J. Eur. Math. Soc. 14, 1455–1511

DOI 10.4171/JEMS/337

J. Bourgain · A. Gamburd

A spectral gap theorem in $\mathrm{SU}(d)$

Received February 5, 2012

Abstract. We establish the spectral gap property for dense subgroups of $\mathrm{SU}(d)$ ($d \geq 2$), generated by finitely many elements with algebraic entries; this result was announced in [BG3]. The method of proof differs, in several crucial aspects, from that used in [BG] in the case of SU(2).

0. Introduction and outline

For $k \geq 2$ let $g_1, \ldots, g_k$ be a finite set of elements in $G = \mathrm{SU}(d)$ ($d \geq 2$). We associate with them an *averaging* (or *Hecke*) *operator* $z_{g_1,\ldots,g_k}$, taking $L^2(\mathrm{SU}(d))$ into $L^2(\mathrm{SU}(d))$:

$$z_{g_1,\ldots,g_k} f(x) = \sum_{j=1}^{k} (f(g_j x) + f(g_j^{-1} x)).$$

We denote by $\mathrm{supp}(z)$ the set $\{g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}\}$ and by Γ_z the group generated by $\mathrm{supp}(z)$. It is clear that $z_{g_1,\ldots,g_k}$ is self-adjoint and that the constant function is an eigenfunction of z with eigenvalue $\lambda_0(z) = 2k$. Let $\lambda_1(z_{g_1,\ldots,g_k})$ denote the supremum of the eigenvalues of z on the orthogonal complement of the constant functions in $L^2(\mathrm{SU}(d))$. We say that z *has a spectral gap* if

$$\lambda_1(z_{g_1,\ldots,g_k}) < 2k.$$

It is common to, alternatively, refer to the situation described above by saying that *the spectral gap property holds for* Γ_z.

In this paper we generalize the result on the spectral gap for finitely generated subgroups of SU(2), established in [BG], to dense subgroups of $\mathrm{SU}(d)$ ($d \geq 2$), generated by finitely many elements with algebraic entries.

Theorem 1. *Assume that* $\{g_1, \ldots, g_k\} \subset \mathrm{SU}(d) \cap \mathrm{Mat}_{d\times d}(\overline{\mathbb{Q}})$, *and that the group generated by* $g_1, \ldots, g_k$ *is Zariski dense*[1] *in* $\mathrm{SL}_d(\mathbb{C})$. *Then the associated Hecke operator* $z_{g_1,\ldots,g_k}$ *has a spectral gap.*

J. Bourgain: School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA; e-mail: bourgain@ias.edu

A. Gamburd: Mathematics Ph.D. Program, The CUNY Graduate Center, 365 Fifth Avenue, New York, NY 10016, USA; e-mail: agamburd@gc.cuny.edu

[1] Note that the Zariski-density assumption is equivalent to the topological density of the group generated by $\{g_1, \ldots, g_k\}$ in $\mathrm{SU}(d)$.

Various applications of such a spectral gap result (to, among other things, the Banach–Ruziewicz problem, the theory of quasi-crystals, and the question, arising in the theory of quantum computation, of whether a "computationally universal" set is necessarily "efficiently universal") are discussed in [BG].

It should be pointed out, however, that the method of proof in the present paper differs, in several crucial aspects, from the one given in [BG] in the case of SU(2).

In [BG], the proof of the spectral gap proceeded by, first, establishing a "product theorem" for general subsets of SU(2). Both the statement and the proof of the latter result is not unrelated to the product theorem in $\mathrm{SL}_2(p)$, established by Helfgott [H] (and generalized to groups of higher rank by Breuillard, Green and Tao [BGT] and by Pyber and Szabó [PS][2]); a key ingredient in the proof of the pertinent product theorem in the aforementioned papers is the exact size of intersections of "multiplicatively stable" subsets of the group with maximal tori.

In contrast, the approach we follow in the present paper is akin to the one in [BG1, BG2], and is based, crucially, on multi-scale arguments (available for groups defined over $\mathbb{C}$ or $\mathbb{Z}/p^n\mathbb{Z}$), and Lie algebra point of view.[3] The salient features of this approach can be encapsulated as follows: (a) first, using "tools from arithmetic combinatorics", we construct in the "approximate group" (see [Tao], [BG], [BG1, BG2] for background) an "approximately one-dimensional structure" in a suitable neighborhood of the identity; (b) subsequently, this structure serves as the main building block to recover the full Lie algebra; (c) certain "escape" (from hyperplanes) issues, coming into play in (b), are addressed, using, in an essential way, the theory of random matrix products.

In connection with (c), it should be pointed out, that, whereas in [BG2] the "classical" theory of random matrix products (see, for example, [BL]) for Zariski dense subgroups of SL_d (as developed by, among others, Furstenberg [F], Goldsheid–Guivarc'h [GG], Goldsheid–Margulis [GM], Guivarc'h–Raugi [GR], and Guivarc'h [G]) was directly applicable, in the present $\mathrm{SU}(d)$ setting nontrivial difficulties arise, due to the absence of proximal (in the obvious sense) elements, necessitating the use of non-Archimedean local fields and exterior powers of the Lie algebra (cf. [A]).

It is our expectation that the method of proof of the spectral gap result developed in the present paper in the context of $\mathrm{SU}(d)$ should also be applicable to other continuous semisimple Lie groups; we intend to pursue this in a forthcoming paper.

The main ingredient from arithmetic combinatorics, alluded to in (a) above, is an extension of the "discretized ring theorem" (see [B1, B2]) from $\mathbb{R}$ to $\mathbb{C}$ (see Proposition 2 at the end of the Introduction), and, crucially, to Cartesian products $\mathbb{C}^d$. This extension is obtained in §1–§8: parts of the argument are closely related to [B2]. We remark, that, in this part of the argument, several steps are presented in a somewhat greater generality than what is, strictly speaking, necessary for the purposes of this paper.

[2] Mention should be made, too, of the groundbreaking work of Hrushovski [Hr], and of the work of Breuillard and Green [BrGr] on the classification of approximate subgroups of the unitary group, yielding an elegant and far-reaching generalization of Jordan's theorem [J].

[3] It might be worth remarking, that, in the stressed crucial reliance on multi-scale and Lie algebra structures, this approach is reminiscent of the Solovay–Kitaev algorithm in quantum computation [DN].

Returning to the proof of the spectral gap result in SU(d), let us conclude this introduction by giving a rough summary of the various steps in the argument.

As mentioned above, the overall approach is akin to the one used in [BG1, BG2]. Let

$$\nu = \frac{1}{2k}\sum_{i=1}^{k}(\delta_{g_i} + \delta_{g_i^{-1}}) \tag{0.1}$$

be the probability measure supported on the generators $g_1, \dots, g_k$. Denoting by P_δ an approximate identity on $G = \mathrm{SU}(d)$, and taking $\delta \to 0$, our first objective is to prove that, for $\tau > 0$ (some fixed small constant), we can ensure that

$$\|\nu^{(\ell)} * P_\delta\|_\infty < \delta^{-\tau} \tag{0.2}$$

for $\ell < C(\tau)\log(1/\delta)$. Here $\nu^{(\ell)}$ is the ℓ-fold convolution power of ν. This is achieved by iterating an "L^2-flattening lemma" (see Lemma 10.7 in §10) which is the main technical step in this part of the argument. First, an application (originating in [BG0], and by now standard) of the noncommutative Balog–Szemerédi–Gowers lemma (proved in [Tao]) reduces the matter to the study of "approximate groups" $H \subset G$. Note that these objects are defined combinatorially, and, a priori, have no algebraic structure. Our goal is to show, roughly speaking, that if H is a δ-approximate group such that $\nu^{(\ell)}(H)$ is "large" (where $\ell \sim \log(1/\delta)$), then H has to be "almost all" of G, "up to δ-approximation". This will, then, provide the desired contradiction.

The first step in our program is to produce in H a large set of elements that are "approximately diagonal" (in a suitable basis). The key idea underlying the proof in this step originates in the work of Helfgott [H]. Let us point out, however, that, in contrast to [H], and to the subsequent papers pertaining to the product theorems in $\mathrm{SL}_d(p)$ and other finite simple groups ([BGT], [GH], [PS]), the precise size of our diagonal set is not important. The construction of this almost diagonal set appears in §9. The fact that the generators $g_1, \dots, g_k$ have algebraic entries plays a role here, but not the assumption on the Zariski density of $\langle g_1, \dots, g_k\rangle$.

The relevant statement is Proposition 9 in §9. It should be stressed, that, compared with [BG1, BG2] (and, also, with [BGT], [PS]), a significant difference is that we do not rely on regular elements to produce the almost diagonal set, and Proposition 9 provides such a construction in a greater generality.

The "almost diagonal" set of matrices is processed further using the discretized ring theorem in $\mathbb{C}^d$, resulting in our main building block: a structured, "essentially one-dimensional" set in the Lie algebra. A further amplification requires addressing certain "escape" issues that depend on the assumption of Zariski density. Thus, in §11, we establish the crucial "L^2-flattening lemma" for convolution powers, conditional on the "escape from hyperplane" assumption ($*$), which is addressed in §12 for $d = 3$ and §14 in the general case.

Similarly to the approach originating in [BG1, BG2], proving the escape property relies on the theory of random matrix products. Recall that the two main assumptions in this theory are proximality and strong irreducibility. In contrast to the case of Zariski dense subgroups of $\mathrm{SL}_d(\mathbb{R})$, elements in SU($d$) are obviously not expanding in the usual

sense, and the application of the theory of random matrix products requires considering non-Archimedean places (here, again, we use the fact that the elements $g_1, \dots, g_k$ are algebraic) and, also, representations on wedge products of the adjoint representation (see §12, 13, 14). A treatment of random matrix product theory in the context of general local fields may be found in the recent paper of Aoun [A].

Once (0.2) is established, the final step in the proof of the spectral gap requires application of basic results pertaining to the representation theory of $\mathrm{SU}(d)$. One way to proceed (as was done in [BG]) is to use the idea, originating in the work of Sarnak and Xue [SX], of exploiting "high multiplicity" of nontrivial eigenvalues (which follows from "high dimensionality" of nontrivial irreducible representations); in the continuous setting of a compact group this idea was implemented in [GJS] by summing over the suitably chosen range of representations, and then applying Poisson summation. In §10, we follow a different route, which, is, in a sense, more "geometric" (cf. [BY]). First, a new argument for $d = 2$ is given. Next, using $\mathrm{SU}(2)$-subgroups in $\mathrm{SU}(d)$, the general case is treated (this type of argument was used earlier in the work of Burger and Sarnak [BS]). One of the ingredients in this part of the argument is a convolution principle, stated in Lemma 10.35, which appears to be a rather basic result, of independent interest, pertaining to the harmonic analysis on the unitary group.

The paper is divided into two parts. In the second part (§9–§14), Theorem 1 is proved, following the steps summarized above. The first part (§1–§8) is "purely combinatorial", culminating in Propositions 2, 6 and 7, that are needed for the $\mathrm{SU}(d)$ analysis. The first part is closely related to the proof of the discretized ring theorem in $\mathbb{R}$, presented in [B2]; the generalization to the higher dimensional setting necessitates reproducing several technical portions from that paper.

The counterpart in $\mathbb{C}$ of the main theorem from [B2] can be stated as follows.

Proposition 2. *Given $0 < \sigma < 2$ and $\kappa, \kappa' > 0$, $\rho > 0$, there are $\varepsilon_0, \varepsilon_0', \varepsilon_1 > 0$ such that the following holds.*

Let $A \subset \mathbb{C} \cap B(0,1)$ satisfy

(8.1) $N(A, \delta) = \delta^{-\sigma}$ *(δ small enough),*
(8.2) $N(A \cap B(z,t), \delta) < t^{\kappa} N(A, \delta)$ *if $\delta < t < \delta^{\varepsilon_0}$ and $z \in \mathbb{C}$.*

Let μ be a probability measure on $\mathbb{C} \cap B(0,1)$ such that

(8.3) $\mu\big(B(z,t)\big) < t^{\kappa'}$ *if $\delta < t < \delta^{\varepsilon_0'}$ and $z \in \mathbb{C}$.*

Let $z_1, z_2 \in \mathbb{C}$ satisfy

(8.4) $\delta^{\varepsilon_0'} < |z_1| \sim |z_2| < 1$ *and* $|\mathrm{Im}(z_1/z_2)| > \rho$.

Then one of the following holds:

(8.5) $N(A + A, \delta) > \delta^{-\sigma-\varepsilon_1}$,
(8.6) $N(A + bA, \delta) > \delta^{-\sigma-\varepsilon_1}$ *for some $b \in \operatorname{supp} \mu$,*
(8.7) $N(A + z_1 A, \delta) + N(A + z_2 A, \delta) > \delta^{-\sigma-\varepsilon_1}$.

Part 1: Generalizing the discretized ring theorem

The aim in what follows is to establish higher dimensional analogues of the discretized sum/product theory from [B2], in particular, for subsets of $\mathbb{C}$ and $\mathbb{C}^d$.

1. Basic notation and assumptions

Let $\delta = 2^{-m}$ (m large) and $A \subset [0,1]^d$ be a collection of δ-separated points in $\mathbb{R}^d$ (alternatively we could take for A a union of δ-intervals). Assume

$$|A| = \delta^{-\sigma} \tag{1.1}$$

for some fixed $0 < \sigma < d$ ($|\ |$ denotes 'cardinality' in (1.1) but may also be used for Lebesgue measure if appropriate).

By a *size ρ interval*, we mean a d-dimensional box $\prod_{i=1}^d [a_i, a_i + \rho]$.

For $B \subset \mathbb{R}^d$ and $r > 0$, we denote by $N(B, r)$ the corresponding metrical entropy number.

We assume A satisfies the following *nonconcentration* property:

$$|A \cap I| < \rho^\kappa |A| \quad \text{if } \delta < \rho < \delta^{\varepsilon_0} \text{ and } I \text{ is a size } \rho \text{ interval} \tag{1.2}$$

for some $\kappa > 0$ and $\varepsilon_0 = \varepsilon_0(\sigma) > 0$ small enough.

Let μ be a distribution on $\mathcal{L}(\mathbb{R}^d, \mathbb{R}^d)$ (the space of linear maps on $\mathbb{R}^d$) satisfying certain assumptions to be specified (see Theorem 1 in §7). Our aim is to show that for some $\varepsilon_1 > 0$ (depending on the parameters), we have

$$N(A+A, \delta) > \delta^{-\sigma-\varepsilon_1} \quad \text{or} \quad N(A+bA, \delta) > \delta^{-\sigma-\varepsilon_1} \quad \text{for some } b \in \operatorname{supp} \mu. \tag{1.3}$$

Let T be a large constant (depending on the parameters and to be specified) and

$$m = Tm_1. \tag{1.4}$$

We also consider a dyadic partition into intervals

$$I_{n,k} = \prod_{i=1}^d [k_i 2^{-n}, (k_i+1)2^{-n}[\quad \text{where} \quad 0 \le k_i < 2^n \ \text{ and } \ n \ge 0.$$

We call $I_{n,k}$ a 2^{-n}*-interval*.

2. Initial regularization of the set

We extract from A a large subset with a 'tree structure'. This construction is independent of assumptions (1.2), (1.3).

We introduce a subset $A_1 \subset A$, a subset $\mathcal{S} \subset \{1, \dots, m_1\}$ and for $s \in \mathcal{S}$ a dyadic integer $2 \le R_s < 2^{d(n_s - sT)}$, where $sT < n_s < (s+1)T - 4$, with the following properties.

(2.1) If $s \notin \mathcal{S}$ and I is a 2^{-sT}-interval, then there is at most one $2^{-(s+1)T}$-interval $J \subset I$ such that $J \cap A_1 \neq \emptyset$. Take $R_s = 1$ and $n_s = sT$ in this case.

(2.2) If $s \in \mathcal{S}$ and I is a 2^{-sT}-interval with $I \cap A_1 \neq \emptyset$, then the number of 2^{-n_s}-intervals $J \subset I$ such that $J \cap A_1 \neq \emptyset$ is R_s and each such J-interval contains a single $2^{-(s+1)T}$-interval J' intersecting A_1. Hence also

$$R_s \sim N(A \cap I, 2^{-(s+1)T}). \tag{2.3}$$

Moreover, there is a pair of 2^{-n_s}-intervals $J_1, J_2 \subset I$ such that $J_1 \cap A_1 \neq \emptyset$, $J_2 \cap A_1 \neq \emptyset$ and

$$2 \cdot 2^{-n_s} < \operatorname{dist}(J_1, J_2) < 10 \cdot 2^{-n_s}. \tag{2.4}$$

(2.5) $|A_1| = \prod_{s \in \mathcal{S}} R_s > (cT^{-2})^{m_1} |A| > \delta^{-\sigma + (\log T)/T}$.

The construction is straightforward. We start at the bottom of the tree, considering for each $2^{-(m_1-1)T}$-interval I such that $I \cap A \neq \emptyset$ the number of $2^{-m_1 T}$-intervals $J \subset I$ with $J \cap A \neq \emptyset$. If their number is less than 10^{3d}, fix one such $2^{-m_1 T}$-interval $J = J_I$.

If their number is larger than 10^{3d}, introduce the largest integer (depending on I)

$$(m_1 - 1)T < n < m_1 T - 4$$

for which there is a pair of 2^{-n}-intervals $J_1, J_2 \subset I$ with $J_1 \cap A \neq \emptyset$, $J_2 \cap A \neq \emptyset$ and

$$2 \cdot 2^{-n} < \operatorname{dist}(J_1, J_2) < 10 \cdot 2^{-n}.$$

It is easily seen that from our definition of n,

$$N(A \cap I, 2^{-n}) \sim N(A \cap I, 2^{-m_1 T}).$$

Define R to be the dyadic integer such that the number of 2^{-n}-intervals $J \subset I$ with $J \cap A \neq \emptyset$ is between R and $2R$. Thus

$$N(A \cap I, 2^{-m_1 T}) \sim R < 2^{d(n - (m_1 - 1)T)}.$$

Obviously the integers n and R (depending on I) take at most T values. We may therefore clearly introduce a subset $A^{(m_1-1)} \subset A$ with

$$|A^{(m_1-1)}| > CT^{-2}|A| \tag{2.6}$$

satisfying one of the following alternatives:

(2.7) If I is an $2^{-(m_1-1)T}$-interval, then there is at most one $2^{-m_1 T}$-interval $J \subset I$ with $J \cap A_1 \neq \emptyset$. In this case, $m_1 - 1 \notin \mathcal{S}$.

(2.8) If I is a 2^{-sT}-interval with $I \cap A_1 \neq \emptyset$, then (2.2) holds for some $n = n_{m_1-1}$ and $R = R_{m_1-1}$. In this case, $m_1 - 1 \in \mathcal{S}$.

Next, repeat the construction for the set $A^{(m_1-1)}$ considering $2^{-(m_1-2)T}$-intervals I with $I \cap A^{(m_1-1)} \neq \emptyset$ and $2^{-(m_1-1)T}$-subintervals $J \subset I$. We obtain $A^{(m_1-2)}$ as the intersection of $A^{(m_1-1)}$ and a collection of $2^{-(m_1-1)T}$-intervals; moreover

$$|A^{(m_1-2)}| > cT^{-2}|A^{(m_1-1)}| \tag{2.9}$$

and $A^{(m_1-2)}$ satisfies either (2.1) or (2.2) with $s = m_1 - 2$, for some $(m_1 - 2)T < n_{m_1-2} < (m_1 - 1)T - 4$ and $R_{m_1-2} < 2^{d(n_{m_1-2}-(m_1-2)T)}$.

By construction

$$A^{(m_1-2)} \cap I = A^{(m_1-1)} \cap I$$

if I is a $2^{-(m_1-1)T}$-interval intersecting $A^{(m_1-2)}$. Hence properties (2.1), (2.2) at level $m_1 - 1$ remain preserved.

The continuation of the process is clear. We obtain

$$A \supset A^{(m_1-1)} \supset A^{(m_1-2)} \supset \cdots \supset A^{(s)} \supset A^{(s-1)} \supset \cdots \supset A^{(1)}$$

where

$$|A^{(s-1)}| > CT^{-2}|A^{(s)}|, \tag{2.10}$$

and

$$A^{(s-1)} \cap I = A^{(s)} \cap I$$

if I is a 2^{-sT}-interval intersecting $A^{(s-1)}$. Hence $A^{(s-1)}$ keeps the properties of $A^{(s)}$ at scales 2^{-n} for $n \geq sT$.

Let $A_1 = A^{(1)}$. Iteration of (2.10) gives (2.5).

Denote $\mathcal{S} = \{s_1 < \cdots < s_t\}$. For each $c \in \{0, 1\}^t$, we will introduce an element $x_c \in A_1 \subset A$.

Since $s_1 \in \mathcal{S}$, it follows from (2.2) that there is a pair of $2^{-n_{s_1}}$-intervals I_0, I_1 intersecting A_1 such that

$$2 \cdot 2^{-n_{s_1}} < \operatorname{dist}(I_0, I_1) < 10 \cdot 2^{-n_{s_1}}. \tag{2.11}$$

Denote by $I_0' \subset I_0$ and $I_1' \subset I_1$ the 2^{-s_2T}-intervals intersecting A_1. Again by (2.2), there are pairs $I_{0,0}, I_{0,1} \subset I_0'$ and $I_{1,0}, I_{1,1} \subset I_1'$ of $2^{-n_{s_2}}$-intervals satisfying

$$2 \cdot 2^{-n_{s_2}} < \operatorname{dist}(I_{0,0}, I_{0,1}) < 10 \cdot 2^{-n_{s_2}}, \tag{2.12}$$

$$2 \cdot 2^{-n_{s_2}} < \operatorname{dist}(I_{1,0}, I_{1,1}) < 10 \cdot 2^{-n_{s_2}}. \tag{2.12$'$}$$

Continuing the construction, we eventually obtain 2^{-s_tT}-intervals $I_c = I_{c_1,\ldots,c_t}$ for $(c_1, \ldots, c_t) \in \{0, 1\}^t$ such that $I_c \cap A_1 \neq \emptyset$ and with the property that if $c_1 = c_1', \ldots, c_\tau = c_\tau', c_{\tau+1} \neq c_{\tau+1}'$, then

$$2 \cdot 2^{-n_{s_{\tau+1}}} < \operatorname{dist}(I_c, I_{c'}) < 10 \cdot 2^{-n_{s_{\tau+1}}}. \tag{2.13}$$

Take

$$x_c \in I_c \cap A_1 \quad \text{for } c \in \{0, 1\}^t. \tag{2.14}$$

Fix some $\beta > 0$ (to be specified) and define

$$\mathcal{S}_1 = \{1 \le s \le m_1;\ (s+1)T - n_s > \beta T\} \tag{2.15}$$

(the *porous levels*). Obviously $\mathcal{S}_1 \supset \{1, \dots, m_1\} \setminus \mathcal{S}$.

Let $s_1 < \cdots < s_{t_1}$ be an enumeration of the elements of $\mathcal{S}_1$.

Let $\varepsilon_2 > 0$ (to be specified) and assume first that

$$t_1 > \varepsilon_2 m_1, \tag{2.16}$$

which we refer to as the *porous case*. The amplification in this situation can be performed exactly as in the $d = 1$ case. The argument is repeated in the next sections.

If $t_1 \le \varepsilon_2 m_1$, then $|\mathcal{S}| > (1 - \varepsilon_2)m_1$ at most levels $s_\tau \in \mathcal{S}$, and (2.13) implies

$$2 \cdot 2^{-T} < 2^{s_\tau T} \operatorname{dist}(I_c, I_{c'}) < 10 \cdot 2^{-(1-\beta)T} \tag{2.17}$$

if $c_1 = c_1', \dots, c_{\tau-1} = c_{\tau-1}'$ and $c_\tau \ne c_\tau'$.

This is the *nonporous case* and requires a different argument.

3. The porous case (bunching together of levels)

Let $\mathcal{S} = \{\mathcal{S}_1 < \cdots < \mathcal{S}_{t_1}\}$ and assume (2.16).

We construct from A_1 a new system of sets $B_{k_1,\dots,k_j}$ $(j \le t_1)$ with a 'porosity property' at each level.

Denote by B_{k_1}, $1 \le k_1 \le K_1 = \prod_{s \le s_1} R_s$, the collection of nonempty intersections $A_1 \cap I$, where I is a $2^{-n_{s_1}}$-interval. By (2.1), (2.2), for each B_{k_1} there is at most one $2^{-(s_1+1)T}$-interval J such that $\emptyset \ne A_1 \cap J = B_{k_1}$. Hence (reducing $|A_1|$ by a factor c_d) we may assume

(3.1) $\operatorname{diam} B_{k_1} \le 2^{-(s_1+1)T}$,
(3.2) $\operatorname{dist}(B_{k_1}, B_{k_1'}) > 2^{-(s_1+1-\beta)T}$ if $k_1 \ne k_1'$.

Fixing k_1, let $B_{k_1 k_2}$, $1 \le k_2 \le \prod_{s_1 < s \le s_2} R_s = K_2$, be the collection of nonempty intersections $B_{k_1} \cap I$ where I is a $2^{-n_{s_2}}$-interval. Again, each B_{k_1,k_2} is contained in a single $2^{-(s_2+1)T}$-interval and

(3.3) $B_{k_1} = \bigcup_{k_2 \le K_2} B_{k_1}$,
(3.4) $\operatorname{diam} B_{k_1 k_2} < 2^{-(s_2+1)T}$,

and we may ensure

(3.5) $\operatorname{dist}(B_{k_1,k_2}, B_{k_1',k_2'}) > 2^{-(s_2+1-\beta)T}$ for $(k_1, k_2) \ne (k_1', k_2')$.

Continuing, we obtain a system $B_{k_1,\dots,k_j}$ $(1 \le k_i \le K_i,\ j \le t_1)$ with the following properties:

(3.6) $|\bigcup_{1 \le k_1 \le K_1} B_{k_1}| \ge C^{-t_1}|A_1| > C^{-m_1}|A_1|$,
(3.7) $B_{k_1,\dots,k_j} = \bigcup_{1 \le k \le K_{j+1}} B_{k_1,\dots,k_j,k}$,

(3.8) $\operatorname{diam} B_{k_1,\dots,k_j} \le 2^{-T\beta}\lambda_j$,
(3.9) $\operatorname{dist}(B_{k_1,\dots,k_j}, B_{k'_1,\dots,k'_j}) > \lambda_j$ if $\bar{k} \ne \bar{k}'$,

where we denoted

$$\lambda_j = 2^{-(s_j+1-\beta)T}. \tag{3.10}$$

Next we introduce a new system $C_{\ell_1,\dots,\ell_s}$ ($1 \le \ell_s \le L_s$ and $1 \le s \le t_2$). Define

$$M = [2^{T^{2/3}}] \tag{3.11}$$

and let

$$10^3 < D \in \mathbb{Z}_+, \tag{3.12}$$

to be specified.

We consider the system $B_{k_1,\dots,k_j}$ constructed above. Starting from t_1, let $r_1 \in \mathbb{Z}_+$ be minimum such that

$$K_{t_1} \cdots K_{t_1-r_1} > M^{r_1+1}. \tag{3.13}$$

We distinguish two cases.

If $r_1 \le 10^3$, identify levels $t_1 - r_1, \dots, t_1$ to a single one, with branching

$$L_{t_2} = K_{t_1} \cdots K_{t_1-r_1} > M^{r_1+1}. \tag{3.14}$$

The sets $C_{\ell_1,\dots,\ell_{t_2}}$ are $B_{k_1,\dots,k_{t_1}}$, hence

(3.15) $\operatorname{diam} C_{\ell_1,\dots,\ell_{t_2}} < \sigma_{t_2}\mu_{t_2}$,
(3.16) $\operatorname{dist}(C_{\ell_1,\dots,\ell_{t_2}}, C_{\ell'_1,\dots,\ell'_{t_2}}) > \mu_{t_2}$ if $\bar{\ell} \ne \bar{\ell}'$,

where $\mu_{t_2} = \lambda_{t_1}$ and

$$\sigma_{t_2}^{-1} = 2^{\beta T} > M^{D(r_1+1)} \tag{3.17}$$

assuming, if (3.11) holds,

$$T > 10^{10}(D/\beta)^3. \tag{3.18}$$

If $r_1 > 10^3$, identify levels $t_1 - r_1, \dots, t_1 - r_1/100 + 1$ to a single one, with branching

$$L_{t_2} = K_{t_1-r_1} \cdots K_{t_1-r_1/100+1} > \frac{M^{r_1+1}}{K_{r_1-r_1/100} \dots K_{t_1}} > M^{r_1+1-(r_1/100+1)} > M^{\frac{99}{100}r_1} \tag{3.19}$$

(from definition of r_1). In order to ensure proper separation, reduce the sets $B_{k_1,\dots,k_{t_1-r_1/100}}$ to their subset

$$B_{k_1,\dots,k_{t_1-r_1/100},\underbrace{1,\dots,1}_{r_1/100}} = C_{\ell_1,\dots,\ell_{t_2}}.$$

By (3.8), (3.9), the mutual distance between those sets is at least $\lambda_{t_1-r_1/100} \equiv \mu_{t_2}$, while their diameter is at most $\lambda_{t_1} = \sigma_{t_2}\mu_{t_2}$ with

$$\sigma_{t_2}^{-1} = 2^{\frac{\beta}{100}r_1 T} > M^{D(r_1+1)} \tag{3.20}$$

(by (3.18)).

We have reduced the size of A_1 by at most a factor $K_{t_1-r_1/100}\cdots K_{t_1} < M^{r_1/100+1} < M^{r_1/90}$.

Next, repeat (if possible) the procedure, starting from level $t_1 - r_1$ to obtain a level $t_1 - r_1 - r_2$, etc.

If at some level $t' = t_1 - r_1 - r_2 - \cdots$ we cannot continue the process, it means that

$$K_1 \cdots K_{t'} \le M^{t'+1} < 2^{T^{2/3}t_1} \le 2^{m_1 T^{2/3}} < (1/\delta)^{T^{-1/3}}. \tag{3.21}$$

Hence

$$|A \cap I| \ge |B_{k_1,\ldots,k_{t'}}| \overset{(3.6)}{>} \delta^{T^{-1/3}} C^{-m_1}|A_1| \overset{(2.5)}{>} \delta^{2T^{-1/3}}|A| \tag{3.22}$$

where I is some $2^{-s_{t'}T}$-interval.

Recall the nonconcentration assumption (1.2). It follows from (3.22) that either $2^{-s_{t'}T} > \delta^{\varepsilon_0} = 2^{-\varepsilon_0 m_1 T}$ or $\delta^{2T^{-1/3}} < 2^{-s_{t'}T\kappa}$. Hence

$$t' \le s_{t'} < \max(\varepsilon_0 m_1, \kappa^{-1}T^{-1/3}m_1) < \frac{\varepsilon_2}{2}m_1 \tag{3.23}$$

assuming

$$\varepsilon_0 < \varepsilon_2/2 \quad \text{and} \quad T^{-1/3} < \frac{1}{2}\kappa\varepsilon_2. \tag{3.24}$$

Since by (2.16), $t_1 > \varepsilon_2$, this will ensure that $t' < \frac{1}{2}t_1$ and hence

$$r_1 + r_2 + \cdots = t_1 - t' > \frac{1}{2}t_1 > \frac{1}{2}\varepsilon_2 m_1. \tag{3.25}$$

Consequently, we replaced $B_{k_1,\ldots,k_j}$ $(1 \le j \le t_1)$ by a subtree $C_{\ell_1,\ldots,\ell_s}$ $(1 \le s \le t_2)$ with the following properties:

(3.26) $C_{\ell_1,\ldots,\ell_{s-1}} = \bigcup_{\ell \le L_s} C_{\ell_1,\ldots,\ell_s,\ell} \subset A$,

(3.27) $\operatorname{dist}(C_{\ell_1,\ldots,\ell_s}, C_{\ell'_1,\ldots,\ell'_s}) \ge \mu_s$ if $(\ell_1,\ldots,\ell_s) \ne (\ell'_1,\ldots,\ell'_s)$,

(3.28) $\operatorname{diam} C_{\ell_1,\ldots,\ell_s} < \sigma_s\mu_s$, where $2^{-\beta T} > \sigma_s > \delta^{1/2}$,

(3.29) $\prod_s (L_s \wedge \sigma_s^{-1/D}) > M^{\frac{99}{100}(r_1+r_2+\cdots)} = M^{\gamma m_1}$, where

$$\gamma = \frac{99}{100m_1}(r_1 + r_2 + \cdots) > \frac{1}{3}\varepsilon_2, \tag{3.30}$$

(3.31) $\left|C_\phi = \bigcup_{\ell_1 \le L_1} C_{\ell_1}\right| > M^{-\frac{1}{90}(r_1+r_2+\cdots)}c^{-m_1}|A_1| > M^{-\frac{\gamma}{80}m_1}|A|$.

The sets $C_{\overline{\ell}}$ are subsets of the discrete set A.

In what follows, it will be convenient to replace our discrete sets by unions of size-δ intervals, defining

$$A' = \{x \in \mathbb{R};\ \operatorname{dist}(x, A) < \delta/2\} \tag{3.32}$$

and similarly, for $\overline{\ell} = (\ell_1,\ldots,\ell_s)$,

$$C'_{\overline{\ell}} = \{x \in \mathbb{R};\ \operatorname{dist}(x, C_{\overline{\ell}}) < \delta/2\}. \tag{3.33}$$

Hence

$$|A'| = \delta|A| = \delta^{1-\sigma}, \tag{3.34}$$

$$|C'_{\overline{\ell}}| = \delta|C_{\overline{\ell}}| \tag{3.35}$$

(using $|\ |$ to denote both measure and cardinality).

4. Porous case (amplification)

Assume a probability measure μ on $\mathcal{L}(\mathbb{R}^d, \mathbb{R}^d)$ and $\kappa' > 0$ satisfy the following conditions:

(4.1) $\|b\| \leq 1$ if $b \in \operatorname{supp} \mu$,
(4.2) given a unit vector $v \in \mathbb{R}^d$ and a vector $w \in \mathbb{R}^d$, we have $\mu[b;\ |bv - w| < \rho] < c\rho^{\kappa'}$ for all $\delta < \rho < 1$.

We denote by $\mathbb{E} = \mathbb{E}_b$ the μ-expectation. Our aim is to estimate from below the equality

$$|C'_\phi + C'_\phi| + \mathbb{E}[|C'_\phi + bC'_\phi|].$$

Let us first show that we may replace the b-distribution so as to ensure moreover the property

(4.3) b is invertible and $\|b^{-1}\| < 3$ for $b \in \operatorname{supp} \mu$.

This is seen as follows. Consider the map

$$b \mapsto \tfrac{1}{3}(2 \cdot \mathbb{1} + b) = b'$$

and the image distribution μ' of μ. Clearly (4.2) still holds and (4.3) is now satisfied. Also

$$|C'_\phi + b'C'_\phi| \leq |C'_\phi + C'_\phi + C'_\phi + C'_\phi + C'_\phi + bC'_\phi| \lesssim \left(\frac{|C_\phi + C_\phi|}{|C_\phi|}\right)^6 |C'_\phi + bC'_\phi|$$

and hence

$$\mathbb{E}'[|C'_\phi + b'C'_\phi|] \lesssim \left(\frac{|C_\phi + C_\phi|}{|C_\phi|}\right)^6 \mathbb{E}[|C'_\phi + bC'_\phi|]. \tag{$*$}$$

Thus it will suffice to establish a lower bound on $\mathbb{E}[|C'_\phi + bC'_\phi|]$ under assumptions (2.1)–(2.3).

Recalling (3.29), denote

$$M_s = L_s \wedge \sigma_s^{-1/D} \qquad (1 \leq s \leq t_2) \tag{4.4}$$

satisfying

$$\prod_{s=1}^{t_2} M_s > M^{\gamma m_1}. \tag{4.5}$$

We choose the parameter D to satisfy

$$D > 10/\kappa'. \tag{4.6}$$

Starting from $s = 1$, we have $C'_\phi = \bigcup_{\ell_1 \leq L_1} C'_{\ell_1}$, where the C'_{ℓ_1} are contained in intervals of size $\sigma_1 \mu_1$ and separation $> \mu_1$.

Thus

$$C'_\phi + bC'_\phi = \bigcup_{\substack{\ell_1 \leq L_1 \\ \ell'_1 \leq L_1}} (C'_{\ell_1} + bC'_{\ell'_1}).$$

Partition $[0,1]^d$ into intervals I_α of size $\eta > \mu_1$ where η is chosen such that

$$M_1 = \max_\alpha |\{\ell_1 \le L_1;\ C'_{\ell_1} \cap I_\alpha \ne \emptyset\}| = |\{\ell_1 \le L_1;\ C'_{\ell_1} \cap I_0 \ne \emptyset\}|. \tag{4.7}$$

For each α denote

$$\mathcal{E}_\alpha = \{\ell_1 \le L_1;\ C'_{\ell_1} \cap I_\alpha \ne \emptyset\} \quad \text{and} \quad D_\alpha = \bigcup_{\ell_1 \in \mathcal{E}_\alpha} C'_{\ell_1} \subset I_\alpha + B(0, \sigma_1\mu_1).$$

Then

$$C'_\phi + bC'_\phi \subset \bigcup_\alpha (D_\alpha + bD_0)$$

and from the preceding

$$|C'_\phi + bC'_\phi| > c \sum_\alpha |D_\alpha + bD_0|. \tag{4.8}$$

Fixing α, we have

$$D_\alpha + bD_0 = \bigcup_{\substack{\ell_1 \in \mathcal{E}_\alpha \\ \ell'_1 \in \mathcal{E}_0}} (C'_{\ell_1} + bC'_{\ell'_1}) \tag{4.9}$$

and certainly

$$|D_\alpha + bD_0| > c \max_{\ell'_1 \in \mathcal{E}_0} \sum_{\ell_1 \in \mathcal{E}_\alpha} |C'_{\ell_1} + bC'_{\ell'_1}| > \frac{c}{M_1} \sum_{\ell_1 \in \mathcal{E}_\alpha,\, \ell'_1 \in \mathcal{E}_0} |C'_{\ell_1} + bC'_{\ell'_1}|. \tag{4.10}$$

On the other hand, fixing $\xi_\ell \in C_\ell$, we have $|\xi_\ell - \xi_{\ell'}| > \mu_1$ for $\ell \ne \ell'$ and

$$C'_\ell + bC'_{\ell'} \subset \xi_\ell + b\xi_{\ell'} + B(0, 2\sigma_1\mu_1). \tag{4.11}$$

Therefore the sets in (4.9) will be mutually disjoint if

$$\min_{\substack{k,\ell \in \mathcal{E}_r \\ k',\ell' \in \mathcal{E}_0}} |(\xi_k + b\xi_{k'}) - (\xi_\ell + b\xi_{\ell'})| > 4\sigma_1\mu_1. \tag{4.12}$$

Here condition (4.2) comes into play.

Note that if $k' = \ell'$, then $|\xi_k - \xi_\ell| > \mu_1 \gg \sigma_1\mu_1$, so that we may assume $k' \ne \ell'$.

Fix $k, \ell \in \mathcal{E}_r$ and $k' \ne \ell' \in \mathcal{E}_0$ and denote $v = (\xi_{k'} - \xi_{\ell'})/|\xi_{k'} - \xi_{\ell'}|$. It follows from (4.3) that the μ-measure of the b's for which

$$\left| bv + \frac{\xi_k - \xi_\ell}{|\xi_{k'} - \xi_{\ell'}|} \right| < 4\sigma_1$$

is at most $C\sigma_1^\kappa$. Hence (4.12) holds for b outside a set of μ-measure at most

$$C|\mathcal{E}_0|^2|\mathcal{E}_r|^2\sigma_1^\kappa \le CM_1^4\sigma_1^\kappa < \sigma_1^{\kappa/2} \tag{4.13}$$

by (4.4), (4.5). For such b, we get

$$|D_\alpha + bD_0| = \sum_{\substack{\ell_1 \in \mathcal{E}_\alpha \\ \ell_1' \in \mathcal{E}_0}} |C'_{\ell_1} + bC'_{\ell_1'}|. \tag{4.14}$$

From (4.10), (4.14), it follows that

$$|D_\alpha + bD_0| > \sum_{\substack{\ell_1 \in \mathcal{E}_\alpha \\ \ell_1' \in \mathcal{E}_0}} \varphi_{\ell_1,\ell_1'}(b)|C'_{\ell_1} + bC'_{\ell_1'}| \tag{4.15}$$

where $\varphi_{\ell_1,\ell_1'}$ takes values in $\{1, c/M_1\}$ and by (4.13),

$$\mu[\varphi_{\ell_1,\ell_1'} \neq 1] < \sigma_1^{\kappa/2}. \tag{4.16}$$

Summing over α (4.8), (4.15) imply

$$|C'_\phi + bC'_\phi| > c \sum_{\ell_1 \le L_1,\, \ell_1' \in \mathcal{E}_0} \varphi_{\ell_1,\ell_1'}(b)|C'_{\ell_1} + bC'_{\ell_1'}| \tag{4.17}$$

with $\varphi_{\ell_1,\ell_1'}$ as above.

Next, restrict (ℓ_1, ℓ_1') to the set $\{1 \le \ell_1 \le L_1\} \times (\{1 \le \ell_1' \le L_1\} \setminus \mathcal{E}_0)$ and repeat the construction. Note that if (ℓ_1, ℓ_1') is restricted to a product set $\mathcal{F} \times \mathcal{F}'$, we partition into intervals I_α of size $\eta > \mu_1$ such that

$$M_1 = \max_\alpha |\{\ell_1 \in \mathcal{F};\ C'_{\ell_1} \cap I_\alpha \neq \emptyset\}| \vee \max_\alpha |\{\ell_1' \in \mathcal{F}';\ C'_{\ell_1'} \cap I_\alpha \neq \emptyset\}|$$

and obtained as either a set $\mathcal{E}_0 = \{\ell_1 \in \mathcal{F};\ C'_{\ell_1} \cap I_0 \neq \emptyset\}$ or a set $\mathcal{E}_0 = \{\ell_1' \in \mathcal{F}';\ C'_{\ell_1'} \cap I_0 \neq \emptyset\}$. Because of assumption (4.3), both cases may be treated similarly.

Exhausting the set $\{1 \le \ell_1 \le L_1\} \times \{1 \le \ell_1' \le L_1\}$ in $\sim L_1/M_1$ steps, we get

$$|C'_\phi + bC'_\phi| > c\frac{M_1}{L_1} \sum_{\ell_1,\ell_1' \le L_1} \varphi_{\ell_1,\ell_1'}(b)|C'_{\ell_1} + bC'_{\ell_1'}| \tag{4.18}$$

with $\varphi_{\ell_1,\ell_1'}$ satisfying (4.13). Equivalently

$$|C'_\phi + bC'_\phi| > \sum_{\ell_1,\ell_1' \le L_1} \psi_{\ell_1,\ell_1'}(b)|C'_{\ell_1} + bC'_{\ell_1'}| \tag{4.19}$$

with $\psi_{\ell_1,\ell_1'}$ taking values in $\{cM_1/L_1, c/L_1\}$ and

$$\mu[\psi_{\ell_1,\ell_1'} \neq cM_1/L_1] < \sigma_1^{\kappa'/2}. \tag{4.20}$$

Therefore

$$\mathbb{E}[\log \psi_{\ell_1,\ell_1'}] > (1 - \sigma_1^{\kappa'/2})\left(\log c\frac{M_1}{L_1}\right) + \sigma_1^{\kappa'/2}\left(\log \frac{c}{L_1}\right) > \log \frac{\sqrt{M_1}}{L_1}. \tag{4.21}$$

We assume here $\sigma_1^{\kappa'/2} < 1/2$, which will be fulfilled if

$$T > \frac{10}{\beta\kappa'} \tag{4.22}$$

(since $\sigma_s < 2^{-\beta T}$).

Repeat with the sets

$$C'_{\ell_1} + bC'_{\ell'_1} = \bigcup_{\ell_2,\ell'_2 \lesssim L_2} (C'_{\ell_1,\ell_2} + bC'_{\ell'_1,\ell'_2})$$

to obtain

$$|C'_{\ell_1} + bC'_{\ell'_1}| > \sum_{\ell_2,\ell'_2} \psi_{\ell_1,\ell_2;\ell'_1,\ell'_2}(b)|C'_{\ell_1,\ell_2} + bC'_{\ell'_1,\ell'_2}| \tag{4.23}$$

where again

$$\mathbb{E}_x[\log \psi_{\ell_1,\ell_2;\ell'_1,\ell'_2}] > \log\left(\frac{1}{L_2} M_2^{1/2}\right). \tag{4.24}$$

Iteration clearly provides the minorization

$$\begin{aligned} |C'_\phi + bC'_\phi| &> \sum_{\substack{\ell_1,\dots,\ell_{t_2}\\ \ell'_1,\dots,\ell'_{t_2}}} \psi_{\ell_1,\ell'_1}(b)\cdots\psi_{\ell_1,\dots,\ell_{t_2};\ell'_1,\dots,\ell'_{t_2}}(b)|C'_{\ell_1,\dots,\ell_{t_2}} + bC'_{\ell'_1,\dots,\ell'_{t_2}}| \\ &\geq \sum_{\overline{\ell},\overline{\ell}'} \psi_{\ell_1,\ell'_1}\cdots\psi_{\overline{\ell};\overline{\ell}'}|C'_{\ell_1,\dots,\ell_{t_2}}| \end{aligned} \tag{4.25}$$

where by (4.21), (4.24), etc.

$$\mathbb{E}_x[\psi_{\ell_1,\ell'_1}\psi_{\ell_1,\ell_2;\ell'_1,\ell'_2}\cdots] \geq e^{\mathbb{E}[\log\psi_{\ell_1,\ell'_1}]+\mathbb{E}[\log\psi_{\ell_1,\ell_2;\ell'_1,\ell'_2}]+\cdots} > \prod_{s=1}^{t_2} \frac{M_s^{1/2}}{L_s}. \tag{4.26}$$

Therefore

$$\mathbb{E}[|C'_\phi + bC'_\phi|] > \left(\prod_{s=1}^{t_2} M_s^{1/2}\right) \sum_{\ell_1,\dots,\ell_{t_2}} |C'_{\ell_1,\dots,\ell_{t_2}}| > M^{\frac{\gamma}{2}m_1}|C'_\phi|. \tag{4.27}$$

Recalling $(*)$, it follows that if μ satisfies (4.1) and (4.2),

$$|C'_\phi + C'_\phi| + \mathbb{E}[|C'_\phi + bC'_\phi|] > M^{\frac{\gamma}{14}m_1}|C'_\phi|. \tag{4.28}$$

Therefore, by (3.31), (3.30),

$$\begin{aligned} N(A+A,\delta) + \mathbb{E}[N(A+bA,\delta)] &> M^{\frac{\gamma}{14}m_1}|C_\phi| > M^{\frac{\gamma}{20}m_1}|A| \\ &> \delta^{-\frac{1}{60}\varepsilon_2 T^{-1/3}}|A|. \end{aligned} \tag{4.29}$$

5. Nonporous case (1)

Assume $|\mathcal{S}_1| \le \varepsilon_2 m_1$ and denote

$$\mathcal{S}' = \{1, \dots, m\} \setminus \mathcal{S}_1 \subset \mathcal{S} \tag{5.1}$$

satisfying

$$t' = |\mathcal{S}'| > (1 - \varepsilon_2) m_1 \tag{5.2}$$

and (2.17) if $\tau \in \mathfrak{Z}' = \{1 \le \tau \le t;\ s_\tau \in \mathcal{S}'\}$ ($t = |\mathcal{S}|$).

For notational simplicity, we identify $\mathcal{S}'$ with $\{1, \dots, m_1\}$. Recalling the system $\{x_c\}_{c \in \{0,1\}^t}$ of points from A introduced in (2.14) and (2.17), our starting point is a system $\{x_c\}_{c \in \{0,1\}^{m_1}} \subset A$ such that if $c_1 = c'_1, \dots, c_s = c'_s$, $c_{s+1} \ne c'_{s+1}$, then

$$2 \cdot 2^{-(s+1)T} < |x_c - x_{c'}| < 10 \cdot 2^{-(s+1-\beta)T}. \tag{5.3}$$

Denote $J = \left[\frac{1}{10d} 2^{(1-\beta)T}\right]$ and $k = k(T) \in \mathbb{Z}_+$.

We construct in the k-fold sumset kA of A, for $s = 1, \dots, m$, points

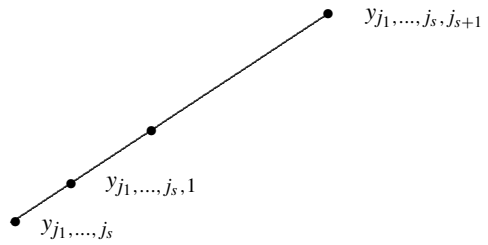
$$(y_{j_1,\dots,j_s})_{1 \le j_1 \le J, \dots, 1 \le j_s \le J} \tag{5.4}$$

with the following properties:

(5.5) $|y_{j_1,\dots,j_s,j_{s+1}} - y_{j_1,\dots,j_s}| < \frac{1}{10d} 2^{-sT}$,
(5.6) $2^{-(s+1)T} < |y_{j_1,\dots,j_s,1} - y_{j_1,\dots,j_s}| < \frac{1}{10dJ} 2^{-sT}$,
(5.7) for fixed $j_1, \dots, j_s$, we have (setting $y_\emptyset = 0$ for $s = 0$)

$$|(y_{j_1,\dots,j_{s+1}} - y_{j_1,\dots,j_s}) - j_{s+1}(y_{j_1,\dots,j_s,1} - y_{j_1,\dots,j_s})| < 4^{-T} 2^{-sT}.$$

Thus (5.7) means that the points $(y_{j_1,\dots,j_s,j_{s+1}})_{1 \le j_{s+1} \le J}$ lie approximately on some line segment emanating from $y_{j_1,\dots,j_s}$ and of length between $2^{-sT-\beta T}$ and 2^{-sT}:



The construction is done as follows. The points $y_{j_1,\dots,j_s}$ will be of the form

$$y_{j_1,\dots,j_s} = x_{c^{(1)}} + \dots + x_{c^{(k)}} \tag{5.8}$$

for certain $c^{(1)}, \dots, c^{(k)} \in \{0, 1\}^{m_1}$ such that $c^{(1)}_{s'} = \dots = c^{(k)}_{s'} = 0$ for $s' > s$.

Define $d^{(1)}, \dots, d^{(k)} \in \{0,1\}^{m_1}$ by

$$\begin{cases} d^{(\ell)}_{s'} = c^{(\ell)}_{s'} & \text{if } s' \le s, \\ d^{(\ell)}_{s+1} = 1, & \\ d^{(\ell)}_{s'} = 0 & \text{if } s' > s+1. \end{cases}$$

From (5.3), for each $\ell = 1, \dots, k$,

$$2^{-(s+1)T} < |x_{c^{(\ell)}} - x_{d^{(\ell)}}| < \frac{1}{10dJ} 2^{-sT}. \tag{5.9}$$

Taking $k = k(T)$ sufficiently large ($\log k(T) \sim T$), we may clearly specify a subset $\mathcal{L} = \{\ell_1 < \dots < \ell_J\} \subset \{1, \dots, k\}$ such that for all $\ell \in \mathcal{L}$,

$$|x_{c^{(\ell)}} - x_{d^{(\ell)}} - \eta 2^{-(s+1)T} v| < 2^{-sT-3T} \tag{5.10}$$

for some unit vector $v \in \mathbb{R}^d$ and some $1 < \eta < 2^{\beta T}$.

Define

$$y_{j_1,\dots,j_s,j} = \sum_{\ell \notin \{\ell_1,\dots,\ell_j\}} x_{c^{(\ell)}} + \sum_{\ell \in \{\ell_1,\dots,\ell_j\}} x_{d^{(\ell)}}. \tag{5.11}$$

Hence (5.5), (5.6) follow from (5.8), (5.11) and (5.9).

By (5.10),

$$\begin{aligned} y_{j_1,\dots,j_s,j} - y_{j_1,\dots,j_s} &= (x_{d^{(\ell_1)}} - x_{c^{(\ell_1)}}) + \dots + (x_{d^{(\ell_j)}} - x_{c^{(\ell_j)}}) \\ &= j\eta 2^{-(s+1)T} v + O(j 2^{-sT-3T}), \end{aligned}$$

implying (5.7).

6. Nonporous case (2)

We make the following further assumption on the distribution μ of $b \in \mathcal{L}(\mathbb{R}^d, \mathbb{R}^d)$.

(6.1) *There is a function $\theta(\rho) \to 0$ for $\rho \to 0$ such that if v, w are unit vectors in $\mathbb{R}^d$ then*

$$\mu[b;\ \langle bv, w\rangle| < \rho] < \theta(\rho).$$

Strictly speaking, all we require is that for some $\rho > 0$,

$$\max_{|v|=1=|w|} \mu[b;\ |\langle bv, w\rangle| < \rho] < \theta \tag{6.2}$$

with θ sufficiently small.

Fix a constant

$$\varepsilon_3 > 0 \tag{6.3}$$

(to be specified).

Property (6.2) will be used in the following

Lemma 6.4. *Let $v_1, \dots, v_d \in \mathbb{R}^d$ be unit vectors and $\rho^{-1}2^{-T} < \eta_1, \dots, \eta_d < 1/J$. Define*

$$P_i = \{j\eta_i v_i;\ 1 \le j \le J\} \quad \text{for } i = 1, \dots, d.$$

Then

$$\mathbb{E}\Big[\min_{x \ne y \in b_1 P_1 + \cdots + b_d P_d} |x - y| < 2^{-T}\Big] < \varepsilon_3 \tag{6.5}$$

where $\mathbb{E}$ refers to the d-fold product measure $\mu \otimes \cdots \otimes \mu = \mu^{(d)}$.

Proof. Write

$$b_1 P + \cdots + b_d P = \Big\{\sum_{i=1}^{d} j_i \eta_i b_i v_i;\ 1 \le j_i \le J\Big\}.$$

We need to ensure that for $|j_1| + \cdots + |j_d| = 0$,

$$|j_1\eta_1 b_1 v_1 + \cdots + j_d \eta_d b_d v_d| > 2^{-T}. \tag{6.6}$$

It suffices to impose the conditions

$$\begin{cases} |b_1 v_1| > \rho, \\ \operatorname{dist}(b_2 v_2, [b_1 v_1]) > \rho, \\ \qquad \vdots \\ \operatorname{dist}(b_d v_d, [b_1 v_1, \dots, b_{d-1} v_{d-1}]) > \rho. \end{cases} \tag{6.7}$$

By (6.2), clearly

$$\mu^{(d)}[(b_1, \dots, b_d);\ (6.7) \text{ fails}] < d\theta < \varepsilon_3$$

for appropriate θ. This proves the lemma. □

Let $\{y_{j_1,\dots,j_s}\}$ be the systems obtained in §5 satisfying (5.5)–(5.7). We denote $Y = \{y_{j_1,\dots,j_{m_1}}\}$ and $Y_{j_1,\dots,j_s} = \{y_{j_1,\dots,j_s,j_{s+1},\dots,j_{m_1}}\}$. By (5.5),

$$Y_{j_1,\dots,j_s} \subset B\Big(y_{j_1,\dots,j_s}, \frac{1}{5d}, 2^{-sT}\Big). \tag{6.8}$$

Denoting by $\mathbb{E}$ the expectation with respect to $\mu^{(d)}$, we establish a lower bound on

$$\mathbb{E}[N(b_1 Y + \cdots + b_d Y, \delta)]$$

following an argument similar to that used in §4.

From (5.7), (6.5), the expectation for the points $b_1 y_{j_1^{(1)}} + \cdots + b_d y_{j_1^{(d)}}$ to be at least 2^{-T} apart is $> 1 - \varepsilon_3$ (we use here that $|y_j - j y_1| < 4^{-T}$). Hence, by (6.8),

$$N(b_1 Y + \cdots + b_d Y, \delta) < \varphi(b_1, \dots, b_d) \sum_{1 \le j_1^{(i)} \le J} N(b_1 Y_{j_1^{(1)}} + \cdots + b_d Y_{j_1^{(d)}}, \delta) \tag{6.9}$$

where $\varphi(b) \in \{1, J^{-d}\}$ and $\mathbb{E}[\varphi = 1] > 1 - \varepsilon_3$. Thus

$$\mathbb{E}[\log \varphi] > \varepsilon_3 \log J^{-d} = -\log J^{d\varepsilon_3}. \tag{6.10}$$

Similarly

$$\begin{aligned} N(b_1 Y_{j_1^{(1)}} + \cdots + b_d Y_{j_1^{(d)}}, \delta) \\ > \varphi_{j_1^{(1)},\ldots,j_1^{(d)}}(b) \sum_{1 \le j_2^{(i)} \le J} N(b_1 Y_{j_1^{(1)}, j_2^{(1)}} + \cdots + b_d Y_{j_1^{(d)}, j_2^{(d)}}, \delta) \end{aligned} \tag{6.11}$$

with

$$\mathbb{E}[\log \varphi_{j_1^{(1)},\ldots,j_1^{(d)}}] > -\log J^{d\varepsilon_3}. \tag{6.12}$$

Iterating, we obtain

$$N(b_1 Y_1 + \cdots + b_d Y_d, \delta) > \sum_{J^{(1)},\ldots,J^{(d)}} \varphi(b) \varphi_{j_1^{(1)},\ldots,j_1^{(d)}}(b) \varphi_{j_1^{(1)}, j_2^{(1)},\ldots,j_1^{(d)}, j_2^{(d)}}(b) \cdots \tag{6.13}$$

where $J^{(i)} = (j_1^{(i)}, \ldots, j_{m_1}^{(i)})$, and the expectation of the summands in (6.13) is at least

$$e^{\mathbb{E}[\log \varphi] + \mathbb{E}[\log \varphi_{j_1^{(1)},\ldots,j_1^{(d)}}] + \cdots} > J^{-\varepsilon_3 d m_1}. \tag{6.14}$$

Hence

$$\mathbb{E}[N(b_1 Y + \cdots + b_d Y, \delta)] > J^{d m_1 - \varepsilon_3 d m_1} > [c 2^{(1-\beta)T}]^{(1-\varepsilon_3) d m_1}. \tag{6.15}$$

Recalling that in §5 we identified $\mathcal{S}'$ with $\{1, \ldots, m_1\}$ and (5.2), (6.5) gives

$$\begin{aligned} \mathbb{E}[N(b_1 \tilde{A} + \cdots + b_d \tilde{A}, \delta)] &> [c 2^{(1-\beta)T}]^{(1-\varepsilon_2)(1-\varepsilon_3) d m_1} \\ &> \delta^{-(1-\beta)(1-\varepsilon_2)(1-\varepsilon_3)(1-c/T)d} \end{aligned} \tag{6.16}$$

where $\tilde{A}$ is the sumset $kA \supset Y$.

Again from the sumset inequalities

$$N(b_1 \tilde{A} + \cdots + b_d \tilde{A}, \delta) \ge \Big[\prod_{i=1}^{d} N(A + b_i A, \delta)\Big]^k \cdot \frac{1}{|A|^{kd-1}} \tag{6.17}$$

it follows by (6.16) that for some $b \in \operatorname{supp} \mu$,

$$\begin{aligned} N(A + bA, \delta) &> |A|^{1 - \frac{1}{kd}} \delta^{-\frac{1}{k}(1-\beta)(1-\varepsilon_2)(1-\varepsilon_3)(1-c/T)} \\ &> \delta^{\frac{\sigma}{kd} - \frac{1}{k}(1-\beta)(1-\varepsilon_2)(1-\varepsilon_3)(1-c/T)} |A|. \end{aligned} \tag{6.18}$$

Recalling the hypothesis in Lemma 6.4, we assume

$$2^{-\beta T} < \rho. \tag{6.19}$$

7. Summary

Recall the parameters

σ	(1.1),	κ, ε_0	(1.2),	T	(1.4),	ε_1	(1.3),	ε_2	(2.16),
κ'	(4.2),	k	§5,	θ, ρ	(6.2),	ε_3	(6.3),		

and the conditions (3.18), (3.24), (4.6), (4.22), (6.19).

In view of (6.18), take

$$\beta = \varepsilon_2 = \varepsilon_3 = 10^{-2}(1 - \sigma/d) \tag{7.1}$$

(recall that $0 < \sigma < d$) and assume in (1.2) that

$$\varepsilon_0 < \frac{1}{200}(1 - \sigma/d). \tag{7.2}$$

In (6.2), ρ depends on ε_3, hence on $1 - \sigma/d$. From (3.18), (3.24), (4.6), (6.19), we impose on T the condition

$$T > 10^{13}(\kappa'\beta)^{-3} + 10(\kappa\varepsilon_2)^{-3} + \frac{1}{\beta}\log\frac{1}{\rho} \tag{7.3}$$

taking

$$T \sim 10^{20}\left(1 - \frac{\sigma}{d}\right)^{-3}\left(\kappa^{-3} + (\kappa')^{-3} + \log\frac{1}{\rho}\right). \tag{7.4}$$

Recall also that $k = k(T)$, $\log k \sim T$.

From (4.29), (6.18), it follows that

$$\begin{aligned} N(A + A, \delta) + N(A + bA, \delta) &> \min(\delta^{-\frac{1}{60}\varepsilon_2 T^{-1/3}}, \delta^{\frac{\sigma}{kd} - \frac{1}{k}(1-\beta)(1-\varepsilon_2)(1-\varepsilon_3)(1-c/T)}) \cdot |A| \\ &> \delta^{-\tau(\sigma,\kappa,\kappa',\rho)}|A| \end{aligned} \tag{7.5}$$

for some $b \in \operatorname{supp}\mu$.

We proved the following

Proposition 1. *Let $A \subset [0, 1]^d$ and $N(A, \delta) = \delta^{-\sigma}$ for some fixed $0 < \sigma < d$. Assume for some $\kappa > 0$,*

(7.6) $N(A \cap I, \delta) < \delta_1^{\kappa} N(A, \delta)$ *if $\delta < \delta_1 < \delta^{\varepsilon_0}$ and $I \subset \mathbb{R}^d$ a size δ_1-interval (where $\varepsilon_0 = \frac{1}{200}(1 - \sigma/d)$).*

Let further μ be a probability measure on $\mathcal{L}(\mathbb{R}^d, \mathbb{R}^d)$ satisfying

(7.7) $\|b\| \le 1$ *for $b \in \operatorname{supp}\mu$,*

(7.8) *there is $\kappa' > 0$ such that*

$$\max_{\substack{v, w \in \mathbb{R}^d \\ |v|=1}} \mu[|bv - w| < \delta_1] > c\delta_1^{\kappa'} \quad \textit{for } \delta < \delta_1 < 1,$$

(7.9) *there is* $\rho > 0$ *such that*

$$\max_{|v|=1=|w|} \mu[|\langle bv, w\rangle| < \rho] < \frac{1}{100d}(1-\sigma/d).$$

Then there is some $b \in \operatorname{supp}\mu$ *such that*

$$N(A+A,\delta) + N(A+bA,\delta) > \delta^{-\sigma-\tau}, \tag{7.10}$$

where $\tau = \tau(\sigma,\kappa,\kappa',\rho) > 0$.

Assume $u_1,\dots,u_r \in \mathcal{L}(\mathbb{R}^d,\mathbb{R}^d)$ are such that $\|u_i\| \le 1$ and for any unit vectors $v, w \in \mathbb{R}^d$,

$$\max_{1\le s\le r} |\langle u_s v, w\rangle| > \rho \tag{7.11}$$

(note that r may be restricted to some $r(d,\rho)$).

Let $J = J(d,\sigma) \in \mathbb{Z}_+$ be sufficiently large and let μ_1 be the normalized image measure on $\mathcal{L}(\mathbb{R}^d,\mathbb{R}^d)$ under the map

$$(j_1,\dots,j_r) \mapsto b = j_1u_1 + \cdots + j_ru_r \qquad (1 \le j_s \le J).$$

If $v, w \in \mathbb{R}^d$, $|v| = 1 = |w|$ and t is a scalar, we have, assuming $|\langle u_1 v, w\rangle| > \rho$,

$$\begin{aligned}\mu_1[|t + bv\cdot w| < \rho/2] \\ = J^{-r} \sum_{j_2,\dots,j_r} |\{j_1 \le J;\ |t + j_1(u_1v\cdot w) + \cdots + j_r(u_rv\cdot w)| < \rho/2\}| < 1/J.\end{aligned}$$

Let μ_0 on $\mathcal{L}(\mathbb{R}^d,\mathbb{R}^d)$ satisfy (7.7), (7.8). Then the image measure μ of $\mu_0 \otimes \mu_1$ under the map $(b,b') \mapsto b + b'$ will clearly satisfy both (7.8), (7.9).

Thus one has

Proposition 1′. *Let* $A \subset [0,1]^d$ *and* $N(A,\delta) = \delta^{-\sigma}$ *for some* $0 < \sigma < d$. *Assume* A *has the nonconcentration property* (7.6). *Let* μ *be a probability measure on* $\mathcal{L}(\mathbb{R}^d,\mathbb{R}^d)$ *satisfying* (7.7), (7.8). *Let further* $u_1,\dots,u_r \in \mathcal{L}(\mathbb{R}^d,\mathbb{R}^d)$ *with* $\|u_s\| \le 1$ *and* $\rho > 0$ *be such that*

$$\min_{|u|=1=|v|} \max_s |\langle u_s v, w\rangle| > \rho. \tag{7.12}$$

Then either

$$N(A+A,\delta) > \delta^{-\sigma-\tau},$$

or

$$N(A+bA,\delta) > \delta^{-\sigma-\tau} \quad \textit{for some } b \in \operatorname{supp}\mu,$$

or

$$N(A+u_sA,\delta) > \delta^{-\sigma-\tau} \quad \textit{for some } s = 1,\dots,r,$$

where $\tau = \tau(\sigma,\kappa,\kappa',\rho) > 0$.

8. Discretized ring theorem in $\mathbb{C}$

Using Proposition 1′, we prove the following

Proposition 2. *Given* $0 < \sigma < 2$ *and* $\kappa, \kappa' > 0$, $\rho > 0$, *there are* $\varepsilon_0, \varepsilon_0', \varepsilon_1 > 0$ *such that the following holds. Let* $A \subset \mathbb{C} \cap B(0, 1)$ *satisfy*

(8.1) $N(A, \delta) = \delta^{-\sigma}$ (δ *small enough*),
(8.2) $N(A \cap B(z, t), \delta) < t^{\kappa} N(A, \delta)$ *if* $\delta < t < \delta^{\varepsilon_0}$ *and* $z \in \mathbb{C}$.

Let μ *be a probability measure on* $\mathbb{C} \cap B(0, 1)$ *such that*

(8.3) $\mu\big(B(z, t)\big) < t^{\kappa'}$ *if* $\delta < t < \delta^{\varepsilon_0'}$ *and* $z \in \mathbb{C}$.

Let $z_1, z_2 \in \mathbb{C}$ *satisfy*

(8.4) $\delta^{\varepsilon_0'} < |z_1| \sim |z_2| < 1$ *and* $|\mathrm{Im}(z_1/z_2)| > \rho$.

Then one of the following holds:

(8.5) $N(A + A, \delta) > \delta^{-\sigma-\varepsilon_1}$,
(8.6) $N(A + bA, \delta) > \delta^{-\sigma-\varepsilon_1}$ *for some* $b \in \operatorname{supp} \mu$,
(8.7) $N(A + z_1 A, \delta) + N(A + z_2 A, \delta) > \delta^{-\sigma-\varepsilon_1}$.

This may be seen as the extension to $\mathbb{C}$ of the main result from [B2].

Proof. We identify $\mathbb{C}$ with $\mathbb{R}^2$ viewing complex multiplication by $z = x + iy$ as

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathcal{L}(\mathbb{R}^2, \mathbb{R}^2).$$

Condition (8.3) has to be upgraded to (7.8) (i.e. removing the restriction $t < \delta^{\varepsilon_0'}$). We proceed as follows. Define

$$t_0 = \inf\{t > \delta;\ \max_z \mu(B(z, t)) \geq t^{\frac{1}{2}\kappa'}\}$$

obtained for $z = b$ say. It follows from (8.3) that $t_0 \geq \delta^{\varepsilon_0'}$. Denote

$$\mu_1 = \frac{\mu|_{B(b,t_0)}}{\mu(B(b, t_0))}.$$

From the definition of t_0, it follows that if $\delta/t_0 < t \leq 1$ and $z \in \mathbb{C}$ then

$$\mu_1(B(z, tt_0)) < \frac{(tt_0)^{\frac{1}{2}\kappa'}}{\mu(B(b, t_0))} = t^{\frac{1}{2}\kappa'}. \tag{8.8}$$

In particular, there are $b', b'' \in B(b, t_0) \cap \operatorname{supp} \mu$ such that $|b' - b''| > ct_0$.

Let μ_2 be the image measure of μ_1 under the map $z \mapsto \frac{z-b'}{b''-b'}$. Clearly $\operatorname{supp} \mu_2 \subset B(0, C)$, and from (8.8),

$$\sup_z \mu_2(B(z, t)) < 2t^{\frac{1}{2}\kappa'} \quad \text{for } \delta^{1-\varepsilon_0'} < t < 1,$$

hence

$$\operatorname{supp}_z \mu_2(B(z,t)) < 2t^{\frac{1}{4}\kappa'} \quad \text{for } \delta < t < 1. \tag{8.9}$$

Regarding (7.12), we take $u_1 = 1$, $u_2 = z_1/z_2$. From (8.4),

$$\max\left(|\operatorname{Im} z|, \left|\operatorname{Im} \frac{z_1}{z_2} z\right|\right) \gtrsim \rho \quad \text{if } |z| = 1,$$

which gives (7.2).

By Proposition 1′, either (8.5) or one of (8.10), (8.11) below holds:

(8.10) There is some $b \in \operatorname{supp} \mu$ such that

$$N\left(A + \frac{b-b'}{b''-b'} A, \delta\right) > \delta^{-\sigma-\tau}.$$

Then

$$N((b''-b')A + (b-b')A, \delta) > |b'-b''|^d \delta^{-\sigma-\tau} > c\delta^{-\sigma-\tau+d\varepsilon_0'} > \delta^{-\sigma-\tau/2}$$

for ε_0' small enough. From the sumset inequalities

$$N(A + bA, \delta) > \delta^{-\sigma-\tau/8} \quad \text{for some } b \in \operatorname{supp} \mu.$$

(8.11) $N(A + \frac{z_2}{z_1} A, \delta) > \delta^{-\sigma-\tau}$, implying

$$N(z_1 A + z_2 A, \delta) > \delta^{d\varepsilon_0' - \sigma-\tau} > \delta^{-\sigma-\tau/2}$$

and

$$N(A + z_1 A, \delta) + N(A + z_2 A, \delta) > \delta^{-\sigma-\tau/4}.$$

This proves Proposition 2. □

Iteration of Proposition 2 gives

Corollary 3. *Given $\sigma, \kappa, \kappa', \rho, \varepsilon_1 > 0$, there are $\varepsilon_0, \varepsilon_0' > 0$ and some $r \in \mathbb{Z}_+$ such that the following holds. Let $\delta > 0$ be small enough. Let $A, B \subset \mathbb{C} \cap B(0,1)$ satisfy*

(8.12) $N(A, \delta) = \delta^{-\sigma}$,

(8.13) $N(A \cap B(z,t), \delta) < t^\kappa N(A, \delta)$ *for* $\delta < t < \delta^{\varepsilon_0}$ *and* $z \in \mathbb{C}$,

(8.14) *there is a probability measure μ on B such that*

$$\mu(B(z,t)) < t^{\kappa'} \quad \text{if } \delta < t < \delta^{\varepsilon_0'} \text{ and } z \in \mathbb{C},$$

(8.15) *there are $b_0, b_1, b_2 \in B$ such that*

$$|b_0 - b_1| \sim |b_0 - b_2| \sim \delta^{\varepsilon_0'} \quad \text{and} \quad \left|\operatorname{Im} \frac{b_0 - b_1}{b_0 - b_2}\right| > \rho.$$

Then there are elements $z_1, \dots, z_r$ obtained as products of at most r elements from B such that

$$N(z_1 A + \cdots + z_r A, \delta) > \delta^{-2+\varepsilon_1}. \tag{8.16}$$

Recall the following result from [B2, Theorem 6 and its proof].

Proposition 4. *Let μ be a probability measure on* $[0, 1]$ *satisfying, for some constants $\kappa > 0$, C,*

$$\mu(I) < C\rho^{\kappa} \quad \text{if } I \text{ is a } \rho\text{-interval}, \ \delta < \rho < 1 \tag{8.17}$$

(δ is assumed to be small enough). Then for some $s = s(\kappa, C) \in \mathbb{Z}_+$, the set $sA^{(s)} - sA^{(s)}$, where $A = \operatorname{supp}\mu$ and $sA^{(s)}$ is the s-fold sumset of the s-fold product set $A^{(s)}$ of A, is δ-dense in $[0, 1]$.

Note that in the conclusion of Proposition 4, we may clearly replace δ by any given power of δ (as a consequence of the statement).

Proposition 5. *Given $\kappa, \varepsilon_1 > 0$, there are $\varepsilon_0 > 0$ and $s \in \mathbb{Z}_+$ such that the following holds for $\delta > 0$ small enough. Let $A \subset \mathbb{C} \cap B(0, 1)$ satisfy*

$$N(A \cap B(z, t), \delta) < t^{\kappa} N(A, \delta) \tag{8.18}$$

for all $z \in \mathbb{C}$ and $\delta < t < \delta^{\varepsilon_0}$. Then there is a line segment $T \subset \mathbb{C}$ of size at least δ^{ε_1} such that each point in T is δ-close to an element from $sA^{(s)} - sA^{(s)}$.

Again in the conclusion, δ may be replaced by any fixed power of δ.

Proof. We may clearly assume $1 \in A$, replacing A by $\frac{1}{z}A$ with $z \in A$ the element of largest norm. Denote by $\tilde{A}$ sets of elements obtained from A by (boundedly many) sums of products.

Using Proposition 4, it is easily seen that it suffices to obtain a segment $T \subset \mathbb{C}$ of size at least δ^{ε_2} such that

$$N(\tilde{A} \cap T_\delta, \delta) > \delta^{-1+\varepsilon_2} \tag{8.19}$$

where T_δ denotes the δ-neighborhood of T and $\varepsilon_2 = \varepsilon_2(\varepsilon_1)$.

Following the proof of Proposition 2, we start by specifying some point $z_0 \in A$ and $\delta^{\varepsilon_0} < t_0 < 1$ such that for all $\delta < t < t_0$ and $z \in \mathbb{C}$,

$$N(A \cap B(z, t), \delta) < (t/t_0)^{\kappa/2} N(A \cap B(z_0, t_0), \delta). \tag{8.20}$$

By translation, we may assume $z_0 = 0$. Performing another rescaling, we obtain a δ-separated set $A \subset B(0, 1)$ such that

(8.21) $0 \in A$, $1 \in A$,
(8.22) $|A \cap B(z, t)| < t^{\kappa/2}|A|$ if $\delta < t < c$ and $z \in \mathbb{C}$.

Define next

$$|\eta| = \max_{z \in A} |\operatorname{Im} z| \tag{8.23}$$

and let

$$z_1 = t_1 + i\eta \in A. \tag{8.24}$$

If $|\eta| > c$, we may apply Corollary 3 with $A = B$ since (8.15) holds with $\varepsilon_0' = 0$, $\rho = 0(1)$ (take $b_0 = 0$, $b_1 = 1$, $b_2 = z_1$). From (8.16), $N(\tilde{A}, \delta) > \delta^{-2+\varepsilon_2}$, implying (8.19) for some segment $T \subset \mathbb{C}$.

Assume $\eta = o(1)$. Let ν be the image measure (on $[0, 1]$) of $\frac{1}{|A|}1_A$ under the map $z \mapsto \operatorname{Re} z$. It follows from (8.22), (8.23) that

(8.25) $\nu(I) < \rho^{\kappa/3}$ if $I \subset \mathbb{R}$ is a ρ-interval, $\eta < \rho < c$.

We apply Proposition 4 to ν (with δ replaced by η), concluding that $\widetilde{\operatorname{supp} \nu}$ and hence $\widetilde{\operatorname{Re} A}$ can be made η-dense in $[0, 1]$.

Hence, by (8.23), this implies that

$$[0, 1] \subset \tilde{A} + B(0, K\eta) \tag{8.26}$$

for some constant K.

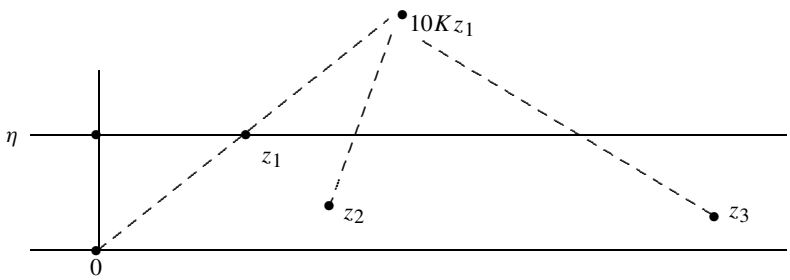
In order to fulfill condition (8.15), we proceed as follows. Take $z_2, z_3 \in \tilde{A}$ such that

$$|\operatorname{Im} z_2|, |\operatorname{Im} z_3| < K\eta, \tag{8.27}$$

$$|\operatorname{Re} z_2 - 10Kt_1| < K\eta, \tag{8.28}$$

$$10K\eta < |\operatorname{Re} z_2 - \operatorname{Re} z_3| < 11K\eta \tag{8.29}$$

(which is possible by (8.26)).



If we let $b_0 = 2Kz_1$, $b_1 = z_2$, $b_2 = z_3$, then (8.15) clearly holds with $\rho = O(1)$ and

$$\eta \equiv \delta^{\varepsilon_0'} \tag{8.30}$$

for some $\varepsilon_0' > 0$.

We distinguish two cases. If ε_0' in (8.30) is small enough, we may again apply Corollary 3 and conclude as in the case $\eta = o(1)$. Otherwise, we proceed as follows. Denote

$$z_4 = 10Kz_1 - z_2, \tag{8.31}$$

$$A_1 = \{z \in \tilde{A};\ 0 < \operatorname{Re} z < 1,\ |\operatorname{Im} z| < K\eta\}, \tag{8.32}$$

$$A_2 = z_4 A_1. \tag{8.33}$$

By (8.26),

$$[0, 1] \subset A_1 + B(0, K\eta), \tag{8.34}$$

$$A_2 \subset z_4[0, 1] + B(0, 20K^2\eta^2), \tag{8.35}$$

$$z_4[0, 1] \subset A_2 + B(0, 20K^2\eta^2). \tag{8.36}$$

One easily verifies that

$$\begin{aligned} R &= \{z = x + iy;\ 0 \le x \le 1, 0 \le y \le \eta\} \\ &\subset A_1 + A_2 + \{z = x + iy;\ 0 \le x \le c\eta,\ 0 \le y \le c\eta^2\} \subset \tilde{A} + C\eta R. \end{aligned} \tag{8.37}$$

In particular, there is some $z_5 \in \tilde{A}$ such that $\operatorname{Re} z_5 \sim \eta$ and $\operatorname{Im} z_5 \sim \eta^2$. From (8.37), also

$$R \subset \tilde{A} + z_5 R \tag{8.38}$$

and hence, multiplying both sides of (8.38) by z_5,

$$\begin{aligned} z_5 R &\subset \tilde{A} + z_5^2 R, \\ R &\subset \tilde{A} + z_5^2 R. \end{aligned} \tag{8.39}$$

After a few iterations, we conclude that

$$[0, 1] \subset \tilde{A} + B(0, \delta) \tag{8.40}$$

and in particular (8.19) holds. This completes the proof of Proposition 5. □

Proposition 6. *Given $\sigma > 0$, there are $C(\sigma) > 0$ and $s < s(\sigma) \in \mathbb{Z}_+$ such that for $\delta > 0$ small enough the following holds. Let $A \subset \mathbb{C} \cap B(0, 1)$ and*

$$N(A, \delta) > \delta^{-\sigma}. \tag{8.41}$$

Then there is a line segment $T \subset \mathbb{C}$ of size δ^γ with $0 < \gamma < C(\sigma)$ such that each point in T is $\delta^{\gamma+1/2}$-close to an element of $sA^{(s)} - sA^{(s)}$.

Proof. Assume A consists of δ-separated points. Take $t_0 > \delta$ minimum such that for some $z_0 \in A$,

$$|A \cap B(z_0, t_0)| \ge t_0^{\sigma/2}|A|. \tag{8.42}$$

Since obviously $|A \cap B(z_0, t_0)| \lesssim (t_0/\delta)^2$, it follows that

$$t_0 \gtrsim \delta^{\frac{2-\sigma}{2-\sigma/2}}. \tag{8.43}$$

From the definition of t_0,

$$|A \cap B(z, t)| \le (2t)^{\sigma/2}|A| \quad \text{if } \delta < t \le t_0 \text{ and } z \in \mathbb{C}. \tag{8.44}$$

Also, there is $z_1 \in A$ such that $|z_0 - z_1| = t_0$. Define

$$A_1 = (z_1 - z_0)^{-1}((A - z_0) \cap B(0, t_0)). \tag{8.45}$$

From (8.42), (8.44), if $\delta/t_0 < t < 1$ and $z \in \mathbb{C}$,

$$|A_1 \cap B(z, t)| \le |A \cap B(z_0 + (z_1 - z_0)z, tt_0)| \le (2tt_0)^{\sigma/2}|A| \le (2t)^{\sigma/2}|A_1|. \tag{8.46}$$

By (8.43),

$$|A_1 \cap B(z, t)| < t^\kappa |A_1| \quad \text{for } \delta < t < 1 \tag{8.47}$$

and

$$\kappa = \frac{\sigma}{4-\sigma} \tag{8.48}$$

(note that A_1 consists of δ-separated points).

Apply Proposition 5 to A_1 with $\kappa = \sigma/(4-\sigma), \varepsilon_1 = 1/2$ ($\varepsilon_0 = 0$) to obtain a segment T_1 of size $\delta^{1/2}$ such that

$$T_1 \subset sA_1^{(s)} - sA_1^{(s)} + B(0,\delta) \tag{8.49}$$

with $s = s(\sigma) \in \mathbb{Z}_+$. From (8.45) the rescaling of T_1 by a factor t_0 gives a segment T of size $\delta^{1/2}t_0^s = \delta^\gamma$ for which, by (8.49),

$$T \subset sA^{(s)} - sA^{(s)} + B(0, t_0^s\delta). \tag{8.50}$$

This proves Proposition 6. □

Remark. From the statement of Proposition 6, it also follows that for any given integer $r \in \mathbb{Z}_+$, assuming (8.41), there is a segment $T \subset \mathbb{C}$ of size δ^γ such that each point of T is $\delta^{\gamma+r}$-close to an element from $sA^{(s)} - sA^{(s)}$, where $\gamma = \gamma(\sigma, r)$ and $s = s(\sigma, r)$.

There is the following Cartesian version of Proposition 6 for $\mathbb{C}^d$ equipped with its product ring structure. This is the result we need for our SU(d)-analysis (see Corollary 10).

Proposition 7. *Let $A \subset \mathbb{C}^d \cap B(0,1)$ satisfy*

$$N(A,\delta) > \delta^{-\sigma} \tag{8.51}$$

for some $0 < \sigma \le d$. Then there is a unit vector $\xi \in \mathbb{C}^d$ such that

$$[0,\delta^\gamma]\xi \subset sA^{(s)} - sA^{(s)} + B(0,\delta^{\gamma+1}) \tag{8.52}$$

for some $0 \le \gamma < C(d,\sigma)$ and $s \in \mathbb{Z}_+$, $s < s(d,\sigma)$.

Proof. We proceed by induction on the dimension d. From Proposition 6 and the Remark, the statement holds for $d = 1$.

Next, assume it holds up to dimension d. Let $A \subset \mathbb{C}^{d+1} \cap B(0,1)$ and

$$N(A,\delta) > \delta^{-\sigma} \tag{8.53}$$

for some $\sigma > 0$.

We will denote again by $\tilde{A}$ sets of the form $sA^{(s)} - sA^{(s)}$ for varying s. If $I \subset \{1,\dots,d+1\}$, π_I stands for the coordinate restriction.

Rearranging the coordinates, we may assume that $B = \pi_{\{1,\dots,d\}}(A)$ satisfies

$$N(B,\delta) > \delta^{-\frac{d}{d+1}\sigma} > \delta^{-\sigma/2}. \tag{8.54}$$

From the induction hypothesis, there is a unit vector $\xi \in \mathbb{C}^d = [e_1,\dots,e_d]$ such that

$$[0,\delta^\gamma]\xi \subset sB^{(s)} - sB^{(s)} + B(0,\delta^{\gamma+1}) \tag{8.55}$$

for some $0 \le \gamma \le \gamma(\sigma)$, $s \in \mathbb{Z}_+$, $s < s(d, \sigma)$. Hence we may introduce a function

$$\varphi : [0, \delta^\gamma] \to \tilde{A} \tag{8.56}$$

satisfying

$$|\pi_{[1,\dots,d]}\varphi(x) - x\xi| < \delta^{1+\gamma} \quad \text{for } 0 \le x \le \delta^\gamma. \tag{8.57}$$

We will distinguish several cases.

Case 1: $N(\pi_{d+1}(\varphi([0, \delta^\gamma])), \delta^{2(1+\gamma)}) < \delta^{-1/2}$. Then there are elements $x_1, x_2 \in [0, \delta^\gamma]$ with $|x_1 - x_2| \gtrsim \delta^{\gamma+1/2}$ such that $|\pi_{d+1}(\varphi(x_1) - \varphi(x_2))| < \delta^{2(1+\gamma)}$. Hence, from (8.57), for $0 \le x < \delta^\gamma$,

$$\begin{aligned}\varphi(x)[\varphi(x_1) - \varphi(x_2)] &= (x\pi_{\{1,\dots,d\}}(\varphi(x_1) - \varphi(x_2)) \cdot \xi, 0) \\ &\quad + O(\delta^{1+\gamma}|\varphi(x_1) - \varphi(x_2)| + \delta^{2(1+\gamma)}) \\ &= x \cdot \delta^{\gamma_1}\xi' + O(\delta^{1+\gamma+\gamma_1})\end{aligned} \tag{8.58}$$

where $\delta^{\gamma_1} = |\pi_{[1,\dots,d]}(\varphi(x_1) - \varphi(x_2))| \sim |x_1 - x_2| \gtrsim \delta^{\gamma+1/2}$ and $\xi' = \delta^{-\gamma_1}(\xi, 0)$, a unit vector in $\mathbb{C}^{d+1}$. Therefore

$$[0, \delta^{\gamma+\gamma_1}]\xi' \subset \tilde{A} + B(0, \delta^{\gamma+\gamma_1+1}). \tag{8.59}$$

Case 2: $N(\pi_{d+1}(\varphi([0, \delta^\gamma])), \delta^{2(1+\gamma)}) \ge \delta^{-1/2}$. In particular, $S = \pi_{d+1}(\tilde{A})$ satisfies

$$N(S, \delta^{2(1+\gamma)}) > \delta^{-1/2}$$

and an application of the $d = 1$ result gives a segment $J \subset \mathbb{C}e_{d+1}$ of size δ^{γ_1} such that

$$J \subset \tilde{S} + B(0, \delta^{\gamma_1+1}). \tag{8.60}$$

Case 2.1: Assume φ is approximately linear in the sense that for all x, y with $x + y \in [0, \delta^\gamma]$,

$$|\varphi(x + y) - \varphi(x) - \varphi(y)| < \delta^{\gamma+1/2}. \tag{8.61}$$

Take $m = [\delta^{-1/4}]$ and $t_j = \frac{j}{m}\delta^\gamma$ $(1 \le j \le m)$. Clearly (8.61) implies that

$$\varphi(t_j) = \varphi(t_1) + \varphi(t_{j-1}) + O(\delta^{\gamma+1/2}) = j\varphi(t_1) + O(\delta^{\gamma+1/4}). \tag{8.62}$$

Therefore

$$\{j\varphi(t_1);\ 1 \le j \le m\} \subset \tilde{A} + B(0, \delta^{\gamma+1/4}). \tag{8.63}$$

Note that $\delta^{\gamma+1/4} \approx |t_1| \le |\varphi(t_1)| \lesssim \delta^{1/4}$. Let $\xi' = \varphi(t_1)/|\varphi(t_1)| \in \mathbb{C}^{d+1}$.

It follows from (8.63) that

$$[0, \lambda]\xi' \subset \tilde{A} + B(0, \delta^{1/4}\lambda) \tag{8.64}$$

with $\lambda = |\varphi(t_1)|\delta^{-1/4}$.

Case 2.2: Assume there are $x, y \in [0, \delta^\gamma]$ with $x + y \in [0, \delta^\gamma]$ such that

$$|\varphi(x + y) - \varphi(x) - \varphi(y)| > \delta^{\gamma+1/2}. \tag{8.65}$$

Denoting $\zeta = \varphi(x+y) - \varphi(x) - \varphi(y) \in \tilde{A}$, it follows from (8.57) that

$$|\pi_{[1,\dots,d]}\zeta| \lesssim \delta^{1+\gamma}, \tag{8.66}$$

hence

$$|\zeta_{d+1}| > \delta^{\gamma+1/2}. \tag{8.67}$$

Taking $r \in \mathbb{Z}_+$ (an integer to be specified), write

$$\begin{aligned}\tilde{A} &\supset \zeta^r \tilde{A} \supset (0, \zeta_{d+1}^r \tilde{S}) + O(\delta^{r(1+\gamma)}) \\ &\underset{(8.60)}{\supset} (0, \zeta_{d+1}^r J) + O(\delta^{r(1+\gamma)} + |\zeta_{d+1}|^r \delta^{\gamma_1+1}) \\ &= (0, \zeta_{d+1}^r J) + O(|\zeta_{d+1}|^r \delta^{\gamma_1+1})\end{aligned} \tag{8.68}$$

using (8.66), (8.67) and taking r large enough. Again (8.68) provides a segment $[0, \delta^{\gamma_2}]\xi'$ with $\delta^{\gamma_2} = |\zeta_{d+1}|^r \delta^{\gamma_1}$, contained in $\tilde{A} + B(0, \delta^{\gamma_2+1})$.

In summary, we certainly obtain a unit vector $\xi' \in \mathbb{C}^{d+1}$ such that for some $0 \le \gamma' \le C(d,\sigma)$,

$$[0, \delta^{\gamma'}]\xi' \subset \tilde{A} + B(0, \delta^{\gamma'+1/4}) \tag{8.69}$$

(as there is only a $\delta^{1/4}$ gain in (8.64)). Since the same statement holds with δ replaced by δ^4 (note that then σ in (8.41) needs to be replaced by $\sigma/4$), we have proved (8.52) in $\mathbb{C}^{d+1}$. □

Corollary 8. *Denote by* $\mathbb{C}^d \simeq \Delta \subset \mathrm{Mat}_{d\times d}(\mathbb{C})$ *the diagonal matrices. Assume* $A \subset \mathrm{Mat}_{d\times d}(\mathbb{C})$ *satisfies*

(8.70) $A \subset B(0,1)$,
(8.71) $N(A,\delta) > \delta^{-\sigma}$,
(8.72) $\mathrm{dist}(x,\Delta) < \delta$ *for* $x \in A$.

Then there is $\xi \in \Delta$ *with* $\|\xi\| = 1$ *such that*

(8.73) $[0, \delta^{\alpha}]\xi \subset s'A^{(s)} - s'A^{(s)} + B(0, \delta^{\alpha+\beta})$

where $0 \le \alpha < c(d,\sigma)$, $\beta > c(d,\sigma) > 0$ *and* $s, s' \in \mathbb{Z}_+$ *with* $s, s' < s(d,\sigma)$.

Proof. From (8.71), also $N(A, \delta^{1-\sigma/2d}) > \delta^{-\sigma/2}$. Let $k \in \mathbb{Z}_+$ to be specified and

$$\delta_1 = \delta^{\frac{1}{k}(1-\sigma/2d)}.$$

Clearly

$$N(A, \delta^{1-\sigma/2d}) \le \prod_{0\le\ell<k} \max_y N(A \cap B(y, \delta_1^{\ell}), \delta_1^{\ell+1}).$$

It follows that there is a subset $A_1 \subset A$ and $\delta_1^{k-1} \le \delta_2 \le 1$ such that

(8.74) $\mathrm{diam}\, A_1 \le \delta_2$,
(8.75) $N(A_1, \delta_1\delta_2) > \delta^{-\sigma/2k} > \delta_1^{-\sigma/2}$.

By (8.72), for each $x \in A$, there is $x' \in \Delta$ with $|x - x'| < \delta$; the set $B_1 = \{x';\ x \in A_1\}$ still satisfies (8.74), (8.75). Take $\zeta \in B_1$ and denote

$$B = \frac{1}{\delta_2}(B_1 - \zeta). \tag{8.76}$$

Hence

(8.77) $B \subset \Delta \cap B(0, 1)$,
(8.78) $N(B, \delta_1) > \delta_1^{-\sigma/2}$,
(8.79) if $x \in B$, then $\operatorname{dist}(x, \frac{A_1 - A_1}{\delta_2}) \le 2\frac{\delta}{\delta_2}$.

Apply Proposition 7 to $B \subset \mathbb{C}^d$. This gives a unit vector $\xi \in \Delta$ such that

$$[0, \delta_1^{\gamma}]\xi \subset sB^{(s)} - sB^{(s)} + B(0, \delta_1^{1+\gamma}) \tag{8.80}$$

for some $\gamma < \gamma(d, \sigma)$ and $s \in \mathbb{Z}_+$ with $s < s(d, \sigma)$.

From (8.74), (8.79),

$$\operatorname{dist}(x, (A_1 - A_1)^{(s)}/\delta_2^s) < 2s\delta/\delta_2 \quad \text{for } x \in B^{(s)}$$

and hence

$$sB^{(s)} - sB^{(s)} \subset \delta_2^{-s}(s'A^{(s)} - s'A^{(s)}) + B(0, c_s\delta/\delta_2). \tag{8.81}$$

From (8.80), (8.81),

$$[0, \delta_1^{\gamma}\delta_2^s]\xi \subset s'A^{(s)} - s'A^{(s)} + B(0, \delta_1^{1+\gamma}\delta_2^s + c_s\delta\delta_2^{s-1}). \tag{8.82}$$

Note that by definition of δ_1,

$$\frac{\delta}{\delta_2} < \delta^{\sigma/2d} < \delta_1^{1+\gamma}$$

provided

$$k > 2d(1 + \gamma(d, \sigma))\sigma^{-1}. \tag{8.83}$$

Hence (8.73) holds with $\delta^{\alpha} = \delta_1^{\gamma}\delta_2^s$ and $\beta = \frac{1}{k}(1 - \sigma/2d)$.

Remark. We also note that the element $\xi \in \Delta \simeq \mathbb{C}^d$ belongs to the algebra generated by $\{x' - y';\ x, y \in A\} \subset \mathbb{C}^d$.

Part II: Analysis on the unitary group

We now return to Theorem 1 and carry out the program sketched in the Introduction.

9. Construction of near-diagonal elements

The main results from this section are formulated in Proposition 9 and Corollary 10.

Let $q \ge 2$ and $g_1, \ldots, g_q$ be fixed algebraic elements in U(d) which freely generate the free group F_q. Let $\Gamma = \langle g_1, \ldots, g_q \rangle$.

Denote by W_ℓ the set of elements of Γ that may be obtained as a word of length $\leq \ell$ in $\{g_1, g_1^{-1}, \dots, g_q, g_q^{-1}\}$. Thus $W_\ell \subset W_{\ell+1}$. The following properties hold:

(9.1) $|W_\ell| \sim (2q-1)^\ell$,
(9.2) there is a constant $C_1 > 0$ such that $\|x-1\| > C_1^{-\ell}$ for $x \in W_\ell \setminus \{1\}$. (This is a noncommutative diophantine property, introduced in [GJS] and used in connection with the spectral gap theorem in [BG]).

More generally, if $P(x_1, \dots, x_r)$ is a polynomial with integer coefficients and variables $x_i \in \mathrm{Mat}_{d\times d}(\mathbb{C})$, then

(9.3) if $x_1, \dots, x_r \in W_\ell$, either $P(x_1, \dots, x_r) = 0$ or $|P(x_1, \dots, x_r)| > C^{-\ell}$ where C depends on Γ and the degree of P.

For $\delta > 0$, define

$$W_{\ell,\delta} = \{x \in W_\ell;\ \|x-1\| < \delta\}.$$

One may cover $\mathrm{U}(d)$ by at most $(c/\delta)^{2d^2}$ balls B_α of size $\delta/2$ and take α such that $|B_\alpha \cap W_{\ell/2}| \gtrsim \delta^{2d^2}|W_{\ell/2}|$. Then $(B_\alpha \cap W_{\ell/2})^{-1}(B_\alpha \cap W_{\ell/2}) \subset W_{\ell,\delta}$ and by (9.1),

(9.4) $|W_{\ell,\delta}| \gtrsim \delta^{2d^2}(2q-1)^{\ell/2}$.

The key idea underlying the proof of the following result originates in the work of Helfgott [H].

Lemma 9.5. *Assume $A \subset \mathrm{U}(d)$, $b_1, \dots, b_r \in W_\ell$ and $\delta > 0$ with $\ell < \log(1/\delta)$, such that*

(9.6) $N(A, \delta) > \delta^{-\sigma}$,
(9.7) $\operatorname{span} A \subset \operatorname{span}(b_1, \dots, b_r)$,

where "span" refers to the linear span in $\mathrm{Mat}_{d\times d}(\mathbb{C})$. Then there are $i \in \{1, \dots, r\}$, $a \in A$, $A_1 \subset (A \cup A^{-1} \cup \{b_1, b_1^{-1}, \dots, b_r, b_r^{-1}\})^{(s)}$ (the s-fold product set) and $\delta_1 > 0$ such that

(9.8) $\delta^C < \delta_1 < \delta$ *(where $C = C(\Gamma)$),*
(9.9) $s \in \mathbb{Z}_+$, $s < s(\Gamma, \sigma)$,
(9.10) *the elements of A_1 are δ_1-separated and $|A_1| > \delta^{-\sigma/2r}$,*
(9.11) $\|xab_i^{-1} - ab_i^{-1}x\| < \delta_1$ *for $x \in A_1$.*

Proof. We may assume that $b_1, \dots, b_r$ are linearly independent in $\mathrm{Mat}_{d\times d}(\mathbb{C})$. Consider the map

$$\varphi : \operatorname{span}(b_1, \dots, b_r) \to \mathbb{C}^r : x \mapsto (\operatorname{Tr} xb_1^*, \dots, \operatorname{Tr} xb_r^*).$$

Clearly, by (9.3),

$$\|\varphi^{-1}\| \sim \|[(\operatorname{Tr} b_i b_j^*)_{1\leq i,j\leq r}]^{-1}\| \lesssim |\det[(b_i b_j^*)_{1\leq i,j\leq r}]|^{-1} \lesssim C_2^{-\ell}. \tag{9.12}$$

Let $A' \subset A$ be a δ-separated set with $|A'| > \delta^{-\sigma}$, By (9.12),

$$|\varphi(x) - \varphi(y)| > C_2^{-\ell}\delta \quad \text{for } x \neq y \text{ in } A',$$

and hence, for some $i = 1, \dots, r$,

$$N(\operatorname{Tr} A' b_i^{-1}, C_2^{-\ell}\delta) > \delta^{-\sigma/r}. \tag{9.13}$$

Take $A'' \subset A'$ such that

(9.14) $|A''| > \delta^{-\sigma/r}$,
(9.15) $|\operatorname{Tr} ab_i^{-1} - \operatorname{Tr} a'b_i^{-1}| > C_2^{-\ell}\delta$ for $a \neq a$ in A''.

Denote by

$$\mathcal{A}_s = (A \cup A^{-1} \cup \{b_1, b_1^{-1}, \dots, b_r, b_r^{-1}\})^{(s)}$$

the s-fold product set and let

$$\delta_1 = C_2^{-\ell}\delta. \tag{9.16}$$

Since $\ell < \log(1/\delta)$, trivially $N(\mathcal{A}_s, \delta_1) \lesssim (1/\delta_1)^{2d^2} < (1/\delta)^{2d^2(1+\log C_2)}$. Hence, there is some $s \in \mathbb{Z}_+$ with

$$\log s < 4rd^2\sigma^{-1}(1 + \log C_2) \tag{9.17}$$

such that

$$N(\mathcal{A}_{2(s+1)}, \delta_1) < \delta^{-\sigma/2r} N(\mathcal{A}_s, \delta_1). \tag{9.18}$$

For $a \in A''$, consider the restricted conjugacy classes

$$C_a = \{xab_i^{-1}x^{-1};\ x \in \mathcal{A}_s\} \subset \mathcal{A}_{2s+2}.$$

By (9.15), $\operatorname{dist}(C_a, C_{a'}) > \delta_1$ for $a \neq a'$ in A'' and hence there is $a \in A''$ such that

$$N(C_a, \delta_1) < N(\mathcal{A}_{2s+2}, \delta_1)\delta^{\sigma/r} < N(\mathcal{A}_s, \delta_1)\delta^{\sigma/2r} \tag{9.19}$$

(invoking (9.14), (9.18)).

Consider the map $\mathcal{A}_s \to C_a : x \mapsto zab_i^{-1}x^{-1}$. It follows from (9.19) that there is some $x_0 \in \mathcal{A}_s$ and a subset $\mathcal{A} \subset \mathcal{A}_s$ with the following properties:

(9.20) the elements of $\mathcal{A}$ are δ_1-separated and $|\mathcal{A}| > \delta^{-\sigma/2r}$,
(9.21) $\|xab_i^{-1}x - x_0ab_i^{-1}x_0\| < \delta_1$ for $x \in \mathcal{A}$.

Hence the set $A_1 = x_0^{-1}\mathcal{A}$ satisfies (9.11). This proves the lemma. □

Our aim is to prove the following

Claim ($*$). *Given $\delta > 0$, there are $0 < \delta_1 < \delta$ and a subset $A \subset W_\ell$ such that*

(9.22) $\ell \sim \log(1/\delta) \sim \log(1/\delta_1)$,
(9.23) *the elements of A are δ_1-separated and $|A| > \delta_1^{-c}$,*

(9.24) *in an appropriate orthonormal basis*

$$\operatorname{dist}(x, \Delta) < \delta_1,$$

where, as before, $\mathbb{C}^d \simeq \Delta \subset \mathrm{Mat}_{d\times d}(\mathbb{C})$.

More generally, the same statement (with essentially the same proof) holds if W_ℓ is replaced by a large subset $H \subset W_\ell$, namely $\log|H| \sim \ell$ (see the discussion preceding Proposition 9).

Compared with [BG2], it should be noted that the construction of the almost diagonal set A does not use regular elements and this makes the argument a bit more complicated. On the other hand, Proposition 9 below gives a more general result of some independent interest.

Assume $(*)$ fails for some (sufficiently small) δ. By induction on $1 \le d_1 \le d$, we then establish the following statement.

$(**)$ *If* $\log(1/\delta_1) \sim \log(1/\delta)$, *there is an element* $x \in W_{\ell,\delta_1}$ *with* $\ell < C\log(1/\delta)$ *such that* x *has at least* d_1 *distinct eigenvalues.*

Next, we show that $(**)$ for $d_1 = d$ implies $(*)$, hence obtaining a contradiction.

Proof of $(**)\Rightarrow(*)$. Take $x \in W_{\ell,\delta}$, $\log(1/\delta) < \ell < C\log(1/\delta)$ with d distinct eigenvalues $\lambda_1, \dots, \lambda_d$. Since by (9.3),

$$\prod_{i\neq j} |\lambda_i - \lambda_j|^2 \sim |\mathrm{Res}(P_x, P_x')| > C^{-\ell}$$

where P_x denotes the characteristic polynomial of x, it follows that

$$|\lambda_i - \lambda_j| > C_3^{-\ell} \quad \text{for } 1 \le i \neq j \le d. \tag{9.25}$$

Take $L > \ell$, $L \sim \ell$ and L/ℓ sufficiently large (according to the argument that follows).

Assume

$$\mathrm{span}(W_{L,2\delta}) = \mathrm{span}(W_{L/2,\delta_1}) \tag{9.26}$$

where

$$\delta_1 = (2C_3)^{-\ell} < \delta. \tag{9.27}$$

Take $b_1', \dots, b_r' \in W_{L/2,\delta_1}$ such that (9.26) = $\mathrm{span}(b_1', \dots, b_r')$. Note that $b_i = b_i' x \in W_{L/2+\ell,\delta_1+\delta} \subset W_{L,2\delta}$ and $b_1, \dots, b_r$ are linearly independent. Hence, by (9.26),

$$\mathrm{span}(b_1, \dots, b_r) = \mathrm{span}(W_{L,2\delta}). \tag{9.28}$$

Apply Lemma 9.5 with $A = W_{L/2,\delta_1}$ and $\delta = C_1^{-L}$ (cf. (9.2)). By (9.4),

$$|W_{L/2,\delta_1}| \gtrsim \delta_1^{2d^2}(2q-1)^{L/4} > 3^{L/8}$$

if $L > 8d^2(\log C_3)\ell$. Hence we may take $\sigma > 1/(10\log C_1)$.

From the lemma, we obtain $i = 1, \dots, r$, $a \in W_{L/2,\delta_1}$ and $A_1 \subset W_{sL,2s\delta} \subset W_{sL}$ such that for some $C_1^{-L} > \delta_2 > C_1^{-cL}$:

(9.29) the elements of A_1 are δ_2-separated and $|A_1| > 3^{L/16r}$,

(9.30) $\|yab_i^{-1} - ab_i^{-1}y\| < \delta_2$ for $y \in A_1$.

Note that $\xi = ab_i^{-1} = ax^{-1}(b_i')^{-1} = x^{-1} + O(\delta_1)$ so that the eigenvalues of ξ satisfy essentially the same separation property (9.25). Choosing an orthonormal basis that makes ξ diagonal, it follows from (9.30) and (9.25) that the off-diagonal elements of $y \in A_1$ are bounded by $\delta_2 C_3^{\ell} = \delta_3$. Take a subset $A \subset A_1$ of δ_3-separated elements, $|A| > C_3^{-2d^2\ell}|A_1| > 3^{L/20r} > \delta_3^{-c}$ (assuming $L > 100rd^2(\log C_3)\ell$). Hence A satisfies $(*)$ (with $\ell = sL$ and $\delta_1 = \delta_3$).

Next, assume that (9.26) fails, thus

$$\dim \operatorname{span}(W_{L,2\delta}) > \dim \operatorname{span}(W_{L/2,\delta_1}).$$

Replace L by $L/2$ and δ by $\delta_1/2$ and repeat the argument.

After at most d^2 steps (and assuming L/ℓ large enough), we reach the same conclusion. This proves the implication $(**)\Rightarrow(*)$. □

Proof of $(**)$ (*assuming* $(*)$ *fails*). For $d_1 = 1$, the statement is trivial. For $d_1 = 2$, we may argue as follows. If T is a commutative subgroup of $\mathrm{GL}_d(\mathbb{C})$, then

$$|W_\ell \cap T| \lesssim \ell \tag{9.31}$$

(using the fact that commutative subgroups of F_q, the free group on q elements, are cyclic).

Hence, if $\ell > c\log(1/\delta_1)$, it follows from (9.4), (9.31) that

$$W_{\ell,\delta_1} \not\subset \{z\mathbb{1};\ z \in \mathbb{C},\ |z| = 1\}$$

and hence W_{ℓ,δ_1} contains an element with at least two distinct eigenvalues.

We now turn to the inductive step. Assume $(**)$ holds for $2 \le d_1 < d$. We follow the proof of $(**)\Rightarrow(*)$. Take $x \in W_{\ell,\delta}$, $\ell < c\log(1/\delta)$, with d_1 distinct eigenvalues $\lambda_1, \dots, \lambda_{d_1}$, hence satisfying

(9.32) $|\lambda_i - \lambda_j| > C_3^{-\ell}$ for $1 \le i \ne j \le d_1$.

Repeating the reasoning following (9.26) (with the same notation), we obtain some $\xi \in W_{L+\ell,2\delta_1+\delta}$, $\|\xi - x^{-1}\| = O(\delta_1)$ and $A_1 \subset W_{sL,2s\delta}$ such that

(9.33) the elements of A_1 are δ_2-separated and $|A_1| > \delta_2^{-c}$,
(9.34) $\|y\xi - \xi y\| < \delta_2$ for $y \in A_1$,

where $\log(1/\delta_2) \sim L$ and $C\ell < L < C'\ell$.

Take a subset $A_2 \subset A_1A_1^{-1} \subset W_{2sL}$ satisfying

(9.35) $A_2 \subset B(\mathbb{1}, C_3^{-2\ell})$,
(9.36) the elements of A_2 are $\delta_3 = C_3^{2\ell}\delta_2$-separated and

$$|A_2| > C_3^{-8d^2\ell}|A_1| > |A_1|^{1/2} > \delta_3^{-c}.$$

Obviously from (9.34) we have

(9.37) $\|y\xi - \xi y\| < 2\delta_2$ for $y \in A_2$.

If ξ has at least $d_1 + 1$ distinct eigenvalues, we are done.

Hence, assume ξ has only d_1 distinct eigenvalues $\lambda'_1, \dots, \lambda'_{d_1}$. Since $\|\xi - x^{-1}\| \lesssim \delta_1 = (2C_3)^{-\ell}$, it follows from (9.32) that $\{\lambda'_1, \dots, \lambda'_{d_1}\}$ is an $O(\delta_1)$-perturbation of $\{\lambda_1^{-1}, \dots, \lambda_{d_1}^{-1}\}$ and in particular

$$|\lambda'_i - \lambda'_j| > \frac{1}{2} C_3^{-\ell} \quad \text{for } 1 \le i \ne j \le d_1. \tag{9.38}$$

Diagonalize ξ in a basis $e'_1, \dots, e'_n$ and write $\{1, \dots, n\} = \bigcup_{s=1}^{d_1} I_s$ where

$$\xi e'_i = \lambda'_s e'_i \quad \text{for } i \in I_s. \tag{9.39}$$

We denote by R_I the restriction to $I \subset \{1, \dots, n\}$.

It follows from (9.38), (9.37) that

$$\|y - y'\| \lesssim C_3^{\ell} \delta_2 \tag{9.40}$$

where

$$y' = \bigoplus_{s=1}^{d_1} R_{I_s} y R_{I_s} = \bigoplus_{s=1}^{d_1} y'_s. \tag{9.41}$$

For $s = 1, \dots, d_1$, let $y'_s = U_s P_s$, $P_s = ((y'_s)^* y'_s)^{1/2}$, be the polar decomposition of y'_s. Since by (9.40),

$$\|(y'_s)^* y'_s - \mathbb{1}_{I_s}\| \lesssim C_3^{\ell} \delta_2, \tag{9.42}$$

it follows that

$$\|y'_s - U_s\| \lesssim C_3^{\ell} \delta_2. \tag{9.43}$$

We distinguish two cases.

(i) Assume that for all $y \in A_2$ and $s = 1, \dots, d_1$,

$$\operatorname{dist}(y'_s, \{z \mathbb{1}_{I_s};\ z \in \mathbb{C}\}) < \delta_3. \tag{9.44}$$

From (9.40), y is an $O(\delta_3)$-perturbation of a diagonal matrix. Hence A_2 satisfies $(*)$ (with $\ell = 2sL$, $\delta_1 = \delta_3$), a contradiction.

(ii) Let $y \in A_2$ and $s = 1, \dots, d_1$ (say $s = 1$) such that

$$\operatorname{dist}(y'_1, \{z \mathbb{1}_{I_1};\ z \in \mathbb{C}\}) \ge \delta_3. \tag{9.45}$$

Hence, by (9.43),

$$\operatorname{dist}(U_1, \{z \mathbb{1}_{I_1};\ z \in \mathbb{C}\}) > \frac{1}{2} \delta_3 \tag{9.46}$$

and U_1 has at least two eigenvalues that are $\frac{1}{2}\delta_3$-separated.

Take for $s = 1, \dots, d_1$ a basis $\{e_i''; \ i \in I_s\}$ of $[e_i'; \ i \in I_s]$ diagonalizing U_s. If

$$U_s e_i'' = \mu_i e_i'' \quad \text{for } \ i \in I_s \tag{9.47}$$

we have

$$\begin{aligned} |1-\mu_i| \le \|\mathbb{1}_{I_s} - U_s\| &\underset{(9.43)}{<} \|\mathbb{1}_{I_s} - y_s'\| + O(C_3^{\ell}\delta_2) < \|\mathbb{1} - y\| + \|y - y'\| + O(C_3^{\ell}\delta_2) \\ &\underset{\substack{(9.35)\\(9.40)}}{<} C_3^{-2\ell} + O(C_3^{\ell}\delta_2) < 2C_3^{-2\ell} \end{aligned} \tag{9.48}$$

and

$$(\xi \cdot (\oplus_s U_s))(e_i'') = \mu_i \lambda_s' e_i'' \quad \text{for } i \in I_s. \tag{9.49}$$

By assumption, we may take $\mu_1, \mu_2, \{1, 2\} \subset I_1$, such that

$$|\mu_1 - \mu_2| > \frac{1}{2}\delta_3. \tag{9.50}$$

From (9.38), (9.48), we have for $i_1 \in I_{s_1}, i_2 \in I_{s_2}, s_1 \ne s_2$,

$$|\mu_{i_1}\lambda_{s_1}' - \mu_{i_2}\lambda_{s_2}'| > \frac{1}{2}C_3^{-\ell} - 4C_3^{-2\ell} > \frac{1}{3}C_3^{-\ell}. \tag{9.51}$$

In view of (9.50), (9.51), $\xi(\oplus_s U_s)$ has at least $d_1 + 1$ eigenvalues that are $\frac{1}{2}\delta_3$ apart.

Consider the element $\xi y \in W_{(2s+1)L+\ell, 3\delta_1+\delta} \subset W_{2(s+1)L, 2\delta}$. Since by (9.40), (9.43) we have $\|\xi y - \xi(\oplus_s U_s)\| \lesssim C_3^{\ell}\delta_2$ and $\delta_3 = C_3^{2\ell}\delta_2$, also ξy has at least $d_1 + 1$ distinct eigenvalues. Hence $(**)$ holds for $d_1 + 1$. □

This completes the proof of $(*)$.

We also need the following extension. Assume $H \subset W_\ell$, $1 \in H = H^{-1}$ such that

$$\log |H| \sim \ell. \tag{9.52}$$

The s-fold product set $H^{(s)}$ obviously satisfies $H^{(s)} \subset W_{s\ell}$.

On the other hand, from Razborov's product theorem in the free group (see [R])

$$|H \cdot H \cdot H| \gg |H|^{2-\varepsilon} \qquad (\varepsilon > 0). \tag{9.53}$$

Hence, for $\alpha < \log 2/\log 3$,

$$|H^{(s)}| > |H|^{s^\alpha}. \tag{9.54}$$

(Note that any statement of the form $\log |H^{(s)}|/\log |H| \to \infty$ as $s \to \infty$ suffices for our purpose.)

Replacing the sets $W_{\ell'}$, $\ell' < \ell$, by product sets $H^{(s)}$, a straightforward adaptation of previous analysis permits us to obtain again a set $A \subset H^{(s)}$, for some s, satisfying (9.23) and (9.24). This gives

Proposition 9. *Let $g_1, \dots, g_q$ be algebraic elements in* $\mathrm{U}(d)$ $(q \geq 2)$ *generating a free group. Take $H \subset W_\ell(g_1, \dots, g_q)$, ℓ sufficiently large, such that*

$$\log |H| \sim \ell. \tag{9.55}$$

There is $A \subset H^{(s)}$ $(s < C)$ and $\delta > 0$ such that

(9.56) $\log(1/\delta) \sim \ell$,
(9.57) *the elements of A are δ-separated and $|A| > \delta^{-c}$,*
(9.58) *in an appropriate orthonormal basis,*

$$\mathrm{dist}(x, \Delta) < \delta \quad \textit{for } x \in A. \tag{9.59}$$

Corollary 10. *Let $g_1, \dots, g_q \in \mathrm{SU}(d)$ $(q \geq 2)$ be algebraic and free. Let $H \subset W_\ell(g_1, \dots, g_q)$, ℓ large enough, be such that*

(9.60) $\log |H| \sim \ell$.

Then there are $\delta_0 > \delta > 0$ with

(9.61) $\log(1/\delta_0) \sim \log(1/\delta) \sim \ell$

and $\xi = (\xi_{ij})_{1 \leq i,j \leq d}$ with

(9.62) $\xi_{ji} = \overline{\xi_{ij}}$, $\xi_{ii} = 0$ *and* $\|\xi\| = 1$

such that the following holds. Let $\eta \in \mathcal{L}(\mathbb{C}^d)$, $\|\eta\| < \delta$ and $t \in [0, \delta_0]$. Then

$$\Big\| 1 + t \sum_{i,j} \xi_{ij} \eta_{ij} (e_i \otimes e_j) - x \Big\| < \delta_0^{1+\gamma} \|\eta\| \tag{9.63}$$

for some $x \in (H \cup \{1 + \eta, (1 + \eta)^{-1}\})^{(s)}$, $s < C$ and where $\gamma > 0$ is a fixed constant.

Proof. First apply Proposition 9 to H. We obtain $A \subset H^{(s_1)}$, $s_1 < C$ and $\delta_1 > 0$, $\ell \sim \log(1/\delta_1)$ such that the elements of A are δ_1-separated,

$$\log |A| \sim \ell \tag{9.64}$$

and (after a base change)

$$\mathrm{dist}(x, \Delta) < \delta_1 \quad \text{for } x \in A. \tag{9.65}$$

Denote by V the vector space $M_{d \times d}(\mathbb{C})$ for $x \in \mathrm{SU}(d)$ and consider the adjoint representation ρ_x, $\rho_x(z) = x^{-1} z x$, acting unitarily on V.

We will apply Corollary 8 to the set

$$\mathcal{A} = \{\rho_x;\ x \in A\} \subset \mathrm{U}(V). \tag{9.66}$$

To each $x \in A$, associate

$$x' = \sum x_{ii}\, e_i \otimes e_i \in \Delta,$$

for which, by (9.65),

$$\|x - x'\| \lesssim \delta_1. \tag{9.67}$$

Since $\det x = 1$, it follows that

$$\left|1 - \prod |x_{ii}|\right| \le \left|1 - \prod x_{ii}\right| \lesssim \delta_1 \tag{9.68}$$

and

$$\left|1 - |x_{ii}|\right| \lesssim \delta_1 \qquad (1 \le i \le d). \tag{9.69}$$

Also

$$\|\rho_x - \rho_{x'}\| \lesssim \delta_1 \tag{9.70}$$

where $\rho_{x'} \in \Delta_V = \{\text{diagonal elements of } \mathrm{Mat}(V)\}$.

For $x, y \in A$, we have

$$\begin{aligned}\|\rho_{x'} - \rho_{y'}\| &\sim \max_{i \ne j} \left|\frac{x_{ii}}{x_{jj}} - \frac{y_{ii}}{y_{jj}}\right| \gtrsim \max_i \left|\frac{x_{ii}^{d-1}}{\prod_{j \ne i} x_{jj}} - \frac{y_{ii}^{d-1}}{\prod_{j \ne i} y_{jj}}\right| \\ &\gtrsim \max_i |x_{ii}^d - y_{ii}^d| - O(\delta_1) \qquad \text{(by (9.68))}.\end{aligned}$$

Hence, if $\|\rho_{x'} - \rho_{y'}\| < \delta_1$, there are $k_i \in \{0, 1, \dots, d-1\}$ $(1 \le i \le d)$ such that

$$\left\| y - \sum_i e\left(\frac{k_i}{d}\right) x_{ii}(e_i \otimes e_i) \right\| \lesssim \delta_1.$$

Since the elements of A are δ-separated, we may find a subset $A_1 \subset A$ such that $|A_1| \sim |A|$ and

$$\|\rho_{x'} - \rho_{y'}\| > C\delta_1 \quad \text{for } x, y \in A_1,$$

hence, by (9.70),

$$\|\rho_x - \rho_y\| > \delta_1 \quad \text{for } x, y \in A_1.$$

It follows that

$$N(\mathcal{A}, \delta_1) \gtrsim |A| > \delta_1^{-c}.$$

Thus $\mathcal{A}$ satisfies (8.70)–(8.72) with δ replaced by δ_1.

By Corollary 8, we obtain $\xi = (\xi_{ij}) \in \Delta_V$ with $\|\xi\| = 1$ such that (8.73) holds.

Thus for $t \in [0, \delta_1^\alpha]$, there is $M \in s'\mathcal{A}^{(s)} - s'\mathcal{A}^{(s)}$ such that

$$\left\| t \sum \xi_{ij} z_{ij} (e_i \otimes e_j) - M(z) \right\| < \delta_1^{\alpha+\beta} \tag{9.71}$$

for all $z \in V$ with $\|z\| \le 1$.

Moreover (by the Remark following Corollary 8), ξ belongs to the algebra generated by $\{\rho_{x'} - \rho_{y'};\ x, y \in A\}$. Since $\rho_{x'} \in \Delta_V$ has diagonal elements x_{ii}/x_{jj}, it follows that $\xi_{ii} = 0$.

Also

$$\langle \rho_x(e_i \otimes e_j), e_i \otimes e_j \rangle = \overline{\langle \rho_x(e_j \otimes e_i), e_j \otimes e_i \rangle}$$

for $x \in \mathrm{U}(d)$, hence

$$\langle M(e_i \otimes e_j), e_i \otimes e_j \rangle = \overline{\langle M(e_j \otimes e_i), e_j \otimes e_j \rangle}.$$

Therefore we may take ξ with $\xi_{ji} = \overline{\xi_{ij}}$ in (9.71).

Note that $\mathcal{A}^{(s)} = \rho_{A^{(s)}}$ and $\rho_{A^{(s)}}\eta = \{x^{-1}\eta x;\ x \in A^{(s)}\}$.

If $\|\eta\| < \delta$, it follows that

$$\begin{aligned} M\eta + 1 &= \prod_{\alpha=1}^{s'}(1 + x_\alpha^{-1}\eta x_\alpha) \prod_{\alpha=s'+1}^{2s'}(1 - x_\alpha^{-1}\eta x_\alpha) + O(\delta\|\eta\|) \\ &= \prod_{\alpha=1}^{s'} x_\alpha^{-1}(1+\eta)x_\alpha \prod_{\alpha=s'+1}^{2s'} x_\alpha^{-1}(1+\eta)^{-1}x_\alpha + O(\delta\|\eta\|) \end{aligned}$$

for some $x_\alpha \in A^{(s)}$. Hence

$$M\eta + 1 \in (H \cup \{1+\eta, (1+\eta)^{-1}\})^{2s'(2ss_1+1)} + B(0, C\delta\|\eta\|)$$

and there is x in a product set of $H \cup \{1+\eta, (1+\eta)^{-1}\}$ such that

$$\|M\eta + 1 - x\| \lesssim \delta\|\eta\|. \tag{9.72}$$

Taking $z = \eta/\|\eta\|$ in (9.71), it follows that

$$\left\|1 + t\sum \xi_{ij}\eta_{ij}(e_i \otimes e_j) - x\right\| \lesssim \delta_1^{\alpha+\beta}\|\eta\| + \delta\|\eta\|. \tag{9.73}$$

Take $\delta < \delta_1^{\alpha+\beta}$. We obtain (9.63) with $\delta_0 = \delta_1^\alpha$, $\gamma = \beta/\alpha$. This proves Corollary 10. □

10. Expansion in SU(d) (1)

Let $g_1, \dots, g_k \in G = \mathrm{SU}(d)$ be algebraic elements and assume $\Gamma = \langle g_1, \dots, g_k\rangle$ is Zariski dense in G. Denote

$$\nu = \frac{1}{2k}\sum_{i=1}^{k}(\delta_{g_i} + \delta_{g_i^{-1}}), \tag{10.1}$$

which is a symmetric probability measure on G.

Our aim is to establish a spectral gap, i.e.

$$\|f * \nu\|_2 \le (1-\varepsilon)\|f\|_2 \quad \text{for } f \in L_0^2(G). \tag{10.2}$$

Invoking a result of Breuillard and Gelander [BrGe], we may assume that $k = 2$ and $\{g_1, g_2\}$ generate the free group F_2.

Note that G is $d_1 = d^2 - 1$-dimensional over $\mathbb{R}$.

For $\delta > 0$ denote

$$P_\delta = \frac{1_{B(1,\delta)}}{|B(1,\delta)|}, \tag{10.3}$$

an approximate identity.

As we show below, (10.2) is a consequence of the following main proposition.

Proposition 11. *For any given $\tau > 0$, there is a positive integer $\ell < C(\tau)\log(1/\delta)$ such that*

$$\|\nu^{(\ell)} * P_\delta\|_\infty < \delta^{-\tau} \tag{10.4}$$

where $\nu^{(\ell)} = \underbrace{\nu * \cdots * \nu}_{\ell}$ denotes the ℓ-fold convolution.

Note that (10.4) may be replaced by the a priori weaker statement

$$\|\nu^{(\ell)} * P_\delta\|_2 < \delta^{-\tau}. \tag{10.5}$$

Indeed, since $P_\delta < C(P_\delta * P_\delta)$, one has, for $x \in G$,

$$(\nu^{(2\ell)} * P_\delta)(x) \le C\langle \nu^{(\ell)} * P_\delta, \tau_{x^{-1}}(\nu^{(\ell)} * P_\delta)\rangle \le \|\nu^{(\ell)} * P_\delta\|_2^2$$

where $(\tau_{x^{-1}} f)(y) = f(yx^{-1})$.

Note that since $\{g_1, g_2\}$ are algebraic and free, one gets trivially

$$\|\nu^{(\ell)} * P_\delta\|_2 < \delta^{-\frac{1}{2}d_1+\theta} \tag{10.6}$$

for some $\theta > 0$. Proposition 11 will therefore follow from a bounded number of applications of

Lemma 10.7 (L^2-flattening lemma). *Given $\gamma > 0$, there is $\kappa > 0$ such that for each $\delta > 0$ small enough and $\ell \sim \log(1/\delta)$, if*

$$\|\nu^{(\ell)} * P_\delta\|_2 > \delta^{-\gamma} \tag{10.8}$$

then

$$\|\nu^{(2\ell)} * P_\delta\|_2 < \delta^{\kappa}\|\nu^{(\ell)} * P_\delta\|_2. \tag{10.9}$$

We use $|\ |$ to denote either the Haar measure on G or the cardinality of a discrete set.

Denote $\mu = \nu^{(\ell)} * P_\delta$ and assume (10.9) fails, i.e.

$$\|\mu * \mu\|_2 > \delta^{0+}\|\mu\|_2. \tag{10.10}$$

From a noncommutative version of the BSG theorem due to Tao [Tao, Thm. 5.4], we obtain a subset H of G, H a union of δ-balls, and a discrete set $X \subset G$ with the following properties:

(10.11) $H = H^{-1}$,
(10.12) $H.H \subset H.X \cap X.H$,
(10.13) $|X| < \delta^{0-}$,
(10.14) $\mu(aH) > \delta^{0+}$ for some $a \in G$,
(10.15) $|H| < \delta^{\gamma}$.

Properties (10.11)–(10.13) mean that H is an 'approximate group'. Note that (10.12), (10.13), (10.15) imply

(10.16) $|H^{(s)}| <_{(s)} \delta^{0-}|H| < \delta^{\gamma-}$ for any given $s \in \mathbb{Z}_+$

where $H^{(s)}$ stands for the s-fold product set.

For notational simplicity, let H' denote product sets $H^{(s)}$ for unspecified (but bounded) $s \in \mathbb{Z}_+$.

The proof of Lemma 7, and hence of Proposition 11, will be completed by showing that there is no approximate group H satisfying (10.14), (10.15).

This is the same approach as in [BG] for SU(2). But, as discussed in the introduction, the argument used here differs from that of [BG], and is analogous to [BG2] on expansion in $\mathrm{SL}_d(p^n)$.

We first show how to derive (10.2) from Proposition 11.

In [BG] treating $G = \mathrm{SU}(2)$, we relied on extension in [GJS] of the Sarnak–Xue technique, based on suitable averaging of characters of the irreducible representations on spaces of homogeneous polynomials. The argument presented below gives an alternative approach that is perhaps more geometric and 'general' in the sense of being applicable to other groups.

We will reduce the problem to a convolution property on the group G (Lemma 10.35 below). The relevant inequality will then be established first for $G = \mathrm{SU}(2)$ and next in general for $G = \mathrm{SU}(d)$, using SU(2)-embeddings.

Let $G = \mathrm{SU}(d)$ and denote $(\rho_g f)(x) = f(xg)$ acting on $L^2(G)$. Letting ν be the discrete, symmetric probability measure (10.1), we have to establish (10.2). Assume to the contrary that

$$\|f * \nu\|_2 > 1 - \varepsilon \tag{10.18}$$

where $f \in L^2_0(G)$, $\|f\|_2 = 1$.

We introduce a Littlewood–Paley decomposition on G (which is a standard construction in harmonic analysis: see, for example, Chapter 4 in [S]).

For $f \in L^2(G)$, $0 < \delta < 1$, let

$$(f * P_\delta)(x) = \fint_{B(1,\delta)} f(xg)\, dg \tag{10.19}$$

with P_δ introduced in (10.13) and $\fint$ denoting the average, and denote

$$\begin{aligned} \Delta_1 f &= (f * P_{2^{-1}}) - \int_G f, \\ \Delta_k f &= (f * P_{2^{-k}}) - (f * P_{2^{-k+1}}) \quad \text{for } k \geq 2. \end{aligned} \tag{10.20}$$

Thus we have the decomposition

$$f = \sum_{k \geq 1} \Delta_k f \tag{10.21, }$$

satisfying the square function property

$$\frac{1}{C}\Big(\sum \|\Delta_k f\|_2^2\Big)^{1/2} \leq \|f\|_2 \leq C\Big(\sum \|\Delta_k f\|_2^2\Big)^{1/2}. \tag{10.22}$$

Since $\rho_g(f * P_\delta) = (\rho_g f) * P_\delta$, it follows that $\Delta_k f * \nu = \Delta_k(f * \nu)$. Hence, by (10.22), for all $\ell \in \mathbb{Z}_+$,

$$\|f * \nu^{(\ell)}\|_2 \sim \Big(\sum_{k \geq 1} \|(\Delta_k f) * \nu^{(\ell)}\|_2^2\Big)^{1/2}. \tag{10.23}$$

Note that from the Zariski-density assumption for Γ, no elements of $L_0^2(G) \setminus \{0\}$ are Γ-invariant. Hence

(10.24) $f \to 0$ (weakly) if $f \in L_0^2(G)$ with $\|f\|_2 = 1$ satisfies (10.18) with $\varepsilon \to 0$.

Therefore we may assume

$$f = \sum_{k \geq k_0} \Delta_k f \tag{10.25}$$

where $k_0 = k_0(\varepsilon) \to \infty$ as $\varepsilon \to 0$.

Let $\ell_0 \in \{2^m\}$ be fixed and sufficiently large (to be specified). From (10.18), (10.22), (10.23) and (10.25), taking ε small enough we have

$$\|f * \nu^{(\ell_0)}\|_2 > (1-\varepsilon)^{\ell_0} > 1/2$$

and

$$\sum_{k > k_0} \|\Delta_k f * \nu^{(\ell_0)}\|_2^2 > c \sum_{k \geq k_0} \|\Delta_k f\|_2^2 \tag{10.26}$$

with c independent of ℓ_0. Therefore there is some $k > k_0$ such that

$$F = \frac{\Delta_k f}{\|\Delta_k f\|_2} \tag{10.27}$$

satisfies

$$\|F * \nu^{(\ell_0)}\|_2 > c. \tag{10.28}$$

Take $\ell \sim k$ (to be specified). From (10.28),

$$\|F * \nu^{(\ell_0 \ell)}\|_2 > c^{\ell}. \tag{10.29}$$

Let $\delta = 4^{-k}$. Then, by (10.27), $F \approx F * P_\delta$ and (10.29) implies

$$\|F * \mu\|_2 > c^{\ell} \tag{10.30}$$

where $\mu = \nu^{(\ell_0 \ell)} * P_\delta$.

Fix $\tau > 0$. If we take

$$\ell_0 \ell > C(\tau) \log \frac{1}{\delta},$$

hence

$$\ell > \frac{C(\tau) k}{\ell_0}, \tag{10.31}$$

Proposition 11 gives

$$\|\mu\|_\infty < \delta^{-\tau}. \tag{10.32}$$

Rewrite (10.30) as

$$\int_G \left| \int_G F(xg)\mu(g)\, dg \right|^2 dx > c^{2\ell},$$

and hence by (10.32),

$$\delta^{-2\tau} \int_G \left| \int_G F(xg)\overline{F(x)}\,dx \right| dg \geq \int_G \int_G \left| \int_G F(xh^{-1}g)\overline{F(x)}\,dx \right| \mu(g)\mu(h)\,dg\,dh > c^{2\ell}. \tag{10.33}$$

Denoting $F_1(x) = \overline{F(x^{-1})}$, it follows from (10.33) that

$$\|F_1 * F\|_1 > c^{2\ell}\delta^{2\tau} > \delta^{C(\tau)/\ell_0+2\tau}. \tag{10.34}$$

In order to obtain a contradiction, it will therefore suffice to apply

Lemma 10.35. *Given $c > 0$, there is $c' > 0$ such that if $\delta_1 > 0$ is small enough and $F_1, F_2 \in L^2(G)$ satisfy $\|F_1\|_2 \leq 1$, $\|F_2\|_2 \leq 1$ and*

$$\|F_2 * P_{\delta_1}\|_2 < \delta_1^c, \tag{10.36}$$

then

$$\|F_1 * F_2\|_1 < \delta_1^{c'}. \tag{10.37}$$

Indeed, by (10.27), F satisfies (10.36) with $\delta_1 = 2^{-k/2}$ say and (10.37) contradicts (10.34) by taking first τ small enough and then ℓ_0 large enough.

Returning to Lemma 10.35 for $G = \mathrm{SU}(d)$, note that it obviously fails for $d = 1$.

We will first establish the lemma for $G = \mathrm{SU}(2)$ and then derive the statement for $G = \mathrm{SU}(d)$, $d > 2$.

Proof of Lemma 10.35 for $G = \mathrm{SU}(2)$. Denoting by T the convolution operator by F_2 acting on $L^2(G)$, we have to prove that

$$\|T\| < \delta_1^{c'}. \tag{10.38}$$

It suffices to verify (10.38) for the action of T in the irreducible unitary representations of SU(2), that is, on the spaces $W_n = [z^k w^{n-k};\ 0 \leq k \leq n]$ of homogeneous polynomials on the unit sphere of $\mathbb{C}^2$. From the theory of induced representations (Frobenius' theorem) applied to the diagonal subgroup $D = \left\{R_\theta = \left(\begin{smallmatrix} e^{2\pi i\theta} & 0 \\ 0 & e^{-2\pi i\theta} \end{smallmatrix}\right);\ 0 \leq \theta < 1\right\}$, we see that the IUR of G are contained in one of the following two representations ρ_0, ρ_1 (depending on n being even or odd).

(i) ρ_0 is acting by right translation on the subspace V_0 of $L^2(G)$ of functions that are left invariant under the action of D. Thus $f \in V_0$ if $f(x) = f(R_\theta x)$ and f factors over $D \setminus G \simeq S^2$. Equivalently, ρ_0 may be seen as the representation of SO(3) on $L^2(S^2)$ by rotation.

(ii) ρ_1 is acting by right translation on the subspace V_1 of $L^2(G)$ of functions satisfying

$$f(R_\theta x) = e^{i\theta} f(x). \tag{10.39}$$

To establish (10.38), we need to show that

$$\|T|_{V_0}\| < \delta_1^{c'} \quad \text{and} \quad \|T|_{V_1}\| < \delta_1^{c'}. \tag{10.40}$$

We consider the action on V_1 (the case of V_0 is analogous).

Let $f \in V_1$, $\|f\|_2 = 1$. We have to prove that $\|f * F_2\|_2 < \delta_1^{c'}$. In view of (10.36), we can assume that

$$\|f * P_{\delta_2}\|_2 < \delta_2 \tag{10.41}$$

with $\delta_2 = \delta_1^{c'}$. Write

$$\|Tf\|_2^2 = \int_{G\times G}\left[\int_G f(xy_1^{-1})\overline{f(xy_2^{-1})}\,dx\right]F(y_1)\overline{F(y_2)}\,dy_1\,dy_2 \le \left\|\int_G f(x)\overline{f(x\cdot)}\,dx\right\|_2.$$

Squaring again and using that $f \in V_1$, it follows that

$$\begin{aligned}\|Tf\|_2^4 &\le \int_{G\times G\times G} f(x)\overline{f(xy)}\,\overline{f(x_1)}f(x_1y)\,dx\,dx_1\,dy\\ &= \int_{G\times G\times G}\int_0^1 f(x)\overline{f(R_\theta xy)}\,\overline{f(x_1)}\;f(R_\theta x_1 y)\,dx\,dx_1\,dy\,d\theta\\ &= \int_{G\times G\times G} f(x)\overline{f(y)}\,\overline{f(x_1)}\left[\int_0^1 f(R_\theta x_1 x^{-1}R_{-\theta}y)\,d\theta\right]dx\,dx_1\,dy\end{aligned}$$

and

$$\|Tf\|_2^8 \le \int_G\left\|\int_0^1 f(R_\theta x R_{-\theta}\cdot)\,d\theta\right\|_2^2 dx = \int_{D\backslash G}\|S_x f\|_2^2\,dx \tag{10.42}$$

where we denoted

$$S_z f(x) = \int_0^1 f(R_\theta z R_{-\theta}x)\,d\theta. \tag{10.43}$$

For $z = \left(\begin{smallmatrix} r & se^{i\psi} \\ -se^{-i\psi} & r\end{smallmatrix}\right)$, $s \neq 0$, the operator S_z acting on $L^2(G)$ is smoothing, since $\langle R_\theta z R_{-\theta};\ 0 \le \theta \le 1\rangle = G$. In fact, geometrically if we identify G with the unit sphere in $\mathbb{C}^2$ through the map $g = \left(\begin{smallmatrix} v & -\bar{w} \\ w & \bar{v}\end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} v \\ w\end{smallmatrix}\right)$, S_z is obtained by a circular average with circle of radius s centered at $\left(\begin{smallmatrix} rv \\ rw\end{smallmatrix}\right)$ in the plane spanned by $\left(\begin{smallmatrix} -w \\ v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} iw \\ iv\end{smallmatrix}\right)$.

In view of (10.41), we obtain (10.42) $< \delta_2^c$ and hence $\|Tf\|_2 < \delta_1^{cc'/8}$. This proves (10.40).

Next we treat the general case, using the result for $d = 2$.

Proof of Lemma 10.35 for $G = \mathrm{SU}(d)$, $d > 2$. Take a subgroup H of G, $H \simeq \mathrm{SU}(2)$, considering for instance the embedding $\mathrm{SU}(2) \to \mathrm{SU}(d) : h \mapsto \sum_{i,j=1}^2 h_{ij}\, e_i \otimes e_j$. Write

$$\begin{aligned}\|F_1 * F_2\|_1 &= \int_G\left|\int_G F_1(g)F_2(g^{-1}x)\,dg\right|dx\\ &= \int_G\int_G\left[\int_H\left|\int_H F_1(hg)F_2(g^{-1}h^{-1}yx)\,dh\right|dy\right]dx\,dg.\end{aligned} \tag{10.44}$$

Fixing $x, g \in G$, introduce the following functions φ_1, φ_2 on H:

$$\varphi_1(y) = F_1(yg), \qquad \varphi_2(y) = F_2(g^{-1}yx), \tag{10.45}$$

for which the expression [ ] in (10.44) becomes

$$\int_H \left| \int_H \varphi_1(h)\varphi_2(h^{-1}y)\, dh \right| dy = \|\varphi_1 * \varphi_2\|_{L^1(H)}.$$

In order to reach the conclusion by applying Lemma 10.35 on H, it will suffice to bound $\|\varphi_1 * P_{\delta_2}\|_{L^2(H)} < \delta_1^{c_1}$, for some $\delta_2 > \delta_1$, $\log(1/\delta_2) \sim \log(1/\delta_1)$, in the mean over $x, g \in G$ (cf. (10.44)). Thus what is needed is an estimate of the form

$$\int_G \int_G \int_H \left| \fint_{B_H(1,\delta_2)} F_2(g^{-1}y_1yx)\, dy_1 \right|^2 dy\, dx\, dg < \delta_1^c,$$

hence

$$\int_G \int_G \left| \fint_{B_H(1,\delta_2)} F_2(g_1yg_2)\, dy \right|^2 dg_1\, dg_2 < \delta_1^c. \tag{10.46}$$

Here $B_H(1, \delta_1) = \{y \in H;\ \|1 - y\| < \delta_1\}$.

Rewrite (10.46) as

$$\int_G \int_G \fint_{B_H(1,2\delta_2)} F_2(g_2)\overline{F_2(g_1yg_1^{-1}g_2)}\, dy\, dg_1\, dg_2. \tag{10.47}$$

Fix $y \in B_H(1, 2\delta_2)$, $\|1 - y\| > \delta_2^2$ (the contribution of $\|1 - y\| \le \delta_2^2$ to (10.47) is at most $O(\delta_2^3)$). We obtain

$$\iint F_2(g)\overline{F_2(xg)}\, \eta(dx)\, dg \tag{10.48}$$

where η is the image measure $\Phi[\lambda_G]$ under the map

$$\Phi = \Phi_y : G \to G : g \mapsto gyg^{-1}. \tag{10.49}$$

Next, writing η_* for the image of η under $x \mapsto x^{-1}$, we have

$$|(10.48)|^2 \le \int \left| \int F_2(xg)\, \eta(dx) \right|^2 dg \le \int \left| \int F_2(xg)\, (\eta * \eta_*)(dx) \right|^2 dg,$$

and similarly, for $r \in \mathbb{Z}_+$,

$$|(10.48)|^{2r} \le \int \left| \int F_2(xg)\, (\eta * \eta_*)^{(r)}(dx) \right|^2 dg \tag{10.50}$$

where $\eta^{(r)} = \eta * \cdots * \eta$ (r-fold convolution).

Returning to Φ, diagonalize $y = \left(\begin{smallmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{smallmatrix}\right)$, $\delta_2^2 < |\theta| < 2\delta_2$. Hence

$$\Phi(y) = 1 + i\theta gvg^{-1} + O(\theta^2) \tag{10.51}$$

where $v = e_1 \otimes e_1 - e_2 \otimes e_2 \in \mathrm{su}(d)$ and

$$\Phi(g_1)^{-1}\Phi(g_2)\Phi(g_3)^{-1}\cdots\Phi(g_{2r}) = 1+i\theta(-g_1vg_1^{-1}+g_2vg_2^{-1}\cdots+g_{2r}vg_{2r}^{-1})+O(\theta^2).$$

For $r = r(d)$ large enough, the map

$$(g_1, g_2, \ldots, g_{2r}) \mapsto -g_1vg_1^{-1} + g_2vg_2^{-1} - \cdots + g_{2r}vg_{2r}^{-1}$$

gives a smooth density on su(d). Hence $(\eta*\eta_*)^{(r)}$ is a smooth density on $B(1, C|\theta|) \subset G$ $\big($with derivative estimates in terms of $1/|\theta| < 1/\delta_2^2\big)$.

Recall that F_2 satisfies $\|F_2 * P_{\delta_1}\|_2 < \delta_1^c$. Taking for δ_2 an appropriate power of δ_1, from the preceding we get

$$\begin{aligned}(10.50) &= \|(\eta * \eta_*)^{(r)} * F_2\|_2\\ &< \|((\eta * \eta_*)^{(r)} * P_{\delta_1}) * F_2\|_2 + O(\delta_1\delta_2^{-2})\\ &< \|(\eta * \eta_*)^{(r)}\|_1\|P_{\delta_1} * F_2\|_2 + O(\delta_1\delta_2^{-2}) < \delta_1^c + O(\delta_1\delta_2^{-2}) < \delta_1^{c'}.\end{aligned}$$

This proves (10.46) and Lemma 10.35. □

11. Expansion in SU(d) (2)

It remains to show that there is no approximate group H satisfying (10.11)–(10.15).

Since H is a union of δ-balls, (10.14) is equivalent to

$$\nu^{(\ell)}(aH) > \delta^{0+}. \tag{11.1}$$

Recall that $\ell \sim \log(1/\delta)$. Writing, for $k < \ell$,

$$\nu^{(\ell)}(aH) = \sum_x \nu^{(\ell-k)}(x)\nu^{(k)}(xaH),$$

it follows from (11.1) that for some $x \in G$,

$$\nu^{(k)}(xaH) > \delta^{0+}$$

and hence

$$\nu^{(2k)}(H.H) > \delta^{0+}. \tag{11.2}$$

In particular, recalling Kesten's bound [K] for random walks on F_2,

$$|H.H \cap W_k| > \sqrt{2}^k \quad \text{if } 2^k > (1/\delta)^{0+}. \tag{11.3}$$

Denote by $V \subset \mathrm{Mat}_{d\times d}(\mathbb{C})$ the real vector space of anti-Hermitian matrices of zero trace $\big($i.e. the Lie algebra of $G = \mathrm{SU}(d)\big)$, which is irreducible under the adjoint representation of G and hence of its Zariski dense subgroup Γ.

We make the following assumption on ν.

Assumption $(*)$**.** *There is $\omega > 0$ such that for a proper subspace L of V and k large enough, one has the estimate*

$$\nu^{(k)}[g \in G;\ g^{-1}Lg = L] < e^{-\omega k}. \tag{11.4}$$

Let $a \in V \setminus \{0\}$ and $2^k > (1/\delta)^{0+}$. Consider the increasing subspaces L_s of V defined by

$$L_1 = \operatorname{span}[a],$$
$$L_{s+1} = \operatorname{span}[g^{-1}L_s g;\ g \in H.H \cap W_k].$$

Taking s such that $L_{s+1} = L_s = L$, we find that $g^{-1}Lg = L$ for $g \in H.H \cap W_k$ and (11.2), (11.4) imply that $L = V$. Since $(H.H \cap W_k)^{(s)} \subset H^{2s} \cap W_{sk}$, we proved that under $(*)$, if $a \in V \setminus \{0\}$ and L is a proper subspace of V, then, for $2^k > (1/\delta)^{0+}$, there is $g \in H' \cap W_k$ such that $g^{-1}ag \notin L$.

Equivalently, if $a, b \in V \setminus \{0\}$, there is $g \in H' \cap W_k$ such that

$$\operatorname{Tr} g^{-1}agb^* \neq 0. \tag{11.5}$$

Recalling that g_1, g_2 are algebraic, (11.5) implies the following quantitative statement as a consequence of the effective Nullstellensatz (see Theorem 5.1 in [BY] and the comment on its generalization to polynomials with coefficients in the ring of integers in a fixed number field K, $[K : \mathbb{Q}] < \infty$).

Lemma 11.6. *Assume $(*)$. If $2^k > (1/\delta)^{0+}$ and $a, b \in V \setminus \{0\}$, there is $g \in H' \cap W_k$ such that*

$$|\operatorname{Tr} g^{-1}agb^*| \geq C^{-k}\|a\|\,\|b\| \tag{11.7}$$

where C is some constant depending on the generators g_1, g_2 of Γ.

Next, apply Corollary 10 to $H.H \cap W_k$ and $2^k > (1/\delta)^{0+}$. We obtain

$$i\xi \in V, \quad \xi_{jj} = 0 \quad (1 \leq j \leq d), \quad \|\xi\| = 1 \tag{11.8}$$

such that for $\delta_0 > \delta_1 > 0$, $\log(1/\delta_0) \sim \log(1/\delta_1) \sim k$,

$$\operatorname{dist}\Big(1 + t\sum \xi_{ij}\eta_{ij}(e_i \otimes e_j),\ H'\Big) < \delta_1^{1+\delta}\|\eta\| \tag{11.9}$$

whenever $1 + \eta \in H'$, $\|\eta\| < \delta_1$ and $t \in [0, \delta_0]$.

Note that $\eta + \eta^* = O(\|\eta\|^2)$ and $\operatorname{Tr}\eta = O(\|\eta\|^2)$ and hence there is an element $a \in V$ such that $\|\eta - a\| \lesssim \delta_1\|\eta\|$. Thus from (11.9),

$$\operatorname{dist}\Big(1 + t\sum \xi_{ij}a_{ij}(e_i \otimes e_j),\ H'\Big) < \delta_0^{1+\gamma}\|\eta\| \quad \text{for } t \in [0, \delta_0]. \tag{11.10}$$

We may further replace in (11.10) a by any conjugate $g^{-1}ag$ for $g \in H'$. Take $k_0 \sim \log(1/\delta_0)$ and small enough to ensure that

$$C^{-k_0} > \delta_0^{\gamma/2} \tag{11.11}$$

where C is the constant from Lemma 11.6.

Applying Lemma 11.6 with a as above and $b = i\bar{\xi} \in V$ (where $\bar{\xi}_{ij} = \xi_{ji}$) gives some $g \in H' \cap W_{k_0}$ such that

$$\max_{i,j} |(g^{-1}ag)_{ij}\xi_{ij}| \gtrsim \left|\sum_{i,j}(g^{-1}ag)_{ij}\xi_{ij}\right| > C^{-k_0}\|\eta\|. \tag{11.12}$$

Let $\zeta \in V$ with $\|\zeta\| = 1$ be defined by normalization of $((g^{-1}ag)_{ij}\xi_{ij})_{1\le i,j\le d}$. Clearly, from (11.10) and the preceding,

$$\operatorname{dist}(1 + t\zeta, H') < \delta_0^{1+\gamma}\|\eta\| \quad \text{for } t \in [0, \delta_0 C^{-k_0}\|\eta\|] \overset{(11.11)}{\supset} [0, \delta_0^{1+\gamma/2}\|\eta\|]. \tag{11.13}$$

Again from Lemma 11.6, there are $g_1, \dots, g_{d_1} \in H' \cap W_{k_0}$ ($d_1 = d^2 - 1$) such that

$$|\det(g_s^{-1}\zeta g_s;\ 1 \le s \le d_1)| > C_1^{-k_0}. \tag{11.14}$$

Since in (11.13) we may replace ζ by conjugates $g^{-1}\zeta g$ with $g \in H'$, it easily follows from (11.14) that

$$\operatorname{dist}(1 + tV, H') < \delta_0^{1+\gamma}\|\eta\|$$

for

$$t \in [0, \delta_0 C_1^{-k}\|\eta\|] \supset [0, \delta_0^{1+\gamma/2}\|\eta\|]. \tag{11.15}$$

Hence, we proved (redefining δ_0 and γ)

Lemma 11.16. *Let* $1 + \eta \in H'$, $\|\eta\| < \delta_1$. *Then*

$$\operatorname{dist}(1 + tV, H') < \delta_0^{1+\gamma}\|\eta\| \quad \textit{for } t \in [0, \delta_0\|\eta\|]. \tag{11.17}$$

Fix a small constant ε and let $k = [\varepsilon \log(1/\delta)]$. Thus $\delta_0 = \delta^{\varepsilon_0}$, $\delta_1 = \delta^{\varepsilon_1}$ with $\varepsilon_0 \sim \varepsilon_1 \sim \varepsilon$ in Lemma 11.16.

The final step consists in using Lemma 11.16 to derive a contradiction on (10.16), i.e.

$$|H'| < \delta^{\gamma-}. \tag{11.18}$$

Fix an element $g_1 = 1 + \eta_1 \in H.H \cap W_{k_1} \cap B(1, \delta_1)$, $g_1 \neq 1$, which by (11.3) is possible for $k_1 < (1/d_1)\log(1/\delta_1)$. It follows that

$$\delta_1^C < \|\eta_1\| = t_1 < \delta_1. \tag{11.19}$$

From (11.17),

$$\operatorname{dist}(1 + tV, H') < \delta_0^{1+\gamma} t_1 \quad \text{for } t \in [0, \delta_0 t_1]. \tag{11.20}$$

Hence, for any $t_2 \in [\delta_0^{1+\gamma/2} t_1, \delta_0 t_1]$, H' contains some element $1 + \eta$ with $\|\eta\| \approx t_2$. Applying again Lemma 11.16 shows that

$$\operatorname{dist}(1 + tV, H') < \delta_0^{1+\gamma} t_2 \quad \text{for } t \in [0, \delta_0 t_2], \tag{11.21}$$

and therefore H' contains elements $1 + \eta$ with $\|\eta\| \approx t_3$ for any $t_3 \in [\delta_0^{1+\gamma/2} t_2, \delta_0 t_2]$ and hence any $t_3 \in [\delta_0^{2(1+\gamma/2)} t_1, \delta_0^2 t_1]$.

After r steps, we see that H' contains elements $1+\eta$ with $\|\eta\| \approx t$ for any $t \in [\delta_0^{r(1+\gamma/2)} t_1, \delta_0^r t_1]$. Taking $r = [2/\gamma] + 1$, it follows that H' contains elements $1+\eta$ where $\|\eta\| \approx t$, for any $t \in [\delta, \delta_0^r t_1]$.

Another application of Lemma 11.16 implies that

$$\operatorname{dist}(1 + tV, H') < \delta_0^\gamma t \quad \text{for } t \in [0, \delta_2] \tag{11.22}$$

where

$$\delta_2 = \delta_0^{r+1} t_1. \tag{11.23}$$

We claim that

$$G \cap B(1, \delta_2) \subset H'. \tag{11.24}$$

Then

$$|H'| > \delta_2^{d_1} > \delta^{(\varepsilon_0(r(\gamma)+1)+C\varepsilon_1)d_1},$$

contradicting (11.18) for ε small enough.

Proof of (11.24). Take $g_0 \in G \cap B(1, \delta_2)$. Then $g_0 = 1 + \eta_0$ and there is $a_0 \in V$ such that $\|a_0 - \eta_0\| \lesssim \delta_2^2$. By (11.22), $\operatorname{dist}(1 + a_0, H') < \delta_0^\gamma \delta_2$ and we take $h_1 \in H'$ such that

$$\|g_0 h_1^{-1} - 1\| = \|g_0 - h_1\| \lesssim \delta_2^2 + \delta_0^\gamma \delta_2 \lesssim \delta_0^\gamma \delta_2. \tag{11.25}$$

Next, write $g_1 = g_0 h_1^{-1} = 1 + \eta_1$ and take $a_1 \in V$ with $\|a_1 - \eta_1\| \lesssim \|a_1\|^2$. By (11.22), $\operatorname{dist}(1 + a_1, H') < \delta_0^\gamma \|a_1\|$ and we obtain $h_2 \in H'$ such that

$$\|g_0 h_1^{-1} h_2^{-1} - 1\| = \|g_1 - h_2\| \lesssim \|a_1\|^2 + \delta_0^\gamma \|a_1\| \lesssim \delta_0^{2\gamma} \delta_2. \tag{11.26}$$

Since H' is a union of δ-balls, a few iterations give the desired conclusion.

This completes the proof of the spectral gap, conditional on Assumption $(*)$.

12. Proof of Assumption $(*)$ for $d = 3$

Assume $H \subset \Gamma$ and L a nontrivial subspace of $V = \mathrm{su}(d)$ satisfying

(12.1) $\nu^{(k)}(H) > e^{-\varepsilon k}$,
(12.2) $g^{-1} L g = L$ for $g \in H$,

where in (12.1) we assume ε is a sufficiently small constant (depending on Γ and ν) and k is large. Our purpose is to get a contradiction for $d = 3$. This will illustrate the method in the simplest case. The argument in the general case is given in §14. Essential use is made of the theory of random matrix products as developed by Furstenberg and Guivarch. A treatment of this theory in the setting of general local fields appears in [A].

Recall that $\Gamma \subset \mathrm{SU}(k)$, where k is the algebraic closure of $\mathbb{Q}$. We will consider V and L as vector spaces over k, hence $V = \{g \in \mathrm{Mat}_{d\times d}(k);\ \operatorname{Tr} g = 0\}$.

(i) Exploiting the theory of random matrix products requires proximal elements. Following the approach of Tits [Tits] (see also [G]), proximal elements in a suitable setting may be produced by passing to an appropriate local field.

Fix $g_0 \in \Gamma$ with eigenvalues $(\lambda_j)_{1\le j\le d}$ such that not all quotients $\lambda_j/\lambda_{j'}$ are roots of unity. If $\lambda_j/\lambda_{j'}$ is not root of unity, there is a local field $k \subset K_v$ such that $v(\lambda_j/\lambda_{j'}) \neq 1$. Hence

$$|\{v(\lambda_j);\ 1 \le j \le d\}| \ge 2.$$

For $d = 3$, either

$$v(\lambda_1) > v(\lambda_2) > v(\lambda_3) \tag{12.3}$$

or

$$v(\lambda_1) = v(\lambda_2) > v(\lambda_3) \tag{12.4}$$

(if $v(\lambda_1) > v(\lambda_2) = v(\lambda_3)$, replace g_0 by g_0^{-1}).

Denote by ρ the adjoint representation on V.

If (12.3) holds, the representation $\rho|\Gamma$ on $V \otimes K_v$ has ρ_{g_0} as proximal element and since it is totally irreducible (by the Zariski-density assumption), random matrix product theory implies that (12.1), (12.2) are not compatible for $\varepsilon > 0$ small enough.

Thus we may assume that the situation (12.3) cannot be realized for any $g \in \Gamma$.

(ii) Consider the representation of Γ on $\bigwedge^2(V \otimes K_v)$, which we also denote ρ.

If e_1, e_2, e_3 diagonalizes g_0, $g_0 e_i = \lambda_i e_i$ $(1 \le i \le 3)$, the eigenvector

$$\xi = (e_3 \otimes e_1) \wedge (e_3 \otimes e_2) \tag{12.5}$$

of ρ_{g_0} has dominant eigenvalue λ_1^2/λ_3^2, by (12.4).

Denote

$$\mathcal{S} = \mathrm{span}_k[\rho_g(\xi);\ g \in \Gamma], \tag{12.6}$$

a subspace of $\bigwedge^2 V$. The restriction of ρ to $\mathcal{S}$ is totally irreducible. Otherwise, there would be a proper subspace $\mathcal{S}_1$ of $\mathcal{S}$ which is invariant under a finite index subgroup Γ_1 or Γ. Hence $\mathcal{S}_1 \otimes \mathbb{C}$ would be invariant for ρ_g, $g \in \bar{\Gamma}_1$ = Zariski closure of Γ_1. Since $\bar{\Gamma} = \mathrm{SL}_d(\mathbb{C})$ and $\bar{\Gamma}_1$ is a finite index subgroup of $\bar{\Gamma}$, it follows that $\bar{\Gamma}_1 = \mathrm{SL}_d(\mathbb{C})$. In particular $\mathcal{S}_1$ is Γ-invariant, hence $\mathcal{S}_1 = \mathcal{S}$. Also

$$\mathcal{S} \otimes \mathbb{C} = \mathrm{span}_{\mathbb{C}}[\rho_g(\xi);\ g \in \mathrm{SL}_d(\mathbb{C})]. \tag{12.7}$$

Since ρ restricted to $\mathcal{S} \otimes K_v$ has a proximal element, it follows again from random matrix product theory and (12.1) that

$$\mathcal{S} = \mathrm{span}[\rho_g(\eta);\ g \in H] \quad \text{for any } \eta \in \mathcal{S} \setminus \{0\}. \tag{12.8}$$

We used here that the probabilistic estimates depend on ν but not on the vector η.

(iii) The space $\bigwedge^2 V$ decomposes as

$$\bigwedge^2 V = \bigwedge^2 L \underline{\oplus} \bigwedge^2 L^\perp \underline{\oplus} (L \wedge L^\perp) = \mathfrak{S}_1 \underline{\oplus} \mathfrak{S}_2 \underline{\oplus} \mathfrak{W} \tag{12.9}$$

and by (12.2), each of the components is invariant under ρ_g for $g \in H$. Take an element $g_1 \in H$ such that not all quotients of its eigenvalues are roots of unity (this is certainly possible, since $\log |H \cap W_k| \sim k$). Arguing as in (i) and since case (12.3) was ruled out, we are in the situation (12.4) (in some local field K_w). Consider the representation on $\bigwedge^2(V \otimes K_w)$ as in (ii). Note that if $\mathfrak{X}$ is a subspace of $\bigwedge^2 V$ invariant under ρ_{g_1}, then its eigenvector $(e_3' \otimes e_1') \wedge (e_3' \otimes e_2')$ with top exponent will either be orthogonal to $\mathfrak{X}$ or belong to $\mathfrak{X} \otimes K_w$, hence to $\mathfrak{X}$.

Therefore, considering the decomposition (12.9), it follows that $(e_3' \otimes e_1') \wedge (e_3' \otimes e_2') = \eta$ belongs to one of the spaces $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{W}$. Also, by (12.7), $\mathcal{S}$ contains any element of the form $(x \otimes y) \wedge (x \otimes z)$ with $x, y, z \in k^3$ and $\langle x, y\rangle = 0 = \langle x, z\rangle$. In particular $\eta \in \mathcal{S}$ and it follows from (12.8) that $\mathcal{S}$ is contained in one of the spaces $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{W}$.

There are now three cases to consider.

Case I: $\mathcal{S} \subset \bigwedge^2 L$. Since $(x \otimes y) \wedge (x \otimes z) \in \bigwedge^2 L$ for all $x, y, z \in k^3$ with $\langle x, y\rangle = 0 = \langle x, z\rangle$, it follows that $x \otimes y \in L$ whenever $x, y \in k^3$ and $\langle x, y\rangle = 0$. Therefore $L = V$, a contradiction.

Case II: $\mathcal{S} \subset \bigwedge^2 L^\perp$. The same argument as in Case I applies.

Case III: $\mathcal{S} \subset L \wedge L^\perp$. Note that if $a, b \in V$ and $a \wedge b \in L \wedge L^\perp$, then L and $L^\perp$ each contain a nontrivial linear combination of a and b.

Assume $\dim L \le \dim L^\perp$, hence $\dim L \le 4$. Considering the sectors $(x \otimes y) \wedge (x \otimes z) \in L \wedge L^\perp$, it follows from the preceding that for each $x \in k^3$, there is some $x' \neq 0$ with $\langle x, x'\rangle = 0$ such that

$$x \otimes x' \in L. \tag{12.10}$$

Our next aim is to show that (12.10) forces $\dim L \ge 5$, hence again a contradiction.

Consider the real algebraic variety

$$\Omega = \{(x, y) \in \mathbb{C}^3 \times \mathbb{C}^3;\ \langle x, y\rangle = 0 \text{ and } x \otimes y \in L \otimes \mathbb{C}\} \tag{12.11}$$

(an intersection of quadrics).

By (12.10), we may introduce a real-analytic function $\varphi : O \to \mathbb{C}^3 \setminus \{0\}$, $O \subset \mathbb{C}^3$ some open set, such that for all $x \in O$,

(12.12) $\langle x, \varphi(x)\rangle = 0$,
(12.13) $x \otimes \varphi(x) \in L \otimes \mathbb{C}$.

We distinguish two further cases.

(a) *φ has 2-dim range (over $\mathbb{C}$).* If $\operatorname{Im}\varphi \subset [e_1, e_2]$, then necessarily, for $x = x_1e_1 + x_2e_2 + x_3e_3$, $\varphi(x)$ is parallel to $-\bar{x}_2e_1 + \bar{x}_1e_2$ by (12.12), implying

$$(x_1e_1 + x_2e_2 + x_3e_3) \otimes (-\bar{x}_2e_1 + \bar{x}_1e_2) \in L \otimes \mathbb{C} \tag{12.14}$$

for all $x \in O$ and hence for all $x \in \mathbb{C}^3$.

Since the functions $x_1^2, x_2^2, x_1x_2, x_1x_3, x_2x_3$ are linearly independent,

$$e_1 \otimes e_2, e_2 \otimes e_1, e_1 \otimes e_1 - e_2 \otimes e_2, e_3 \otimes e_2, e_3 \otimes e_1 \in L$$

and $\dim L \geq 5$.

(b) *φ has 3-dim range.* We may clearly find elements $x_1, x_2, x_3, x_4, x_5 \in O$ such that for each triplet $\{i, j, k\} \subset \{1, 2, 3, 4, 5\}$ of distinct integers, each of the systems $\{x_i, x_j, x_k\}$ and $\{\varphi(x_i), \varphi(x_j), \varphi(x_k)\}$ consists of linearly independent vectors.

We claim that $\{x_i \otimes \varphi(x_i);\ i = 1, \ldots, 5\}$ are linearly independent, which can be seen as follows. Fix an index $i = 1$. From our assumptions, there is $T \in \mathcal{L}(\mathbb{C}^3, \mathbb{C}^3)$ such that $Tx_2 = Tx_3 = 0$ and $\langle Tx_1, \varphi(x_1)\rangle \neq 0$, $\langle Tx_1, \varphi(x_4)\rangle = 0 = \langle Tx_1, \varphi(x_5)\rangle$. Hence

$$\langle Tx_2, \varphi(x_2)\rangle = 0 = \langle Tx_3, \varphi(x_3)\rangle$$

and writing

$$x_4 = a_4x_1 + b_4x_2 + c_4x_3, \qquad x_5 = a_5x_1 + b_5x_2 + c_5x_3,$$

we get

$$\langle Tx_4, \varphi(x_4)\rangle = a_4\langle Tx_1, \varphi(x_4)\rangle = 0 = \langle Tx_5, \varphi(x_5)\rangle.$$

This completes the proof of the main theorem for SU(3).

13. Lemmas on linear independence

Lemma 13.1. *Let $1 \leq k \leq d$ and $\varphi_1, \ldots, \varphi_k$ be continuous complex, linearly independent functions on $\mathbb{C}^d$. Then*

$$\dim[x_i\varphi_j(x);\ 1 \leq i \leq d \text{ and } 1 \leq j \leq k] \geq k\left(d - \frac{k-1}{2}\right), \tag{13.2}$$

where $x_i\varphi_j(x)$ are viewed as functions on $\mathbb{C}^d$.

Proof. The proof is by induction on d. Denote by $e_1, \ldots, e_d$ the unit vector basis of $\mathbb{C}^d$. Take $k_1 \leq k$. Since $\varphi_1, \ldots, \varphi_{k_1}$ are linearly independent functions, there are $\xi_1, \ldots, \xi_{k_1} \in \mathbb{C}^d$ such

$$\det[\varphi_j(\xi_{j'})]_{1\leq j, j'\leq k_1} \neq 0. \tag{13.3}$$

By a linear transformation, we may assume that $\xi_1, \ldots, \xi_{k_1} \in [e_1, \ldots, e_{k_1}]$ and hence $\varphi_j|_{[e_1,\ldots,e_{k_1}]}$ $(1 \leq j \leq k_1)$ are linearly independent.

We distinguish two cases.

Case 1: $k = d$. Taking $k_1 = d - 1$, we can assume that $\varphi_j|_{[e_1,\ldots,e_{d-1}]}(1 \leq j \leq d-1)$ are linearly independent. Denote $x' = x_1'e_1 + \cdots + x_{d-1}'e_{d-1}$.

From the induction hypothesis, there is a subset $\Omega \subset \{(i, j);\ 1 \leq i, j \leq d-1\}$ such that $|\Omega| \geq d(d-1)/2$ and $(x_i'\varphi_j(x'))_{(i,j)\in\Omega}$ are linearly independent functions of x'. We claim that

$$(x_i\varphi_j(x))_{(i,j)\in\Omega} \cup (x_d\varphi_j(x))_{1\leq j\leq d}$$

are linearly independent, which will imply that $\dim[x_i\varphi_j(x)] \geq d(d-1)/2 + d$.

Suppose the claim fails. Then there is a nontrivial linear combination

$$\sum_{(i,j)\in\Omega} a_{ij}x_i\varphi_j(x) + \sum_{j=1}^{d} a_{dj}x_d\varphi_j(x) = 0.$$

Setting $x_d = 0$, we get

$$\sum_{(i,j)\in\Omega} a_{ij}x_i'\varphi_j(x') = 0, \quad \text{hence} \quad a_{ij} = 0 \quad \text{for } (i,j) \in \Omega.$$

Therefore $x_d \sum_{j=1}^{d} a_{dj}\varphi_j(x) = 0$ and $\sum_{j=1}^{d} a_{dj}\varphi_j(x) = 0$, since the φ_j are continuous. Hence, also $a_{dj} = 0$, a contradiction.

Case 2: $k < d$**.** Take $k_1 = k$ and argue as above to obtain

$$\dim[x_i\varphi_j(x)] \geq k\left(d - 1 - \frac{k-1}{2}\right) + k = k\left(d - \frac{k-1}{2}\right).$$

This proves the lemma. □

Remark. The assumption that the φ_j are continuous in Lemma 13.1 cannot be dropped. Take, for instance, a basis $e_1, \ldots, e_d$ and define

$$\varphi_j(e_j) = 1, \quad \varphi_j(x) = 0 \quad \text{if } x \neq e_j.$$

Since $x_i\varphi_j = \delta_{ij}\varphi_j$, $\dim[x_i\varphi_j;\ 1 \leq i, j \leq d] = d$.

Lemma 13.4. *Let $1 \leq k \leq d-1$ and $\varphi : O \to G_{d,k}$, $O \subset \mathbb{C}^d$ some open set, a continuous map satisfying $\varphi(x) \subset [x]^\perp$. Then*

$$\dim[x \otimes \varphi(x);\ x \in O] \geq (k+1)d - 1. \tag{13.5}$$

Proof. One may clearly choose a subspace E of $\mathbb{C}^d$ such that $\dim E = d - k + 1$ and

(13.6) $\dim[\varphi(x) \cap E] = 1$,
(13.7) $\mathrm{Proj}_{E^\perp}\varphi(x) = E^\perp$,

for $x \in O$. Hence

$$\dim[x \otimes \varphi(x)] \geq \dim[x \otimes (\varphi(x) \cap E)] + \dim[x \otimes P_{E^\perp}\varphi(x)] = (13.8) + d(k-1).$$

Introduce a continuous function $\psi : O \to \mathbb{C}^d \setminus \{0\}$ such that $\psi(x) \in \varphi(x) \cap E$, hence $\langle x, \psi(x)\rangle = 0$. Since clearly $\dim[\psi_1, \ldots, \psi_d] \geq 2$, application of Lemma 13.1 with $k = 2$ gives

$$(13.8) \geq \dim[x \otimes \psi(x)] \geq 2k - 1$$

This proves Lemma 13.4.

14. Assumption ($*$) (general case)

Following the preceding analysis for $d = 3$, we may introduce the set $\mathcal{D}$ of all $(d_+, d_-) \in \{1, \dots, d-1\}^2$ for which there is $g \in \Gamma$ and a local field K_v such that the exponents of g may be ordered as

$$v(\lambda_1) = \cdots = v(\lambda_{d_+}) > v(\lambda_{d_++1}) \geq \cdots > v(\lambda_{d-d_-+1}) = \cdots = v(\lambda_d) \tag{14.1}$$

where $d_+, d_- < d$, as we assume $v(\lambda_i)$ $(1 \leq i \leq d)$ are not all equal and $d_+ + d_- \leq d$.

Fixing a configuration $(d_+, d_-) \in \mathcal{D}$, we obtain a proximal representation by considering the extension of the adjoint representation to the exterior power

$$\bigwedge^D (V \otimes K_v) \tag{14.2}$$

where $D = d_+ d_-$. The proximal vector is given by

$$\xi = \bigwedge_{\substack{1 \leq i \leq d_+ \\ d-d_- < j \leq d}} (e_i \otimes e_j) \tag{14.3}$$

in a suitable orthonormal basis $\{e_1, \dots, e_d\}$; the eigenvalue is $(\lambda_1/\lambda_d)^D$.

Denote

$$\mathcal{S} = \mathrm{span}_k[\rho_g(\xi);\ g \in \Gamma], \tag{14.4}$$

a subspace of $\bigwedge^D V$. Again from Zariski density of Γ in $\mathrm{SL}_d(\mathbb{C})$,

$$\mathcal{S} \otimes \mathbb{C} = \mathrm{span}_{\mathbb{C}}[\rho_g(\xi);\ g \in \mathrm{GL}_d(\mathbb{C})] \tag{14.5}$$

and Γ acts strongly irreducibly on $\mathcal{S}$.

From random matrix product theory, also

$$\mathcal{S} = \mathrm{span}[\rho_g(\eta);\ g \in H] \quad \text{for any } \eta \in \mathcal{S} \setminus \{0\} \tag{14.6}$$

provided H satisfies

$$\nu^{(k)}(H) > e^{-\varepsilon k} \tag{14.7}$$

with k large enough and ε small enough.

Assume we are given a nontrivial subspace L of V satisfying

$$\rho_g(L) = L \quad \text{for } g \in H. \tag{14.8}$$

The space $\bigwedge^D V$ decomposes as the direct sum

$$\bigwedge^{D_0} L \wedge \bigwedge^{D_1} L^\perp \tag{14.9}$$

where $D_0 + D_1 = D$. Note also that since L was obtained as complexification of a subspace of su(d), we have $L = L^*$.

Taking some element $g \in H$ which has the property that its eigenvalue quotients are not all roots of unity and considering an appropriate valuation, we obtain some type

$(d_+, d_-) \in \mathcal{S}$ with expanding vector $\eta \in \bigwedge^D V$ of the type (14.3). Note that we may always assume that $d_+ \geq d_-$ since g may be replaced by g^{-1}.

Since the components of the decomposition (14.9) are g-invariant, we conclude that

$$\eta \in \bigwedge^{D_0} L \wedge \bigwedge^{D_1} L^{\perp} \tag{14.10}$$

for some D_0, D_1 with $D = D_0 + D_1$. By (14.6),

$$\mathcal{S} \subset \bigwedge^{D_0} L \wedge \bigwedge^{D_1} L^{\perp}. \tag{14.11}$$

We also note that from (14.5), $\mathcal{S} \otimes \mathbb{C}$ contains any element of the form

$$\bigwedge_{\substack{1 \leq i \leq d_+ \\ 1 \leq j \leq d_-}} (x_i \otimes y_j) \tag{14.12}$$

where $\{x_1, \ldots, x_{d_+}, y_1, \ldots, y_{d_-}\}$ are orthogonal vectors in $\mathbb{C}^d$ (for the Hermitian inner product).

By (14.11), it follows that L (respectively $L^{\perp}$) will contain D_0 (respectively D_1) linearly independent elements from

$$\operatorname{span}[x_i \otimes y_j;\ 1 \leq i \leq d_+,\ 1 \leq j \leq d_-]. \tag{14.13}$$

Note that if $D_1 = 0$, then obviously L contains (14.13) and hence any element $x \otimes y$ with $\langle x, y \rangle = 0$. Thus $L = V = \{x \in \mathrm{Mat}_{d \times d}(\mathbb{C});\ \operatorname{Tr} x = 0\}$ would be trivial.

Hence we assume $D_0, D_1 \geq 1$.

It follows from (14.13) that, given orthogonal subspaces E_+, E_- of $\mathbb{C}^d$, $\dim E_+ = d_+$, $\dim E_- = d_-$,

$$\dim(L \cap (E_+ \otimes E_-)) + \dim(L^{\perp} \cap (E_+ \otimes E_-)) = \dim(E_+ \otimes E_-). \tag{14.14}$$

Hence

$$\dim \operatorname{Proj}_L(E_+ \otimes E_-) + \dim \operatorname{Proj}_{L^{\perp}}(E_+ \otimes E_-) = \dim(E_+ \otimes E_-). \tag{14.15}$$

Denoting $F_0 = \operatorname{Proj}_L(E_+ \otimes E_-)$, $F_1 = \operatorname{Proj}_{L^{\perp}}(E_+ \otimes E_-)$, clearly $E_+ \otimes E_- \subset F_0 + F_1$ and (14.15) implies $E_+ \otimes E_- = F_0 + F_1$. Therefore

$$\operatorname{Proj}_L(E_+ \otimes E_-) \subset E_+ \otimes E_-, \qquad \operatorname{Proj}_{L^{\perp}}(E_+ \otimes E_-) \subset E_+ \otimes E_-. \tag{14.16}$$

Next, let $x, y \in \mathbb{C}^d \setminus \{0\}$, $\langle x, y \rangle = 0$. From (14.16),

$$\operatorname{Proj}_L(x \otimes y) \in \bigcap_{\substack{x \in E_+ \\ y \in E_-}} (E_+ \otimes E_-) \equiv S_{x,y} \subset V. \tag{14.17}$$

Assume $d_+, d_- \geq 2$.

We claim that $S_{x,y} = [x \otimes y]$. For if $T \in S_{x,y}$, we have

$$\operatorname{Im} T \subset \bigcap E_-, \tag{14.18}$$

where E_- ranges over all d_--dimensional subspaces of $[x]^\perp$ such that $y \in E_-$. Since $d_+ \geq 2$ we have $d_- < d - 1$ and (14.18) $= [y]$.

Similarly, since $T^* \in \bigcap_{x \in E_+, y \in E_-} (E_- \otimes E_+)$, it follows that

$$(\operatorname{Ker} T)^\perp = \operatorname{Im} T^* \subset [x].$$

Hence $T \in [x \otimes y]$, proving the claim.

Thus

$$\operatorname{Proj}_L(x \otimes y) \in [x \otimes y] \quad \text{and} \quad \operatorname{Proj}_{L^\perp}(x \otimes y) \in [x \otimes y],$$

implying that

$$x \otimes y \in L \quad \text{if } \operatorname{Proj}_L(x \otimes y) \neq 0, \tag{14.19}$$

and similarly for $L^\perp$.

Fixing orthogonal vectors $e, e' \in \mathbb{C}^d \setminus \{0\}$, either $\operatorname{Proj}_L(e \otimes e') \neq 0$ or $\operatorname{Proj}_{L^\perp}(e \otimes e') \neq 0$. If $\operatorname{Proj}_L(e \otimes e') \neq 0$, clearly $\operatorname{Proj}_L(x \otimes y) \neq 0$ for $x \in U$, $y \in U'$, $\langle x, y \rangle = 0$, with U (resp. U') some neighborhood of e (resp e'). From (14.19),

$$(U \otimes U') \cap V \subset L, \tag{14.20}$$

which is easily seen to imply that $V = L$, a contradiction.

It remains to consider the case $d_+ = 1$ (and similarly $d_- = 1$).

Taking $E_+ = [x]$, $x \in \mathbb{C}^d \setminus \{0\}$, it follows from (14.14) that given any subspace E_- of $[x]^\perp$ with $\dim E_- = d_-$, there is a decomposition $E_- = W_0 + W_1$ such that $x \otimes W_0 \subset L$, $x \otimes W_1 \subset L^\perp$. Therefore clearly, for given $x \in \mathbb{C}^d \setminus \{0\}$,

$$\dim(L \cap (x \otimes [x]^\perp)) + \dim(L^\perp \cap (x \otimes [x]^\perp)) = d - 1. \tag{14.21}$$

Specifying $k_0 = \dim(L \cap (x \otimes [x]^\perp))$, $k_1 = \dim(L^\perp \cap (x \otimes [x]^\perp))$ for x restricted to some open subset $O \subset \mathbb{C}^d$, Lemma 13.4 in §13 implies

$$\dim L \geq (k_0 + 1)d - 1 \quad \text{and} \quad \dim L^\perp \geq (k_1 + 1)d - 1,$$

and hence, by (14.21),

$$d^2 - 1 \geq (d + 1)d - 2,$$

giving a contradiction and completing the proof of the main theorem.

Acknowledgments. The authors are grateful to Peter Sarnak for discussions relating to §10.

The first author was supported, in part, by NSF grants DMS-0808042 and DMS-0835373. The second author was supported, in part, by DARPA via AFOSR grant FA9550-08-1-0315, by NSF grant DMS-0645807, and by the Sloan Foundation.

References

[A] Aoun, R.: Random subgroups of linear groups are free. Duke Math. J. **160**, 117–173 (2011) Zbl pre05986341 MR 2838353

[BeY] Berenstein, C., Yger, A.: Effective Bezout identities in $\mathbb{Q}[z_1, \ldots, z_n]$. Acta Math. **166**, 69–120 (1991) Zbl 0724.32002 MR 1088983

[BL] Bougerol, P., Lacroix, J.: Products of Random Matrices with Applications to Schrödinger Operators. Birkhäuser, Boston (1985) Zbl 0572.60001 MR 0886674

[B1] Bourgain, J.: On the Erdős–Volkmann and Katz–Tao ring conjectures. Geom. Funct. Anal. **13**, 334–365 (2003) Zbl 1115.11049 MR 1982147

[B2] Bourgain, J.: The discretized sum-product and projection theorems. J. Anal. Math. **112**, 193–236 (2010) Zbl 1234.11012 MR 2763000

[BY] Bourgain, J., Yehudayoff, A.: Monotone expansion. Preprint (2011)

[BG] Bourgain, J., Gamburd, A.: On the spectral gap for finitely-generated subgroups of SU(2). Invent. Math. **171**, 83–121 (2008) Zbl 1135.22010 MR 2358056

[BG0] Bourgain, J., Gamburd, A.: Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. Ann. of Math. **167**, 625–642 (2008) Zbl 1216.20042 MR 2415383

[BG1] Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: I. J. Eur. Math. Soc. **10**, 987–1011 (2008) Zbl 1193.20059 MR 2443926

[BG2] Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: II. J. Eur. Math. Soc. **11**, 1057–1103 (2009) Zbl 1193.20060 MR 2538500

[BG3] Bourgain, J., Gamburd, A.: Spectral gaps in $\mathrm{SU}(d)$. C. R. Math. Acad. Sci. Paris **348**, 609–611 (2010) Zbl 1198.22006 MR 2358056

[BrGe] Breuillard, E., Gelander, T.: On dense free subgroups of Lie groups. J. Algebra **261**, 448–467 (2003) Zbl 1014.22007 MR 1966638

[BrGr] Breuillard, E., Green, B.: Approximate groups III: the unitary case. Preprint (2010)

[BGT] Breuillard, E., Green, B., Tao, T.: Approximate subgroups of linear groups. Geom. Funct. Anal. **21**, 774–819 (2011) Zbl 1229.20045 MR 2827010

[BS] Burger, M., Sarnak, P.: Ramanujan duals II. Invent. Math. **106**, 1–11 (1991) Zbl 0774.11021 MR 1123369

[DN] Dawson, C. M., Nielsen, M. A.: The Solovay–Kitaev algorithm. Quantum Inform. Comput. **6**, 81–95 (2006) Zbl 1152.81706 MR 2212257

[F] Furstenberg, H.: Noncommuting random products. Trans. Amer. Math. Soc. **108**, 377–428 (1963) Zbl 0203.19102 MR 0163345

[GJS] Gamburd, A., Jakobson, D., Sarnak, P.: Spectra of elements in the group ring of SU(2). J. Eur. Math. Soc. **1**, 51–85 (1999) Zbl 0916.22009 MR 1677685

[GH] Gill, N., Helfgott, H.: Growth of small generating sets in $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$. Int. Math. Res. Notices **2011**, 4226–4251 Zbl 1234.20059 MR 2836020

[GG] Goldsheid, I. Ya., Guivarc'h, Y.: Zariski closure and the dimension of the Gaussian law of the product of random matrices. I. Probab. Theory Related Fields **105**, 109–142 (1996) Zbl 0854.60006 MR 1389734

[GM] Goldsheid, I. Ya., Margulis, G. A.: Lyapunov exponents of a product of random matrices. Russian Math. Surveys **44**, no. 5, 11–71 (1989) Zbl 0705.60012 MR 1040268

[G] Guivarc'h, Y.: Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire. Ergodic Theory Dynam. Systems **10**, 483–512 (1990) Zbl 0715.60008 MR 1074315

[GR] Guivarc'h, Y., Raugi, A.: Propriétés de contraction d'un semi-groupe de matrices inversibles. Israel J. Math. **65**, 165–196 (1989) Zbl 0677.60007 MR 0998669

[H] Helfgott, H.: Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. of Math. (2) **167**, 601–623 (2008) Zbl 1213.20045 MR 2415382

[Hr] Hrushovski, E.: Stable group theory and approximate subgroups. J. Amer. Math. Soc. **25**, 189–243 (2012) Zbl pre06005474 MR 2833482

[J] Jordan, C.: Mémoire sur les équations différentielles linéaires à intégrale algébrique. J. Reine Angew. Math. **84**, 89–215 (1878) JFM 09.0234.01

[K] Kesten, H.: Symmetric random walks on groups. Trans. Amer. Math. Soc. **92**, 336–354 (1959) Zbl 0092.33503 MR 0109367

[PS] Pyber, L., Szabó, E.: Growth in finite simple groups of Lie type. Preprint (2010)

[R] Razborov, A.: A product theorem in free groups. Preprint (2007)

[SX] Sarnak, P., Xue, X.: Bounds for multiplicities of automorphic representations. Duke Math. J. **64**, 207–227 (1991) Zbl 0741.22010 MR 1131400

[S] Stein, E.: Singular Integrals and Differentiability Properties of Functions. Princeton Univ. Press (1970) Zbl 0207.13501 MR 0290095

[Tao] Tao, T.: Product set estimates for non-commutative groups. Combinatorica **28**, 547–594 (2008) Zbl pre05494691 MR 2501249

[Tits] Tits, J.: Free subgroups in linear groups. J. Algebra **20**, 250–270 (1972) Zbl 0236.20032 MR 0286898