists $g \in \mathbb{F}_N$ such that $g \neq e$ and $\varphi(g) \neq 0$. So φ satisfies the conditions for Theorem 2.1 and hence

$$\left\|\sum_{i=1}^{N} u_i \otimes (u_i^{\mathrm{op}})^* + u_i^* \otimes u_i^{\mathrm{op}}\right\|_{\mathcal{M} \overline{\otimes} \mathcal{M}^{\mathrm{op}}} > 2\sqrt{2N - 1}. \quad \square$$

2.2. Outline of the strategy of proof

In this section, we give an overview of the strategy of proof. We start with the following remark:

Remark 2.3. To prove Theorem 2.1, it suffices to show that

$$\exists n, \varphi(a^{2n})^{\frac{1}{2n}} > 2\sqrt{2N-1},$$

by Hölder's inequality.

More precisely, let τ be a normalized trace on $\mathcal{M}\overline{\otimes}\mathcal{M}^{\mathrm{op}}$, a simple application of Stirling's formula shows that for any N there exists $\varepsilon > 0$ and n_0 such that for any $n \geq n_0$,

$$\tau(a^{2n}) > \varepsilon \cdot (2\sqrt{2N-1})^{2n} n^{-3/2}.$$

Looking into the assumptions of Theorem 2.1, as soon as there is an element $g \in \mathbb{F}_N$, $g \neq e$ such that $\varphi(g) = \eta > 0$, the traciality condition implies that all the conjugates of g take the same trace value η, therefore, we can obtain a lower bound by observing the following: given N, there exists $\varepsilon > 0$ such that for n large enough, the number of canonical paths on the free group on N generators of length n, starting from the identity element and ending in a conjugacy class is at least εn times the number of paths starting from the identity that end at a Cayley distance ≤ 1 from their starting point.

In turn, thanks to the positivity of the trace, this proves that there exists $\varepsilon > 0$ and n_0 such that for any $n \geq n_0$,

$$\varphi(a^{2n}) > \varepsilon \cdot (2\sqrt{2N-1})^{2n} n^{-1/2}.$$

Here, we 'gained' a factor n in the subcritical part.

This is not enough to conclude because $n^{-1/2} = o(1)$ and we would not be able to prove Theorem 2.1 without estimates on further conjugacy classes of elements other than g.

Fortunately, there is a way to do so thanks to the fact that φ is of positive type. Indeed, if a finite collection of g_i satisfy $\varphi(g_i) > \eta$ uniformly, then, assuming that the number of elements is large enough (for a threshold that depends on η), one can show that a positive proportion with a ratio independent on the number of g_i's of the products $g_i g_j$ satisfies $\varphi(g_i g_j) > 0$ uniformly as well. Thanks to this additional estimate and after picking the g_i's a suitable amount of congujates of g, one can 'gain' an additional factor n in the subcritical part, and obtain the following there exists $\varepsilon > 0$ and n_0 such that for any $n \geq n_0$,

$$\varphi(a^{2n}) > \varepsilon \cdot (2\sqrt{2N-1})^{2n} n^{+1/2}.$$

Now, the exponent $+1/2$ is positive, so for n large enough, the L^n norm is bigger than $2\sqrt{2N-1}$, which allows us to conclude thanks to Remark 2.3.

2.3. Some notations

We always assume $\mathbb{F}_N$ to be equipped with a set of distinguished generators $S = \{s_1, \ldots, s_N\}$. Denote by $\mathbb{W}_N$ the set of words on the alphabet $S \cup S^{-1}$. For any $w \in \mathbb{W}_N$, denote by $l(w)$ its length. Words in $\mathbb{W}_N$ encode elements of $\mathbb{F}_N$ via the following map:

$$g \colon \mathbb{W}_N \to \mathbb{F}_N$$

$$w_1 \ldots w_n \mapsto w_1 \cdots w_n.$$

Recall that a word $w_1 \ldots w_n \in \mathbb{W}_N$ is said to be *reduced* if for any $i \leq n-1$, $w_i^{-1} \neq w_{i+1}$. The map g is not injective but any γ in $\mathbb{F}_N$ admits a unique reduced preimage. We will identify when convenient γ with its writing as a reduced word w in $\mathbb{W}_N$. In particular, set $l(\gamma) := l(w)$.

Define, for any $k \in \mathbb{N}$ and $w = w_1 \ldots w_k \in W_N$ of length k, the circular permutation of w by

$$\sigma_1(w) = w_k w_1 \ldots w_{k-1}.$$

For any $t \in \mathbb{Z}$, let $\sigma_t := \sigma_1^t$. We say $w \in \mathbb{W}_N$ is *cyclically reduced* if $\sigma_t(w)$ is reduced for any t (note that it is equivalent to w and $\sigma_1(w)$ being reduced). If w is a reduced word, w can uniquely be written as

$$w = uvu^{-1},$$

where v is cyclically reduced u is a reduced word. The element v will be referred to as the *root* of w and denoted by $r(w)$.

3. Lower bound for positive characters of $\mathbb{F}_N$

3.1. Overview of the section

Let φ be as in Theorem 2.1 and $g_0 \neq e$ such that $\varphi(g_0) = \alpha > 0$. We will see soon (Corollary 3.3) that without loss of generality, g_0 can be chosen to be of even length $2l_0$, $l_0 \in \mathbb{N}$. And since we might as well consider $r(g_0)$, it can be assumed to be cyclically reduced. This section is devoted to proving the following proposition:

Proposition 3.1. *There exists a constant $C > 0$ such that for any $k \geq l_0$,*

$$\sum_{l(g)=2k} \varphi(g) \geq Ck^2(2N-1)^k.$$

Note that the constant C that we obtain above may be explicitly computed from N, l_0 and α but its precise value is inessential. Our goal is to exhibit a large enough family of words in $\mathbb{F}_N$ on which we can bound φ from below. To do so, we combine two different operations:

- The first operation consists of conjugating elements thanks to the tracial property. However, as explained in Section 2, by a simple calculation using the estimate given in Lemma 4.1, it can be seen that considering only conjugates of g_0 is not enough to obtain a sufficiently good lower bound on $\varphi(a^{2n})$.
- The second operation is to multiply elements for which we already have a lower bound and apply Lemma 3.2. This is, however, a bit cumbersome because simplifications may occur, and estimating the length of the products obtained this way. (to be able to use Lemma 4.1) requires some caution.

The proof is divided into four different steps:

- Step 0 - we show that we can obtain new elements of positive trace by multiplication (Lemma 3.2).
- Step 1 - we fix an integer i and apply Lemma 3.2 to the conjugates of g_0 of length $2i$ to obtain a set $\mathcal{R}_i$ new elements of quantified positive trace which have a length approximately $4i$ and are roots. The control on the length is essential to guarantee that our sets $\mathcal{R}_i$ do not overlap too much when i varies. This will be essential during step 3.
- Step 2 - we apply circular permutations to the elements of $\mathcal{R}_i$ to construct a bigger set $\mathcal{R}_i^\sigma$ of roots with positive traces.
- Step 3 - we consider the sets $\mathscr{C}_i(k)$ of elements of length $2k$ with roots in D_i, show that they are essentially disjoint and big enough (in terms of the trace) to conclude.

3.2. Step 0: locating more positivity through multiplication

The following lemma allows obtaining new elements of positive trace through multiplication.

Lemma 3.2. *Let* $k \in \mathbb{N}$ *and* $a > 0$. *Let* $h_1, \ldots, h_k$ *be such that* $\varphi(h_i) = \alpha$ *for any* $i \in \{1, \ldots, k\}$. *Then,*

$$\sum_{1 \le i,j \le k} \varphi(h_i^{-1} h_j) \ge k^2 \alpha^2.$$

Proof. Set $h_0 = e$ and consider the matrix

$$A = (\varphi(h_i^{-1} h_j))_{0 \le i,j \le k}.$$

Since φ is positive definite, A is positive. Let $\varepsilon > 0$. Consider the vector $v = (1, -\varepsilon, \ldots, -\varepsilon) \in \mathbb{C}^k$. Denote by b the mean of $(\varphi(h_i^{-1}h_j))_{0<i,j\leq k}$. Note that

$$v^t A v = 1 - 2k\alpha\varepsilon + k^2 b\varepsilon^2.$$

Set $\varepsilon = \frac{1}{k\alpha}$. By positivity of A, we have:

$$0 \leq 1 - 2 + \frac{b}{\alpha^2}.$$

Hence, $b \geq \alpha^2$. $\quad\square$

We can now justify that g_0 can be assumed to be of even length.

Corollary 3.3. *Let φ be a character on $\mathbb{F}_N$ such that there exists $g_0 \neq e$ with $\varphi(g_0) > 0$. Then there exists g_1 of even length such that $\varphi(g_1) > 0$.*

Proof. Set $\alpha := \varphi(g_0)$. Assume that g_0 is of odd length, otherwise simply take $g_1 = g_0$. Choose k large enough so that $\alpha^2 k^2 > k$ and $h_1, \ldots, h_k$ distinct conjugates of g_0. Note that the h_i are of odd length and hence the $h_i^{-1}h_j$ are of even length.

$$\sum_{1\leq i \neq j \leq k} \varphi(h_i^{-1}h_j) = \sum_{1\leq i,j\leq k} \varphi(h_i^{-1}h_j) - \sum_{1\leq i\leq k} \varphi(h_i^{-1}h_i)$$
$$\geq \alpha^2 k^2 - k$$
$$> 0.$$

This implies that there exists $i_1, j_1 \leq k$ such that $\varphi(h_{i_1}^{-1}h_{j_1}) > 0$. Set $g_1 = h_{i_1}^{-1}h_{j_1}$. $\quad\square$

3.3. Step 1: products of conjugates of g_0

The construction will depend on a parameter k_0. We could set a value for it right away, but it would not help with the clarity of the argument. We only need to know that it is large enough and only depends on g_0, N, and α.

Let $i \in \mathbb{N}$, $i > l_0$ and consider the set $\mathcal{C}_i$ of all conjugates of g_0 or g_0^{-1} of length $2i$. Denote by R_0 the set of conjugates of g_0 or g_0^{-1} of length $2l_0$. Note that since g_0 is assumed to be cyclically reduced:

$$|\mathcal{C}_i| = |R_0| \, (2N-2)(2N-1)^{i-l_0-1} = c_0(2N-1)^i, \tag{3.1}$$

where $c_0 = |R_0| \, (2N-2)(2N-1)^{-l_0-1}$. In the course of the proof, we will apply circular permutations σ_j to the words we obtain to generate new words. In order to guarantee at that future step that we indeed obtain new words, we remove from the beginning some pathological elements of $\mathcal{C}_i$. For any $j \in \mathbb{N}$, define:

$$\mathcal{C}_i(j) := \left\{ g \in \mathcal{C}_i : \forall n, m \in \{k_0 + 1, \ldots, i - l_0\} \, (|n - m| = 2j) \Rightarrow g_n = g_m \right\}, \qquad (3.2)$$

where g_n denotes the n-th letter of g. Let $g \in \mathcal{C}_i(j)$, $g = wr_0w^{-1}$ where w is a reduced word, $r_0 \in R_0$ and no cancellation occur in this product. The condition above amounts to saying that w is $2j$-periodic, except maybe for its first k_0 letters. Hence it is determined by the choice of its $k_0 + 2j$ first letters and consequently

$$|C_i(j)| \le c_0 (2N - 1)^{2j + k_0 + l_0}. \qquad (3.3)$$

Define

$$\mathcal{C}_i' := \mathcal{C}_i \setminus \bigcup_{j \le \frac{i - l_0}{k_0}} \mathcal{C}_i(j). \qquad (3.4)$$

Lemma 3.4. *For i large enough and $k_0 \ge 4$, we have*

$$|\mathcal{C}_i'| \ge \frac{c_0}{2} (2N - 1)^i. \qquad (3.5)$$

Proof. Since formula (3.4) only involves values of j below $(i - l_0)/k_0$ and we assume $k_0 \ge 4$, we infer from (3.3) that

$$|\mathcal{C}_i(j)| \le c_0 (2N - 1)^{k_0 + 2\frac{i - l_0}{k_0} + l_0} \le K (2N - 1)^{i/2},$$

where $K = c_0 (2N - 1)^{k_0 + l_0/2}$. Hence, using (3.1),

$$|\mathcal{C}_i'| \ge |\mathcal{C}_i| - \frac{i - l_0}{k_0} K (2N - 1)^{i/2} \ge \frac{c_0}{2} (2N - 1)^i$$

for i large enough. $\quad \square$

Define:

$$\mathcal{R}_i := \left\{ r(g) : g \in \mathcal{C}_i' \cdot \mathcal{C}_i', l(g) > 4i - 2k_0 \right\}.$$

Remark 3.5. Let us keep in mind the form of the elements that we are dealing with. Let $h, h' \in \mathcal{C}_i'$. This means that there exists r_0 and r_0' in R_0 and u, u' in $\mathbb{F}_N$ such that $h = ur_0u^{-1}$ and $h' = u'r_0'(u')^{-1}$. Write $u = wv$ and $u' = wv'$ such that no cancellations occur in the product $v^{-1}v'$. Then $r(hh')$ belongs to $\mathcal{R}_i$ if and only if $l(w) < k_0$. In this case, $r(hh') = vr_0v^{-1}v'r_0'v'^{-1}$ and $l(r(hh')) = l(h) + l(h') - 4l(w) \ge 4i - 4k_0$.

Lemma 3.6. *For i and k_0 large enough, the following estimate holds:*

$$\sum_{g \in \mathcal{R}_i} \varphi(g) \ge \frac{c_0}{8} \alpha^2 (2N - 1)^{2i - k_0}.$$

Proof. For any $g \in \mathcal{C}'_i$, there are at most $c_0(2N-1)^{i-k_0}$ elements g' of $\mathcal{C}'_i$ for which $l(gg') \leq 4i - 2k_0$. Indeed, the first k_0 letters of g' must coincide with the first k_0 letters of g in order for at least k_0 simplifications to occur. This means that:

$$\sum_{g,g' \in \mathcal{C}'_i} \varphi(gg') \leq c_0(2N-1)^{i-k_0} |\mathcal{C}'_i| + \sum_{\substack{g,g' \in \mathcal{C}'_i \\ l(gg')>4i-2k_0}} \varphi(gg').$$

Then, by Lemma 3.2 (note that considering gg' or $g^{-1}g'$ does not modify the following sum since $\mathcal{C}'_i = (\mathcal{C}'_i)^{-1}$):

$$\sum_{\substack{g,g' \in \mathcal{C}'_i \\ l(gg')>4i-2k_0}} \varphi(gg') \geq |\mathcal{C}'_i|^2 \alpha^2 - c_0(2N-1)^{i-k_0} |\mathcal{C}'_i|$$

$$\geq \frac{c_0^2 \alpha^2}{4}(2N-1)^{2i} - \frac{c_0^2}{2}(2N-1)^{2i-k_0}$$

$$\geq \frac{c_0^2 \alpha^2}{8}(2N-1)^{2i},$$

where we assume in the last line that k_0 is large enough so that,

$$(2N-1)^{-k_0} \leq \frac{\alpha^2}{4}.$$

Finally, note that at most $(2N-1)^{k_0}$ pairs $h, h' \in \mathcal{C}'_i$ can give rise to the same element $r(hh') \in \mathcal{C}^{(2)}_i$. This means that

$$(2N-1)^{k_0} \sum_{g \in \mathcal{R}_i} \varphi(g) \geq \sum_{\substack{g,g' \in \mathcal{C}'_i \\ l(gg')>4i-2k_0}} \varphi(gg'),$$

which is the desired estimate. $\square$

3.4. Step 2: circular permutations

To guarantee that we construct new elements by circular permutations, we rely on the following observation.

Lemma 3.7. *Let $g, g' \in \mathbb{F}_N$ and $t \in \mathbb{N}$. Assume that g and g' can be written as follows*

$$g = uau^{-1}b \quad \text{and} \quad g' = u'a'(u')^{-1}b' \quad \text{with } l(a) = l(a'), l(u) = l(u'), l(b) = l(b'),$$

and no cancellation in the products. Then if $g = \sigma_t(g')$, u is $2t$-periodic.

Proof. Denote by l the length of u. We may assume that $2t < l$ otherwise the statement is void. For $i \in \{t+1, \ldots, l\}$, note that the i-th letter of g is u_i and the i-th letter of $\sigma_t(g')$ is u'_{i-t}. So

$$u_i = u'_{i-t} \text{ for } i \in \{t+1, \ldots, l\}.$$

Now we look at the occurrences of u^{-1} and $(u')^{-1}$ in g and $\sigma_t(g')$ *i.e.* the i-th letters of g and $\sigma_t(g')$ for $i \in \{l + l(a) + t + 1, \ldots, l + l(a) + l\}$. We obtain

$$u_i = u'_{i+t} \text{ for } i \in \{1, \ldots, l-t\}.$$

Combining the two equalities, we get that $u_i = u_{2t+i}$ for $i \in \{1, \ldots, l - 2t\}$. □

Define:

$$\mathcal{R}_i^\sigma := \left\{ \sigma_j(g) : 0 \leq j \leq \frac{i - l_0}{k_0}, g \in \mathcal{R}_i \right\}.$$

Lemma 3.8. *For i and k_0 large enough, the following estimate holds:*

$$\sum_{g \in \mathcal{R}_i^\sigma} \varphi(g) \geq \left\lfloor \frac{i - l_0}{k_0} \right\rfloor \frac{c_0}{8} \alpha^2 (2N - 1)^{2i - k_0}.$$

Proof. Given the estimate obtained in Lemma 3.6, it suffices to prove that for any $0 \leq j, j' \leq (i - l_0)/k_0$ and $g, g' \in \mathcal{R}_i$,

$$\sigma_j(g) = \sigma_{j'}(g') \Rightarrow (g = g' \text{ and } j = j').$$

Let us assume that $\sigma_j(g) = \sigma_{j'}(g')$. If $j = j'$ then immediately $g = g'$ and we get the expected conclusion. So assume by contradiction that $j \neq j'$. Set $t = j' - j$, we have

$$g = \sigma_{-j} \circ \sigma_j(g) = \sigma_{-j} \circ \sigma_{j'}(g') = \sigma_t(g').$$

According to Remark 3.5, g and g' can be written as follows:

$$g = u r_0 u^{-1} v s_0 v^{-1} \quad g' = u' r_0' (u')^{-1} v' s_0' (v')^{-1}$$

where r_0, s_0, r_0', s_0' belong to R_0 and no cancellations occur in the products above. Still by Remark 3.5, u and v have the same length (same for u' and v') and since $l(g) = l(g')$, we get that u, u', v, v' are words of the same length l. By Lemma 3.7, u is $2t$-periodic. Since g is an element of $\mathcal{R}_i$, g comes from a product hh', $h, h' \in \mathcal{C}_i'$. Write $h = wv_0w^{-1}$. We have $w = w_1 \ldots w_{i-l_0-l} u$. By construction of $\mathcal{C}_i'$, w cannot be $2t$-periodic starting from its k_0-th letter, which is a contradiction (see (3.4), (3.2), and recall that by assumption $t \leq \frac{i - l_0}{k_0}$). □

3.5. Step 3: conjugation

For any $k \geq 2i$, define:

$$\mathscr{C}_i(k) := \{g \in \mathbb{F}_N : l(g) = 2k, r(g) \in \mathcal{R}_i^\sigma\}.$$

Lemma 3.9. *Let i, i' large enough and assume that $|i - i'| \geq k_0$. Let $k \geq 2i, 2i'$. Then,*

- $\mathscr{C}_i(k)$ *and* $\mathscr{C}_{i'}(k)$ *are disjoint,*
- *There exists $C' > 0$ independent of k or i such that:*

$$\sum_{g \in \mathscr{C}_i(k)} \varphi(g) \geq C'i(2N-1)^k.$$

Proof. For the first point, recall that by Remark 3.5, the elements of $\mathcal{R}_i$ have length between $4i$ and $4i - 4k_0 + 4$. Since those elements are roots, applying circular permutations to them does not change their length. Hence, the elements of $\mathcal{R}_i^\sigma$ also have length between $4i$ and $4i - 4k_0 + 4$. So if $|i - i'| \geq k_0$ then $\mathcal{R}_i^\sigma$ and $\mathcal{R}_{i'}^\sigma$ are disjoint so $\mathscr{C}_i(k)$ and $\mathscr{C}_{i'}(k)$ are disjoint.

Let g be a cyclically reduced element of length $4i$ in $\mathbb{F}_N$. Note for $k > 2i$, there are $(2N-2)(2N-1)^{k-2i-1}$ elements of $\mathbb{F}_N$ of length $2k$ and root g. This means that any element of $\mathcal{D}_i$ is the root of at least $(2N-2)(2N-1)^{k-i-1}$ elements in $\mathscr{C}_i(k)$. Hence,

$$\sum_{g \in \mathscr{C}_i(k)} \varphi(g) \geq (2N-2)(2N-1)^{k-2i-1} \sum_{g \in \mathcal{R}_i^\sigma} \varphi(g).$$

By Lemma 3.8, we obtain the expected estimate. $\quad\square$

Proof of Proposition 3.1. Note that for any $k \geq l_0$, $\sum_{l(g)=2k} \varphi(g) > 0$ so it suffices to prove Proposition 3.1 for large values of k. Fix a rank i_0 such that for $i, i' \geq i_0$, Lemma 3.9 applies. Let $k \in \mathbb{N}$, $k \geq 2(i_0 + k_0)$ (so that the sums below are non empty). By Lemma 3.9, we have:

$$\sum_{|g|=2k} \varphi(g) \geq \sum_{\substack{i_0 \leq i \leq k/2 \\ k_0 | i}} \sum_{g \in \mathscr{C}_i(k)} \varphi(g)$$

$$\geq \sum_{\substack{i_0 \leq i \leq k/2 \\ k_0 | i}} C'i(2N-1)^k$$

$$\geq Ck^2(2N-1)^{2k},$$

where C is a small enough constant independent of k. $\quad\square$

4. Proof of the main theorem

Lemma 4.1. *Let $n \in \mathbb{N}$ and $k < n$. Let $g \in \mathbb{F}_N$ such that $l(g) = 2k$. Then:*

$$|\{w \in \mathbb{W}_N : l(w) = 2n, g(w) = g\}| = \left(\binom{2n}{n-k} - \binom{2n}{n-k-1} \right) (2N-1)^{n-k} =: N_{n,k}.$$

Proof. We interpret words as paths on the Cayley graph of $\mathbb{F}_N$. Note that the quantity we consider only depends on $l(g)$. A way to generate paths going from e to *any* element of length $2k$ is first to choose at which times the path is going to go away from e and at which times the path is going to come back towards e. Since the path is going to an element of length $2k$, it has to go $n + k$ times away from e and $n - k$ back to e. The number of possible choices there, for a path of length $2n$, is given by the Catalan triangle

$$C_{n,k} = \binom{2n}{n-k} - \binom{2n}{n-k-1}.$$

Moreover, when we chose to go away from e, there are *at least* $2N-1$ possible directions, and $2N$ possible directions for the first time, thus obtaining

$$C_{n,k} 2N (2N-1)^{n+k-1}$$

paths. Finally, since, for now, all we have fixed is the length of the target of the path and not a particular point, we have to divide this result by the number of elements of length $2k$ in $\mathbb{F}_N$ *i.e.* $2N(2N-1)^{2k-1}$, to get the desired estimate. $\square$

We are now ready to prove our main theorem.

Proof of Theorem 2.1. Let $n \in \mathbb{N}$. First remark that by Lemma 4.1 and Proposition 3.1,

$$
\begin{aligned}
\varphi(a^{2n}) &= \sum_{w \in \mathbb{W}_N} \varphi(g(w)) \\
&\geq \sum_{k \leq n} C_{n,k} (2N-1)^{n-k} \sum_{|g|=2k} \varphi(g) \\
&\geq C \sum_{l_0 \leq k \leq n} C_{n,k} k^2 (2N-1)^n.
\end{aligned}
$$

Note that given the expression of $C_{n,k}$,

$$\sum_{l_0 \leq k \leq n} k^2 C_{n,k} \geq \sup_{l_0 \leq k \leq n} k^2 \sum_{k \leq i \leq n} C_{n,k} = \sup_{l_0 \leq k \leq n} k^2 \binom{2n}{n-k}.$$

Now chose $k = n^{1/3}$. For n large,

$$\binom{2n}{n-k} \sim \frac{2^{2n}}{\sqrt{\pi n}} \left(\frac{n}{n+k}\right)^{n+k} \left(\frac{n}{n-k}\right)^{n-k}$$

$$\sim \frac{2^{2n}}{\sqrt{\pi n}} e^{-k+o(1)} e^{k+o(1)}$$

$$\sim \frac{2^{2n}}{\sqrt{\pi n}}.$$

Hence, for n large enough,

$$\varphi(a^{2n}) \geq \frac{C}{\sqrt{\pi}} n^{1/6} 2^{2n} (2N-1)^n > 2^{2n} (2N-1)^n.$$

Which concludes the proof by Remark 2.3.   □

Proof of Corollary 1.2. Let τ be a faithful trace on $\mathcal{M}$ and consider $L^2(\mathcal{M}, \tau)$. It follows from Theorem 1.1 that all reduced words in u_i and their inverses form an orthonormal family. Since the GNS representation of the von Neumann subalgebra generated by u_1, u_2 is faithful; it allows to conclude that is isomorphic to $L(\mathbb{F}_2)$.   □

References

[1] Philippe Biane, Segal-Bargmann transform, functional calculus on matrix spaces and the theory of semi-circular and circular systems, J. Funct. Anal. 144 (1) (1997) 232–286.

[2] Joel M. Cohen, Cogrowth and amenability of discrete groups, J. Funct. Anal. 48 (3) (1982) 301–309.

[3] A. Connes, Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$, Ann. Math. (2) 104 (1) (1976) 73–115.

[4] Damien Gaboriau, Russell Lyons, A measurable-group-theoretic solution to von Neumann's problem, Invent. Math. 177 (3) (2009) 533–540.

[5] R.I. Grigorchuk, Symmetrical random walks on discrete groups, in: Multicomponent Random Systems, in: Adv. Probab. Related Topics, vol. 6, Dekker, New York, 1980, pp. 285–325.

[6] Harry Kesten, Symmetric random walks on groups, Trans. Am. Math. Soc. 92 (1959) 336–354.

[7] Franz Lehner, A characterization of the Leinert property, Proc. Am. Math. Soc. 125 (11) (1997) 3423–3431.

[8] Franz Lehner, $\mathbb{M}_n$-espaces, sommes d'unitaires et analyse harmonique sur le groupe libre, PhD thesis, 1997, Thèse de doctorat dirigée par Pisier, Gilles Mathématiques Paris 6 1997.

[9] A.Ju. Ol'šanskiĭ, On the question of the existence of an invariant mean on a group, Usp. Mat. Nauk 35 (4(214)) (1980) 199–200.

[10] Gilles Pisier, Quadratic forms in unitary operators, Linear Algebra Appl. 267 (1997) 125–137.

[11] Dan Voiculescu, The analogues of entropy and of Fisher's information measure in free probability theory. VI. Liberation and mutual free information, Adv. Math. 146 (2) (1999) 101–166.