ISRAEL JOURNAL OF MATHEMATICS **236** (2020), 305–316
DOI: 10.1007/s11856-020-1975-2

ON A CARDINAL INVARIANT RELATED TO THE HAAR MEASURE PROBLEM*

BY

GIANLUCA PAOLINI

Department of Mathematics "Giuseppe Peano"
Università degli Studi di Torino
Via Carlo Alberto 10, Turin 10123, Italy
e-mail: gianluca.paolini@unito.it

AND

SAHARON SHELAH

Einstein Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
and
Department of Mathematics, Hill Center—Busch Campus
Rutgers, The State University of New Jersey
110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA
e-mail: shelah@math.huji.ac.il

ABSTRACT

In [6], given a metrizable profinite group G, a cardinal invariant of the continuum $\mathfrak{fm}(G)$ was introduced, and a positive solution to the Haar Measure Problem for G was given under the assumption that $\mathrm{non}(\mathcal{N}) \leqslant \mathfrak{fm}(G)$. We prove here that it is consistent with ZFC that there is a metrizable profinite group G_* such that $\mathrm{non}(\mathcal{N}) > \mathfrak{fm}(G_*)$, thus demonstrating that the strategy of [6] does not suffice for a general solution to the Haar Measure Problem.

* Partially supported by European Research Council grant 338821. No. 1148 on Shelah's publication list. The present paper was written while the first author was a post-doc research fellow at the Einstein Institute of Mathematics of the Hebrew University of Jerusalem, supported by European Research Council grant 338821.
Received September 27, 2018 and in revised form June 20, 2019

1. Introduction

It is well-known that every compact group admits a unique translation-invariant probability measure, its Haar measure. A long-standing[1] open problem asks:

Problem (Haar Measure Problem): Does every infinite compact group have a non-Haar-measurable subgroup?

In [3] the problem was settled in the positive under the assumption that the compact group is not an infinite metrizable profinite group. Furtheremore, in [1] it was proved that it is consistent with ZFC that every infinite compact group has a non-Haar-measurable subgroup. Very recently, progress has been made toward a solution to the Haar Measure Problem for infinite metrizable profinite groups. In fact, in [6] the authors introduced a certain cardinal invariant of the continuum $\mathfrak{fm}(G)$, depending on a metrizable profinite group G, and proved (see Section 2 for definitions):

Fact ([6]): Let G be an infinite metrizable profinite group. If $\mathrm{non}(\mathcal{N}) \leqslant \mathfrak{fm}(G)$, then G has a non-Haar-measurable subgroup.

Also in [6], the authors conjectured:

CONJECTURE ([6]): *Let G be an infinite metrizable profinite group. Then*

$$\mathrm{non}(\mathcal{N}) \leqslant \mathfrak{fm}(G).$$

In this work we refute the conjecture above, thus demonstrating that the strategy of [6] does not suffice for a general solution to the Haar Measure Problem.

MAIN THEOREM: *It is consistent with ZFC that there exists an infinite metrizable profinite group G_* such that:*

$$\mathrm{non}(\mathcal{N}) > \mathfrak{fm}(G_*).$$

Notice that in the aforementioned work from [1], the exibithed models of ZFC witnessing that the Haar Measure Problem has consistently a positive answer do not satisfy CH, while, despite the failure of the main conjecture in [6] proved in this paper, the work of [6] shows the remarkable result that in all the models of ZFC satisfying CH the Haar Measure Problem has a positive answer.

[1] The problem dates back at least to 1963, when in [4, Section 16.13(d)] the problem was posed and settled in the positive in the abelian case.

2. Preliminaries

Convention 1: (1) We denote by ω the set of natural numbers.
(2) Given $n < \omega$, we identify n with the set $\{0, \dots, n-1\} = [0, n)$.
(3) Given a set X we denote by $\mathcal{P}(X)$ the set of subsets of X.
(4) Given a set X and $n < \omega$, we denote by $[X]^n$ the set of subsets of X of power n.

Definition 2: A **metrizable profinite group** G is a profinite group of the form $\varprojlim^{\bar{\varphi}}_{i<\omega} G_i$, for $\bar{\varphi} = (\varphi_i : i < \omega)$ and $\varphi_i \in \mathrm{Hom}(G_{i+1}, G_i)$, i.e., G is an inverse $\bar{\varphi}$-limit of an $(\omega, <)$-inverse system of finite groups. When the homorphisms φ_i are clear from the context, we might forget to mention $\bar{\varphi}$ and simply write $\varprojlim_{i<\omega} G_i$.

Notation 3: Given a metrizable profinite group we denote by μ its Haar measure, i.e., the unique translation-invariant probability measure defined on G.

Notation 4: Let $1 < n < \omega$, $A \subseteq G^n$ and $g \in G$. We let

$$A_g = \{(h_1, \dots, h_{n-1}) \in G^{n-1} : (h_1, \dots, h_{n-1}, g) \in A\}.$$

Definition 5: Let G be a metrizable profinite group.

(1) We say that $X \subseteq G^n$ is an **elementary algebraic set** if there is a group word $w(\bar{x}, \bar{z})$, with $|\bar{x}| = n$, and a sequence of parameters $\bar{c} \in G^{|\bar{z}|}$ such that:
$$X = \{\bar{a} \in G^{|\bar{x}|} : G \models w(\bar{a}, \bar{c}) = e\}.$$
(2) We say that $X \subseteq G^n$ is an **elementary algebraic null set** if X is an elementary algebraic set which is null with respect to μ (cf. Notation 3).
(3) We say that $X \subseteq G$ is **Fubini–Markov** if either of the following happens:
  (a) X is an elementary algebraic null set;
  (b) there is $1 < n < \omega$ and an elementary algebraic null set $A \subseteq G^n$ such that
$$X = \{g \in G : \mu(A_g) > 0\}.$$

Definition 6: Let G be a metrizable profinite group. The **cardinal invariant** $\mathfrak{fm}(G)$ is the smallest size of a collection of Fubini–Markov sets whose union has measure 1.

Fact 7: Let $G = \varprojlim^{\bar{\varphi}}_{i<\omega} G_i$ be a metrizable profinite group and let π_i be the canonical projection of G onto G_i, for $i < \omega$. Let $U \subseteq G$ be a closed set of the form

$$U = \bigcap_{i<\omega} \pi_i^{-1}(B_i),$$

with $B_i \subseteq G_i$ and $\varphi_i(B_{i+1}) = B_i$, for $i < \omega$. Then

$$\mu(U) = \lim_{i\to\infty} \frac{|B_i|}{|G_i|}.$$

Proof. Notice that:

$$\begin{aligned}\mu(U) =& \mu\Big(\bigcap_{i<\omega} \pi_i^{-1}(B_i)\Big)\\ =& \lim_{i\to\infty} \mu(\pi^{-1}(B_i)) && \text{(by [2, Chapter 18, item 2f, p. 363])}\\ =& \lim_{i\to\infty} \frac{|B_i|}{|G_i|} && \text{(by [2, Chapter 18, Example 18.2.3]).}\end{aligned}$$ ∎

Definition 8: We denote by $\mathcal{N}$ the ideal of null sets in the Cantor space 2^ω, and by $non(\mathcal{N})$ the minimal cardinality of a non-null subset of 2^ω.

3. Building appropriate finite groups

Notation 9: Let G be a group and $\bar{g} = (g_i : i < n)$, for $n < \omega$, a finite sequence of elements of G. Given $I \subseteq n$ we let $g_I = \prod_{i\in I} g_i \in G$ (if $I = \emptyset$, then $g_I = e$).

Definition 10: For $2 \leqslant 4m \leqslant n < \omega$ such that $\frac{2}{2^m} + \frac{1}{n^2} < \frac{1}{m}$, let $\mathbf{CR}_{(n,m)}$ be the class of triples $(G, \bar{y}, \bar{z})$ such that:

- (a) G is a finite group;
- (b) $\bar{y} = (y_i : i < n)$ is a sequence of pairwise commuting elements of G each of order 2 and such that $\langle \bar{y}\rangle_G$ is a subgroup of order 2^n;
- (c) $\bar{z} = (z_I : I \in [n]^m)$ and $z_I \in G$;
- (d) for every $I \subseteq n$ and $J \in [n]^m$, $[y_I, z_J] = e$ iff $I \in \{J, \emptyset\}$ (cf. Notation 9);
- (e) if $s \in G - \{e\}$, then $|\{t \in G : [s,t] = e\}| < |G|/n^2$.

Lemma 11: *For $n, m < \omega$ as in Definition 10,*

$$\mathbf{CR}_{(n,m)} \neq \emptyset$$

(cf. Definition 10).

Proof. Let G_0 be the Abelian group $\bigoplus\{\mathbb{Z}_2 y_i : i < 2n\}$ (where $\mathbb{Z}_2 y_i$ is the group with two elements with generator y_i), and, for $I \subseteq n$, let $y_I = \sum\{y_i : i \in I\}$ (i.e., we are using Notation 9 in additive notation). For $I \subseteq n$, let $\pi_I \in \mathrm{Aut}(G_0)$ be such that for every $J \subseteq n$ with $J \notin \{\emptyset, I\}$ we have that

$$\pi_I(y_J) \neq y_J \quad \text{and} \quad \pi_I(y_I) = y_I.$$

[Why must such π_I's exist? Let $(y^I_\ell : \ell < 2n)$ be a basis of G_0 such that $y^I_0 = y_I$, if $I \neq \emptyset$, and any $x \in G_0 - \{e\}$ otherwise (it is well known that every $x \in G_0 - \{e\}$ can be extended to a basis of G_0). Let π'_I be such that $\pi'_I(y^I_\ell) = y_{n+\ell}$, for $\ell \in (0, n)$, and $\pi'_I(y^I_0) = y^I_0$. Then any extension of π'_I to a $\pi_I \in \mathrm{Aut}(G_0)$ is as wanted.]

Let G_1 be the group generated by $G_0 \cup \{z_I : I \in [n]^m\}$ freely except for:

(i) the equations of G_0;
(ii) if $I \subseteq n$ and $x \in G_0$, then $z_I^{-1} x z_I = \pi_I(x)$.

Let G be $\mathrm{Sym}(G_1)$ (the group of permutations of the set G_1), interpreting G_1 as a subgroup of G, and let $\mathbf{n} = |G_1|$. Then clearly $\mathbf{n} > n^2$ (which will be used at the end of the proof). Now, we claim that $(G, \bar{y}, \bar{z}) \in \mathbf{CR}_{(n,m)}$, for $\bar{y} = (y_i : i < n)$ and $\bar{z} = (z_I : I \in [n]^m)$. Clearly, clauses (a)–(d) of Definition 10 hold. Finally, concerning condition (e), notice that if $s \in G - \{e\}$, then

$$|\{t \in G : [s,t] = e\}| \leqslant \frac{\mathbf{n}!}{(\mathbf{n}-1)!} = \mathbf{n} \leqslant (\mathbf{n}-1)! = |G|/\mathbf{n} < |G|/n^2. \qquad \blacksquare$$

Definition 12: Let $\mathbf{CR}$ be the set of tuples $\mathbf{p}$ such that

$$\begin{aligned}\mathbf{p} =&(k_{\mathbf{p}}, m_{\mathbf{p}}, n_{\mathbf{p}}, (G_{(\mathbf{p},1)}, \bar{y}^1, \bar{z}^1), G_{(\mathbf{p},2)})\\ =&(k, m, n, (G_1, \bar{y}^1, \bar{z}^1), G_2),\end{aligned}$$

and:

$(*)_0$ (a) $0 < k < m < n < \omega$;
(b) $2 \leqslant 4m \leqslant n$;
(c) $2^k m = n$ and $k << n$;
(d) $\frac{2}{2^m} + \frac{1}{n^2} < \frac{1}{m}$.

$(*)_1$ $(G_1, \bar{y}^1, \bar{z}^1) \in \mathbf{CR}_{(n,m)}$ (cf. Definition 10).

$(*)_2$ (a) We let $\mathfrak{c}_{\mathbf{p}} = \mathfrak{c} : n \times n \to G_1$ be such that for $i_0, i_1 < n$ we have:
(α) $\mathfrak{c}(i_0, i_1) = e$, if $i_0 \neq i_1$;
(β) $\mathfrak{c}(i_0, i_1) := y^1_i$, if $i_0 = i_1 = i$;

(b) G_2 is the group generated freely by

$$G_1 \cup \{y_i^\ell = y_{(\ell,i)} : \ell \in \{2,3\}, i < n\}$$

except for:

(α) the equations of G_1;

(β) y_i^ℓ has order 2, for every $\ell \in \{2,3\}$ and $i < n$;

(γ) y_i^ℓ and y_j^ℓ commute, for every $\ell \in \{2,3\}$ and $i, j < n$;

(δ) for every $\ell \in \{2,3\}$, $i < n$ and $g \in G_1$, y_i^ℓ commutes with g;

(ϵ) $[y_i^2, y_j^3] = \mathfrak{c}(i,j)$, for every $i, j < n$.

Notation 13: For uniformity of notation, given the context of Definition 12, and in particular k, m and n as there, we will let $n = n_2 = n_3$.

Lemma 14: *Let $\mathbf{p} \in \mathbf{CR}$ (cf. Definition 12). Then:*

(1) *$G_2 = G_{(\mathbf{p},2)}$ is finite, G_1 is a normal subgroup of G_2 and G_2/G_1 is Abelian.*

(2) *for every $x \in G_2$, there are unique $\mathcal{U}_\ell = \mathcal{U}(\ell) = \mathcal{U}_\ell(x) = \mathcal{U}(\ell, x) \subseteq [0, n_\ell)$ (cf. Notation 13), for $\ell \in \{2,3\}$, and $y_{(1,x)} \in G_1$, such that*

$$x = y_{(3,\mathcal{U}(3))} y_{(2,\mathcal{U}(2))} y_{(1,x)},$$

where, for $\ell \in \{2,3\}$, we let

$$y_{(\ell,\mathcal{U}(\ell))} = \prod_{i \in \mathcal{U}(\ell)} y_i^\ell.$$

Proof. Clear. ∎

Lemma 15: *Let $\mathbf{p} \in \mathbf{CR}$ (cf. Definition 12), $G_2 = G_{(\mathfrak{p},2)}$, and $k = k_{\mathbf{p}}$. If $x_0, \ldots, x_{k-1} \in G_2$, then for some $I_* \subseteq [0, n_2)$ (cf. Notation 13) we have:*

(a) *$|I_*| = n_2/2^k$ (recall that $n_2/2^k = n/2^k = 2^k m/2^k = m$);*

(b) *if $\ell < k$, then $\mathcal{U}_2(x_\ell) \cap I_* \in \{I_*, \emptyset\}$ (cf. Lemma 14(2)).*

Proof. For $\eta \in 2^k$, let

$$I_\eta = \{i < n_2 : \text{if } \ell < k, \text{ then } i \in \mathcal{U}_2(x_\ell) \Leftrightarrow \eta(\ell) = 1\}.$$

So $(I_\eta : \eta \in 2^k)$ is a partition of $[0, n_2)$ into 2^k parts, hence for some $\eta \in 2^k$ we have that $|I_\eta| \geqslant n_2/2^k$ (recall that $2^k \mid n_2$ and $k << n_2$). Now, let $I_* \subseteq I_\eta$ be such that it satisfies clause (a) of the statement of the lemma. Then I_* is as wanted. ∎

Lemma 16: *Let* $\mathbf{p} \in \mathbf{CR}$ *(cf. Definition 12). If* $x_\ell \in G_2 = G_{(\mathbf{p},2)}$*, for* $\ell < k = k_{\mathbf{p}}$*, then for some* $I_* \subseteq n$ *and* $c, c_* \in G_2$ *we have:*

(a) $c = y^3_{I_*}$ *and* $c_* = z^1_{I_*}$*;*
(b) $G_2 \models [[x_\ell, c], c_*] = e$*;*
(c) $|I_*| = n_2/2^k$*;*
(d) $(B_I : I \subseteq I_*)$ *is a partition of* G_2 *into sets of equal size such that*

$$G \models [[x, c], c_*] = e \text{ iff } x \in B_\emptyset \cup B_{I_*},$$

where, for $I \subseteq I_*$*, we let*

$$B_I = \{a \in G_2 : [a, c] = y^1_I\};$$

(e) $|\{(x, y) \in G_2 \times G_2 : G_2 \models [[[x, c], c_*], y] = e\}| \leqslant \frac{|G_2 \times G_2|}{m}$.

Proof. Let $x_\ell \in G_2$, for $\ell < k$, and let $I_* \subseteq [0, n_2)$ be as in Lemma 15 with respect to $(x_0, \ldots, x_{k-1})$. Let $c = \prod\{y^3_i : i \in I_*\} = y_{(3,I_*)}$ and $c_* = z^1_{I_*}$ (cf. Definitions 10 and 12). We have to show that (I_*, c, c_*) are as wanted. To this extent, let $a \in G_2$ and let

$$a = y_{(3,\mathcal{U}(3))} y_{(2,\mathcal{U}(2))} y_{(1,a)}$$

be as in Lemma 14(2), for $\mathcal{U}(\ell) = \mathcal{U}(\ell, a) \subseteq [0, n_\ell)$, and $\ell \in \{2, 3\}$. Notice that for $\ell \in \{2, 3\}$ and $I_\ell \subseteq [0, n_\ell)$ we have that $(y^\ell_{I_\ell})^{-1} = y^\ell_{I_\ell}$ (cf. Notation 9), since each element of the product has order 2 and they all commute with each other. Then for any $a \in G_2$ we have that (recalling Lemma 14 and letting $y_{(\ell,\mathcal{U}(\ell))} = y_{(\ell,\mathcal{U}(\ell,a))}$):

$$\begin{aligned}
[a, c] &= a^{-1} c^{-1} a c \\
&= (y_{(1,a)})^{-1} y_{(2,\mathcal{U}(2))} y_{(3,\mathcal{U}(3))} y_{(3,I_*)} y_{(3,\mathcal{U}(3))} y_{(2,\mathcal{U}(2))} y_{(1,a)} y_{(3,I_*)} \\
&= y_{(2,\mathcal{U}(2))} y_{(3,\mathcal{U}(3))} y_{(3,I_*)} y_{(3,\mathcal{U}(3))} y_{(2,\mathcal{U}(2))} y_{(3,I_*)} \\
&= y_{(2,\mathcal{U}(2))} y_{(3,I_*)} y_{(2,\mathcal{U}(2))} \hat{y}_{(3,I_*)} && [\text{by } 12(*)_2(b)(\beta)\text{–}(\gamma)] \\
&= y_{(2,\mathcal{U}(2)\cap I_*)} y_{(3,I_*)} y_{(2,\mathcal{U}(2)\cap I_*)} y_{(3,I_*)} && [\text{by } 12(*)_2(a)(\beta)+(b)(\epsilon)] \\
&= y_{(2,\mathcal{U}(2)\cap I_*)} y_{(3,\mathcal{U}(2)\cap I_*)} y_{(2,\mathcal{U}(2)\cap I_*)} y_{(3,\mathcal{U}(2)\cap I_*)} && [\text{by } 12(*)_2(a)(\beta)+(b)(\epsilon)] \\
&= \prod_{i \in \mathcal{U}(2)\cap I_*} \mathfrak{c}_2(i, i) && [\text{by } 12(*)_2(b)(\epsilon)] \\
&= y^1_{\mathcal{U}(2)\cap I_*} && [\text{by } 12(*)_2(a)(\beta)] \\
&= y^1_{\mathcal{U}(2,a)\cap I_*}.
\end{aligned}$$

Hence, recapitulating, we have

$$(\star) \qquad [a, c] = y^1_{\mathcal{U}(2,a) \cap I_*}.$$

Concerning clause (b), by Equation ($\star$) for $a = x_\ell$, Lemma 15 and the fact that the triple $(G_{(\mathbf{p},1)}, \bar{y}^1, \bar{z}^1) \in \mathbf{CR}_{(n,m)}$ we have that $[x_\ell, c] = e$ or $[x_\ell, c] = y^1_{I_*}$, and in both cases $[x_\ell, c]$ commutes with $z^1_{I_*} = c_*$ (cf. Definition 10(d)). Clause (c) holds by Lemma 15, since by choice $|I_*| = n_2/2^k$. As for clause (d), clearly, the $(B_I : I \subseteq I_*)$ are pairwise disjoint, since $a \in B_{I_1} \cap B_{I_2}$ implies $y^1_{I_1} = [a, c] = y^1_{I_2}$, and for $I_1 \neq I_2$ we have that $y^1_{I_1} \neq y^1_{I_2}$ (cf. Definition 10(b)); moreover, by Equation ($\star$), if $a \in G_2$, then $[a, c] = y^1_{\mathcal{U}(2,a) \cap I_*} \in \{y^1_I : I \subseteq I_*\}$, and for $I \subseteq I_*$ we have that $[y^1_I, y^1_{I_*}] = e$ if and only if $I \in \{\emptyset, I_*\}$ (cf. Definition 10(d)); and finally the pieces of the partition are of equal size since, given a finite set X, a subset Y of X and two subsets c_1 and c_2 of Y we have that

$$|\{Z \subseteq X : Z \cap Y = c_1\}| = |\{Z \subseteq X : Z \cap Y = c_2\}|.$$

Concerning clause (e), let:

(a) $X = \{(x, y) \in G_2 \times G_2 : [[[x, c], c_*], y] = e\}$;
(b) $X_1 = \{(x, y) \in G_2 \times G_2 : [x, c] \in \{y^1_{I_*}, e\}\}$;
(c) $X_2 = \{(x, y) \in X : [x, c] \in \{y^1_I : I \subseteq I_*, I \notin \{I_*, \emptyset\}\}\}$.

Clearly $X = X_1 \cup X_2$ and $X_1 \cap X_2 = \emptyset$. Now, on one hand, we have

$$(1) \qquad |X_1| \leqslant |G_2 \times G_2| \cdot \frac{|\{\emptyset, I_*\}|}{2^{|I_*|}} = |G_2 \times G_2| \cdot \frac{2}{2^{|I_*|}},$$

while, on the other hand, we have

$$(2) \qquad |X_2| \leqslant \frac{|G_2 \times G_2|}{n^2}.$$

[Why does (2) hold? First of all notice that:

$\oplus_1$ if $x \in B_I$, $\mathcal{U}(2, x) \cap I_* = I \subseteq I_*$, $I \notin \{I_*, \emptyset\}$, then:
  (a) $[[x, c], c_*] \neq e$ (by clause (d) of the current lemma);
  (b) $[[x, c], c_*] \in G_1$ (because by ($\star$) $[x, c] = y^1_{\mathcal{U}(2,x) \cap I_*} \in G_1$, and $c_* = z^1_{I_*} \in G_1$).

Secondly, notice that:

$\oplus_2$ (a) if $t = G_1 - \{e\}$, then

$$\begin{aligned} Z_t :=& \{x \in G_2 : [t, x] = e\} \\ =& \{x \in G_2 : x = y_{(3,\mathcal{U}(3))} y_{(2,\mathcal{U}(2))} y_{(1,x)} \text{ and } [y_{(1,x)}, t] = e\} \quad \text{(cf. Lemma 14)}; \end{aligned}$$

(b) and so for $t = G_1 - \{e\}$ we have

$$\begin{aligned}|Z_t| \leqslant & 2^{n_3} \cdot 2^{n_2} \cdot |\{y_1 \in G_1 : [y_1, t] = e\}| \\ \leqslant & |G_2| \cdot \frac{1}{|G_1|} \cdot \max_{t \in G_1 - \{e\}} |\{y_1 \in G_1 : [y_1, t] = e\}|;\end{aligned}$$

(c) and thus, by (b) and Definition 10(e), we have

$$t \in G_1 - \{e\} \ \Rightarrow \ |Z_t| \leqslant |G_2| \cdot \frac{1}{n^2}.$$

Hence, we have

$$\begin{aligned}|X_2| \leqslant & |G_2| \cdot \max_{\substack{x \in G_2 \\ \mathcal{U}(2,x) \cap I_* \notin \{\emptyset, I_*\}}} |\{y \in G_2 : [[[x, c], c_*], y] = e\}| \\ \leqslant & |G_2| \cdot \max_{t \in G_1 - \{e\}} |\{y \in G_2 : [y, t] = e\}| && [\text{by } \oplus_1] \\ \leqslant & \frac{|G_2 \times G_2|}{n^2} && [\text{by } \oplus_2(\text{c})].\end{aligned}$$

That is, Equation (2) holds as promised. This closes the "Why (2)?" above.]

Hence, putting together (1) and (2) we have

$$\begin{aligned}|\{(x, y) \in G_2 \times G_2 : G_2 \models [[[x, c], c_*], y] = e\}| \leqslant & |G_2 \times G_2| \cdot \left(\frac{2}{2^{|I_*|}} + \frac{1}{n^2}\right) \\ \leqslant & \frac{|G_2 \times G_2|}{m},\end{aligned}$$

by the choice of m and n, in fact by (c) of this lemma we have that $|I_*| = n_2/2^k$ and, by Definition (12)$(*)_0$(d) and Notation 13,

$$n_2/2^k = n/2^k = 2^k m/2^k = m. \qquad \blacksquare$$

Conclusion 17: *Assume that* $\mathbf{p} \in \mathbf{CR}$ *(cf. Definition 12). If* $x_\ell \in G_2 = G_{(\mathbf{p},2)}$, *for* $\ell < k = k_{\mathbf{p}}$, *then for some* $c_1, c_2 \in G_2$ *we have:*

(a) $G_2 \models [[x_\ell, c_1], c_2] = e$;

(b) $\{y \in G_2 : G_2 \models [[[x_\ell, c_1], c_2], y] = e\} = G_2$;

(c) $|\{(x, y) \in G_2 \times G_2 : G_2 \models [[[x, c_1], c_2], y] = e\}| \leqslant |G_2 \times G_2|/m$.

Proof. This is clear from Lemma 16 letting $c_1 = c$ and $c_2 = c_*$, for c, c_* as there. $\blacksquare$

4. The solution

Notation 18: (Recall the notation of Definition 12.) We choose (f_1, g_1) and (f_2, g_2) such that:

(a) f_1, g_1, f_2, g_2 are strictly increasing functions from ω^ω;
(b) $f_\ell(n) > g_\ell(n)$, for $\ell \in \{1, 2\}$ and $n < \omega$;
(c) (f_1, g_1) and (f_2, g_2) are sufficiently different (as in [5]), e.g., for every $i < \omega$ we have $2^{2^{f_1(i)}} < g_2(i)$ and $2^{2^{f_2(i)}} < g_2(i+1)$;
(d) for every $i < \omega$, there is $\mathbf{p}_i \in \mathbf{CR}$ (cf. Definition 12) such that:
 (i) $f_1(i) = |G_{(\mathbf{p}_i,2)}|$;
 (ii) $g_2(i) = k_{\mathbf{p}_i}$;
(e) $\sum_{i<\omega} \frac{g_2(i)}{f_2(i)} < \infty$;
(f) for $i < \omega$, let $(m^*_i, m^{**}_i) = (g_2(i), f_2(i))$;
(g) for $i < \omega$, let $k_{\mathbf{p}_i} = k_i$, $m_{\mathbf{p}_i} = m_i$, $n_{\mathbf{p}_i} = n_i$ and $G^*_i = G_{(\mathbf{p}_i,2)}$;
(h) let $G_* = \prod_{i<\omega} G^*_i$.

Observation 19: (1) For every $i < \omega$, G^*_i is a finite group.
(2) G_* is a metrizable profinite group (cf. Definition 2).

Proof. Item (1) is by Lemma 14. Item (2) is by definition. ∎

Notation 20: (1) We denote by $w(x, y, \bar{z})$, for $\bar{z} = (z_1, z_2)$, the group word

$$[[[x, z_1], z_2], y].$$

From now till the end of the paper the letter w will denote this specific word.
(2) Recall Notation 3, i.e., we denote by μ the Haar measure.

Notation 21: (1) For $\bar{c} \in G_* \times G_*$, let

$$X_{\bar{c}} = \{x \in G_* : \mu(\{y \in G_* : w(x, y, \bar{c})\}) > 0\}.$$

(2) Let $\mathfrak{C} = \{\bar{c} \in G_* \times G_* : \mu(\{(x, y) \in G_* \times G_* : w(x, y, \bar{c})\}) = 0\}$.

LEMMA 22: *A sufficient condition for $\mathfrak{fm}(G_*) \leqslant \lambda$ (cf. Definition 6) is:*

$(\star)_1$ *there is $\mathcal{F} \subseteq \prod_{i<\omega}[G^*_i]^{k_i}$ of cardinality $\leqslant \lambda$ such that*

(A) $$\Big(\forall \eta \in \prod_{i<\omega} G^*_i\Big)(\exists \nu \in \mathcal{F})[\eta(i) \in \nu(i)].$$

Proof. For every $\nu \in \mathcal{F}$ and $i < \omega$, $\nu(i) \in [G^*_i]^{k_i}$, hence, by Conclusion 17, there are $c^\nu_{i,1}, c^\nu_{i,2} \in G^*_i \times G^*_i$ such that letting $\bar{c}^\nu_i = (c^\nu_{i,1}, c^\nu_{i,2})$ we have:

(a) if $x \in \nu(i)$, then $|\{y \in G^*_i : w(x, y, \bar{c}^\nu_i) = e\}| = |G^*_i|$;
(b) $|\{(x, y) \in G^*_i \times G^*_i : w(x, y, \bar{c}^\nu_i) = e\}| \leqslant |G^*_i \times G^*_i|/m$.

Let now $\bar{c}_\nu = (\bar{c}_{\nu(1)}, \bar{c}_{\nu(2)}) \in G_* \times G_*$, where, for $\ell \in \{1, 2\}$, $\bar{c}_{\nu(\ell)} = (c^\nu_{i,\ell} : i < \omega)$. Then we have (recalling Notation 21):

(a') $G_* \subseteq \{X_{\bar{c}_\nu} : \nu \in \mathcal{F}\}$ (by Fact 7, (A) of the statement, and (a) above);
(b') $\bar{c}_\nu \in \mathfrak{C}$ (by Fact 7 and (b) above).

Hence, by (a') and (b'), we have that $\{X_{\bar{c}_\nu} : \nu \in \mathcal{F}\}$ is a witness for $\mathfrak{fm}(G_*) \leqslant \lambda$. ∎

Lemma 23: *Recalling Notation 18*(f), *a sufficient condition for* non$(\mathcal{N}) > \lambda$ *(cf. Definition 8) is:*

$(\star)_2$ *for every $Y \subseteq \prod_{i<\omega} m^{**}_i$ of cardinality $\leqslant \lambda$ there is ν such that:*
(a) $\nu \in \prod_{i<\omega} [m^{**}_i]^{m^*_i}$;
(b) *if $\eta \in Y$, then, for infinitely many $i < \omega$, we have that $\eta(i) \in \nu(i)$.*

Proof. This is because denoting by μ (resp. μ^*) the Lebesgue measure (resp. the outer Lebesgue measure) of the Polish space $\prod_{i<\omega} m^{**}_i$ we have that

$$\begin{aligned}
\mu^*(Y) &\leqslant \mu^*(\underbrace{\{\eta \in X : \exists^\infty i(\eta(i) \in \nu(i))\}}_{X_\infty}) && [\text{by } (\star)_2(\text{b})] \\
&\leqslant \mu\Big(\bigcap_{n<\omega} \underbrace{\{\eta \in X : \bigvee_{i \geqslant n} \eta(i) \in \nu(i)\}}_{X_n}\Big) && [X_\infty \subseteq X_n,\ \forall n < \omega] \\
&\leqslant \lim_{n\to\infty} \mu(\{\eta \in X : \bigvee_{i \geqslant n} \eta(i) \in \nu(i)\}) && [X_n \text{ measurable, } X_n \supseteq X_{n+1}] \\
&\leqslant \lim_{n\to\infty} \frac{m^*_n}{m^{**}_n} = 0 && [\text{cf. Notation 18}(f) \text{ and properties of } f_2, g_2 \text{ there}].
\end{aligned}$$

∎

Theorem 24: *Assume that* $\mathbf{V} \models CH$. *Then for some $\aleph_2$-c.c. proper (in fact even cardinal preserving) forcing $\mathbb{P}$ we have that in $\mathbf{V}[\mathbb{P}]$ both of the conditions below are satisfied:*

(a) *the statement $(\star)_1$ from Lemma 22 for $\lambda = \aleph_1$;*
(b) *the statement $(\star)_2$ from Lemma 23 for $\lambda = \aleph_1$.*

Proof. This is by [5, Theorem 2] and the choice of $(f_1, g_1), (f_2, g_2)$ in Notation 18. ∎

Proof of the Main Theorem. This follows from Lemmas 22 and 23, and Theorem 24. ∎

References

[1] W. R. Brian and M. W. Mislove, *Every infinite compact group can have a non-measurable subgroup*, Topology and its Applications **210** (2016), 144–146.

[2] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 11, Springer, Berlin, 2005.

[3] S. Hernández, K. H. Hofmann and S. A. Morris, *Nonmeasurable subgroups of compact groups*, Journal of Group Theory **19** (2016), 179–189.

[4] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis. Vol. I*, Die Grundlehren der mathematischen Wissenschaften, Vol. 115, Academic Press, New York; Springer, Berlin–Göttingen–Heidelberg, 1963.

[5] J. Kellner and S. Shelah, *Decisive creatures and large continuum*, Journal of Symbolic Logic **74** (2009), 73–104.

[6] A. J. Przeździecki, P. Szewczak and B. Tsaban, *The Haar measure problem*, Proceedings of the American Mathematical Society **147** (2019), 1051–1057.