TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 378, Number 4, April 2025, Pages 2363–2428
https://doi.org/10.1090/tran/9309
Article electronically published on January 30, 2025

RANDOM WALK ON GROUP EXTENSIONS

ALIREZA SALEHI GOLSEFIDY AND SRIVATSA SRINIVAS

Abstract. We study random walks on various group extensions. Under certain bounded generation and bounded scaled conditions, we estimate the spectral gap of a random walk on a quasi-random-by-nilpotent group in terms of the spectral gap of its projection to the quasi-random part. We also estimate the spectral gap of a random-walk on a product of two quasi-random groups in terms of the spectral gap of its projections to the given factors. Based on these results, we estimate the spectral gap of a random walk on the $\mathbb{F}_q$-points of a perfect algebraic group $\mathbb{G}$ in terms of the spectral gap of its projections to the almost simple factors of the semisimple quotient of $\mathbb{G}$. These results extend a work of Lindenstrauss and Varjú and an earlier work of the authors. Moreover, using a result of Breuillard and Gamburd, we show that there is an infinite set $\mathcal{P}$ of primes of density one such that, if k is a positive integer and $\mathbb{G} = \mathbb{U} \rtimes (\mathrm{SL}_2)^m_{\mathbb{Q}}$ is a perfect group and $\mathbb{U}$ is a unipotent group, then the family of all the Cayley graphs of $\mathbb{G}(\mathbb{Z}/\prod_{i=1}^k p_i\mathbb{Z})$, $p_i \in \mathcal{P}$, is a family of expanders.

Contents

1. Introduction and statement of main results

Suppose $X_1, X_2, \dots$ is a sequence of independent identically distributed (i.i.d.) random-variables with values in a finite group G and the probability law of X_i's is given by the probability measure μ. For a positive integer ℓ, an ℓ-step *random walk* on G with respect to the measure μ is given by

$$X^{(\ell)} := X_\ell X_{\ell-1} \cdots X_1.$$

Received by the editors January 6, 2023, and, in revised form, July 1, 2024.
2020 *Mathematics Subject Classification.* Primary 60B15, 05C48, 05C81, 60J10.
The first author was supported by the NSF grants 1602137, 1902090, 2302519.

The probability law of $X^{(\ell)}$ is given by the ℓ-fold convolution

$$\mu^{(\ell)} := \underbrace{\mu * \cdots * \mu}_{\ell \text{ times}}$$

of μ. In general, if X and Y are two independent random-variables with probability laws μ_X and μ_Y, respectively, then the probability law of XY is given by

$$(\mu_X * \mu_Y)(x) := \sum_{x' \in G} \mu_X(x')\mu_Y(x'^{-1}x).$$

We say a measure μ is *symmetric* if $\mu(x) = \mu(x^{-1})$ for every $x \in G$. We say a random-variable X is symmetric if its probability law is symmetric. Let

$$T_\mu : L^2(G) \to L^2(G), \quad T_\mu(f) := \mu * f.$$

When μ is a symmetric measure, T_μ is a self-adjoint operator, and so it has orthonormal basis with real eigenvalues. Moreover, considering $T_\mu(f) = \sum_{x \in G} \mu(x)\, x \cdot f$ where $(x \cdot f)(x') := f(x^{-1}x')$, we can see that T_μ is an averaging operator, and so its operator norm $\|T_\mu\|_{\mathrm{op}}$ is 1. Assuming the support μ generates G, no non-zero element in the space $L^2(G)^\circ$ of functions orthogonal to the constant functions is fixed by T_μ. We define the *spectral gap* of μ to be

$$\lambda(\mu) := \|T_\mu|_{L^2(G)^\circ}\|_{\mathrm{op}},$$

and inspired by the definition of the Lyapunov exponent, we let $\mathcal{L}(\mu) := -\log \lambda(\mu)$. For a random-variable X, we let $\lambda(X) := \lambda(\mu_X)$ and $\mathcal{L}(X) := \mathcal{L}(\mu_X)$, where μ_X is the probability law of X.

The main goal of this article is to start with a group extension

$$1 \to B \to G \xrightarrow{\pi} H \to 1$$

and a random-walk with respect to a random-variable X with values in G, and control the spectral gap $\lambda(X)$ in terms of group properties of H and B, and the spectral gap of properties of $\pi(X)$ (and if needed, the spectral gap of the induced random-walk on G/H). The first result of this type is due to Lindenstrauss and Varjú. In [24], they consider the following splitting short exact sequence

$$1 \to \mathbb{F}_p^n \to \mathrm{ASL}_n(\mathbb{F}_p) \xrightarrow{\pi} \mathrm{SL}_n(\mathbb{F}_p) \to 1,$$

and show that the following statement holds: *suppose X is a symmetric random-variable with values in $\mathrm{ASL}_n(\mathbb{F}_p)$ whose range generates $\mathrm{ASL}_n(\mathbb{F}_p)$. Suppose X is uniformly distributed on its range and its range has k_0 elements. Then $\mathcal{L}(X)$ has a positive lower bound which depends only on $\mathcal{L}(\pi(X))$, n, and k_0.* In the mentioned work, authors asked if a similar type of result holds for $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$. In [13], we give an affirmative answer to this question. Here, we give many results of this nature. In particular, we prove a generalization of Lindenstrauss-Varjú's result by studying quasi-random-by-nilpotent groups. Moreover, we generalize our earlier work from $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$ to a product of finite almost simple groups of Lie type.

We take an axiomatic approach and isolate certain group theoretic conditions for H and B, in order to be able to study a random-walk on an extension G of H by B. These conditions are labelled by (G1)-(G9) and have the following two main characteristics:

(1) (Bounded scaled) The maximum length of chain of normal subgroups is bounded; this means the given bound for $\mathcal{L}(X)$ (indirectly) depends on this number.
(2) (Bounded generation) For actions on various algebraic structures, we ask to obtain the smallest substructure which contains an element x using the orbit of x in *bounded number of steps*; again this means the given bound for $\mathcal{L}(X)$ depends on this number.

To go over our main results, we state these group theoretic conditions. These conditions and the results will be restated in the relevant sections. In what follows c, C_i's, m_0, and d_0 are positive numbers that we treat as constants. We refer the reader to Section 2 for the undefined notation.

(**G1**) H is a c-quasi-random group; that means $\deg \pi \geqslant |H|^c$ for every non-trivial representation π of H (see Section 2.3 for further discussion).
(**G2**) $|Z(H)| \leqslant \log |H|$, where $Z(H)$ is the center of H.
(**G3**) For every $x \in H$,

$$Z(H)(\textstyle\prod_{C_1} \mathrm{Cl}(x))(\prod_{C_1} \mathrm{Cl}(x))^{-1} \supseteq N_x,$$

where $\mathrm{Cl}(x)$ is the conjugacy class of x and N_x is the normal closure of the group generated by x; that means this is the smallest normal subgroup of H which contains x.
(**G4**) A is a $\mathbb{Z}[H]$-module where $\mathbb{Z}[H]$ is the group ring of H over $\mathbb{Z}$.
(**G5**) $|A| \leqslant |H|^{C_2}$.
(**G6**) For every $x \in A$,

$$\textstyle\prod_{C_3} \mathcal{O}_x \prod_{C_3} \mathcal{O}_x^{-1} = M_x,$$

where $\mathcal{O}_x$ is the H-orbit of x and M_x is the $\mathbb{Z}[H]$-submodule generated by x.
(**G7**) U is a finite nilpotent group of nilpotency class m_0.
(**G8**) There is a unital commutative ring R such that

$$L(U) := \bigoplus_{i=1}^{m_0} \gamma_i(U)/\gamma_{i+1}(U)$$

is a Lie algebra over R, where $\gamma_i(U)$ is the i-th lower central series of U. Moreover, $\gamma_1(U)/\gamma_2(U)$ can be generated by d_0 elements as an R-module.
(**G9**) The following is a short exact sequence

$$1 \to U \hookrightarrow G \xrightarrow{\pi} H \to 1,$$

and $G/\gamma_2(U)$ is c-quasi-random.

Theorem A (Product of quasi-random groups)**.** *Suppose H_L and H_R are two finite groups which satisfy* (G1)–(G3)*. Suppose*

$$C_4^{-1} \log |H_R| \leqslant \log |H_L| \leqslant C_4 \log |H_R|.$$

Suppose $X := (X_L, X_R)$ is a symmetric random-variable with values in $G := H_L \times H_R$ whose range generates G. Suppose there exist positive numbers c_0 and α_0 such

that

$$\mathcal{L}(X_L) \geqslant c_0, \quad \mathcal{L}(X_R) \geqslant c_0, \quad \text{and} \quad \mathbb{P}(X = x) \geqslant \alpha_0$$

for every x in the range of X. Then, $\mathcal{L}(X) \gg \min\{c_0, 1\}$, where the implied constant depends only on the given constants in (G1)–(G3).

Let's point out that $\mathrm{SL}_2(\mathbb{F}_p)$ satisfies (G1)–(G3). Therefore, the special case of Theorem A for $H_L = H_R = \mathrm{SL}_2(\mathbb{F}_p)$ gives an affirmative answer to the question of Lindenstrauss and Varjú; this case was discussed in the author's earlier work (see [13]).

Theorem B (Quasi-random-by-Abelian groups)**.** *Suppose H and A satisfy* (G1), (G4), (G5), *and* (G6). *Suppose G is an extension of H by A; that means there is a short exact sequence*

$$1 \to A \hookrightarrow G \xrightarrow{\pi} H \to 1.$$

Suppose Z is a symmetric random-variable with values in G whose range generates G. Suppose there exist positive numbers c_0 and α_0 such that

$$\mathcal{L}(\pi(Z)) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$ where the implied constant depends only on the given parameters c, C_i's given in (G4)–(G6), *and α_0.*

Since the pair of groups $H := \mathrm{SL}_n(\mathbb{F}_p)$ and $A := \mathbb{F}_p^n$ clearly satisfy conditions (G1) and (G4)-(G6), Theorem B is generalization of the mentioned result of Lindenstrauss and Varjú. We show that these conditions hold for $H := \mathbb{H}(F)$ and $A := \mathbb{V}(F)$ if $\mathbb{H}$ is a connected, simply-connected, semisimple F-group where F is a finite field of characteristic larger than the square of the dimension of $\mathbb{V}$ and $\mathbb{V}(F)$ does not have a non-zero $\mathbb{H}(F)$-fixed point (see Proposition 44). Hence, by Theorem B, we can control spectral gap of a random-walk on an H-by-A extension by the spectral gap of the projection to H. Notice, here, we do not assume that the given short exact sequence splits; therefore Theorem B can be applied to both of the following short exact sequences

$$1 \to \mathfrak{sl}_n(\mathbb{F}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_p) \to 1,$$

and

$$1 \to \mathfrak{sl}_n(\mathbb{F}_q) \to \mathrm{SL}_n(\mathbb{F}_q[t]/\langle t^2\rangle) \to \mathrm{SL}_n(\mathbb{F}_q) \to 1,$$

for every prime $p > (n^2-1)^2$ and every q which is a power of p.

It is worth pointing out that in [1], Alon, Lubotzky, and Wigderson studied random-walks in the finite group

$$K_p := \mathbb{F}_2^{p+1} \rtimes \mathrm{SL}_2(\mathbb{F}_p), \tag{1}$$

where p is a prime, $\mathbb{F}_2^{p+1}$ is identified with the set

$$\mathbb{F}_2^{\mathbb{P}^1(\mathbb{F}_p)} := \{f : \mathbb{P}^1(\mathbb{F}_p) \to \mathbb{F}_2\}$$

of functions from the $\mathbb{F}_p$-points of the projective line $\mathbb{P}^1$ to the finite field $\mathbb{F}_2$ with two elements, and $\mathrm{SL}_2(\mathbb{F}_p)$ acts on $\mathbb{F}_2^{\mathbb{P}^1(\mathbb{F}_p)}$ by left-translations. In [1, Theorem 4.2], it is proved that for every prime p, there is a symmetric random-variable Z_p with values in K_p such that

$$\mathcal{L}(\pi(Z_p)) \geqslant c_0, \quad \text{and} \quad \mathbb{P}(Z = z) = \frac{1}{8},$$

where c_0 is a fixed positive number and z is in the range of Z, and at the same time,

$$\mathcal{L}(Z_p) \leqslant -\log\left(1-\frac{2}{p+1}\right) \ll \frac{1}{p-1}.$$

This example shows the importance of the conditions (G5) and (G6).

Our next result together with Theorem B allows us to control the spectral gap of a random-walk on a quasi-random-by-nilpotent group.

Theorem C (Quasi-random-by-nilpotent)**.** *Let G be a finite group and U a normal subgroup of G. Suppose U is a nilpotent group which satisfies* (G7) *and* (G8)*. Suppose $G/\gamma_2(U)$ is c-quasi-random, where $\gamma_2(U)$ is the commutator subgroup of U. Let $\pi : G \to G/\gamma_2(U)$ be the natural quotient map. Suppose X is a symmetric random-variable with values in G, and $\mathcal{L}(\pi(X)) \geqslant c_0$ where c_0 is a positive number. Then $\mathcal{L}(X) \gg c_0$ where the implied constant depends only on the parameters m_0, d_0, and c.*

The following theorems can be viewed as sample results that can be obtained using Theorems A, B, and C. To formulate these theorems, we have to introduce a few notation.

Suppose $\mathbb{H}$ and $\mathbb{U}$ are subgroups of $(\mathrm{GL}_n)_{\mathbb{Q}}$ with the following properties:

(1) $\mathbb{H}$ is a connected, simply connected, semisimple group, and $\mathbb{H}_i$'s are its $\mathbb{Q}$-almost simple factors.
(2) $\mathbb{U}$ is a subgroup of the upper-triangular unipotent matrices.
(3) $\mathbb{G} := \mathbb{H} \ltimes \mathbb{U}$ is a perfect group.

Let $\underline{H}_i$, $\underline{U}$, and $\underline{G}$ be the closures of $\mathbb{H}_i$, $\mathbb{U}$, and $\mathbb{G}$ in $(\mathrm{GL}_n)_{\mathbb{Z}}$, respectively. Suppose $p_1, \dots, p_k$ are large enough primes, depending only on $\mathbb{G} \subseteq (\mathrm{GL}_n)_{\mathbb{Q}}$ (see Section 8 for a more precise information on how large p_i's should be). Suppose F_i is a finite field of characteristic p_i, and let $H_{i,j} := \underline{H}_i(F_j)$, $G := \underline{G}(\prod_{i=1}^k F_i)$, and $U := \underline{U}(\prod_{i=1}^k F_i)$. Then the following is a splitting short exact sequence

$$1 \to U \to G \to \oplus_{i,j} H_{i,j} \to 1,$$

where $\oplus_{i,j} H_{i,j}$ is the direct sum of these groups.

Theorem D (Perfect to simple factors: finite fields)**.** *In the setting of the previous paragraph, suppose $Z := (X_{1,1}, \dots, X_{s,k}, Y)$ is a symmetric random-variable with values in G where $X_{i,j}$ is a random-variable with values in $H_{i,j}$ and Y is a random-variable with values in U. Assume the range of Z generates G. Suppose c_0 and α_0 are positive numbers such that for every integer j in $[1,s]$ and i in $[1,k]$,*

$$\mathcal{L}(X_{j,i}) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$, where the implied constant depends on $\dim \mathbb{G}$*, k (number of fields), and α_0.*

Roughly, Theorem D states that the problem of understanding the spectral gap of a random-walk in the $\prod_{i=1}^k F_i$-points of a perfect group can be reduced to the one for the F_i-points of its almost simple factors. Next, we prove a similar result for the $\mathbb{Z}/q\mathbb{Z}$-points of a perfect group where q has a bounded number of prime factors.

Suppose $\underline{G}$ is as above, v_0 is a fixed positive integer, and q_{s} is a square-free positive integer such that $\gcd(q_{\mathrm{s}}, q_0) = 1$. Suppose p_i's are distinct prime factors of q_{s}. Let $q := q_{\mathrm{s}}^{v_0}$, $U_q := \underline{U}(\mathbb{Z}/q\mathbb{Z})$, $G_q := \underline{G}(\mathbb{Z}/q\mathbb{Z})$, $H_q := \underline{H}(\mathbb{Z}/q\mathbb{Z})$,

$H_{j,i} := \underline{H}_j(\mathbb{Z}/p_i^{v_0}\mathbb{Z})$, and $\overline{H}_{j,i} := \underline{H}_j(\mathbb{Z}/p_i\mathbb{Z})$. Then we get the following short exact sequences

$$1 \to U_q \to G_q \to \underbrace{\bigoplus_{j=1}^{s}\bigoplus_{i=1}^{k} H_{j,i}}_{H_q} \to 1,$$

and for every i and j

$$1 \to H_{j,i}[p_i] \to H_{j,i} \xrightarrow{\pi_{p_i}} \overline{H}_{j,i} \to 1,$$

where π_{p_i} is the residue modulo p_i map and $H_{j,i}[p_i]$ is its kernel.

Theorem E (Perfect to simple factors: bounded number of prime factors)**.** *Suppose G_q, H_q, $H_{j,i}$'s, and U_q are as in the setting in the previous paragraph. Suppose $Z := (X_{1,1}, \dots, X_{s,k}, Y)$ is a symmetric random-variable with values in G_q where $X_{j,i}$ is a random-variable with values in $H_{j,i}$ and Y is a random-variable with values in U_q. Assume the range of Z generates G. Suppose c_0 and α_0 are positive numbers such that for every integer j in $[1, s]$ and i in $[1, k]$,*

$$\mathcal{L}(\pi_{p_i}(X_{j,i})) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$ where the implied constant depends on $\dim \mathbb{G}$, k (number of prime factors), α_0, and v_0 (the power of prime factors).

Theorems D and E have immediate consequences on the study of *strong uniform expansion* in finite groups. For a finite group G which can be generated by k elements, let

$$\mathrm{gen}_k(G) := \{S \subseteq G \mid S = S^{-1}, S \text{ generates } G, |S| \leqslant 2k\},$$

and

$$\mathcal{L}_{G,k} := \min\{\mathcal{L}(U_S) \mid U_S \text{ is a uniform random-variable with values in } S, S \in \mathrm{gen}_k(G)\}.$$

The question of studying $\mathcal{L}_{G,k}$ is raised by Lubotzky and Weiss (see [26]). They ask the following basic question.

Question. Suppose $\{G_i\}_i$ is a family of finite groups and $S_i, S_i' \in \mathrm{gen}_k(G_i)$ for every i. Does $\inf_i \mathcal{L}(U_{S_i}) > 0$ imply $\inf_i \mathcal{L}(U_{S_i'}) > 0$, where U_S is a uniform random-variable with values in S?

In general, the answer to this question is negative. This was first showed in [1] using the concept of zig-zag product of graphs. In fact, Alon, Lubotzky, and Wigderson proved that there are $S_p, S_p' \in \mathrm{gen}_{16}(K_p)$, where K_p is the group given in (1), such that

$$\inf_p \mathcal{L}(U_{S_p}) > 0 \quad \text{and} \quad \inf_p \mathcal{L}(U_{S_p'}) = 0.$$

The family of symmetric groups is another example that provides a negative answer to the Lubotzky-Weiss Question. In his seminal work, Kassabov (see [20]) proved that there is an integer k and $S_n \in \mathrm{gen}_k(\mathrm{Sym}(n))$ where $\mathrm{Sym}(n)$ is the symmetric group such that $\inf_n \mathcal{L}(U_{S_n}) > 0$. It is easy to see that $\inf_n \mathcal{L}(U_{S_n'}) = 0$, where $S_n' := \{(1\,2), (1\,2\cdots n)^{\pm 1}\}$ (see [21, Proposition 3.5.8] or [8, §3, Ex. 1]). A first affirmative answer to the Lubotzky-Weiss question is given by Breuillard and

Gamburd (see [5]). They proved that there is a function $\varepsilon : \mathbb{R}^+ \to \mathbb{R}^+$ such that $\lim_{\delta\to 0} \varepsilon(\delta) = 0$ and the cardinality of

$$E_\delta(X) := \{p \leqslant X \mid \mathcal{L}_{\mathrm{SL}_2(\mathbb{F}_p),2} < \delta\} \tag{2}$$

is at most $X^{\varepsilon(\delta)}$. Let $E_\delta := \bigcup_{X=2}^{\infty} E_\delta(X)$. Using Theorem E and the mentioned result of Breuillard and Gamburd, we obtain Corollary F.

Corollary F (Strong uniform expansion)**.** *In the setting of Theorem* E*, for every positive integer* $s \geqslant 2$*,*

$$\mathcal{L}_{G_q,s} \gg \min\{\mathcal{L}_{\pi_{p_i}(H_{j,i}),s}\}_{i,j},$$

where the implied constant depends only on $\dim \mathbb{G}$*,* k *(number of prime factors),* s*, and* v_0*. In particular, if in the mentioned setting* $\mathbb{G} = (\mathrm{SL}_2)^m_{\mathbb{Q}} \ltimes \mathbb{U}$*, then for every* $\delta > 0$*,*

$$\inf\{\mathcal{L}_{G_q,2} \mid q = (p_1 \dots p_k)^{v_0}, p_i \in E_\delta\} > 0.$$

2. Notation and preliminary results

2.1. **Conventions.** For a finite group G, we endow $L^2(G)$ with the inner product

$$\langle f, g\rangle := \sum_{x\in G} \overline{f(x)} g(x),$$

where $f, g \in L^2(G)$. For $f \in L^2(G)$, $\check{f} \in L^2(G)$ is given by

$$\check{f}(x) := \overline{f(x^{-1})}.$$

Note that if X is a random variable with values in a group G and probability law μ, then the probability law of X^{-1} is $\check{\mu}$.

For a finite group G and $f, g \in L^2(G)$, the *convolution* of f and g is defined as follows

$$f * g(x) := \sum_{y\in G} f(y) g(y^{-1}x).$$

Suppose a finite group G acts on a finite set H. For a function $f \in L^2(G)$ and $g \in L^2(H)$, we let $\boxtimes : L^2(G) \times L^2(H) \to L^2(H)$ be

$$f \boxtimes g(x) := \sum_{y\in G} f(y) g(y^{-1} \cdot x)$$

for every $x \in H$. We call $\boxtimes$ the *convolution associated to* $G \curvearrowright H$.

For every finite set A, μ_A is the probability counting measure on A.

For a subset A of a finite group G and a positive integer k, we let

$$\textstyle\prod_k A = \{a_1 \dots a_k \mid a_i \in A\}.$$

For a random-variable X with finite range, the Rényi entropy of X is

$$H_2(X) := -\log\left(\sum_x \mathbb{P}(X = x)^2\right).$$

For a group U and a positive integer i, let $\gamma_i(U)$ be its i-th *lower central series*; that means $\gamma_1(U) := U$, and for every positive integer i, $\gamma_{i+1}(U) := [U, \gamma_i(U)]$ is the group generated by all the commutators $[x, y] := xyx^{-1}y^{-1}$ for $x \in U$ and $y \in \gamma_i(U)$. We say a group U is of *nilpotency class* m_0 if $\gamma_{m_0+1}(U) = 1$. For every group G, $G^{\mathrm{ab}} := G/[G, G]$ is the *Abelianization* of G.

2.2. **Entropy gain of Bourgain-Gamburd.** Bourgain and Gamburd in their seminal work [2] proved that multiplying two random-variables substantially increases the Rényi entropy unless there is an algebraic reason for it. The following is a formulation of their result (see [12, 31] or [13, Proposition 16]).

Proposition 1. *Let G be a finite group. Suppose X and Y are two independent random-variables with values in G, and $K \geqslant 2$. If*

$$H_2(XY) \leqslant \frac{H_2(X) + H_2(Y)}{2} + \log K,$$

then there are $A \subseteq G$ and a universal fixed positive number R with the following properties.

(1) (Approximate structure) *A is K^R-approximate subgroup; that means A is symmetric, $1 \in A$, and there is a subset B of $A \cdot A$ such that $|B| \leqslant K^R$ and $A \cdot A \subseteq A \cdot B \cap B \cdot A$.*
(2) (Controlling the size) *$|\log |A| - H_2(X)| \leqslant R \log K$.*
(3) (Almost equidistribution) *For every $a \in A$, $\mathbb{P}(X'X = a) \geqslant \frac{1}{K^R|A|}$ where X' is an independent random-variable whose distribution is identical with the distribution of X^{-1}.*

2.3. **Quasi-random groups and spectral gap.** For a finite group G, let $\widehat{G}$ be the set of irreducible unitary subrepresentations of the regular representation $L^2(G)$. For a positive number c, we say a finite group G is *c-quasi-random* if $\deg \pi \geqslant |G|^c$ for every non-trivial $\pi \in \widehat{G}$ (see [15]). Notice if every non-trivial (complex) representation of G is of dimension at least $|G|^c$. Hence if a c-quasi-random group G has a non-trivial action on a finite set X, then $|X| \geqslant |G|^c$ as the given action induces a (unitary) representation on $L^2(X)$. Therefore every proper subgroup H of G is of index at least $|G|^c$ as $G \curvearrowright G/H$ by left-translations.

For a symmetric measure μ on G, $T_\mu : L^2(G) \to L^2(G), T_\mu(f) := f * \mu$ is a self-adjoint operator, and $\lambda(\mu)$ is equal to the maximum of the absolute value of eigenvalues of $T_\mu|_{L^2(G)^\circ}$. Therefore for every positive integer ℓ,

$$\mathcal{L}(\mu^{(\ell)}) = \ell \mathcal{L}(\mu),$$

where $\mathcal{L}(\mu) = -\log \lambda(\mu)$. The following is a result of Gowers (see [13, Lemma 7] for the given formulation).

Proposition 2. *Suppose G is a c-quasi-random group where c is a positive number. Suppose X is a symmetric random variable with values in G. For a positive integer ℓ, let X_ℓ be an ℓ-step random walk with respect to X. If $H_2(X_{\ell_0}) \geqslant (1 - \frac{c}{2}) \log |G|$ for some positive integer $\ell_0 \leqslant C \log |G|$, then $\mathcal{L}(X) \geqslant \frac{c}{4C}$.*

Gowers also proved the following product result for large subsets of a quasi-random group.

Theorem 3. *Suppose G is a c-quasi-random group where c is a positive number. If A_1, A_2, A_3 are subsets of G and*

$$\frac{\log |A_1| + \log |A_2| + \log |A_3|}{3} \geqslant (1 - c/3) \log |G|,$$

then $A_1 \cdot A_2 \cdot A_3 = G$.

2.4. **Group action and spectral gap.** Suppose G is a finite group and H is a finite set, and G acts on H. For $f \in L^2(H)$ and $x \in G$, we let $(x \cdot f)(y) := f(x^{-1} \cdot y)$. Then $(x, f) \mapsto x \cdot f$ defines a group action of G on $L^2(H)$. The set of G-fixed points under this action is denoted by $L^2(H)^G$, and this is a subspace of $L^2(H)$. The function

$$\boxtimes : L^2(G) \times L^2(H) \to L^2(H), \quad f \boxtimes g := \sum_{y \in G} f(y)\, y \cdot g$$

is bilinear. If X is a random variable with values in G and probability law μ, and Y is a random variable with values in H and probability law η, then the probability law of $X \cdot Y$ is given by $\mu \boxtimes \eta$.

Then for $\mu, \nu \in L^2(G)$ and $f \in L^2(H)$, we have

$$\mu \boxtimes (\nu \boxtimes f) = (\mu * \nu) \boxtimes f.$$

By the discussion in [13, Section 2.3], we have the following result.

Lemma 4. *Suppose G is a finite group, H is a finite set, and G acts on H. Suppose μ is a probability measure on G and μ_G is the probability counting measure on G. Then the following statements hold.*

1. *For every $f \in L^2(H)$, $\mu_G \boxtimes f$ is the orthogonal projection of f to the space $L^2(H)^G$ of G-fixed functions.*
2. *For every $f \in L^2(H)$, we have*

$$\|(\mu - \mu_G) \boxtimes f\|_2 \leqslant \lambda(\mu)\|f\|_2.$$

3. Random walks induced by shifted-automorphism group actions

3.1. **Basics of shifted-automorphism group actions.** We say an action $G \curvearrowright H$ of a group G on a group H is a *shifted-automorphism* group action if there is a group homomorphism $\phi : G \to \mathrm{Aut}(H)$ and a function $c : G \to H$ such that

$$x \cdot y = c(x)(\phi(x))(y)$$

for every $x \in G$ and $y \in H$. We refer to $\phi(x)$ as the *automorphism part* of the action of x and to $c(x)$ as the *translation part* of the action of x (see [13, Section 3]).

In order to get a basic understanding of shifted-automorphism group actions, we recall the definition of the *holomorph of a group*. The holomorph of a group H is the semidirect product $H \rtimes \mathrm{Aut}(H)$ of H and its group of automorphisms $\mathrm{Aut}(H)$ where $\mathrm{Aut}(H)$ acts on H in the natural way, $\theta \cdot y := \theta(y)$. The holomorph of H is denoted by $\mathrm{Hol}(H)$. Lemma 5 gives us a basic characterization of shifted-automorphism actions.

Lemma 5. *For two groups G and H, the following statements hold.*

1. *The holomorph of H acts on H via $(y, \theta) \cdot y' := y\theta(y')$, and this is a shifted-automorphism group action.*
2. *An action $G \curvearrowright H$ is a shifted-automorphism group action if and only if there is a group homomorphism $f : G \to \mathrm{Hol}(H)$ such that $x \cdot y = f(x) \cdot y$ for every $x \in G$ and $y \in H$.*

Proof. For every $(y_1, \theta_1), (y_2, \theta_2) \in \mathrm{Hol}(H)$ and $y \in H$, we have

$$((y_1, \theta_1)(y_2, \theta_2)) \cdot y = (y_1\theta_1(y_2), \theta_1\theta_2) \cdot y = y_1\theta_1(y_2)\theta_1(\theta_2(y)), \tag{3}$$

and

$$(y_1, \theta_1) \cdot ((y_2, \theta_2)) \cdot y) = (y_1, \theta_1) \cdot (y_2\theta_2(y)) = y_1\theta_1(y_2\theta_2(y)) = y_1\theta_1(y_2)\theta_1\theta_2(y)). \tag{4}$$

By (3) and (4), we obtain that this map defines a group action, and clearly it is a shifted-automorphism action.

Suppose the action $G \curvearrowright H$ is a shifted-automorphism group action, its automorphism part is given by $\phi : G \to H$ and its translation part is given by $c : G \to H$. Let

$$f : G \to \mathrm{Hol}(H), \quad f(x) = (c(x), \phi(x)).$$

Then for every $x_1, x_2 \in G$ and $y \in H$, from $(x_1x_2) \cdot y = x_1 \cdot (x_2 \cdot y)$, we deduce that the following holds,

$$c(x_1x_2)\phi(x_1x_2)(y) = c(x_1)\phi(x_1)(c(x_2)\phi(x_2)(y)). \tag{5}$$

Letting $y = 1_H$ in (5), we obtain that

$$c(x_1x_2) = c(x_1)\phi(x_1)(c(x_2)) \tag{6}$$

for every $x_1, x_2 \in G$. From (6), it follows that f is a group homomorphism. Notice that for every $x \in G$ and $y \in H$, we have

$$x \cdot y = c(x)\phi(x)(y) = f(x) \cdot y.$$

The converse is clear. □

Lemma 6 gives us two important examples of shifted-automorphism actions that are of central importance in this work.

Lemma 6.

(1) *For every group H, the following map defines a transitive, shifted-automorphism group action $H \times H \curvearrowright H$, $(x_L, x_R) \cdot y := x_L y x_R^{-1}$. Moreover the automorphism and the translation parts of this action are given by $\phi(x_L, x_R)(y) = x_R y x_R^{-1}$ and $c(x_L, x_R) := x_L x_R^{-1}$, respectively.*

(2) *Suppose H and U are two groups, and $\phi : H \to \mathrm{Aut}(U)$ is a group homomorphism. Let $G := U \rtimes H$ be the semidirect product given by the homomorphism ϕ. Then the following map defines a transitive, shifted-automorphism group action $G \curvearrowright U$, $(u, y) \cdot u' := u\phi(y)(u')$.*

Proof. Proof is easy and left to reader. □

3.2. **Gowers's U^2-norm and shifted-automorphism actions.** Let us recall that for a group action $G \curvearrowright H$, a probability measure μ on G and $f, g \in L^2(H)$, $(\mu \boxtimes f)(y) := \int_G (x \cdot f)(y) d\mu(x)$ for every $y \in H$, and $f * g$ is the convolution of f and g.

In [13], a non-commutative version of Gowers's U^2-norm and its connection with random walks have been discussed. Here we recall some of the crucial results.

Lemma 7. *Suppose G and H are two finite groups and $G \curvearrowright H$ is a shifted-automorphism action. For $f \in L^2(H)$, let $\check{f}(h) := \overline{f(h^{-1})}$ and $|||f||| := \|\check{f} * f\|_2^{1/2}$. Then the following statements hold.*

(1) *$|||\cdot|||$ is a norm and $\|f\|_2 \leqslant |||f|||$ for every non-negative $f \in L^2(H)$.*

(2) *For every $x \in G$ and $f \in L^2(H)$, $|||x \cdot f||| = |||f|||$.*

(3) *For every probability measure μ on G and $f \in L^2(H)$, $|||\mu \boxtimes f||| \leqslant |||f|||$.*

Proof. See [13, Lemma 9]. □

The next lemmas help us compare the randomness gained by a shifted-automorphism action and its automorphism part. These results are essentially proved in [13, Lemma 4 and Corollary 11].

Lemma 8. *Suppose $G \curvearrowright H$ is a shifted-automorphism whose automorphism and translation parts are given by $\phi : G \to \mathrm{Aut}(H)$ and $c : G \to H$. Suppose $X^{(1)}, X^{(2)}$ are two i.i.d. random variables with values in G and $Y^{(1)}, Y^{(2)}$ are two i.i.d. with values in H. Then*

$$H_2((X^{(1)} \cdot Y^{(1)})^{-1}(X^{(2)} \cdot Y^{(2)})) \geqslant H_2(\phi(X^{(1)})({Y^{(1)}}^{-1}Y^{(2)})).$$

Proof. By [13, Lemma 4], we have

$$H_2((X^{(1)} \cdot Y^{(1)})^{-1}(X^{(2)} \cdot Y^{(2)})) \geqslant H_2((X^{(1)} \cdot Y^{(1)})^{-1}(X^{(1)} \cdot Y^{(2)})).$$

Notice that

$$\begin{aligned}(X^{(1)} \cdot Y^{(1)})^{-1}(X^{(1)} \cdot Y^{(2)}) &= (c(X^{(1)})\phi(X^{(1)})(Y^{(1)}))^{-1}(c(X^{(1)})\phi(X^{(1)})(Y^{(2)})) \\ &= \phi(X^{(1)})({Y^{(1)}}^{-1}Y^{(2)}),\end{aligned}$$

and the claim follows. □

We will be using the measure theoretic formulation of Lemma 8 which is given next.

Lemma 9. *Suppose $G \curvearrowright H$ is a shifted-automorphism action whose automorphism part is given by $\phi : G \to \mathrm{Aut}(H)$. Then for every probability measure η on H, the following holds*

$$\|\!|\mu \boxtimes \eta|\!\|^2 \leqslant \|\phi[\mu] \boxtimes (\check{\eta} * \eta)\|_2,$$

where the second $\boxtimes : L^2(\phi(G)) \times L^2(H) \to L^2(H)$ is given based on the automorphism action of $\phi(G)$ on H.

Proof. Let $X^{(1)}$, $X^{(2)}$, $Y^{(1)}$, and $Y^{(2)}$ be two independent random variables such that the probability law of $X^{(i)}$'s is μ and the probability law of $Y^{(i)}$'s is η. Then the probability law of

$$(X^{(1)} \cdot Y^{(1)})^{-1}(X^{(2)} \cdot Y^{(2)})$$

is $\widetilde{(\mu \boxtimes \eta)} * (\mu \boxtimes \eta)$, and the probability law of

$$\phi(X^{(1)})({Y^{(1)}}^{-1}Y^{(2)})$$

is $\phi[\mu] \boxtimes (\check{\eta} * \eta)$. Hence the claim follows from Lemma 8. □

The mentioned norm has another (rather easier) application which has been mentioned in [24, Lemma 5]. Here we quote the formulation presented in [13, Lemma 13]. This result roughly says that if $\check{\eta} * \eta$ is almost a point mass at the identity, then η is almost a point mass.

Lemma 10. *Suppose that η is a probability measure on a finite group H and $\|\eta\|_\infty < \kappa\|\eta\|_2$ where κ is a positive number less than $\sqrt{2}$. Then we have*

$$\|\!|\eta|\!\|^2 \geqslant \sqrt{2 - \kappa^2}\, \check{\eta} * \eta(1).$$

3.3. **Gaining initial entropy in a shifted-automorphism random-walk.** The main goal of this section is to prove Theorem 11.

Theorem 11. *Suppose G and H are finite groups, and G acts on H.*

(H1) (Action) *$G \curvearrowright H$ is a transitive shifted-automorphism action whose automorphism and translation parts are given by ϕ and c.*

(H2) (Automorphism action) *There is a positive number c such that for every $\phi(G)$-orbit $\mathcal{O} \subseteq H$ we have that either $\mathcal{O} = \{1\}$ or $|\mathcal{O}| \geqslant |H|^c > 2$.*

(H3) (Random-variable) *Suppose X is a symmetric random-variable with values in G whose range generates G, and for some positive numbers c_0 and α_0, we have*

$$\mathcal{L}(\phi(X)) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(X = x) \geqslant \alpha_0$$

for every x in the range of X.

Then there exist constants $L \gg_{c,c_0,\alpha_0} 1$ and $C \gg_{\alpha_0} 1$ such that for every random-variable Y which has values in H and is independent of X and every integer $\ell \geqslant L \log |H|$ we have

$$H_2(X_\ell \cdot Y) \geqslant \frac{c}{2} \log |H| - C,$$

where X_ℓ is an ℓ-step random-walk with respect to X.

A result of this type is proved for the affine action of $G := \mathrm{SL}_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ on $H := \mathbb{F}_p^n$ in [24, Theorem 2] and for the left-right action of $G := \mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)$ on $H := \mathrm{PSL}_2(\mathbb{F}_p)$ in [13, Lemma 5].

It is worth pointing out that if G is c-quasi-random, then

$$|G|^c \leqslant |H| \leqslant |G|$$

as $G \curvearrowright H$ is transitive. Moreover every $\phi(G)$-orbit in H with more than 1 element has at least $|G|^c$ many elements. Hence assuming G is c-quasi-random, we can replace the hypothesis (H2) with the following.

(H2') The only $\phi(G)$-fixed point in H is 1.

Here we present an almost identical argument as in the proof of [13, Lemma 5]. Only a few changes are needed.

Proof of Theorem 11. Choose $0 < \kappa_0 < 1$ such that $\sqrt{\alpha_0^2 + (1-\alpha_0)^2} + \sqrt{1-\kappa_0^2}$. Suppose η is the probability law of Y. We are going to consider two cases.

Case 1 (Suppose $\|\eta\|_\infty / \|\eta\|_2 > \kappa_0$). In this case, there is $x_0 \in G$ such that $\eta(x_0)^2 > \kappa_0^2 \|\eta\|_2^2$. Let $\eta_{x_0}^\perp := \eta \mathbb{1}_{G \setminus \{x_0\}}$ where $\mathbb{1}_{G\setminus\{x_0\}}$ is the characteristic function of $G\setminus\{x_0\}$. Since $\eta_{x_0}^\perp$ and μ_{x_0} are perpendicular and $\eta = \eta(x_0)\mu_{\{x_0\}} + \eta_{x_0}^\perp$, we have $\|\eta\|_2^2 = \eta(x_0)^2 + \|\eta_{x_0}^\perp\|_2^2$. Therefore

$$\|\eta_{x_0}^\perp\|_2^2 < (1-\kappa_0^2)\|\eta\|_2^2. \tag{7}$$

By (7), we obtain that

$$\begin{aligned} \|\mu \boxtimes \eta\|_2 &\leqslant \eta(x_0)\|\mu \boxtimes \mu_{\{x_0\}}\|_2 + \|\mu \boxtimes \eta_{x_0}^\perp\|_2 \leqslant \eta(x_0)\|\mu \boxtimes \mu_{\{x_0\}}\|_2 + \|\eta_{x_0}^\perp\|_2 \\ &\leqslant \eta(x_0)\|\mu \boxtimes \mu_{\{x_0\}}\|_2 + \sqrt{1-\kappa_0^2}\,\|\eta\|_2. \end{aligned} \tag{8}$$

Notice that

$$\mu \boxtimes \mu_{\{x_0\}} = \sum_{yG_{x_0} \in G/G_{x_0}} \mu(yG_{x_0})\, \mu_{\{y\cdot x_0\}}, \tag{9}$$

where G_{x_0} is the stabilizer subgroup of G with respect to x_0. Since there are no G-orbits of order 2 in H, by [13, Lemma 15], $\mu(yG_{x_0}) \neq 1$ for every y. Because the minimum of μ in its support is α_0, by (9) we deduce that

$$\|\mu \boxtimes \mu_{\{x_0\}}\|_2 \leqslant \sqrt{\alpha_0^2 + (1-\alpha_0)^2}. \tag{10}$$

Hence by (10) and (8), we obtain that

$$\|\mu \boxtimes \eta\|_2 \leqslant \left(\sqrt{\alpha_0^2 + (1-\alpha_0)^2} + \sqrt{1-\kappa_0^2}\right) \|\eta\|_2. \tag{11}$$

Case 2 (Suppose that $\|\eta\|_\infty / \|\eta\|_2 \leqslant \kappa_0$). Choose $0 < \kappa_1 < 1$ such that $(2-\kappa_0^2)^{-1/2} + 2\kappa_1 < 1$. Since $\mathcal{L}(\phi(X)) \geqslant c_0$, there is a positive integer ℓ_0 which is bounded by a function of c_0 and κ_1 such that $\lambda(\phi(X_{\ell_0})) < \kappa_1$ where X_{ℓ_0} is an ℓ_0-step random-walk with respect to X. Let $\nu := \mu^{(\ell_0)}$, and so $\lambda(\phi[\nu]) < \kappa_1$.

By Lemma 9, we obtain that

$$\|\!|\nu \boxtimes \eta|\!\|^2 \leqslant \|\phi[\nu] \boxtimes (\check{\eta} * \eta)\|_2 \leqslant \|(\phi[\nu] - \mu_{\phi(G)}) \boxtimes (\check{\eta} * \eta)\|_2 + \|\mu_{\phi(G)} \boxtimes (\check{\eta} * \eta)\|_2. \tag{12}$$

Therefore by (12) and Lemma 4, we deduce that

$$\|\!|\nu \boxtimes \eta|\!\|^2 \leqslant \kappa_1 \|\!|\eta|\!\|^2 + \|\mu_{\phi(G)} \boxtimes (\check{\eta} * \eta)\|_2. \tag{13}$$

Notice that $\{\sqrt{|\mathcal{O}|}\,\mu_{\mathcal{O}}\}_{\mathcal{O} \in {}_{\phi(G)}\backslash^H}$ is an orthonormal basis of the space $L^2(H)^{\phi(G)}$ of $\phi(G)$-invariant functions in $L^2(H)$ where ${}_{\phi(G)}\backslash^H$ is the set of $\phi(G)$-orbits in H. Hence by Lemma 4, we obtain

$$\mu_{\phi(G)} \boxtimes (\check{\eta} * \eta) = \sum_{\mathcal{O} \in {}_{\phi(G)}\backslash^H} |\mathcal{O}| \langle \mu_{\mathcal{O}}, \check{\eta} * \eta \rangle \mu_{\mathcal{O}} = \sum_{\mathcal{O} \in {}_{\phi(G)}\backslash^H} (\check{\eta} * \eta)(\mathcal{O})\, \mu_{\mathcal{O}}. \tag{14}$$

By (14), we have

$$\|\mu_{\phi(G)} \boxtimes (\check{\eta} * \eta)\|_2 \leqslant \sum_{\mathcal{O} \in {}_{\phi(G)}\backslash^H} (\check{\eta} * \eta)(\mathcal{O})\, \|\mu_{\mathcal{O}}\|_2. \tag{15}$$

By the hypothesis (H2), for every $\mathcal{O} \in {}_{\phi(G)}\backslash^H$, we have that either $\mathcal{O} = \{1\}$ or $|\mathcal{O}| \geqslant |H|^c$. Therefore by (15), we obtain

$$\|\mu_{\phi(G)} \boxtimes (\check{\eta} * \eta)\|_2 \leqslant \check{\eta} * \eta(1) + |H|^{-c/2}. \tag{16}$$

By (16), (13), and Lemma 10, we deduce that

$$\|\!|\nu \boxtimes \eta|\!\|^2 \leqslant \kappa_1 \|\!|\eta|\!\|^2 + (2-\kappa_0^2)^{-1/2} \|\!|\eta|\!\|^2 + |H|^{-c/2}. \tag{17}$$

Let $\beta := \max\{\sqrt{\alpha_0^2 + (1-\alpha_0)^2} + \sqrt{1-\kappa_0^2}, 2\kappa_1 + (2-\kappa_0^2)^{-1/2}\}$. By (11) and (17), at least one of the following three inequalities holds. Either

$$\|\nu \boxtimes \eta\|_2 \leqslant \beta \|\eta\|_2, \quad \text{or} \quad \|\!|\nu \boxtimes \eta|\!\|^2 \leqslant \beta \|\!|\eta|\!\|^2 \quad \text{or} \quad \|\!|\eta|\!\|^2 \leqslant \kappa_1^{-1} |H|^{-c/2}. \tag{18}$$

Applying (18) repeatedly, by part (3) of Lemma 5, we deduce that for every integer $\ell > 2c \log|H| / (-\log\beta)$ at least one of the following inequalities holds. Either

$$\|\nu^\ell \boxtimes \eta\|_2 \leqslant \beta^{\ell/2} \leqslant |H|^{-c} \quad \text{or} \quad \|\!|\nu^{(\ell)} \boxtimes \eta|\!\|^2 \leqslant \beta^{\ell/2} \leqslant |H|^{-c} \quad \text{or} \quad \|\!|\nu^{(\ell)} \boxtimes \eta|\!\|^2 \leqslant \kappa_1^{-1} |H|^{-c/2}. \tag{19}$$

By (19) and part (1) of Lemma 7, for every integer $\ell > \frac{2c}{-\log\beta} \log|H|$, the following holds

$$\|\nu^{(\ell)} \boxtimes \eta\|_2^2 \leqslant \kappa_1^{-1} |H|^{-c/2},$$

which means that for every integer $\ell > \frac{2\ell_0 c}{-\log\beta}\log|H|$

$$H_2(X_\ell \cdot Y) \geqslant \frac{c}{2}\log|H| + \log\kappa_1.$$

This finishes proof of Theorem 11.

□

4. Random-walk on the direct product of two groups

The main goal of this section is to prove that a random-walk on a product of groups has a spectral gap which depends on the spectral gap on each factor. This is proved under certain assumptions for the groups and the random-walk.

To make the presentation more clear, we list the needed assumptions for the involved groups here, and label them by (Gi)'s. Later, we verify that these statements hold for many families of groups that are of interest.

For a positive number c and a positive integer C_1, we formulate the following axioms for a group H.

(G1) H is a c-quasi-random group.

(G2) $|Z(H)| \leqslant \log|H|$, where $Z(H)$ is the center of H.

(G3) For every $x \in H$,

$$Z(H)(\prod_{\mathsf{C}_1}\mathrm{Cl}(x))(\prod_{\mathsf{C}_1}\mathrm{Cl}(x))^{-1} \supseteq N_x,$$

where $\mathrm{Cl}(x)$ is the conjugacy class of x and N_x is the normal closure of the group generated by x; that means this is the smallest normal subgroup of H which contains x.

Theorem 12. *Suppose c is a positive number, and C_1, C_2 are positive integers. Suppose H_L and H_R are two finite groups which satisfy* (G1)–(G3) *with constants c and C_1. Suppose*

$$\mathsf{C}_2{}^{-1}\log|H_R| \leqslant \log|H_L| \leqslant \mathsf{C}_2\log|H_R|.$$

Suppose $X := (X_L, X_R)$ is a symmetric random-variable with values in $G := H_L \times H_R$ whose range generates G. Suppose there exist positive numbers c_0 and α_0 such that

$$\mathcal{L}(X_L) \geqslant c_0, \quad \mathcal{L}(X_R) \geqslant c_0, \quad \text{and} \quad \mathbb{P}(X = x) \geqslant \alpha_0 \tag{20}$$

for every x in the range of X. Then, $\mathcal{L}(X) \gg \min\{c_0, 1\}$, where the implied constant only depends on $c, \mathsf{C}_1, \mathsf{C}_2, \alpha_0$.

4.1. **Random-walk with respect to couplings of almost Haar measures.** To prove Theorem 12, we notice that after an $O_{c_0}(\log|H|)$-step random-walk, we get a random-variable (Y_L, Y_R) such that the probability laws of Y_L and Y_R are close to the probability counting measure of H. The main goal of this section is to investigate what happens if after one step under a random-walk with respect to such a random-variable (Y_L, Y_R) we do not gain a *substantial amount of entropy.*

Lemma 13. *Suppose c is a positive number, and $\mathsf{C}_1, \mathsf{C}_2$ are positive integers. Suppose H_L and H_R are two finite groups which satisfy* (G1)–(G3) *with constants c and C_1. Suppose*

$$\mathsf{C}_2{}^{-1}\log|H_R| \leqslant \log|H_L| \leqslant \mathsf{C}_2\log|H_R|. \tag{21}$$

Suppose $Y := (Y_L, Y_R)$ is a symmetric random-variable with values in $H_L \times H_R$.

Suppose ε is a positive number and Y satisfies the following properties.

(1) (Coupling of almost Haar measures) *For every $y_L \in H_L$ and $y_R \in H_R$, we have*
$$\mathbb{P}(Y_L = y_L) \leqslant 2|H_L|^{-1} \quad \text{and} \quad \mathbb{P}(Y_R = y_R) \leqslant 2|H_R|^{-1}.$$
(2) (Room for improvement) $H_2(Y) \leqslant (1-\varepsilon)\log|H_L \times H_R|$.

Then there is a positive number γ_0 which depends on ε, c, C_1, and C_2, such that for every $\gamma \leqslant \gamma_0$ at least one of the following statements holds.

(1) (Gaining entropy) $H_2(Y_2) \geqslant H_2(Y) + \gamma \log|H_L \times H_R|$, *where Y_2 is a 2-step random-walk with respect to Y.*
(2) (Graph of an automorphism) *There are proper normal subgroups Z_L and Z_R of H_L and H_R, respectively such that $Z(H_L/Z_L) = \{1\}$, $Z(H_R/Z_R) = \{1\}$, and there exists an isomorphism $\theta : H_L/Z_L \to H_R/Z_R$ such that*
$$\mathbb{P}(\pi_{Z_L \times Z_R}(Y_2) \in \Gamma_\theta) \geqslant |H_L \times H_R|^{-R\gamma},$$
where $\pi_{Z_L \times Z_R} : H_L \times H_R \to H_L/Z_L \times H_R/Z_R$ is the natural quotient map, Γ_θ is the graph of the isomorphism θ, and R is a fixed absolute constant.
(3) (Small cases) $|H_L \times H_R| < \mathsf{C}_3$ *where C_3 is a positive integer which depends on ε, c, C_1, and C_2.*

We follow the same line of argument as in the proof of [13, Lemma 17]. Before we get to the proof of Lemma 13, we prove a lemma on c-quasi-random groups.

Lemma 14. *Suppose c is a positive number and G is a c-quasi-random group. Suppose S is a subset of G and the normal closure of the group generated by S is G; that means the smallest normal subgroup of G which contains S is G. Then there is a subset $\overline{S}$ of S such that $|\overline{S}| \leqslant 1/c$ and the normal closure of the subgroup generated by $\overline{S}$ is G.*

Proof. For every subset S' of G, let $N_{S'}$ be the smallest normal subgroup of G which contains S' as a subset. Let $\Sigma := \{S' \subseteq S \,|\, N_{S'} = G\}$, and suppose $\overline{S}$ is an element of Σ with the smallest number of elements among the elements of Σ. Suppose
$$\overline{S} = \{x_1, \dots, x_n\},$$
and $|\overline{S}| = n$. Let $N_0 := \{1\}$ and $N_i := N_{\{x_1,\dots,x_i\}}$ for every $1 \leqslant i \leqslant n$.

Claim. In the above setting $[N_{i+1} : N_i] \geqslant |G|^c$ for every $0 \leqslant i \leqslant n-1$.

Proof of Claim. Suppose to the contrary that $[N_{i+1} : N_i] < |G|^c$ for some i. Notice that G acts by conjugation on N_{i+1}/N_i, and this action induces a unitary representation on $L^2(N_{i+1}/N_i)$. Since G is c-quasi-random and $\dim L^2(N_{i+1}/N_i) < |G|^c$, we deduce that the G-action on N_{i+1}/N_i is a trivial action. Hence, N_{i+1}/N_i is a subset of the center $Z(G/N_i)$ of G/N_i. Let
$$\overline{N} := N_{\overline{S}\setminus\{x_{i+1}\}},$$
and notice that $G = N_{i+1}\overline{N}$ and $N_i \subseteq \overline{N}$. Therefore, $G/\overline{N}$ is isomorphic to a quotient of N_{i+1}/N_i and a quotient of G; in fact, we have
$$G/\overline{N} \simeq N_{i+1}/N_{i+1} \cap \overline{N} \quad \text{and} \quad N_i \subseteq N_{i+1} \cap \overline{N}.$$
Hence $G/\overline{N}$ is both Abelian and perfect (as it has no non-trivial degree 1 representation). Therefore $G = \overline{N}$. This means $S\setminus\{x_{i+1}\} \in \Sigma$, which contradicts the

assumption that every element of Σ has at least n elements. This finishes proof of the claim. □

By the above claim, we obtain that $|G| = \prod_{i=0}^{n-1}[N_{i+1} : N_i] \geqslant |G|^{nc}$, and so $n \leqslant 1/c$. This finishes the proof. □

Proof of Lemma 13. Suppose γ is a sufficiently small positive number to be specified later, and $|H_L \times H_R| \geqslant \mathsf{C}_3$ for a large enough constant C_3 to be specified later. Let's assume that we do not *gain enough entropy*; that means $H_2(Y_2) < H_2(Y) + \gamma \log|H_L \times H_R|$. Then by Proposition 1, there is an $|H_L \times H_R|^{R\gamma}$-approximate subgroup A of $H_R \times H_L$ such that

$$|\log|A| - H_2(Y)| \leqslant R\gamma \log|H_L \times H_R| \quad \text{and} \quad \mathbb{P}(Y_2 \in A) \geqslant |H_L \times H_R|^{-R\gamma}. \tag{22}$$

By the *coupling of almost Haar measures* condition, we have that

$$\mathbb{P}((Y_L)_2 \in \mathrm{pr}_L(A)) \leqslant 2\frac{|\pi_L(A)|}{|H_L|} \quad \text{and} \quad \mathbb{P}((Y_R)_2 \in \mathrm{pr}_L(A)) \leqslant 2\frac{|\pi_R(A)|}{|H_R|}, \tag{23}$$

where π_L and π_R are projections to the *left* and the *right* components. By the second inequality in (22) and (23), we obtain that

$$|H_L \times H_R|^{-R\gamma} \leqslant \mathbb{P}(Y_2 \in A) \leqslant \mathbb{P}((Y_L)_2 \in \pi_L(A)) \leqslant \frac{2|\pi_L(A)|}{|H_L|}, \tag{24}$$

and

$$|H_L \times H_R|^{-R\gamma} \leqslant \mathbb{P}(Y_2 \in A) \leqslant \mathbb{P}((Y_R)_2 \in \pi_R(A)) \leqslant \frac{2|\pi_R(A)|}{|H_R|}. \tag{25}$$

Inequalities given in (24), (25), and (21) imply that

$$|\pi_L(A)| \geqslant |H_L||H_L|^{-\mathsf{C}_2R\gamma}|H_L|^{-2R\gamma} = |H_L|^{1-(\mathsf{C}_2R-2R)\gamma} \tag{26}$$

and

$$|\pi_R(A)| \geqslant |H_R|^{1-(\mathsf{C}_2R-2R)\gamma}, \tag{27}$$

if $|H_L|^{R\gamma} \geqslant 2$ and $|H_R|^{R\gamma} \geqslant 2$. If $\gamma < c/(3(\mathsf{C}_2R - 2R))$, then by Theorem 3, we deduce that

$$\pi_L(\textstyle\prod_3 A) = H_L \quad \text{and} \quad \pi_R(\prod_3 A) = H_R. \tag{28}$$

Claim. In the above setting, for a small enough γ depending on $\varepsilon, c, \mathsf{C}_1, \mathsf{C}_2$, if $|H_L \times H_R|^{\varepsilon}$ is more than $(\log|H_L|\log|H_R|)^8$, then there are proper normal subgroups $N_L \trianglelefteq H_L$ and $N_R \trianglelefteq H_R$ such that

$$(\textstyle\prod_9 A) \cap (H_L \times Z(H_R)) \subseteq N_L \times Z(H_R)$$
$$\text{and} \quad (\prod_9 A) \cap (Z(H_L) \times H_R) \subseteq Z(H_L) \times N_R.$$

Moreover $Z(H_L) \subseteq N_L$ and $Z(H_R) \subseteq N_R$.

Proof of Claim. By symmetry, it is enough to prove only one of the inclusions. Suppose to the contrary that the normal closure of $\pi_L\big(\prod_9 A \cap (H_L \times Z(H_R))\big)$ is H_L. Then by Lemma 14, there is a subset $\{x_1, \dots, x_n\}$ of $\pi_L\big(\prod_9 A \cap (H_L \times Z(H_R))\big)$ such that $n \leqslant 1/c$ and

$$N_{x_1}N_{x_2}\cdots N_{x_n} = H_L, \tag{29}$$

where N_{x_i} is the smallest normal subgroup of H_L that contains x_i. For every i, there is $e_i \in Z(H_R)$ such that

$$(x_i, e_i) \in \prod_9 A.$$

By (28), for every $h_L \in H_L$, there is an element (h_L, h_R) in $\prod_3 A$. Hence

$$(h_L x_i h_L^{-1}, e_i) = (h_L, h_R)(x_i, e_i)(h_L, h_R)^{-1} \in \prod_{15} A,$$

and so

$$\mathrm{Cl}(x_i) \times Z(H_L) \subseteq \left(\prod_{15} A\right) Z(H_R \times H_L) \tag{30}$$

for every i. By the (G3) condition, (29), and (30), we obtain that

$$H_L \times Z(H_R) \subseteq \left(\prod_{30\mathsf{C}_1\lfloor 1/c\rfloor} A\right) Z(H_R \times H_L). \tag{31}$$

By (28) and (31), we obtain that

$$H_L \times H_R = \left(\prod_{30\mathsf{C}_1\lfloor 1/c\rfloor+3} A\right) Z(H_R \times H_L). \tag{32}$$

By (32), the fact that A is $|H_L \times H_R|^{R\gamma}$-approximate subgroup, and (G2) condition, it follows that

$$\frac{|H_L \times H_R|}{\log|H_L|\log|H_R|} \leqslant \left|\prod_{30\mathsf{C}_1\lfloor 1/c\rfloor+3} A\right| \leqslant |H_L \times H_R|^{R(30\mathsf{C}_1/c+2)\gamma}|A|. \tag{33}$$

On the other hand, by the condition on *Room for improvement* and (22), we have that

$$|A| \leqslant |H_L \times H_R|^{1-\varepsilon+R\gamma}; \tag{34}$$

and so for $\gamma < \varepsilon/(2R)$, by (33) and (34), we obtain that

$$(\log|H_L|\log|H_R|)^{-1} \leqslant |H_L \times H_R|^{R(30\mathsf{C}_1/c+2)\gamma-\varepsilon/2}. \tag{35}$$

Therefore, if $\gamma < \varepsilon/(4R(30\mathsf{C}_1/c+2))$ and $|H_L \times H_R|^{\varepsilon} > (\log|H_L|\log|H_R|)^8$, (35) gives us a contradiction. To finish proof of *Claim*, it is enough to notice that $Z(H_L)N_L$ is still a proper normal subgroup of H_L (as H_L is a perfect group and $Z(H_L)N_L/N_L$ is an Abelian group), and similarly $Z(H_R)N_R$ is a proper normal subgroup of H_R. □

By (28), there are functions $f_R : H_L \to H_R$ and $f_L : H_R \to H_L$ such that

$$\{(x_L, f_R(x_L))\,|\,x_L \in H_L\} \subseteq \prod_3 A \quad \text{and} \quad \{(f_L(x_R), x_R)\,|\,x_R \in H_R\} \subseteq \prod_3 A. \tag{36}$$

By *Claim* and (36), we obtain that

$$\overline{f}_R : H_L/Z(H_L) \to H_R/N_R,\ \overline{f}_R(x_L Z(H_L)) := f_R(x_L)N_R$$

is a group homomorphism, and for every $x_R \in H_R$

$$\overline{f}_R(f_L(x_R)Z(H_L)) = x_R N_R.$$

Moreover, if $(x_L, x_R) \in \prod_3 A$, then $\overline{f}_R(x_L Z(H_L)) = x_R N_R$. Let M_L be the normal subgroup of H_L such that $M_L/Z(H_L) = \ker \overline{f}_R$, and

$$\widetilde{\theta} : H_L/M_L \to H_R/N_R, \quad \theta(x_L M_L) := \overline{f}_R(x_L Z(H_L)).$$

Then $\widetilde{\theta}$ is an isomorphism, M_L is a proper normal subgroup of H_L which contains $Z(H_L)$, and

$$\pi_{M_L \times N_R}\left(\prod_3 A\right) = \Gamma_{\widetilde{\theta}}, \tag{37}$$

where $\pi_{M_L\times N_R} : H_L \times H_R \to H_L/M_L \times H_R/N_R$ is the natural quotient map and Γ_θ is the graph of the isomorphism θ. By (22), we obtain that

$$\mathbb{P}(\pi_{M_L\times N_R}(Y_2) \in \Gamma_{\widetilde{\theta}}) \geqslant |H_L \times H_R|^{-R\gamma}. \tag{38}$$

Let Z_L be the normal subgroup of H_L such that $Z_L/M_L = Z(H_L/M_L)$. Notice that $H := H_L/M_L$ is a perfect group (as the quasi-randomness implies that there is no non-trivial degree 1 representation). Hence, by Grün's lemma,

$$Z(H_L/Z_L) \simeq Z(H/Z(H)) = \{1\}.$$

Let Z_R be the normal subgroup of H_R such that $Z_R/N_R = Z(H_R/N_R)$. Then

$$\theta : H_L/Z_L \to H_R/Z_R \quad \theta(x_L Z_L) := \widetilde{\theta}(x_L M_L) Z_R$$

is a well-defined isomorphism. By (37) and (38), we conclude that

$$\pi_{Z_L\times Z_R}(\textstyle\prod_3 A) = \Gamma_\theta \quad \text{and} \quad \mathbb{P}(\pi_{Z_L\times Z_R}(Y_2) \in \Gamma_\theta) \geqslant |H_L \times H_R|^{-R\gamma}.$$

This finishes the proof. □

4.2. **Spectral gap for a random-walk in a product of two groups: Proof of Theorem 12.** Suppose $\overline{L} := L(c, c_0, \alpha_0)$ and $C := C(\alpha_0)$ are the constants that we obtain from Theorem 11. Let ℓ_0 be the smallest integer which is at least

$$\max\{\overline{L}\log|H_L|, \overline{L}\log|H_R|, 2c_0^{-1}\log|H_L|, 2{c_0}^{-1}\log|H_R|\}.$$

For every non-negative integer i, let $Y^{(i)} := X_{2^i\ell_0}$ be a $2^i\ell_0$-step random-walk with respect to X. Then by the Cauchy-Schwarz inequality, part (2) of Lemma 4, and $\mathcal{L}(X) \geqslant c_0$, we obtain that

$$\begin{aligned}
\|\operatorname{pr}_L[\mu]^{(2^i\ell_0)} - \mu_{H_L}\|_\infty &= \|((\operatorname{pr}_L(\mu)^{(\ell_0)} - \mu_{H_L}) * \mu_{\{1\}}) * \mu_{\{1\}}\|_\infty \\
&\leqslant \|(\operatorname{pr}_L(\mu)^{(2^i\ell_0)} - \mu_{H_L}) * \mu_{\{1\}})\|_2 \\
&\leqslant \lambda(\mu)^{2^i\ell_0} \leqslant 2^{-\ell_0\mathcal{L}(\mu)} \leqslant |H_L|^{-2}.
\end{aligned} \tag{39}$$

By (39) and its similar result for the right component, we deduce that

$$|\mathbb{P}(Y_L^{(i)} = y_L) - |H_L|^{-1}| \leqslant |H_L|^{-2} \quad \text{and} \quad |\mathbb{P}(Y_R^{(i)} = y_R) - |H_R|^{-1}| \leqslant |H_R|^{-2} \tag{40}$$

for every $y_L \in H_L$ and $y_R \in H_R$ where $(Y_L^{(i)}, Y_R^{(i)}) = Y^{(i)}$.

Claim 1. For every positive integer i, every proper normal subgroup Z_L and Z_R of H_L and H_R, respectively such that $Z(H_L/Z_L)$ and $Z(H_R/Z_R)$ are trivial and there is an isomorphism $\theta : H_L/Z_L \to H_R/Z_R$, we have that either

$$\mathbb{P}(\pi_{Z_L\times Z_R}(Y^{(i)}) \in \Gamma_\theta) < |H_L \times H_R|^{-\frac{c^2}{8(1+\mathsf{C}_2)}}$$

or $|H_L| \ll_{c,\alpha_0} 1$.

Proof of Claim 1. Proof of Claim 1 is based on Theorem 11. Let $\overline{H} := H_L/Z_L$ and $G := \overline{H} \times \overline{H}$. Consider the left-right action of G on $\overline{H}$; that means $(x_1, x_2) \cdot x := x_1 x x_2^{-1}$. By Lemma 6, this is a transitive shifted-automorphism action, and its automorphism part is given by

$$\phi : G \to \operatorname{Aut}(\overline{H}), \quad \phi(x_1, x_2)(y) := x_2 y x_2^{-1}.$$

Notice that $y \in \overline{H}$ is a $\phi(G)$-fixed point if and only if $y \in Z(\overline{H})$. Therefore, the only $\phi(G)$-fixed point in $\overline{H}$ is $\{1\}$.

Notice that every $\phi(G)$-orbit is an H_R-orbit where H_R acts by conjugation on H_R/Z_R. Since H_R is c-quasi-random, every non-trivial H_R-orbit has at least $|H_R|^c$ elements.

Let $\psi : H_L \times H_R \to G, \quad \psi(x_L, x_R) := (\pi_{Z_L}(x_L), \theta^{-1}(\pi_{Z_R}(x_R)))$. Notice that ψ is a surjective group homomorphism. Let $\overline{X} := \psi(X)$. Since X is symmetric, so is $\overline{X}$. Since $Z(\overline{H})$ is trivial, $\phi(G) \simeq \overline{H}$ and

$$\mathcal{L}(\phi(\overline{X})) = \mathcal{L}(\theta^{-1}(\pi_{Z_R}(X_R))) = \mathcal{L}(\pi_{Z_R}(X_R)) \geqslant \mathcal{L}(X_R) \geqslant c_0. \tag{41}$$

We also notice that for every $x \in H_L \times H_R$, $\mathbb{P}(\psi(X) = \psi(x)) \geqslant \mathbb{P}(X = x)$, and so

$$\mathbb{P}(\overline{X} = \overline{x}) \geqslant \alpha_0 \tag{42}$$

for every $\overline{x}$ in the range of $\overline{X}$. By the above discussion, (41), and (42), we can apply Theorem 11 for the group G, its action on $\overline{H}$, and the random-variable $\overline{X}$. Hence,

$$H_2(\overline{X}_{2^i\ell_0} \cdot Z) \geqslant \frac{c}{2} \log|\overline{H}| - C \tag{43}$$

for every non-negative integer i, where $C := C(\alpha_0)$ is the constant given by Theorem 11 and Z is a random-variable with values in $\overline{H}$ such that $\mathbb{P}(Z = 1) = 1$. Since H_L is c-quasi-random and $\overline{H}$ is a non-trivial quotient of H_L, we have $|\overline{H}| \geqslant |H_L|^c$. If $|H_L| \gg_{c,\alpha_0} 1$, then by (43) we have

$$H_2(\overline{X}_{2^i\ell_0} \cdot Z) \geqslant \frac{c^2}{4} \log|H_L|. \tag{44}$$

Notice that

$$\mathbb{P}(\overline{X}_{2^i\ell_0} \cdot Z = 1) = \mathbb{P}(\pi_{Z_L \times Z_R}(Y^{(i)}) \in \Gamma_\theta) \quad \text{and} \quad \mathbb{P}(\overline{X}_{2^i\ell_0} \cdot Z = 1) \leqslant 2^{-\frac{1}{2}H_2(\overline{X}_{2^i\ell_0} \cdot Z)}. \tag{45}$$

Therefore, by (44), (45), and (21), we obtain that

$$\mathbb{P}(\pi_{Z_L \times Z_R}(Y^{(i)}) \in \Gamma_\theta) \leqslant |H_L|^{-\frac{c^2}{8}} \leqslant |H_L \times H_R|^{-\frac{c^2}{8(1+\mathsf{C}_2)}}. \tag{46}$$

This finishes proof of Claim 1. □

Claim 2. Assuming $|H_L \times H_R|$ is sufficiently large as a function of the parameters $\alpha_0, c, \mathsf{C}_1$, and C_2, for every non-negative integer i, we have that either

$$\text{(No room for improvement)} \quad H_2(Y^{(i)}) \geqslant \left(1 - \frac{c}{2(1+\mathsf{C}_2)}\right) \log|H_L \times H_R| \tag{47}$$

or

$$\text{(Gaining entropy)} \quad H_2(Y^{(i+1)}) \geqslant H_2(Y^{(i)}) + \gamma \log|H_L \times H_R|, \tag{48}$$

where γ is a positive number that only depends on c, C_1, and C_2.

Proof of Claim 2. Let γ_0 be the constant given by Lemma 13 for the parameters $\varepsilon := \frac{c}{2(1+\mathsf{C}_2)}$, c, C_1, and C_2. Notice that the groups H_L and H_K satisfy (G1)–(G3). Moreover, if the random-variable $Y^{(i)}$ for a given non-negative integer i has *room for improvement* (that means (47) does not hold), then by (40) $Y^{(i)}$ satisfies the conditions of Lemma 13. Hence, by Lemma 13, if $|H_L \times H_R|$ is large enough depending only on the parameters c, C_1, and C_2, then for every positive number $\gamma \leqslant \gamma_0$ we have that either

$$H_2(Y^{(i+1)}) \geqslant H_2(Y^{(i)}) + \gamma \log|H_L \times H_R|, \tag{49}$$

or there are proper normal subgroups Z_L and Z_R of H_L and H_R, respectively, such that $Z(H_L/Z_L) = 1$, $Z(H_R/Z_R) = 1$, and there exists an isomorphism $\theta : H_L/Z_L \to H_R/Z_R$ such that

$$\mathbb{P}(\pi_{Z_L \times Z_R}(Y^{(i+1)}) \in \Gamma_\theta) \geqslant |H_L \times H_R|^{-R\gamma}. \tag{50}$$

By Claim 1, if $\gamma < \frac{c^2}{8R(1+\mathsf{C}_2)}$ and $|H_L|$ is large enough depending on c and α_0, then (50) cannot hold. Therefore, (49) holds. This finishes proof of Claim 2.

Claim 3. Suppose γ is the positive number given in Claim 2. Let i_0 be the smallest integer which is more than $1/\gamma$. Then

$$H_2(Y^{(i_0)}) \geqslant \left(1 - \frac{c}{2(1+\mathsf{C}_2)}\right) \log |H_L \times H_R|. \tag{51}$$

Proof of Claim 3. Suppose to the contrary that (51) does not hold. Since Rényi entropy is non-decreasing in a random-walk, we obtain that for every non-negative integer $i \leqslant i_0$, we have *room for improvement*; that means (47) does not hold. Hence, by Claim 2, for every non-negative integer $i \leqslant i_0$, we *gain entropy*; that means (48) holds. Therefore,

$$H_2(Y^{(i_0)}) \geqslant i_0 \gamma \log |H_L \times H_R| > \log |H_L \times H_R|,$$

which is a contradiction.

Claim 4. In the above setting, $\mathcal{L}(X) \geqslant \frac{c}{2^{i_0+2}(1+\mathsf{C}_2)\max\{\overline{L}, 2/c_0\}}$ if $|H_L \times H_R|$ is large enough depending on the parameters $\alpha_0, c, \mathsf{C}_1$, and C_2.

Proof of Claim 4. Suppose π is a non-trivial representation of $H_L \times H_R$. Then the restriction of π to either H_L or H_R is non-trivial. Since H_R and H_L are c-quasi-random, we deduce that

$$\deg \pi \geqslant \min\{|H_L|^c, |H_R|^c\}. \tag{52}$$

By (21), we have that $\min\{|H_L|, |H_R|\}^{1+\mathsf{C}_2} \geqslant |H_L \times H_R|$. Hence, by (52), we obtain that $H_L \times H_R$ is $\frac{c}{1+\mathsf{C}_2}$-quasi-random.

By Claim 3, we have that

$$H_2(X_{2^{i_0}\ell_0}) \geqslant \left(1 - \frac{c}{2(1+\mathsf{C}_2)}\right) \log |H_L \times H_R|, \tag{53}$$

and ℓ_0 is a positive integer which is at most

$$2\max\{\overline{L}, 2/c_0\} \max\{\log |H_L|, \log |H_R|\}.$$

Therefore by Proposition 2, we obtain that

$$\mathcal{L}(X) \geqslant \frac{c}{2^{i_0+2}(1+\mathsf{C}_2)\max\{\overline{L}, 2/c_0\}}.$$

This finishes proof of Claim 4 and Theorem 12. □

5. Random-walk on an extension of a quasi-random group by an Abelian group

The main goal of this section is to prove that under certain algebraic conditions a random-walk on an extension of a group H by an Abelian group A has a spectral gap which depends on the spectral gap on the quotient H. Similar to the previous section, we list the needed algebraic assumptions for the groups here, and label them by (Gi)'s. To be consistent with the statements given in the previous section, new conditions are labelled by an index $i \geqslant 4$. For a positive number c, and positive integers C_4 and C_5, we formulate the following axioms for a group H and an Abelian group A.

(G1) H is a c-quasi-random group.

(G4) There is a homomorphism $\phi : H \to \mathrm{Aut}(A)$, and H acts on A accordingly. Via this action, A is viewed as a $\mathbb{Z}[H]$-module where $\mathbb{Z}[H]$ is the group ring of H over $\mathbb{Z}$.

(G5) $|A| \leqslant |H|^{\mathsf{C}_4}$.

(G6) For every $x \in A$,

$$\prod_{\mathsf{C}_5} \mathcal{O}_x \prod_{\mathsf{C}_5} \mathcal{O}_x^{-1} = M_x,$$

where $\mathcal{O}_x$ is the H-orbit of x and M_x is the $\mathbb{Z}[H]$-submodule generated by x.

Theorem 15. *Suppose c is a positive number, C_4 and C_5 are positive integers, H is a finite group, A is a finite Abelian group, and they satisfy* (G1), (G4), (G5), *and* (G6). *Suppose G is an extension of H by A; that means there is a short exact sequence*

$$1 \to A \hookrightarrow G \xrightarrow{\pi} H \to 1.$$

Suppose Z is a symmetric random-variable with values in G whose range generates G. Suppose there exist positive numbers c_0 and α_0 such that

$$\mathcal{L}(\pi(Z)) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$ where the implied constant only depends on the given parameters $c, \mathsf{C}_4, \mathsf{C}_5, \alpha_0$.

5.1. **Random-walk on a quasi-random-by-Abelian group: The case of almost uniform quasi-random component.** To prove Theorem 15, we notice that after an $O_{c_0}(\log |H|)$-step random-walk, we get a random-variable $\widehat{Z}$ such that the probability law of $\pi(\widehat{Z})$ is close to the probability counting measure of H. The main goal of this section is to prove an analogue of Lemma 13 in the setting of group extensions. This result describes what happens if after a couple of steps under a random-walk with respect to the random-variable $\widehat{Z}$ we do not gain a *substantial amount of entropy.*

Lemma 16. *Suppose c is a positive number, C_4 and C_5 are positive integers, H is a finite group, A is a finite Abelian group, and they satisfy* (G1), (G4), (G5), *and* (G6). *Suppose G is an extension of H by A. Suppose $\widehat{Z}$ is a symmetric random-variable with values in G. Suppose ε is a positive number and $\widehat{Z}$ satisfies the following properties.*

(1) (Almost uniform quotient) *For every $x \in H$, we have*

$$\mathbb{P}(\pi(\widehat{Z}) = x) \leqslant 2|H|^{-1}.$$

(2) (Room for improvement) $H_2(\widehat{Z}) \leqslant (1-\varepsilon)\log|G|$.

Then there is a positive number γ_0 which depends on $\varepsilon, c, \mathsf{C}_4$, and C_5, such that for every $\gamma \leqslant \gamma_0$ at least one of the following statements holds.

(1) (Gaining entropy) $H_2(\widehat{Z}_2) \geqslant H_2(\widehat{Z}) + \gamma\log|G|$, *where $\widehat{Z}_2$ is a 2-step random-walk with respect to $\widehat{Z}$.*

(2) (Levi subgroup) *There are a proper H-invariant subgroup N of A and a subgroup $\overline{H}$ of G/N such that π induces an isomorphism from $\overline{H}$ to H, and*

$$\mathbb{P}(\pi_N(\widehat{Z}_2) \in \overline{H}) \geqslant |G|^{-R\gamma},$$

where $\pi_N : G \to G/N$ is the natural quotient map and R is a fixed absolute positive constant.

(3) (Small cases) $|G| < \mathsf{C}_6$ *where C_6 is a positive integer which depends on $\varepsilon, c, \mathsf{C}_4$, and C_5.*

We start with a couple of lemmas. The first one gives us a better understanding of the structure an extension G of H by A, where H and A are as in Lemma 16, and the second one is an analogue of Lemma 14.

Lemma 17. *Suppose c is a positive number, C_4 and C_5 are positive integers, H is a finite group, A is a finite Abelian group, and they satisfy* (G1), (G4), (G5), *and* (G6). *Let G be an extension of H by A.*

(1) *G is a perfect group; that means it does not have a non-trivial Abelian quotient.*

(2) *If N is a normal subgroup of G and $\pi(N) = H$, then $N = G$.*

(3) *G is $\frac{c}{1+\mathsf{C}_4}$-quasi-random.*

(4) *Suppose $M_1 \subsetneq M_2$ are two $\mathbb{Z}[H]$-submodules of A. Then H acts non-trivially on M_2/M_1.*

(5) *Suppose M is a $\mathbb{Z}[H]$-submodule of A. Then the only H-fixed point of A/M is the identity.*

Proof. We start by proving the following:

Claim. Suppose N is a normal subgroup of G such that $\pi(N) = H$. Then $M := A \cap N$ is a $\mathbb{Z}[H]$-submodule of A and H acts trivially on A/M.

Proof of Claim. Since A is a normal subgroup of G, M is a normal subgroup of N. Because M is a normal subgroup of N and A is an Abelian group, the conjugation of N factors through $\pi(N)$. Therefore, M is a $\mathbb{Z}[H]$-submodule of A. For every $h \in H$, there is $n_h \in N$ such that $\pi(n_h) = h$. Hence, for every $a \in A$,

$$(h \cdot a)a^{-1} = n_h a n_h^{-1} a^{-1} \in A \cap N.$$

Therefore, H acts trivially on A/M. This finishes proof of *Claim*.

To show the first part, we have to show that the commutator subgroup $[G,G]$ is equal to G. Notice that $\pi([G,G]) = [H,H]$. Since H is a c-quasi-random group, it is perfect. Therefore, $\pi([G,G]) = H$. Therefore, by the previous *Claim*, H acts trivially on A/M where $M := A \cap [G,G]$. Hence, for every $y \in A$, $\pi_M(\mathcal{O}_y) = \pi_M(y)$ where $\mathcal{O}_y$ is the H-orbit of y and $\pi_M : A \to A/M$ is the natural quotient map. By (G6), we obtain that

$$\pi_M(M_y) = \pi_M(y)^{\mathsf{C}_5}\pi_M(y)^{-\mathsf{C}_5}, \quad \text{and so} \quad \pi_M(M_y) = 1. \tag{54}$$

By (54), we conclude that $M = A$. Since $\pi([G,G]) = H$ and $A \subseteq [G,G]$, we conclude that $[G,G] = G$. This finishes proof of the first part.

Since $\pi(N) = H$ and $A = \ker\pi$, $AN = G$. Hence, $G/N \simeq A/(N \cap A)$ is an Abelian group. By the first part G does not have a non-trivial Abelian quotient, and so $G = N$. This finishes proof of the second part.

Suppose ρ is a non-trivial representation of G. Since A is Abelian, $\rho(A)$ is diagonalizable. Hence, there are characters $\chi_1, \dots, \chi_d \in \mathrm{Hom}(A, S^1)$, where $S^1 := \{z \in \mathbb{C} \,|\, |z| = 1\}$, such that

$$\rho(a) = \mathrm{diag}(\chi_1(a), \dots, \chi_d(a)),$$

for every $a \in A$. For every $g \in G$, $\rho(gag^{-1})$ is a conjugate of $\rho(a)$ and its eigenvalues are given by $\chi_i(gag^{-1})$. Notice that $\pi(g)$ acts on A by conjugating by g; this means $\pi(g) \cdot a = gag^{-1}$. This action induces an action on $\widehat{A} := \mathrm{Hom}(A, S^1)$. For $\chi \in \widehat{A}$ and $h \in H$, we let $(h \cdot \chi)(a) := \chi(h^{-1} \cdot a)$. Therefore, for every $h \in H$, we have

$$\{h \cdot \chi_1, \dots, h \cdot \chi_d\} = \{\chi_1, \dots, \chi_d\}.$$

For every i, the H-orbit of χ_i is a subset of $\{\chi_1, \dots, \chi_d\}$. Hence,

$$\deg\rho \geqslant |H \cdot \chi_i| \tag{55}$$

for every i. Because H is c-quasi-random, every H-orbit has either one element or at least $|H|^c$ elements. Thus, by (55), either $\deg\rho \geqslant |H|^c$ or $H \cdot \chi_i = \chi_i$ for every i. Notice that if $H \cdot \chi_i = \chi_i$, then, for every $a \in A$, $\chi_i(\mathcal{O}_a) = \chi_i(a)$ where $\mathcal{O}_a$ is the H-orbit of a. By (G6), we obtain that

$$\chi_i(M_a) = \textstyle\prod_{\mathsf{C}_5} \chi_i(\mathcal{O}_a) \prod_{\mathsf{C}_5} \chi_i(\mathcal{O}_a)^{-1} = 1.$$

Therefore, if for every i, $H \cdot \chi_i = \chi_i$, then A is in the kernel of ρ. This means ρ factors through H; and so $\deg\rho \geqslant |H|^c$. Altogether we obtain that $\deg\rho \geqslant |H|^c$. By (G5), we have $|H|^c \geqslant |G|^{c/(1+\mathsf{C}_4)}$, and the third part follows.

To show part (4), we proceed by contradiction. Suppose H acts trivially on M_2/M_1. Therefore, for every $a \in M_2$, $\pi_{M_1}(\mathcal{O}_a) = \pi_{M_1}(a)$, where $\pi_{M_1} : G \to G/M_1$ is the natural quotient map. Hence, by (G6) and a similar argument as in (54), we obtain that $\pi_{M_1}(M_a) = 1$, where M_a is the $\mathbb{Z}[H]$-module generated by a. Therefore, $M_2 = M_1$, which is a contradiction. This finishes proof of the fourth part.

To show the last part, suppose to the contrary that for some $\mathbb{Z}[H]$-submodule M of A, there exists $xM \in A/M$ which is H-invariant and $x \neq 1$. Let $M' := \langle x \rangle M$. Then H acts trivially on this M'/M, and so M' is a $\mathbb{Z}[H]$-submodule. This contradicts part (4). □

Lemma 18. *Suppose c is a positive number, C_4 and C_5 are positive integers, H is a finite group, A is a finite Abelian group, and they satisfy* (G1), (G4), (G5), *and* (G6). *Suppose S is a subset of A, and let M_S be the $\mathbb{Z}[H]$-submodule of A generated by S. Then there is a subset $\overline{S}$ of S which generates M_S and $|\overline{S}| \leqslant \mathsf{C}_4/c$.*

Proof. Suppose $\overline{S} := \{x_1, \dots, x_m\}$ is a subset of S which is a generating set of the $\mathbb{Z}[H]$-module M_S, and it has the smallest possible number of elements among such subsets. For every integer i in $[1, m]$, let M_i be the $\mathbb{Z}[H]$-submodule generated by $\{x_1, \dots, x_i\}$. Since for every i the set $\overline{S} \backslash \{x_i\}$ does not generate M_S, we have that

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_m = M_S.$$

By the fourth part of Lemma 17, we have that the action of H on M_{i+1}/M_i is non-trivial for every integer in $[1, m-1]$. Because H is c-quasi-random, we obtain that

$$|M_{i+1}/M_i| \geqslant |H|^c. \tag{56}$$

By (56), it follows that

$$|H|^{cm} \leqslant |M_S| \leqslant |A| \leqslant |H|^{\mathsf{C}_4}.$$

Therefore $m \leqslant \frac{\mathsf{C}_4}{c}$. This finishes the proof. □

Proof of Lemma 16. Suppose γ is a sufficiently small positive number to be specified later, and $|G| \geqslant \mathsf{C}_6$ for a large enough C_6 to be specified later. Let's assume that we do not *gain enough entropy*; that means $H_2(\widehat{Z}_2) < H_2(\widehat{Z}) + \gamma \log |G|$. Then by Proposition 1, there is a $|G|^{R\gamma}$-approximate subgroup B of G such that

$$|\log |B| - H_2(\widehat{Z})| \leqslant R\gamma \log |G| \quad \text{and} \quad \mathbb{P}(\widehat{Z}_2 \in B) \geqslant |G|^{-R\gamma}. \tag{57}$$

By the *almost uniform quotient* condition, we have that

$$\mathbb{P}(\pi(\widehat{Z}_2) \in \pi(B)) \leqslant 2\frac{|\pi(B)|}{|H|}. \tag{58}$$

By the second inequality in (57) and (58), we obtain that

$$|G|^{-R\gamma} \leqslant \mathbb{P}(\widehat{Z}_2 \in B) \leqslant \mathbb{P}(\pi(\widehat{Z}_2) \in \pi(B)) \leqslant \frac{2|\pi(B)|}{|H|}. \tag{59}$$

By (G5) and (59), we deduce that

$$\frac{1}{2}|H|^{1-R(1+\mathsf{C}_4)\gamma} \leqslant |\pi(B)|. \tag{60}$$

Therefore, for large enough C_6 and small enough γ, by (60), $|\pi(B)| \geqslant |H|^{1-\frac{c}{3}}$. Hence, by Theorem 3,

$$\pi(\textstyle\prod_3 B) = H. \tag{61}$$

Claim. *In the above setting, for a small enough γ depending on $\varepsilon, c, \mathsf{C}_4$, and C_5, there is a proper $\mathbb{Z}[H]$-submodule N of A such that*

$$(\textstyle\prod_9 B) \cap A \subseteq N.$$

Proof of Claim. Suppose to the contrary that $(\prod_9 B) \cap A$ generates A as a $\mathbb{Z}[H]$-module. Then by Lemma 18, there is a subset $\overline{B} := \{y_1, \dots, y_m\}$ of $(\prod_9 B) \cap A$ such that

$$m \leqslant \frac{\mathsf{C}_4}{c} \quad \text{and} \quad A = M_{y_1} \cdots M_{y_m}, \tag{62}$$

where M_{y_i} is the $\mathbb{Z}[H]$-submodule generated by y_i. Notice that, by (61), there is a function $\theta : H \to G$ such that for every $x \in H$, $\pi(\theta(x)) = x$ (that means f is a *section*) and $\theta(x) \in \prod_3 B$. Notice that for every $x \in H$, we have

$$x \cdot y_i = \theta(x) y_i \theta(x)^{-1} \in \textstyle\prod_7 B.$$

This means for every i

$$\mathcal{O}_{y_i} \subseteq \textstyle\prod_7 B. \tag{63}$$

By (G6), (62), (63), and the fact that B is symmetric, we obtain that

$$A \subseteq \prod_{14m\mathsf{C}_5} B. \tag{64}$$

Using (61) and (64), it follows that

$$G = \prod_{14m\mathsf{C}_5+3} B. \tag{65}$$

Since B is an $|G|^{R\gamma}$-approximate subgroup, using (65) we obtain that

$$|G| \leqslant |B||G|^{(14m\mathsf{C}_5+2)R\gamma} \quad \text{, and so} \quad |G|^{1-(14m\mathsf{C}_5+2)R\gamma} \leqslant |B|. \tag{66}$$

On the other hand, by the *room for improvement* condition and (57), we have

$$\log|B| \leqslant H_2(Z) + R\gamma \log|G| \leqslant (1-\varepsilon+R\gamma)\log|G|. \tag{67}$$

By (62), (66), and (67), we deduce that

$$1-(14\mathsf{C}_4\mathsf{C}_5/c+2)R\gamma \leqslant 1-\varepsilon+R\gamma; \quad \text{and so} \quad \varepsilon \leqslant (14\mathsf{C}_4\mathsf{C}_5/c+3)R\gamma,$$

which is a contradiction if γ is sufficiently small depending on the parameters $\varepsilon, c, \mathsf{C}_4$, and C_5. This finishes proof of the Claim.

Let's recall that by (61), there is a function $\theta : H \to G$ such that $\pi(\theta(x)) = x$ and $\theta(x) \in \prod_3 B$ for every $x \in H$. Therefore, for every $x, x_1, x_2 \in H$, we have

$$\theta(x^{-1})\theta(x) \in (\prod_9 B) \cap A \quad \text{and} \quad \theta(x_1x_2)\theta(x_1)^{-1}\theta(x_2)^{-1} \in (\prod_9 B) \cap A. \tag{68}$$

By (68) and the previous *Claim*, we deduce that there is a proper H-invariant subgroup N of A such that

$$\overline{\theta} : H \to G/N, \quad \overline{\theta}(x) := \theta(x)N$$

is a group homomorphism; notice that since N is a $\mathbb{Z}[H]$-submodule, it is a normal subgroup of G. Because N is a subgroup of $A = \ker\pi$, π induces a group homomorphism $\overline{\pi}$ from G/N to H. For every $x \in H$, we have $\overline{\pi}(\overline{\theta}(x)) = x$. Hence, the restriction of $\overline{\pi}$ to $\overline{H} := \mathrm{Im}(\overline{\theta})$ is an isomorphism. Moreover, we have

$$\mathrm{Im}(\overline{\theta}) \subseteq \pi_N(\prod_3 B), \tag{69}$$

where $\pi_N : G \to G/N$ is the natural quotient map. Next, we show that $\overline{H} = \pi_N(\prod_3 B)$. By (69), it is sufficient to show that $\pi_N(\prod_3 B) \subseteq \overline{H}$. Notice that for every $xN \in \pi_N(\prod_3 B)$, we have

$$(xN)\overline{\theta}(\overline{\pi}(xN))^{-1} \in \pi_N((\prod_9 B) \cap A),$$

and so $xN = \overline{\theta}(\overline{\pi}(xN)) \in \overline{H}$. Altogether, we have found a proper H-invariant subgroup N of A, a subgroup $\overline{H}$ of G/N with the following properties:

(1) $\overline{\pi} : \overline{H} \to H$ is an isomorphism.
(2) $\overline{H} = \pi_N(\prod_3 B)$.

Therefore, by (57), we obtain that

$$\mathbb{P}(\pi_N(\widehat{Z}_2) \in \overline{H}) \geqslant \mathbb{P}(\widehat{Z}_2 \in \prod_3 B) \geqslant |G|^{-R\gamma}.$$

This means if we do not *gain entropy* and are not in the *small cases*, then we can find a desired *Levi subgroup*. □

5.2. **Spectral gap and quasi-random-by-Abelian groups: Proof of Theorem 15.** Let $L := L(c/\mathsf{C}_4, c_0, \alpha)$ and $C := C(\alpha_0)$ be the constants given by Theorem 11. Let ℓ_0 be the smallest integer which is at least

$$\max\{L \log |G|, 2c_0^{-1} \log |H|\}.$$

For every non-negative integer i, let $Z^{(i)} := Z_{2^i \ell_0}$ be a $2^i \ell_0$-step random-walk with respect to Z. Then, similar to the proof of (40), we have

$$|\mathbb{P}(\pi(Z^{(i)}) = x) - |H|^{-1}| \leqslant |H|^{-2} \tag{70}$$

for every $x \in H$.

Claim 1. For every positive integer i, every proper $\mathbb{Z}[H]$-submodule N of A, and every subgroup $\overline{H} \subseteq G/N$ with the property that $\overline{\pi} : \overline{H} \to H$ is an isomorphism, where $\overline{\pi}$ is induced by $\pi : G \to H$, we have that either

$$\mathbb{P}(\pi_N(Z^{(i)}) \in \overline{H}) < |G|^{-\frac{c^2}{8\mathsf{C}_4(1+\mathsf{C}_4)}}$$

or $|H| \ll_{c,\alpha_0,\mathsf{C}_4} 1$.

Proof of Claim 1. Since $\overline{\pi} : \overline{H} \to H$ is an isomorphism, the short exact sequence

$$1 \to \overline{A} \to \overline{G} \to H \to 1$$

splits where $\overline{A} := A/N$ and $\overline{G} := G/N$. Hence, there is an isomorphism $\theta : H \to \overline{H}$ such that $\overline{\pi}(\theta(x)) = x$ for every $x \in H$, and

$$\psi : \overline{G} \to \overline{A} \rtimes H, \quad \psi(g) := (a(g), \overline{\pi}(g)) \tag{71}$$

is an isomorphism, where $a(g) := g\theta(\overline{\pi}(g))^{-1}$. By Lemma 6, $\overline{A} \rtimes H$ has a transitive shifted-automorphism action on $\overline{A}$, which is given by

$$(\bar{a}, x) \cdot \bar{a}' := \bar{a}(x \cdot \bar{a}'). \tag{72}$$

By (71) and (72), we deduce that the following is a shifted automorphism action of $\overline{G}$ on $\overline{A}$:

$$g \cdot \bar{a} := \psi(g) \cdot \bar{a} = a(g)(\overline{\pi}(g) \cdot \bar{a}). \tag{73}$$

Notice that the automorphism part of this action factors through the action of H on $\overline{A}$. More precisely, the automorphism action of $\overline{G}$ is given by the group homomorphism

$$\widehat{\phi} : \overline{G} \to \mathrm{Aut}(\overline{A}), \quad \widehat{\phi}(g)(\bar{a}) := \overline{\pi}(g) \cdot \bar{a}.$$

Hence, by part (5) of Lemma 17, the only $\widehat{\phi}(\overline{G})$-fixed point of $\overline{A}$ is 1. Because H is c-quasi-random, every H-orbit that has more than 1 element has at least $|H|^c$ elements. Thus, every $\widehat{\phi}(\overline{G})$-orbit other than $\{1\}$ has at least $|H|^c$ elements. Notice that by (G5), we deduce that every $\widehat{\phi}(\overline{G})$-orbit other than $\{1\}$ has at least $|\overline{A}|^{c/\mathsf{C}_4}$ elements. Therefore, conditions (H1) and (H2) of Theorem 11 hold for the group action $\overline{G} \curvearrowright \overline{A}$ (with parameter c/C_4, instead of c).

Notice that we also have

$$\mathcal{L}(\widehat{\phi}(\pi_N(Z))) \geqslant \mathcal{L}(\pi(Z)) \geqslant c_0.$$

Hence the condition (H3) of Theorem 11 holds for the random-variable $\pi_N(Z)$.

Altogether, we deduce that we can (and will) apply Theorem 11 for the twisted group action $\overline{G} \curvearrowright \overline{A}$ and the random-variable $\pi_N(Z)$. Therefore,

$$H_2(\pi_N(Z_{2^i\ell_0})) \cdot U_1) \geqslant \frac{c}{2\mathsf{C}_4} \log|\overline{A}| - C \tag{74}$$

for every non-negative integer i, where U_1 is a random-variable with values in $\overline{A}$ and $\mathbb{P}(U_1 = 1) = 1$. Notice that since H acts non-trivially on $\overline{A}$,

$$\log|\overline{A}| \geqslant c \log|H|, \quad \text{and so by (G5)} \quad \log|\overline{A}| \geqslant \frac{c}{1+\mathsf{C}_4} \log|G|.$$

Thus, when $|H|$ is large enough depending on c, α_0 and C_4, by (74), we obtain that

$$H_2(\pi_N(Z_{2^i\ell_0})) \cdot U_1) \geqslant \frac{c^2}{4\mathsf{C}_4(1+\mathsf{C}_4)} \log|G|. \tag{75}$$

Notice that by (73), $\overline{z}$ is in the stabilizer subgroup of $\overline{G}$ associated to 1 if and only if $a(\overline{z}) = 1$. This means the stabilizer subgroup of $\overline{G}$ associated to 1 is $\overline{H}$. Hence,

$$\mathbb{P}(\pi_N(Z_{2^i\ell_0}) \cdot U_1 = 1) = \mathbb{P}(\pi_N(Z_{2^i\ell_0}) \in \overline{H}). \tag{76}$$

Because $\mathbb{P}(\pi_N(Z_{2^i\ell_0}) \cdot U_1 = 1) \leqslant 2^{-\frac{1}{2}H_2(\pi_N(Z_{2^i\ell_0}))\cdot U_1)}$, by (75) and (76), we obtain

$$\mathbb{P}(\pi_N(Z_{2^i\ell_0}) \in \overline{H}) \leqslant |G|^{-\frac{c^2}{8\mathsf{C}_4(1+\mathsf{C}_4)}}. \tag{77}$$

This finishes the proof of Claim 1.

Claim 2. Assuming that $|H|$ is sufficiently large as a function of the parameters c, α, C_4, and C_5, for every non-negative integer i, we have that either

$$\text{(No room for improvement)} \quad H_2(Z^{(i)}) \geqslant \left(1 - \frac{c}{4(1+\mathsf{C}_4)}\right) \log|G|, \tag{78}$$

or

$$\text{(Gaining entropy)} \quad H_2(Z^{(i+1)}) \geqslant H_2(Z^{(i)}) + \gamma \log|G|, \tag{79}$$

where γ is a positive number that only depends on c, C_4, and C_5.

Proof of Claim 2. Let γ_0 be the constant given by Lemma 16 for the parameters, $\varepsilon := \frac{c}{4(1+\mathsf{C}_4)}$, c, C_4, and C_5. Notice that the pair of groups H, A and the group action $H \curvearrowright A$ satisfy (G1), (G4), (G5), and (G6). Moreover, if the random-variable $Z^{(i)}$, for a given non-negative integer i, has *room for improvement* (that means (78) does not hold), then by (70), $Z^{(i)}$ satisfies the conditions of Lemma 16. Hence, by Lemma 16, if $|H|$ is large enough depending only on the parameters c, C_4, and C_5, then for every positive number $\gamma \leqslant \gamma_0$ we have either

$$H_2(Z^{(i+1)}) \geqslant H_2(Z^{(i)}) + \gamma \log|G|, \tag{80}$$

or there are a proper H-invariant subgroup N of A and a *Levi subgroup* $\overline{H}$ of $\overline{G} := G/N$ (that means $\overline{\pi} : \overline{H} \to H$ is an isomorphism, where $\overline{\pi} : \overline{G} \to H$ is induced from $\pi : G \to H$) such that

$$\mathbb{P}(\overline{\pi}(Z^{(i+1)}) \in \overline{H}) \geqslant |G|^{-R\gamma}, \tag{81}$$

where R is a fixed absolute constant. By Claim 1, if $\gamma < \frac{c^2}{8R\mathsf{C}_4(1+\mathsf{C}_4)}$, (81) does not hold. Hence, (80) should hold, which finishes proof of Claim 2. □

Claim 3. Suppose γ is the positive number given in Claim 2. Let i_0 be the smallest integer which is more than $1/\gamma$. Then

$$H_2(Z^{(i_0)}) \geqslant \left(1 - \frac{c}{4(1+\mathsf{C}_4)}\right) \log|G|. \tag{82}$$

Proof of Claim 3. Suppose to the contrary that (82) does not hold. Since Rényi entropy is non-decreasing in a random-walk, we obtain that for every non-negative integer $i \leqslant i_0$, we *gain entropy*; that means (79) holds. Therefore,

$$H_2(Z^{(i_0)}) \geqslant i_0 \gamma \log|G| > \log|G|,$$

which is a contradiction.

Claim 4. In the above setting, $\mathcal{L}(Z) \geqslant \frac{c}{2^{i_0+2}(1+\mathsf{C}_4)\max\{L, 2c_0^{-1}\}}$ if $|H|$ is large enough, depending on the parameters $c, \alpha_0, \mathsf{C}_4$.

Proof of Claim 4. By Lemma 17, G is $\frac{c}{1+\mathsf{C}_4}$-quasi-random. By Claim 3, we have that

$$H_2(Z_{2^{i_0}\ell_0}) \geqslant \left(1 - \frac{c}{4(1+\mathsf{C}_4)}\right) \log|G|. \tag{83}$$

Hence, by Proposition 2 and (83), we deduce that

$$\mathcal{L}(Z) \geqslant \frac{c}{2^{i_0+2}(1+\mathsf{C}_4)\max\{L, 2/c_0\}}.$$

This finishes the proof of Claim 4 and Theorem 15. □

6. Random-walk on an extension of a quasi-random group by a nilpotent group

The main goal of this section is to extend Theorem 15 to a quasi-random-by-nilpotent group. We start by recalling the Lie algebra associated to a nilpotent group U, and state the assumptions on the involved groups.

For a group U and every positive integer i, let $\gamma_i(U)$ be the i-th lower central series of U. For a nilpotent group U of nilpotency class m_0, let

$$L(U) := L_1 \oplus \cdots \oplus L_{m_0},$$

where $L_i := \frac{\gamma_i(U)}{\gamma_{i+1}(U)}$ for every integer i in $[1..m_0]$. For $\overline{x} := x\gamma_{i+1}(U) \in L_i$ and $\overline{y} := y\gamma_{j+1}(U) \in L_j$, let $[\overline{x}, \overline{y}] := [x, y]\gamma_{i+j+1}(U) \in L_{i+j}$, where $[x, y] := xyx^{-1}y^{-1}$. It is well-known that $[,]$ is well-defined, can be linearly extended to $L(U)$, and $L(U)$ is a Lie ring with respect to this bracket (see [18, Chapter VIII, Theorem 9.3]). In this section, we are going to assume that H, U, and G are three finite groups which satisfy the following statements.

(G7) U is a finite nilpotent group of nilpotency class m_0.

(G8) There is a unital commutative ring R such that $L(U)$ is a Lie algebra over R and L_1 can be generated by d_0 elements as an R-module; notice that L_1 is simply the Abelianization U^{ab} of U.

(G9) The following is a short exact sequence

$$1 \to U \hookrightarrow G \xrightarrow{\pi} H \to 1,$$

and $G/\gamma_2(U)$ is c-quasi-random.

Now we can state the main result of this section.

Proposition 19. *Suppose H, U and G are three finite groups which satisfy* (G7), (G8), *and* (G9). *Let $\pi_{\gamma_2(U)} : G \to G/\gamma_2(U)$ be the natural quotient map. Let X be a symmetric random-variable with values in G. Suppose $\mathcal{L}(\pi_{\gamma_2(U)}(X)) \geqslant c_0$ where c_0 is a positive number. Then $\mathcal{L}(X) \gg c_0$ where the implied constant depends only on the given parameters m_0, d_0, and c.*

6.1. **Inducing quasi-randomness.** Here we show Lemma 20.

Lemma 20. *Suppose H, U and G are finite groups that satisfy* (G7), (G8), *and* (G9). *Then the group G is $\frac{c}{C(m_0,d_0)}$-quasi-random, where $C(m_0, d_0)$ is a positive integer which depends only on m_0 and d_0.*

Lemma 21 is essentially proved in [14, Lemma 32].

Lemma 21. *Suppose U is a finite group which satisfies* (G7) *and* (G8). *Suppose S is a subset of U and $S[U, U] = U$. Then*

$$\prod_{C(m_0,d_0)} S = U,$$

where $C(m_0, d_0)$ is a positive integer which depends only on m_0 and d_0.

Proof. Suppose $x_1, \dots, x_{d_0}$ generate L_1 as an R-module. Then for every positive integer k, we have

$$L_k = \sum_{1 \leqslant i_1, \dots, i_k \leqslant d_0} \mathrm{ad}(x_{i_1}) \cdots \mathrm{ad}(x_{i_k})(L_1). \tag{84}$$

Since $S[U, U] = U$, there are s_i's in S such that $s_i \gamma_2(U) = x_i$ for every integer i in $[1..d_0]$. Hence, by (84), we obtain

$$L_k \subseteq \pi_{\gamma_{k+1}(U)}(\textstyle\prod_{d_0^k(3\cdot 2^k-2)} S), \tag{85}$$

where $\pi_{\gamma_{k+1}(U)} : U \to U/\gamma_{k+1}(U)$ is the natural quotient map. By (85), by induction on j, one can deduce that

$$U/\gamma_{j+1}(U) = \pi_{\gamma_{j+1}(U)}(\textstyle\prod_{\sum_{k=1}^{j} d_0^k(3\cdot 2^k-2)} S).$$

Therefore $U = \prod_{3(2d_0)^{m_0+1}} S$. This finishes the proof. □

The following is an immediate consequence of Lemma 21.

Corollary 22. *Suppose U is a finite group that satisfies* (G7) *and* (G8). *Then the following statements hold.*

(1) *If $\overline{U}$ is a subgroup of U and $\overline{U}[U, U] = U$, then $\overline{U} = U$.*
(2) *$|U| \leqslant |U^{\mathrm{ab}}|^{C(m_0,d_0)}$, where $C(m_0, d_0)$ is the function given in Lemma 21.*

Lemma 23. *Suppose A is a finite Abelian group, H is a finite group, and the following is a short exact sequence*

$$1 \to A \hookrightarrow G \xrightarrow{\pi} H \to 1.$$

Suppose G is c-quasi-random. Then the following statements hold.

(1) *$|A| \leqslant |H|^{\frac{1-c}{c}}$.*
(2) *If N is a normal subgroup of G and $\pi(N) = H$, then $N = G$.*

Proof. Since H is a quotient of G and G is c-quasi-random, every non-trivial representation of H has dimension at least $|G|^c$. Therefore, $|H| \geqslant |G|^c$. This implies the first part.

Since $H = \pi(N)$, $G = AN$. Therefore,

$$\frac{G}{N} = \frac{AN}{N} \simeq \frac{A}{A \cap N}.$$

Thus G/N is an Abelian quotient of G. Since G is c-quasi-random, it does not have a non-trivial Abelian quotient. Hence, $G = N$. □

Lemma 24. *Suppose U is a finite nilpotent group, H is a finite group, and the following is a short exact sequence*

$$1 \to U \hookrightarrow G \xrightarrow{\pi} H \to 1.$$

Suppose $\overline{G} := G/\gamma_2(U)$ is c-quasi-random. Suppose N is a normal subgroup of G. If $\pi(N) = H$, then $N = G$.

Proof. Let $\pi_{\gamma_2(U)} : G \to \overline{G}$ be the natural quotient map. Then $\pi_{\gamma_2(U)}(N)$ is a normal subgroup of $\overline{G}$ and $H = \pi(\pi_{\gamma_2(U)}(N))$. By the second part of Lemma 23, we obtain that $\pi_{\gamma_2(U)}(N) = \overline{G}$. Therefore, $U^{\mathrm{ab}} = \pi_{\gamma_2(U)}(N \cap U)$. Hence, by the first part of Corollary 22, $N \cap U = U$. Because, $H = \pi(N)$ and $U \subseteq N$, we deduce that $N = G$. □

Proof of Lemma 20. Suppose ρ is a non-trivial irreducible representation of G. Let $\overline{G} := G/\ker\rho$, $\overline{U} := (U \ker\rho)/\ker\rho$, and $\overline{H} := H/\pi(\ker\rho)$. Then

$$1 \to \overline{U} \hookrightarrow \overline{G} \xrightarrow{\overline{\pi}} \overline{H} \to 1$$

is a short exact sequence where $\overline{\pi}(x \ker\rho) := \pi(x)\pi(\ker\rho)$. Notice that $\overline{\rho}(x \ker\rho) := \rho(x)$ is a non-trivial faithful irreducible representation of $\overline{G}$.

Since $\ker\rho$ is a proper normal subgroup of G, by Lemma 23, $\overline{H}$ is a non-trivial quotient of H. Hence, $\overline{H}$ is a non-trivial quotient of $G/\gamma_2(U)$. Therefore,

$$|\overline{H}| \geqslant |G/\gamma_2(U)|^c. \tag{86}$$

Notice that, by the second part of Corollary 22, we obtain

$$|G/\gamma_2(U)| \geqslant |H||U|^{\frac{1}{C(m_0,d_0)}}, \tag{87}$$

where $C(m_0, d_0)$ is the function given in Lemma 21. Hence, by (86) and (87), we obtain

$$|\overline{H}| \geqslant |H|^c|U|^{\frac{c}{C(m_0,d_0)}}. \tag{88}$$

If $\gamma_2(\overline{U}) = 1$, then $\overline{\rho}$ can be lifted to a non-trivial irreducible representation of $G/\gamma_2(U)$. In this case, because $G/\gamma_2(U)$ is c-quasi-random, by (87), we deduce that

$$\deg\rho \geqslant |G/\gamma_2(U)|^c \geqslant |H|^c|U|^{\frac{c}{C(m_0,d_0)}}. \tag{89}$$

If $\gamma_2(\overline{U}) \neq 1$, then the nilpotency class m_0' of $\overline{U}$ is at least 2 and at most m_0. Consider the action of $\overline{G}$ on $\gamma_{m_0'-1}(\overline{U})$ by conjugation. Since

$$[\gamma_{m_0'-1}(\overline{U}), \gamma_2(\overline{U})] \subseteq \gamma_{m_0'+1}(\overline{U}) = 1,$$

the conjugation action of $\overline{G}$ on $\gamma_{m_0'-1}(\overline{U})$ factors through $\overline{G}/\gamma_2(\overline{U})$. The conjugation action induces an action of $\overline{G}$ on the set $\widehat{\gamma_{m_0'-1}(\overline{U})}$ of equivalent classes of unitary irreducible representations of $\gamma_{m_0'-1}(\overline{U})$. Because this action factors through an

action of $\overline{G}/\gamma_2(\overline{U})$, such an action has a lift to an action of $G/\gamma_2(U)$, and $G/\gamma_2(U)$ is c-quasi-random, we deduce that for every irreducible representation ϑ of $\gamma_{m_0'-1}(\overline{U})$ either $\overline{g}\cdot\vartheta=\vartheta$ for every $\overline{g}\in\overline{G}$ or

$$|\overline{G}\cdot\vartheta| := |\{\overline{g}\cdot\vartheta \,|\, \overline{g}\in\overline{G}\}| \geqslant |G/\gamma_2(U)|^c. \tag{90}$$

Notice that by Clifford's theorem (see [19, Theorem 6.2]), if ϑ is an irreducible subrepresentation of the restriction of $\overline{\rho}$ to $\gamma_{m_0'-1}(\overline{U})$, then

$$\deg\overline{\rho} \geqslant |\overline{G}\cdot\vartheta|. \tag{91}$$

By (90) and (91), we obtain that either

$$\deg\rho \geqslant |G/\gamma_2(U)|^c \quad \text{or} \quad \overline{\rho}(\overline{g}\overline{x}\overline{g}^{-1}) = \overline{\rho}(\overline{x}) \tag{92}$$

for every $\overline{g}\in\overline{G}$ and $\overline{x}\in\gamma_{m_0'-1}(\overline{U})$. The latter implies that $\overline{\rho}(\gamma_{m_0'-1}(\overline{U}))$ is a central subgroup of $\overline{\rho}(\overline{G})$. But this is not possible as $\overline{\rho}$ is faithful and $[\overline{U},\gamma_{m_0'-1}(\overline{U})]\neq 1$. Hence, by (92) and (87), we conclude that

$$\deg\rho \geqslant |H|^c|U|^{\frac{c}{C(m_0,d_0)}} \geqslant |G|^{\frac{c}{C(m_0,d_0)}}.$$

□

6.2. **Spectral gap and a quasi-random-by-nilpotent group: Proof of Proposition 19.** Let ℓ_0 be the smallest integer larger than $2c_0^{-1}\log|G|$. For every non-negative integer i, let $Y^{(i)} := X_{2^i\ell_0}$ be a $2^i\ell_0$-step random-walk with respect to X. Then, similar to (40), we have

$$|\mathbb{P}(\pi_{\gamma_2(U)}(Y^{(i)})=x) - |G|^{-1}| \leqslant |G|^{-2} \tag{93}$$

for every $x\in\pi_{\gamma_2(U)}(G)$.

Claim 1. There is a positive number γ_0 which only depends on the parameters m_0, d_0, c, and c_0 such that for every positive number $\gamma\leqslant\gamma_0$ either

$$\text{(No room for improvement)} \quad H_2(Y^{(i)}) \geqslant \left(1-\frac{c}{2C(m_0,d_0)}\right)\log|G|, \tag{94}$$

or

$$\text{(Gaining entropy)} \quad H_2(Y^{(i+1)}) \geqslant H_2(Y^{(i)}) + \gamma\log|G|, \tag{95}$$

or $|G|\ll_{m_0,d_0,c,c_0} 1$ (small cases).

Proof of Claim 1. Suppose to the contrary that for a large enough (to be specified later) group G neither (94) nor (95) holds. Then, by Proposition 1, there is an $|G|^{R\gamma}$-approximate subgroup $B\subseteq G$ such that

$$|\log|B| - H_2(Y^{(i)})| \leqslant R\gamma\log|G| \quad \text{and} \quad \mathbb{P}(Y^{(i+1)}\in B) \geqslant |G|^{-R\gamma}, \tag{96}$$

where R is a universal constant number. By (93) and (96), we obtain

$$|G|^{-R\gamma} \leqslant \mathbb{P}(Y^{(i+1)}\in B) \leqslant \mathbb{P}(\pi_{\gamma_2(U)}(Y^{(i+1)})\in\pi_{\gamma_2(U)}(B)) \leqslant 2\frac{|\pi_{\gamma_2(U)}(B)|}{|\pi_{\gamma_2(U)}(G)|}. \tag{97}$$

By Corollary 22, we have

$$|G| = |U||H| \leqslant |U^{\mathrm{ab}}|^{C(m_0,d_0)}|H| \leqslant |\pi_{\gamma_2(U)}(G)|^{C(m_0,d_0)}. \tag{98}$$

Hence, by (97) and (98), if $|G|^{R\gamma/C(m_0,d_0)}\geqslant 2$, we have

$$|\pi_{\gamma_2(U)}(B)| \geqslant |\pi_{\gamma_2(U)}(G)|^{1-2R\gamma}. \tag{99}$$

If $\gamma < c/(6R)$, then by Theorem 3 and (99), we obtain

$$\pi_{\gamma_2(U)}(\prod_3 B) = \pi_{\gamma_2(U)}(G). \tag{100}$$

By (100) and Lemma 21, we deduce that

$$\prod_{3C(m_0,d_0)} B = G. \tag{101}$$

By (101) and the fact that B is $|G|^{R\gamma}$-approximate subgroup, we obtain that

$$|G|^{1-(3C(m_0,d_0)-1)R\gamma} \leqslant |B|. \tag{102}$$

On the other hand, since $Y^{(i)}$ has *room for improvement* (that means (94) does not hold), by (96), we deduce that

$$\log|B| \leqslant \left(1 - \frac{c}{2C(m_0,d_0)} + R\gamma\right)\log|G|. \tag{103}$$

Hence, by (103), if $\gamma \leqslant \frac{c}{4RC(m_0,d_0)}$, then

$$\log|B| \leqslant \left(1 - \frac{c}{4C(m_0,d_0)}\right)\log|G|. \tag{104}$$

By (102) and (104), we obtain

$$1 - (3C(m_0,d_0)-1)R\gamma \leqslant 1 - \frac{c}{4C(m_0,d_0)},$$

which is a contradiction for $\gamma < \frac{c}{4RC(m_0,d_0)(3C(m_0,d_0)-1)}$. This finishes proof of Claim 1.

Claim 2. Suppose $|G| \gg_{m_0,d_0,c,c_0} 1$ where the implied constant is the one given by Claim 1 to avoid the *small cases*. Suppose $\gamma_0 := \gamma_0(m_0,d_0,c,c_0)$ is the positive number given in Claim 1. Let i_0 be the smallest integer more than $1/\gamma_0$. Then

$$H_2(Y^{(i_0)}) \geqslant \left(1 - \frac{c}{2C(m_0,d_0)}\right)\log|G|. \tag{105}$$

Proof of Claim 2. Suppose to the contrary that (105) does not hold. Since the Rényi entropy is non-decreasing along a random-walk, we deduce that (94) does not hold for every non-negative integer $i \leqslant i_0$. Hence, by Claim 1, for every non-negative integer $i \leqslant i_0$, we should *gain entropy*; that means (95) should hold. Therefore,

$$H_2(Y^{(i_0)}) > \log|G|,$$

which is a contradiction. This finishes proof of Claim 2.

Finishing proof of Proposition 19. By Lemma 20, G is $\frac{c}{C(m_0,d_0)}$-quasi-random. By Claim 2,

$$H_2(X_{2^{i_0}\ell_0}) \geqslant \left(1 - \frac{c}{2C(m_0,d_0)}\right)\log|G|;$$

and so by Proposition 2, we obtain

$$\mathcal{L}(X) \geqslant \frac{cc_0}{2^{i_0+3}C(m_0,d_0)}.$$

This finishes our proof of Proposition 19.

7. Checking (G1)-(G9) for certain groups

In this section, we are going to prove that certain family of finite groups satisfy the properties (G1)-(G9). The main intention of these results is to provide examples on how to apply Theorem 12, Theorem 15, and Proposition 19. These results are not intended to be viewed as the best of their type.

7.1. Product of finite almost simple groups of Lie type and (G1), (G2), and (G3).

Here, we recall results about finite simple groups of Lie type and study finite product of such groups.

Proposition 25. *For every integer $1 \leqslant i \leqslant m$, suppose q_i is a power of a prime p_i. Suppose $\mathbb{F}_{q_i}$ is a finite field of order q_i, and $\mathbb{H}_i$ is an absolutely almost simple $\mathbb{F}_{q_i}$-group. Let $H_i := \mathbb{H}_i(\mathbb{F}_{q_i})^+$ be the subgroup generated by the elements of order p_i. Suppose there is a positive number C such that*

$$C^{-1} \leqslant \frac{\log|H_i|}{\log|H_j|} \leqslant C \tag{106}$$

for every $1 \leqslant i, j \leqslant m$. Let $H := H_1 \oplus \cdots \oplus H_m$. Then H is c-quasi-random where c is a positive number which only depends on m, C, and $\max\{\dim \mathbb{H}_i | \, 1 \leqslant i \leqslant m\}$.

Proof. By [22], for every i, there is a positive number c_i which only depends on $\dim \mathbb{H}_i$ such that H_i is c_i-quasi-random. Suppose ρ is a non-trivial irreducible representation of G. Then the restriction of ρ to at least one of the H_i's is non-trivial. Hence, by the fact that H_i is c_i-quasi-random and (106), we have

$$\deg \rho \geqslant \min\{|H_i|^{c_i} | \, 1 \leqslant i \leqslant m\} \geqslant |H|^{\frac{\min\{c_i | \, 1 \leqslant i \leqslant m\}}{C(m-1)+1}}.$$

Therefore H is $\frac{\min\{c_i | \, 1 \leqslant i \leqslant m\}}{C(m-1)+1}$-quasi-random. □

Next we address the (G3) property.

Proposition 26. *For every integer $1 \leqslant i \leqslant m$, suppose q_i is a power of a prime p_i. Suppose $\mathbb{F}_{q_i}$ is a finite field of order q_i, and $\mathbb{H}_i$ is an absolutely almost simple $\mathbb{F}_{q_i}$-group. Let $H_i := \mathbb{H}_i(\mathbb{F}_{q_i})^+$ be the subgroup generated by the elements of order p_i. Suppose $H := \bigoplus_{i=1}^m H_i$. Then, there is a constant C which only depends on $\max_i \dim \mathbb{H}_i$ such that, for every $x \in H$,*

$$Z(H) \prod\nolimits_C \mathrm{Cl}(x) \supseteq N_x,$$

where N_x is the smallest normal subgroup of H which contains x.

Proof. Notice that if $x = (x_1, \ldots, x_m) \in H$, then $\mathrm{Cl}(x) = \mathrm{Cl}(x_1) \times \cdots \times \mathrm{Cl}(x_m)$. Hence, for every positive integer C, we have

$$Z(H) \prod\nolimits_C \mathrm{Cl}(x) = \prod\nolimits_{i=1}^m (Z(H_i) \prod\nolimits_C \mathrm{Cl}(x_i)). \tag{107}$$

By [23, Theorem 1.1] (see also [28, Theorem 7.1]), there is a fixed positive integer a such that

$$H_i = Z(H_i) \prod\nolimits_{a\lfloor \log|H_i| / \log|\mathrm{Cl}(x_i)| \rfloor} \mathrm{Cl}(x_i) \tag{108}$$

if $x_i \notin Z(H_i)$. By [22], H_i is c-quasi-random for some positive number c which only depends on $\dim \mathbb{H}_i$. Hence,

$$\frac{\log|H_i|}{\log|\mathrm{Cl}(x_i)|} \leqslant \frac{1}{c} \tag{109}$$

if $x_i \notin Z(H_i)$. By (108) and (109), we conclude that

$$Z(H)\prod_{\lfloor a/c\rfloor}\mathrm{Cl}(x) \supseteq Z(H)\bigoplus_{x_i\notin Z(H_i)} H_i \supseteq N_x.$$

□

Finally, we point out that the order of the center of a semisimple group can be bounded by its dimension from above.

Lemma 27. *For every integer $1 \leqslant i \leqslant m$, suppose q_i is a power of a prime p_i. Suppose $\mathbb{F}_{q_i}$ is a finite field of order q_i, and $\mathbb{H}_i$ is an absolutely almost simple $\mathbb{F}_{q_i}$-group. Let $H_i := \mathbb{H}_i(\mathbb{F}_{q_i})^+$ be the subgroup generated by the elements of order p_i. Suppose $H := \bigoplus_{i=1}^m H_i$. Then,*

$$|Z(H)| \leqslant \log|H|$$

if $|H|$ is sufficiently large depending only on m and $\max\{\dim \mathbb{H}_i\}$.

Proof. Suppose r_i is the absolute rank of $\mathbb{H}_i$. Then $|Z(H_i)| \leqslant r_i + 1$. Hence $|Z(H)| \leqslant \prod_{i=1}^m (1+r_i)$, which finishes the proof. □

7.2. **Certain unipotent group schemes over rings with large characteristic.** In this section, we study unipotent closed subgroups of $(\underline{\mathrm{GL}_n})_A$ where A is a unital commutative ring whose characteristic is either 0 or large compared to n. In order to formulate the main result of this section, we start by reviewing the definition of the exponential and the logarithmic maps.

The exponential and the logarithmic maps can be viewed as elements in the ring of power series with coefficients in $\mathbb{Q}$. We have

$$\exp(x) := \sum_{i=0}^{\infty}\frac{x^i}{i!},\quad \log(1-x) := -\sum_{i=1}^{\infty}\frac{x^i}{i},\quad \exp(\log x) = x,\quad \text{and}\quad \log(\exp x) = x.$$

We view them as functions and *evaluate* them whenever that makes sense.

Let $\underline{\mathrm{Nil}}_n^+$ and $\underline{\mathrm{Uni}}_n^+$ be the closed $\mathbb{Z}$-affine schemes given by the following functors:

$$\underline{\mathrm{Nil}}_n^+(A) := \{x \in \mathfrak{gl}_n(A) \,|\, x_{ij} = 0 \text{ if } i \leqslant j\},$$

and

$$\underline{\mathrm{Uni}}_n^+(A) := \{u \in \mathrm{GL}_n(A) \,|\, u_{ij} = 0 \text{ if } i < j \text{ and } u_{ii} = 1 \text{ for every } i\}.$$

In this section, the i,j entry of a matrix x is denoted by x_{ij}. Notice that for every ring A and $x \in \underline{\mathrm{Nil}}_n^+(A)$, we have $x^n = 0$. Hence, exp and log define isomorphisms between $(\underline{\mathrm{Nil}}_n^+)_{\mathbb{Z}[1/n!]}$ and $(\underline{\mathrm{Uni}}_n^+)_{\mathbb{Z}[1/n!]}$.

Now, we state the main result of this section. This result will be used to study the fibers of a smooth unipotent $\mathbb{Z}[1/q_0]$-group scheme over points in a Zariski-open subset of $\mathrm{Spec}(\mathbb{Z}[1/q_0])$.

Proposition 28. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra. Suppose $\mathfrak{u}$ is a Lie A-subalgebra of $\underline{\mathrm{Nil}}_n^+(A)$. Let $\mathfrak{u}_1 := \mathfrak{u}$ and $\mathfrak{u}_{i+1} := [\mathfrak{u},\mathfrak{u}_i]$ be the Abelian subgroup of $\mathfrak{u}$ which is generated by $\{[x,y] \,|\, x \in \mathfrak{u}, y \in \mathfrak{u}_i\}$, for every positive integer i. Let $U_i := \exp \mathfrak{u}_i$ for every positive integer. Then*

$$\gamma_i(U_1) = U_i$$

for every positive integer i.

The following is a consequence of Proposition 28 that will be used in this work. This result has two key points. (1) In general, there is no satisfactory theory of lower central series for group schemes. Here, for very special group schemes, with the help of the exponential and the logarithmic maps, we define certain subschemes that can be viewed as lower central series. (2) We study the set of rational points of the lower central series of fibers over closed points of the considered group schemes, and describe the Abelianization of these fibers.

Proposition 29. *Suppose* $\underline{U}$ *is a subgroup scheme of* $\underline{\mathrm{Uni}}^+_{n\,\mathbb{Z}[1/\overline{q_0}]}$ *and* $\underline{U}_{\mathbb{Q}}$ *is an algebraic subgroup of* $\underline{\mathrm{Uni}}^+_{n\,\mathbb{Q}}$. *Then there exists a positive multiple* q_0 *of* $\mathrm{lcm}(n!, \overline{q_0})$ *for which the following statements hold.*

Suppose $\mathfrak{u} := \mathrm{Lie}(\underline{U})(\mathbb{Z}[1/q_0])$. *Let* $\mathfrak{u}_1 := \mathfrak{u}$ *and* $\mathfrak{u}_{i+1} := [\mathfrak{u}, \mathfrak{u}_i]$. *Suppose* F *is a field whose characteristic is either* 0 *or not dividing* q_0. *Then,*

(1) $\underline{U}_{\mathbb{Z}[1/q_0]}$ *is a smooth group scheme. In particular, the following statements hold:*
   (a) $\underline{U}_F$ *is a unipotent algebraic group over* F.
   (b) *There is a natural* A*-module isomorphism*

$$\iota_A : \mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A) \to \mathfrak{u} \otimes_{\mathbb{Z}[1/q_0]} A$$

   for every unital commutative $\mathbb{Z}[1/q_0]$*-algebra* A.

(2) *For every positive integer* i, *there is a smooth subgroup scheme* $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})$ *of* $\underline{U}_{\mathbb{Z}[1/q_0]}$ *with the following properties:*
   (a) *For every unital commutative* $\mathbb{Z}[1/q_0]$*-algebra* A, *we have*

$$\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})(A) = \exp(\iota_A^{-1}(\mathfrak{u}_i \otimes_{\mathbb{Z}[1/q_0]} A)).$$

   (b) *For every unital commutative* $\mathbb{Z}[1/q_0]$*-algebra* A, *we have*

$$\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})(A) = \gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]}(A)),$$

   where $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]}(A))$ *is the* i*-th lower central series of the group* $\underline{U}_{\mathbb{Z}[1/q_0]}(A)$.
   (c) *For every positive integer* i, *we have* $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})_F = \gamma_i(\underline{U}_F)$ *where* $\gamma_i(\underline{U}_F)$ *is the* i*-th lower central series of the algebraic group* $\underline{U}_F$.

(3) *For every positive integer* i *and every unital commutative* F*-algebra* B, *we have*

$$\gamma_i(\underline{U}_F)(B) = \gamma_i(\underline{U}_F(B)).$$

(4) *Let* $\underline{U}_F^{\mathrm{ab}}$ *be the Abelianization of the* F*-algebraic group* $\underline{U}_F$. *Then there is a natural* B*-module isomorphism* $f_B : \underline{U}_F^{\mathrm{ab}}(B) \to (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} B$ *which is a composite of natural isomorphisms,*

$$\underline{U}_F^{\mathrm{ab}}(B) \xrightarrow{\sim} \frac{\underline{U}_F(B)}{\gamma_2(\underline{U}_F)(B)} \xrightarrow{\sim} \frac{\mathfrak{u} \otimes_{\mathbb{Z}[1/q_0]} B}{\mathfrak{u}_2 \otimes_{\mathbb{Z}[1/q_0]} B} \xrightarrow{\sim} (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} B$$

   and the second isomorphism is induced by $\iota_B \circ \log$.

Before we get to the proof of Proposition 28, we recall some basic properties of the exponential and the logarithmic maps. Viewing $\exp(x)$ and $\exp(y)$ as elements of the non-commutative ring $\mathbb{Q}\langle\langle x, y\rangle\rangle$ of power series with variables x and y, the Baker-Campbell-Hausdorff-Dynkin formula states that $x\#y := \log(\exp(x)\exp(y))$

is equal to

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \sum_{m_i,n_i\geqslant 0, m_i+n_i>0} \frac{1}{(\sum_{i=1}^{k}(m_i+n_i))\prod_{i=1}^{k}(m_i!n_i!)} Z_{\mathbf{m},\mathbf{n}}(x,y), \tag{110}$$

where $\mathbf{m} := (m_1,\dots,m_k)$, $\mathbf{n} := (n_1,\dots,n_k)$, and

$$Z_{\mathbf{m},\mathbf{n}}(x,y) := [\underbrace{x,\dots,x}_{m_1},\underbrace{y,\dots,y}_{n_1},\dots,\underbrace{x,\dots,x}_{m_k},\underbrace{y,\dots,y}_{n_k}] = \operatorname{ad}(x)^{m_1}\operatorname{ad}(y)^{n_1}\cdots\operatorname{ad}(y)^{n_k-1}(y)$$

is a long commutator. Notice that for every commutative ring A and $x_1,\dots,x_n \in \underline{\mathrm{Nil}}_n^+(A)$, we have $x_1\cdots x_n = 0$. This implies that $\operatorname{ad}(x_1)\cdots\operatorname{ad}(x_{n-1})(x_n) = 0$ for every $x_1,\dots,x_n \in \underline{\mathrm{Nil}}_n^+(A)$. Therefore, $Z_{\mathbf{m},\mathbf{n}}(x,y) = 0$ for every $x,y \in \underline{\mathrm{Nil}}_n^+(A)$ if $\|\mathbf{m}\|_1 + \|\mathbf{n}\|_1 \geqslant n$. Hence, for every unital commutative $\mathbb{Z}[1/n!]$-algebra A and $x,y \in \underline{\mathrm{Nil}}_n^+(A)$,

$$x\#y = \sum_{k=1}^{n-1} \frac{(-1)^{k-1}}{k} \sum_{m_i,n_i\geqslant 0, m_i+n_i>0, \|\mathbf{m}\|_1+\|\mathbf{n}\|_1<n} \frac{1}{(\sum_{i=1}^{k}(m_i+n_i))\prod_{i=1}^{k}(m_i!n_i!)} Z_{\mathbf{m},\mathbf{n}}(x,y). \tag{111}$$

We refer to (111) as the *n-truncated BCHD formula*. Notice that since the multiplication in $\underline{\mathrm{Uni}}_n^+(A)$ is an associative operation, so is $\#$; this means for every $x,y,z \in \underline{\mathrm{Nil}}_n^+(A)$, we have

$$x\#(y\#z) = (x\#y)\#z.$$

Lemma 30. *Suppose A is a unital commutative ring, n is an integer, and $n! \in A^\times$. Suppose $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. Then $\exp(\mathfrak{u})$ is a subgroup of $\underline{\mathrm{Uni}}_n^+(A)$.*

Proof. This is an immediate corollary of the n-truncated BCHD formula. □

For a Lie ring $\mathfrak{u}$, let $\mathfrak{u}_1 := \mathfrak{u}$ and $\mathfrak{u}_{i+1} := [\mathfrak{u}_i,\mathfrak{u}]$ be the Abelian subgroup generated by $[x,y]$'s as x and y range in $\mathfrak{u}_i$ and $\mathfrak{u}$, respectively. Notice that because

$$\operatorname{ad}([x,y])(z) = \operatorname{ad}(x)\operatorname{ad}(y)(z) - \operatorname{ad}(y)\operatorname{ad}(x)(z),$$

for every $x,y,z \in \mathfrak{u}$, we have

$$[\mathfrak{u}_i,\mathfrak{u}_j] \subseteq \mathfrak{u}_{i+j}, \tag{112}$$

where the left hand side is the Abelian subgroup generated by $\{[x,y] |\, x, \in \mathfrak{u}_i, y \in \mathfrak{u}_j\}$. For every $x \in \mathfrak{u}\backslash\{0\}$, let $\nu_{\mathfrak{u}}(x)$ be the largest positive integer i such that $x \in \mathfrak{u}_i$. Let $\nu_{\mathfrak{u}}(0) := \infty$. Notice that by (112), we have

$$\nu_{\mathfrak{u}}([x,y]) \geqslant \nu_{\mathfrak{u}}(x) + \nu_{\mathfrak{u}}(y), \tag{113}$$

for every $x,y \in \mathfrak{u}$. It is worth pointing out that $\nu_{\mathfrak{u}}$ satisfies the usual valuation properties; that means $\nu_{\mathfrak{u}}(x \pm y) \geqslant \min\{\nu_{\mathfrak{u}}(x),\nu_{\mathfrak{u}}(y)\}$ and equality holds if $\nu_{\mathfrak{u}}(x) \neq \nu_{\mathfrak{u}}(y)$.

Based on (113), the following is an immediate consequence of the n-truncated BCHD formula.

Lemma 31. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra and $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. Then, for $x,y \in \mathfrak{u}$,*

$$\nu_{\mathfrak{u}}\left((x\#y) - (x+y+\frac{1}{2}[x,y])\right) \geqslant \nu_{\mathfrak{u}}(x) + \nu_{\mathfrak{u}}(y) + \min\{\nu_{\mathfrak{u}}(x),\nu_{\mathfrak{u}}(y)\}, \tag{114}$$

$$\nu_{\mathfrak{u}}\Big(x\#y\#(-x)\#(-y)-[x,y]\Big)\geqslant \nu_{\mathfrak{u}}(x)+\nu_{\mathfrak{u}}(y)+\min\{\nu_{\mathfrak{u}}(x),\nu_{\mathfrak{u}}(y)\}, \tag{115}$$

and for some $\gamma\in\exp(\mathfrak{u}_{\nu_{\mathfrak{u}}(x)+\nu_{\mathfrak{u}}(y)+\min\{\nu_{\mathfrak{u}}(x),\nu_{\mathfrak{u}}(y)\}})$

$$\exp([x,y])=\gamma[\exp x,\exp y], \tag{116}$$

where $[\exp x,\exp y]=(\exp x)(\exp y)(\exp x)^{-1}(\exp y)^{-1}$.

Proof. We leave (114) to the reader to verify based on the n-truncated BCHD formula. Let $i:=\nu_{\mathfrak{u}}(x)$ and $j:=\nu_{\mathfrak{u}}(y)$. Using (114) for $-x$ and $-y$, we obtain

$$(-x)\#(-y)\in -x-y+\frac{1}{2}[x,y]+\mathfrak{u}_{i+j+\min\{i,j\}}. \tag{117}$$

Another application of (114) together with (117) and (112) implies that,

$$\begin{aligned}(x\#y)\#((-x)\#(-y))&\in\Big(x+y+\frac{1}{2}[x,y]\Big)+\Big(-x-y+\frac{1}{2}[x,y]\Big)+\mathfrak{u}_{i+j+\min\{i,j\}}\\&=[x,y]+\mathfrak{u}_{i+j+\min\{i,j\}}.\end{aligned}$$

Finally, we again use (114) together with (115) to obtain

$$[x,y]\#(y\#x\#(-y)\#(-x))\in[x,y]+[y,x]+\mathfrak{u}_{i+j+\min\{i,j\}}=\mathfrak{u}_{i+j+\min\{i,j\}}.$$

Hence,

$$\exp([x,y])[\exp x,\exp y]^{-1}\in\exp(\mathfrak{u}_{i+j+\min\{i,j\}}).$$

□

Lemma 32. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra and $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. For every positive integer i, let $U_i:=\exp(\mathfrak{u}_i)$. Then, the following statements hold.*

1. *$U_1\supseteq\cdots\supseteq U_n$ is a chain of normal subgroups of U_1, and $U_n=\{1\}$.*
2. *For every positive integer i and j, $[U_i,U_j]\subseteq U_{i+j}$; in particular, $\gamma_i(U_1)\subseteq U_i$ for every positive integer i.*
3. *If $x,y\in\mathfrak{u}_i$, then $\exp(x+y)\in(\exp x)(\exp y)\,U_{2i}$.*

Proof. By Lemma 30, we know that U_i's are subgroups and clearly $U_1\supseteq\cdots\supseteq U_n$. Since $x_1\cdots x_n$ is 0 for every $x_1,\ldots,x_n\in\underline{\mathrm{Nil}}_n^+(A)$, $\mathfrak{u}_n=0$. Thus, $U_n=\{1\}$.

For every $x\in\mathfrak{u}$ and $y\in\mathfrak{u}_i$, we have

$$\mathrm{Ad}(\exp(x))(y)=\exp(\mathrm{ad}(x))(y)\in\mathfrak{u}_i.$$

Hence, for every $x\in\mathfrak{u}$ and $y\in\mathfrak{u}_i$,

$$\exp(x)\exp(y)\exp(x)^{-1}=\exp(\mathrm{Ad}(\exp(x))(y))\in U_i.$$

This implies that for every positive integer i, U_i is a normal subgroup of U_1.

Suppose $x\in\mathfrak{u}_i$ and $y\in\mathfrak{u}_j$. Then, by (116) (in Lemma 31), we obtain

$$[\exp x,\exp y]\in U_{i+j+\min\{i,j\}}\exp([x,y])\subseteq U_{i+j}.$$

Hence, $[U_i,U_j]\subseteq U_{i+j}$. Now, by induction on i, we deduce that $\gamma_i(U_1)\subseteq U_i$ for every positive integer i.

By (114) (in Lemma 31), we have

$$(x+y)\#((-y)\#(-x))\in\mathfrak{u}_{2i}$$

for every positive integer i and $x,y\in\mathfrak{u}_i$. Therefore, in this case, we have

$$\exp(x+y)(\exp y)^{-1}(\exp x)^{-1}\in U_{2i}.$$

□

In Lemma 33, we estimate the logarithm of a long commutator. For $g_1, \dots, g_{m+1} \in \underline{\mathrm{Uni}}_n^+(A)$, we define the long commutator $[g_1, \dots, g_{m+1}]$, recursively. Let $c_1 := g_1$ and $c_{i+1} := [g_{i+1}, c_i]$ for every positive integer $i \leqslant m$.

Lemma 33. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra and $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. Suppose m is a positive integer and $x_0, \dots, x_m \in \mathfrak{u}$. Then*

$$\nu_{\mathfrak{u}}(\log[\exp(x_m), \dots, \exp(x_0)] - [x_m, \dots, x_0]) \geqslant \sum_{i=0}^{m} \nu_{\mathfrak{u}}(x_i) + \min\{\nu_{\mathfrak{u}}(x_i) \mid 0 \leqslant i \leqslant m\}.$$

Proof. We proceed by induction on m. Notice that by (115)

$$\nu_{\mathfrak{u}}(\log[\exp x, \exp y] - [x, y]) \geqslant \nu_{\mathfrak{u}}(x) + \nu_{\mathfrak{u}}(y) + \min\{\nu_{\mathfrak{u}}(x), \nu_{\mathfrak{u}}(y)\},$$

which implies the base of induction. Next, we prove the induction step. Suppose the claim is true for m, and we want to prove it for $m+1$. Let

$$z := \log[\exp(x_m), \dots, \exp(x_0)].$$

Then by (115), we have

(118)
$$\nu_{\mathfrak{u}}(\log[\exp(x_{m+1}), \exp(z)] - [x_{m+1}, z]) \geqslant \nu_{\mathfrak{u}}(x_{m+1}) + \nu_{\mathfrak{u}}(z) + \min\{\nu_{\mathfrak{u}}(x_{m+1}), \nu_{\mathfrak{u}}(z)\}.$$

By the induction hypothesis, we obtain

$$\nu_{\mathfrak{u}}(z - [x_m, \dots, x_0]) \geqslant \sum_{i=0}^{m} \nu_{\mathfrak{u}}(x_i) + \min\{\nu_{\mathfrak{u}}(x_i) \mid 0 \leqslant i \leqslant m\}. \tag{119}$$

By (119) and (113), we deduce that

$$\nu_{\mathfrak{u}}([x_{m+1}, z] - [x_{m+1}, \dots, x_0]) \geqslant \sum_{i=0}^{m+1} \nu_{\mathfrak{u}}(x_i) + \min\{\nu_{\mathfrak{u}}(x_i) \mid 0 \leqslant i \leqslant m\}. \tag{120}$$

By (113), $\nu_{\mathfrak{u}}([x_m, \dots, x_0]) \geqslant \sum_{i=0}^{m} \nu_{\mathfrak{u}}(x_i)$. Hence, by (119), we obtain

$$\nu_{\mathfrak{u}}(z) \geqslant \sum_{i=0}^{m} \nu_{\mathfrak{u}}(x_i). \tag{121}$$

By (118), (121), and (120), we obtain that

$$\nu_{\mathfrak{u}}(\log[\exp(x_{m+1}), \dots, \exp(x_0)] - [x_{m+1}, \dots, x_0]) \geqslant \sum_{i=0}^{m+1} \nu_{\mathfrak{u}}(x_i) + \min\{\nu_{\mathfrak{u}}(x_i) \mid 0 \leqslant i \leqslant m+1\}.$$

This finishes proof of the induction step. □

Corollary 34. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra and $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. For every positive integer i, let $U_i := \exp(\mathfrak{u}_i)$. Then, for every positive integer m and $x_0, \dots, x_m \in \mathfrak{u}$,*

$$\exp([x_m, \dots, x_0]) \in [\exp x_m, \dots, \exp x_0] U_{m+2}.$$

In particular,

$$\exp([x_m, \dots, x_0]) \in \gamma_{m+1}(U_1)\, U_{m+2}.$$

Proof. By Lemma 33, we have

(122)
$$\nu_{\mathfrak{u}}(\log[\exp x_m,\dots,\exp x_0]-[x_m,\dots,x_0])\geqslant\sum_{i=0}^{m}\nu_{\mathfrak{u}}(x_i)+\min\{\nu_{\mathfrak{u}}(x_i)|\,0\leqslant i\leqslant m\}.$$

In particular, we obtain

$$\nu_{\mathfrak{u}}(\log[\exp x_m,\dots,\exp x_0])\geqslant\sum_{i=0}^{m}\nu_{\mathfrak{u}}(x_i) \tag{123}$$

as (113) implies that $\nu_{\mathfrak{u}}([x_m,\dots,x_0])\geqslant\sum_{i=0}^{m}\nu_{\mathfrak{u}}(x_i)$.

By (114) and (122), we obtain

$$\nu_{\mathfrak{u}}(\log[\exp x_m,\dots,\exp x_0]\#(-[x_m,\dots,x_0]))\geqslant\sum_{i=0}^{m}\nu_{\mathfrak{u}}(x_i)+\min\{\nu_{\mathfrak{u}}(x_i)|\,0\leqslant i\leqslant m\}\geqslant m+2.$$

Therefore,

$$[\exp x_m,\dots,\exp x_0]\exp([x_m,\dots,x_0])^{-1}\in U_{m+2}.$$

This finishes proof of this corollary. □

Lemma 35. *Suppose A is a unital commutative $\mathbb{Z}[1/n!]$-algebra and $\mathfrak{u}$ is a Lie subalgebra over A of $\underline{\mathrm{Nil}}_n^+(A)$. For every positive integer i, let $U_i:=\exp(\mathfrak{u}_i)$. Then, $\gamma_{n-i}(U_1)\supseteq U_{n-i}$ for every non-negative integer $i\leqslant n-1$.*

Proof. We proceed by induction on i. By part (1) of Lemma 32, $U_n=\{1\}$, and so the base of induction follows. Suppose $U_{n-i+1}\subseteq\gamma_{n-i+1}(U_1)$. We want to prove that $U_{n-i}\subseteq\gamma_{n-i}(U_1)$. If $i=n-1$, there is nothing to prove as $\gamma_1(U_1)=U_1$. So without loss of generality, we can and will assume that $n-i>1$.

By Part (3) of Lemma 32, $U_{n-i}/U_{2(n-i)}$ is generated by cosets that are represented by elements of the form

$$\exp([x_1,\dots,x_{n-i}]). \tag{124}$$

Hence, U_{n-i}/U_{n-i+1} is generated by cosets that are represented by elements of the form given in (124). By Corollary 34,

$$\exp([x_1,\dots,x_{n-i}])U_{n-i+1}\in\gamma_{n-i}(U_1)U_{n-i+1}.$$

Therefore, $U_{n-i}\subseteq\gamma_{n-i}(U_1)U_{n-i+1}$. By the induction hypothesis, we obtain that $U_{n-i}\subseteq\gamma_{n-i}(U_1)$. □

Proof of Proposition 28. By Part (2) of Lemma 32, for every positive integer i, we have

$$\gamma_i(U_1)\subseteq U_i,$$

and by Lemma 35, for every positive integer i, we have

$$\gamma_i(U_1)\supseteq U_i.$$

Therefore, the claim follows. □

Proof of Proposition 29. By the *spreading out* results ([16, Theorem 9.7.7 and Theorem 12.2.4]; see also [14, Theorem 40 and Section A.1] for an effective version), since $\underline{U}_{\mathbb{Q}}$ is smooth and irreducible, there is a positive integer q_0 such that $\underline{U}_{\mathbb{Z}[1/q_0]}$

is smooth and the fiber $\underline{U}_{\mathbb{Z}/p\mathbb{Z}}$ is a connected algebraic group defined over $\mathbb{Z}/p\mathbb{Z}$ and it is of dimension $\dim \underline{U}_{\mathbb{Q}}$ for every prime p which does not divide q_0.

Since $\underline{U}_{\mathbb{Z}[1/q_0]}$ is a smooth group scheme, there is a natural A-module isomorphism

$$\iota_A : \mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A) \to \mathfrak{u} \otimes_{\mathbb{Z}[1/q_0]} A \tag{125}$$

for every $\mathbb{Z}[1/q_0]$-algebra A, where $\mathfrak{u}$ (see [7, Chapter II, Section 4, Proposition 4.8]). This implies part (1).

By (125), ι_A induces an isomorphism

$$\iota_A : \mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A)_i \to \mathfrak{u}_i \otimes_{\mathbb{Z}[1/q_0]} A \tag{126}$$

for every positive integer i, where

$$\mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A)_i = [\underbrace{\mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A), \dots, \mathrm{Lie}(\underline{U}_{\mathbb{Z}[1/q_0]})(A)}_{i\text{-times}}].$$

By passing to a multiple of q_0, we can and will assume that $\underline{\mathrm{Nil}}^+_n(\mathbb{Z}[1/q_0])/\mathfrak{u}_i$ is a free $\mathbb{Z}[1/q_0]$-module for every positive integer i. Hence, for every positive integer i, $\mathfrak{u}_i$ defines a smooth subscheme of $\underline{\mathrm{Nil}}^+_n$. Because $\exp : \underline{\mathrm{Nil}}^+_{n\,\mathbb{Z}[1/q_0]} \to \underline{\mathrm{Uni}}^+_{n\,\mathbb{Z}[1/q_0]}$ is a $\mathbb{Z}[1/q_0]$-scheme isomorphism and because of Lemma 30, for every positive integer i, the following functor from the category of $\mathbb{Z}[1/q_0]$-algebras to the category of groups is a subgroup scheme of $\underline{U}_{\mathbb{Z}[1/q_0]}$,

$$A \mapsto \exp(\iota_A^{-1}(\mathfrak{u}_i \otimes_{\mathbb{Z}[1/q_0]} A)). \tag{127}$$

We denote this subgroup scheme of $\underline{\mathrm{Uni}}^+_{n\,\mathbb{Z}[1/q_0]}$ by $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})$ (it should be said that this is *only* a notation, and it does not mean *the i-th lower central series* of the group scheme $\underline{U}_{\mathbb{Z}[1/q_0]}$ as it was mentioned earlier there is *no* satisfactory theory of lower central series for an arbitrary group scheme). This implies part (2a).

Notice that $\gamma_1(\underline{U}_{\mathbb{Z}[1/q_0]}) = \underline{U}_{\mathbb{Z}[1/q_0]}$ as the logarithm of this group scheme gives us the Lie algebra of $\underline{U}_{\mathbb{Z}[1/q_0]}$ and $\log : \underline{\mathrm{Uni}}^+_{n\,\mathbb{Z}[1/q_0]} \to \underline{\mathrm{Nil}}^+_{n\,\mathbb{Z}[1/q_0]}$ is an isomorphism of $\mathbb{Z}[1/q_0]$-schemes. Furthermore, by definition, $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})$ is isomorphic to its Lie algebra, and for every unital commutative $\mathbb{Z}[1/q_0]$-algebra A, ι_A induces an isomorphism

$$\iota_A : \mathrm{Lie}(\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]}))(A) \to \mathfrak{u}_i \otimes_{\mathbb{Z}[1/q_0]} A. \tag{128}$$

By (128), we deduce that for every field F which is a $\mathbb{Z}[1/q_0]$-algebra, $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})_F$ is a connected algebraic group over F.

On the other hand, since $\underline{U}_F$ is a connected F-algebraic group, for every positive integer i, we can define its algebraic i-th lower central series $\gamma_i(\underline{U}_F)$, it is a connected F-algebraic subgroup of $\underline{U}_F$, and for every F-algebra B,

$$\mathrm{Lie}(\gamma_i(\underline{U}_F))(B) = \mathrm{Lie}(\underline{U}_F)(B)_i \tag{129}$$

(see [7, Chapter II, Section 5, Propositions 4.8 and 4.9, and Chapter II, Section 6, Proposition 2.3]). By (126), (129), and (128), we conclude that

$$\mathrm{Lie}(\gamma_i(\underline{U}_F))(B) = \mathrm{Lie}(\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]}))(B), \tag{130}$$

for every positive integer i and F-algebra B. By (130) and the fact that both F-algebraic groups $\gamma_i(\underline{U}_F)$ and $\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})_F$ are connected, we deduce that

$$\gamma_i(\underline{U}_F) = \gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})_F. \tag{131}$$

This implies part (2c).

By (127) and Proposition 28, we obtain that

$$\gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]}(A)) = \gamma_i(\underline{U}_{\mathbb{Z}[1/q_0]})(A) \tag{132}$$

for every unital commutative $\mathbb{Z}[1/q_0]$-algebra A; and so part (2b) follows.

By (131) and (132), we obtain that

$$\gamma_i(\underline{U}_F)(B) = \gamma_i(\underline{U}_F(B)) = \exp(\iota_B^{-1}(\mathfrak{u}_i \otimes_{\mathbb{Z}[1/q_0]} B)) \tag{133}$$

for every unital commutative F-algebra B; this finishes proof of part (3).

Since $\underline{\mathrm{Nil}}_n^+(\mathbb{Z}[1/q_0])/\mathfrak{u}_2$ is a free $\mathbb{Z}[1/q_0]$-module, so is $\mathfrak{u}/\mathfrak{u}_2$. Hence, there is a natural A-module isomorphism

$$\pi_A : (\mathfrak{u} \otimes_{\mathbb{Z}[1/q_0]} A)/(\mathfrak{u}_2 \otimes_{\mathbb{Z}[1/q_0]} A) \to (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} A$$

which sends $x \otimes 1 + (\mathfrak{u}_2 \otimes_{\mathbb{Z}[1/q_0]} A)$ to $(x + \mathfrak{u}_2) \otimes 1$. Let

$$\widetilde{f}_A : \underline{U}_{\mathbb{Z}[1/q_0]}(A) \to (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} A, \quad \widetilde{f}_A(x) := \pi_A(\iota_A(\log x) + (\mathfrak{u}_2 \otimes_{\mathbb{Z}[1/q_0]} A)).$$

By Lemma 32 and (127), it follows that $\widetilde{f}_A$ is a natural group homomorphism, it is surjective, and its kernel is $\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]})(A)$. Hence, the following is a natural group isomorphism:

(134)

$$f_A : \frac{\underline{U}_{\mathbb{Z}[1/q_0]}(A)}{\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]})(A)} \to (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} A, \quad f_A(x(\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]})(A))) := \widetilde{f}_A(x).$$

By (131) and (134), we obtain that for every field F which is a $\mathbb{Z}[1/q_0]$-algebra B, f_B induces a natural group isomorphism:

$$\frac{\underline{U}_F(B)}{\gamma_2(\underline{U}_F)(B)} \xrightarrow{\sim} (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} B.$$

Since $\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]})$ and its Lie algebra are isomorphic as $\mathbb{Z}[1/q_0]$-schemes, by (131) $\gamma_2(\underline{U}_F)$ is a connected F-split unipotent F-algebraic group. Hence, by [29, Theorem 14.2.6], $\underline{U}_F$ is isomorphic to $(\underline{U}_F/\gamma_2(\underline{U}_F)) \times \gamma_2(\underline{U}_F)$ as an F-variety. Therefore, for every F-algebra B, there is a natural isomorphism

$$\frac{\underline{U}_F(B)}{\gamma_2(\underline{U}_F)(B)} \xrightarrow{\sim} \left(\frac{\underline{U}_F}{\gamma_2(\underline{U}_F)}\right)(B).$$

Altogether, we get a natural isomorphism (that we still denote by f_B)

$$f_B : \underline{U}_F^{\mathrm{ab}}(B) \xrightarrow{\sim} (\mathfrak{u}/\mathfrak{u}_2) \otimes_{\mathbb{Z}[1/q_0]} B,$$

where B is a unital commutative F-algebra and $\underline{U}_F^{\mathrm{ab}}$ is the Abelianization of the F-algebraic group $\underline{U}_F$. □

7.3. **Modules of product of finite almost simple groups of Lie type and (G6).** The main goal of this subsection is to prove (G6) for certain modules of product of finite almost simple groups of Lie type.

Suppose F is a finite field of characteristic p and order $q := p^n$ where n is a positive integer. We start by studying representations of $\mathrm{SL}_2(F)$ over F. For every positive integer m, $\mathrm{SL}_2(F)$ acts linearly on the space

$$V_m(F) := \left\{ \sum_{i=0}^{m} c_i x^i y^{m-i} \mid c_0, \ldots, c_m \in F \right\} \tag{135}$$

of homogeneous polynomials of degree m with variables x and y over F. This action is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(x,y) := f(ax+cy, bx+dy).$$

Let $\phi : F \to F, \phi(x) := x^p$; let's recall that ϕ generates the group of automorphisms of the field F and it is of order n. Notice that ϕ induces an automorphism of $\mathrm{SL}_2(F)$ that we still denote by ϕ. Let $F[\mathrm{SL}_2(F)]$ be the group ring of $\mathrm{SL}_2(F)$ over the field F. For an $F[\mathrm{SL}_2(F)]$-module M and every integer i, we get a new module $M^{(i)}$ where the Abelian group of $M^{(i)}$ is the same as M and for every $x \in M^{(i)}$ and $h \in \mathrm{SL}_2(F)$, we have

$$h \cdot x := \phi^i(h)x,$$

where $\phi^i(h)x$ is given by the action of H on M. For instance, the action of $\mathrm{SL}_2(F)$ on $V_m^{(i)}(F)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(x,y) := f(a^{p^i}x + c^{p^i}y, b^{p^i}x + d^{p^i}y).$$

For every integer vector $\mathbf{m} := (m_0, \dots, m_{n-1}) \in [0, p-1]^n$, let

$$V_{\mathbf{m}}(F) := V_{m_0}^{(0)}(F) \otimes_F \cdots \otimes_F V_{m_{n-1}}^{(n-1)}(F),$$

and view it as $F[\mathrm{SL}_2(F)]$-module where

$$g \cdot (f_0 \otimes \cdots \otimes f_{n-1}) := (g \cdot f_0) \otimes \cdots \otimes (g \cdot f_{n-1}),$$

for every $g \in \mathrm{SL}_2(F)$ and $(f_0, \dots, f_{n-1}) \in V_{m_0}^{(0)}(F) \times \cdots \times V_{m_n}^{(n-1)}(F)$. Notice that $V_{\mathbf{m}}(F)$ can be identified with the set of polynomials in variables $x_0, y_0, \dots, x_{n-1}, y_{n-1}$ over F that are homogeneous of degree m_j in variables x_j and y_j, and g acts on x_j and y_j as in $V_{m_j}^{(j)}(F)$; this means we can and will view elements of $V_{\mathbf{m}}(F)$ as

$$\sum_{\mathbf{i}} c_{\mathbf{i}} \prod_{j=0}^{n-1} x_j^{i_j} y_j^{m_j - i_j},$$

where the integer vector $\mathbf{i} := (i_0, \dots, i_{n-1})$ ranges in the set $\prod_{j=0}^{n-1}[0, m_j]$ and $c_{\mathbf{i}} \in F$.

The following is an important result of Brauer and Nesbitt (see [4, Section VI.30]) that has been generalized by Steinberg (see [30]).

Proposition 36 (Brauer-Nesbitt)**.** *Suppose F is a finite field of characteristic p and order $q := p^n$. For every integer vector $\mathbf{m}$ in $[0, p-1]^n$, $V_{\mathbf{m}}(F)$ is a simple $F[\mathrm{SL}_2(F)]$-module and every simple $F[\mathrm{SL}_2(F)]$-module is isomorphic to $V_{\mathbf{m}}(F)$ for some such integer vector $\mathbf{m}$.*

Let $u^+(t) := \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $u^-(t) := \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ for $t \in F$, and

$$U^+ := \{u^+(t) \mid t \in F\} \quad \text{and} \quad U^- := \{u^-(t) \mid t \in F\}.$$

Lemma 37 is essentially proved in the mentioned works of Brauer-Nesbitt and Steinberg. But for the reader's convenience, we include its proof.

Lemma 37. *Suppose F is a finite field of characteristic p and of order $q := p^n$. Suppose $\mathbf{m}$ is a non-zero integer vector in $[0, p-1]^n$. Then the set $V_{\mathbf{m}}(F)^{U^+}$ of fixed points of U^+ is equal to*

$$F x_0^{m_0} \cdots x_{n-1}^{m_{n-1}},$$

and the set $V_{\mathbf{m}}(F)^{U^-}$ *of fixed points of* U^- *is equal to*

$$Fy_0^{m_0}\cdots y_{n-1}^{m_{n-1}}.$$

Proof. Suppose $h(x_0,y_0,\dots,x_{n-1},y_{n-1}) := \sum_{\mathbf{i}} c_{\mathbf{i}} \prod_{j=0}^{n-1} x_j^{i_j} y_j^{m_j-i_j}$ is in $V_{\mathbf{m}}(F)^{U^+}$. View h as a polynomial in variables $x_0,\dots,x_{n-1}$ over the ring of coefficients $F[y_0,\dots,y_{n-1}]$. We consider the lexicographic ordering on the monomials in terms of $x_0,\dots,x_{n-1}$, and accordingly define the leading term of a polynomial in $(F[y_0,\dots,y_{n-1}])[x_0,\dots,x_{n-1}]$.

Suppose to the contrary that h is not a multiple of $x_0^{m_0}\cdots x_{n-1}^{m_{n-1}}$. Hence, without loss of generality, we can and will assume that the leading term of h is of the form

$$c_{\mathbf{i}} \prod_{j=0}^{n-1} y_j^{m_j-i_j} \prod_{j=0}^{n-1} x_j^{i_j}$$

for some $\mathbf{i} \neq \mathbf{m}$. For every $t \in F$, we have

$$h = u^+(t)\cdot h = \sum_{\mathbf{i}} c_{\mathbf{i}} \prod_{j=0}^{n-1} x_j^{i_j}(y_j + t^{p^j}x_j)^{m_j-i_j}.$$

For every $\mathbf{i}$, the leading term of $c_{\mathbf{i}} \prod_{j=0}^{n-1} x_j^{i_j}(y_j + t^{p^j}x_j)^{m_j-i_j}$ is equal to

$$c_{\mathbf{i}} t^{\sum_{j=0}^{n-1}(m_j-i_j)p^j} x_0^{m_0}\cdots x_{n-1}^{m_{n-1}}.$$

These add up to $\sum_{\mathbf{i}} c_{\mathbf{i}} t^{\sum_{j=0}^{n-1}(m_j-i_j)p^j}$ times $x_0^{m_0}\cdots x_{n-1}^{m_{n-1}}$. Since the leading term of h is not a multiple of $x_0^{m_0}\cdots x_{n-1}^{m_{n-1}}$, we deduce that

$$\sum_{\mathbf{i}} c_{\mathbf{i}} t^{\sum_{j=0}^{n-1}(m_j-i_j)p^j} = 0$$

for every $t \in F$. Because m_j's are at most $p-1$, the single variable polynomial

$$\sum_{\mathbf{i}} c_{\mathbf{i}} x^{\sum_{j=0}^{n-1}(m_j-i_j)p^j}$$

is of degree at most $q-1$. Since this polynomial has at least q distinct zeros, we obtain that this is the zero polynomial in $F[x]$. Notice that the function $\mathbf{i} \mapsto \sum_{j=0}^{n-1}(m_j-i_j)p^j$ from the set of integer vectors $\mathbf{i}$ in $[0,p-1]^n$ to the set of integers is injective. Hence, $\sum_{\mathbf{i}} c_{\mathbf{i}} x^{\sum_{j=0}^{n-1}(m_j-i_j)p^j} = 0$ implies that $c_{\mathbf{i}} = 0$ for every $\mathbf{i}$. This means $h = 0$ which is a contradiction. By a similar argument, one can show that

$$V_{\mathbf{m}}(F)^{U^-} = Fy_0^{m_0}\dots y_{n-1}^{m_{n-1}}.$$

□

Before we continue with understanding modules of $\mathrm{SL}_2(F)$, we prove a Waring's problem type of result for finite fields. Let's recall that Hardy and Littlewood used Fourier analysis to show that for every integer k there is a positive integer C_k such that every non-negative integer can be written as a sum of C_k elements in $\{x^k \mid x \in \mathbb{Z}\}$. Based on the same principle and certain exponential cancellations, this type of problem has been studied for various finite rings including $\mathbb{Z}/m\mathbb{Z}$ and finite fields. Refined versions of the mentioned Fourier analytic approach, in the finite field case, lead to sharp bounds for C_k. This sharp bound, however, comes with a cost. One needs to assume that $\gcd(|F^\times|,k)$ is less than $\sqrt{|F|}$; this is not a precise inequality, but rather an indication of the magnitude of the upper bound

as $|F|$ gets larger. In our work, we cannot impose this condition on k. So we use a sum-product result to obtain a desired Waring's problem type of result for finite fields. The aforementioned sum-product result is implicitly proved by Bourgain, Katz, and Tao [3, Theorem 4] and explicitly formulated (and proved) by the first author in [11, Lemma 43].

Lemma 38. *For every $\varepsilon > 0$, there is a positive integer C_ε such that the following statement holds. Suppose E is a finite field. Suppose k is a positive integer which is at most $|E|^{1-\varepsilon}$. Then*

$$\sum_{C_\varepsilon}(E^\times)^k - \sum_{C_\varepsilon}(E^\times)^k$$

is equal to the subfield generated by $(E^\times)^k$.

Proof. Notice that $x \mapsto x^k$ is a group homomorphism from the cyclic group $E^\times$ to itself and its image is $(E^\times)^k$. Hence,

$$|(E^\times)^k| = \frac{|E^\times|}{|\{x \in E \mid x^k = 1\}|} \geqslant \frac{|E^\times|}{k} > |E|^{\varepsilon/2} \tag{136}$$

if $|E| \gg_\varepsilon 1$. In particular, for $|E| \gg_\varepsilon 1$, there is $\alpha \in E^\times$ such that $\alpha^k \neq 1$. Let $\beta := \alpha^k - 1$, and

$$B := \beta^{-1}((E^\times)^k - (E^\times)^k).$$

Then $0, 1$ are in B and $|B| \geqslant |E|^{\varepsilon/2}$. Therefore, by (136) and [11, Lemma 43], there is a positive integer $C' := C'_\varepsilon$ depending only on ε such that

$$\sum_{C'}\prod_{C'} B - \sum_{C'}\prod_{C'} B \tag{137}$$

is a subfield K of E. Notice that since $(E^\times)^k$ is a subgroup of $E^\times$,

$$\prod_{C'} B = \beta^{-C'}(\sum_{2^{C'-1}}(E^\times)^k - \sum_{2^{C'-1}}(E^\times)^k). \tag{138}$$

Thus, by (137) and (138), we obtain

$$\beta^{-C'}(\sum_{C'2^{C'-1}}(E^\times)^k - \sum_{C'2^{C'-1}}(E^\times)^k) = K \tag{139}$$

is a subfield of E. Multiplying both sides of (139) by $(E^\times)^k$, we deduce that

$$K = (E^\times)^k K;$$

and so $(E^\times)^k \subseteq K$. Therefore, the subfield generated by $(E^\times)^k$ is a subfield of K. On the other hand, since $(E^\times)^k \subseteq K$, $\beta \in K$. Thus, by (139), we have

$$K = \sum_{C'2^{C'-1}}(E^\times)^k - \sum_{C'2^{C'-1}}(E^\times)^k,$$

which implies that K is generated by $(E^\times)^k$ as a subfield of E. This means K is the subfield generated by $(E^\times)^k$. The claim follows for fields E whose order is large enough in terms of ε. For small fields, the claim is clear. □

Next, we describe $\mathbb{F}_p[\mathrm{SL}_2(F)]$-submodules of $V_{\mathbf{m}}(F)$ where F is a finite field of characteristic p. Suppose the module structure of $V_{\mathbf{m}}(F)$ is given by the representation $\rho_{\mathbf{m}} : \mathrm{SL}_2(F) \to \mathrm{GL}(V_{\mathbf{m}}(F))$. Let $\overline{F}$ be an algebraic closure of F. For a subfield E of $\overline{F}$ which is either a subfield of F or an extension of F, let $A_E \subseteq \mathrm{End}_{\overline{F}}(V_{\mathbf{m}}(\overline{F}))$ be the E-span of $\rho_{\mathbf{m}}(\mathrm{SL}_2(F))$. Then A_E is an E-subalgebra of $\mathrm{End}_{\overline{F}}(V_{\mathbf{m}}(\overline{F}))$. By Proposition 36, $V_{\mathbf{m}}(\overline{F})$ is a simple $\overline{F}[\mathrm{SL}_2(F)]$-module. Therefore, for every field extension E of F, we have that $A_E = \mathrm{End}_E(V_{\mathbf{m}}(E))$. Let $d_0(\mathbf{m}) := \prod_{i=0}^{n-1}(m_i + 1)$ and notice that $d_0 := d_0(\mathbf{m})$ is the dimension of $V_{\mathbf{m}}(E)$ over E. For every integer

vector $\mathbf{i} := (i_0, \dots, i_{n-1}) \in \prod_{i=0}^{n-1}[0, m_i]$, let $e_{\mathbf{i}} := \prod_{j=0}^{n-1} x_j^{i_j} y_j^{m_j - i_j} \in V_{\mathbf{m}}(\mathbb{F}_p)$. Notice that $e_{\mathbf{i}}$'s form an E-basis of $V_{\mathbf{m}}(E)$. Using this basis, we can and will identify $\mathrm{End}_E(V_{\mathbf{m}}(E))$ with $\mathrm{M}_{d_0}(E)$.

Notice that the domain of $\rho_{\mathbf{m}}$ is always $\mathrm{SL}_2(F)$, and so for a subfield E of F, A_E is a subalgebra of $\mathrm{M}_{d_0}(F)$, and it is *not* necessarily a subalgebra of $\mathrm{M}_{d_0}(E)$. In Lemma 39, we describe the algebraic structure of A_E.

Lemma 39. *Suppose E is a subfield of F. Then in the above setting, there exist $g \in \mathrm{GL}_{d_0}(F)$ and a subfield L of F such that $A_E = g\,\mathrm{M}_{d_0}(L)g^{-1}$.*

Proof. Suppose J is the Jacobson radical of A_E. Since A_E is a finite-dimensional E-algebra, J is a nilpotent ideal (see [27, Proposition 4.4]). Then the F-span of J is a nilpotent ideal of $\mathrm{M}_{d_0}(F)$. Therefore $J = 0$. Because A_E is a finite-dimensional E-algebra and its Jacobson radical is 0, A_E is a semisimple E-algebra (see [27, Proposition a]).

Suppose I is an ideal of A_E. Then there is a central idempotent $e \in A_E$ such that $I = eA_E$ (see [27, Section 3.2, Exercise 3]). Because the F-span of A_E is $\mathrm{M}_{d_0}(F)$ and e is a central element of A_E, e is in the center of $\mathrm{M}_{d_0}(F)$. As the center of $\mathrm{M}_{d_0}(F)$ is F, e is an idempotent element of F. Because the only idempotent elements of a field are 0 and 1, we deduce that e is either 0 or 1. This implies that I is either 0 or A_E. Hence, A_E is a simple algebra. By the Wedderburn-Artin theorem (see [27, Section 3.5]) and Wedderburn's little theorem (see [27, Section 13.6]), A_E is isomorphic to $\mathrm{M}_r(L)$ for some field extension L of E and positive integer r. Moreover, L is the center of A_E, and so it is a subfield of the center of the F-span of A_E. Therefore, L is a subfield of F. Since the F-span of A_E is equal to $\mathrm{M}_{d_0}(F)$, by [27, Proposition a, Section 12.4], there is a well-defined isomorphism $A_E \otimes_L F \to \mathrm{M}_{d_0}(F)$ which sends $x \otimes c$ to cx. Hence, $r = d_0$, which means $A_E \simeq \mathrm{M}_{d_0}(L)$. We view A_E and $\mathrm{M}_{d_0}(L) \subseteq \mathrm{End}_F(F^{d_0})$ as two isomorphic L-central simple subalgebras of $\mathrm{End}_L(F^{d_0})$. Then, by the Skolem-Noether theorem (see [27, Section 12.6]), there is an invertible $g \in \mathrm{End}_L(F^{d_0})$ such that $A_E = g\,\mathrm{M}_{d_0}(L)g^{-1}$ (all viewed as subalgebras of $\mathrm{End}_L(F^{d_0})$).

Claim. We can choose g from $\mathrm{End}_F(F^{d_0})$.

Proof of Claim. Notice that $\mathrm{End}_F(F^{d_0})$ is the centralizer of F in $\mathrm{End}_L(F^{d_0})$, where F is embedded in $\mathrm{End}_L(F^{d_0})$ via the scalar multiplication

$$l_{d_0} : F \to \mathrm{End}_L(F^{d_0}), \quad l_{d_0}(c)(v) := cv,$$

for every $c \in F$ and $v \in F^{d_0}$. Notice that for every positive integer r, the scalar multiplication

$$l_r : F \to \mathrm{End}_L(F^r), \quad l_r(c)(x) := cx$$

is a ring embedding.

For every $c \in F\backslash\{0\}$, we have

$$l_{d_0}(c)g\,\mathrm{M}_{d_0}(L)g^{-1}l_{d_0}(c)^{-1} = l_{d_0}(c)A_E l_{d_0}(c)^{-1} = A_E = g\,\mathrm{M}_{d_0}(L)g^{-1},$$

which implies that

$$g^{-1}l_{d_0}(c)g \in C_{\mathrm{End}_L(F^{d_0})}(\mathrm{M}_{d_0}(L)), \tag{140}$$

for every $c \in F$ (this is the centralizer of $\mathrm{M}_{d_0}(L)$ in $\mathrm{End}_L(F^{d_0})$.). Notice that F^{d_0} can be identified with $L^{d_0} \otimes_L F$ as an L-vector space, and via this identification, $c \in F$ acts via multiplication by $1 \otimes c$ and $x \in \mathrm{M}_{d_0}(L)$ acts via multiplication by

$x \otimes 1$. From this point of view, it is clear that L-linear maps of the form $1 \otimes y$ where $y \in \mathrm{End}_L(F)$ are in the centralizer of $\mathrm{M}_{d_0}(L)$. Choosing an L-basis $\{c_1, \dots, c_{[F:L]}\}$ for F, one can see that $e_i \otimes c_j$'s form a basis for $L^{d_0} \otimes_L F$ where e_i's form the standard basis of L^{d_0}. We use this basis and identify $\mathrm{End}_L(F^{d_0})$ with $\mathrm{M}_{d_0[F:L]}(L)$. Now, a direct computation shows that the centralizer of $\mathrm{M}_{d_0}(L) \otimes \mathrm{id}_{[F:L]}$ in $\mathrm{End}_L(L^{d_0} \otimes_L F)$ is precisely $\mathrm{id}_{d_0} \otimes \mathrm{End}_L(F)$; in the matrix form this means

$$C_{\mathrm{M}_{d_0[F:L]}(L)}(\mathrm{M}_{d_0}(L) \otimes \mathrm{id}_{[F:L]}) = \{\mathrm{id}_{d_0} \otimes x \mid x \in \mathrm{End}_L(F)\}, \tag{141}$$

where here $\otimes$ denotes the Kronecker product of matrices. By (140) and (141), we obtain a function $f : F \to \mathrm{End}_L(F)$ such that

$$g(\mathrm{id}_{d_0} \otimes l_1(c))g^{-1} = \mathrm{id}_{d_0} \otimes f(c), \tag{142}$$

where as above $\otimes$ is the Kronecker tensor product of matrices and $l_1(c) : F \to F$ is given by the scalar multiplication. From (142), we deduce that f is a ring embedding. Since F is a finite field, there is $c_0 \in F$ such that $F = L[c_0]$. Suppose $m_{c_0,L}(x)$ is the minimal polynomial of c_0 over L. Then $f(c_0)$ is an $[F : L]$-by-$[F : L]$ matrix over L whose minimal polynomial is equal to $m_{c_0,L}$. Notice that $\deg m_{c_0,L} = [F : L]$, and so the rational canonical form of $f(c_0)$ is equal to the companion matrix of $m_{c_0,L}$. Therefore, $f(c_0)$ and $l_1(c_0)$ have the same rational canonical forms. Hence, they are conjugate of each other in $M_{[F:L]}(L)$. So, there is $g_0 \in \mathrm{End}_L(F)$ such that

$$g_0^{-1} l_1(c) g_0 = f(c) \tag{143}$$

for every $c \in F$. By (142) and (143), we deduce that

$$g^{-1}(\mathrm{id}_{d_0} \otimes l_1(c))g^{-1} = \mathrm{id}_{d_0} \otimes g_0^{-1} l_1(c) g_0 = (\mathrm{id}_{d_0} \otimes g_0)^{-1}(\mathrm{id}_{d_0} \otimes l_1(c))(\mathrm{id}_{d_0} \otimes g_0), \tag{144}$$

for every $c \in F$. Therefore

$$\widehat{g} := g(\mathrm{id}_{d_0} \otimes g_0)^{-1} \in C_{\mathrm{End}_L(F^n)}(F) = \mathrm{End}_F(F^n) \tag{145}$$

(under the mentioned identifications). Notice that

$$\widehat{g}(\mathrm{M}_{d_0}(L) \otimes \mathrm{id}_{[F:L]})\widehat{g}^{-1} = g(\mathrm{M}_{d_0}(L) \otimes \mathrm{id}_{[F:L]})g^{-1} = A_E.$$

The Claim follows. □

From the previous Claim, we obtain that there exists $g \in \mathrm{GL}_{d_0}(F)$ such that $A_E = g\,\mathrm{M}_{d_0}(L)g^{-1}$. □

The following result is an immediate consequence of Lemma 39.

Corollary 40. *In the above setting, suppose $g \in \mathrm{GL}_{d_0}(F)$ and a subfield $L \subseteq F$ are as in Lemma 39; that means $A_E = g\,\mathrm{M}_{d_0}(L)g^{-1}$. Suppose $g^{-1}f := (c_1, \dots, c_{d_0}) \in F^{d_0}$. Then there is a subset J_f of $\{1, \dots, d_0\}$ such that*

$$M_f = \bigoplus_{j \in J_f} c_j(gL^{d_0}), \tag{146}$$

where M_f is the A_E-module generated by f. Moreover, if N is a submodule of M_f, then there is a subset $J_{N,f}$ of J_f such that

$$M_f = N \oplus \bigoplus_{j \in J_{N,f}} c_j(gL^{d_0}).$$

Proof. Notice that for every $v_1, \dots, v_{d_0} \in L^{d_0}$, there is $x \in \mathrm{M}_{d_0}(L)$ such that $xe_i = v_i$ where e_i's form the standard basis of L^{d_0}. Then,

$$\sum_{i=1}^{d_0} c_i(gv_i) = gx(g^{-1}f) \in M_f,$$

which implies that $\sum_{i=1}^{d_0} c_i(gL^{d_0}) \subseteq M_f$. Because $\sum_{i=1}^{d_0} c_i(gL^{d_0})$ is an A_E-module and

$$f = \sum_{i=1}^{d_0} c_i(ge_i) \in \sum_{i=1}^{d_0} c_i(gL^{d_0}),$$

we deduce that

$$M_f = \sum_{i=1}^{d_0} c_i(gL^{d_0}). \tag{147}$$

Choose a subset J_f of $\{1, \dots, d_0\}$ in a way that $\{c_j \mid j \in J\}$ is an L-basis of $\sum_{j=1}^{d_0} Lc_j$. Then for every i, $c_i = \sum_{j \in J_f} a_j c_j$ for some $a_j \in L$. Therefore,

$$c_i(gL^{d_0}) \subseteq \sum_{j \in J_f} c_j(gL^{d_0}),$$

which implies that

$$\sum_{i=1}^{d_0} c_i(gL^{d_0}) = \sum_{j \in J_f} c_j(gL^{d_0}). \tag{148}$$

Suppose for some $w_i \in L^{d_0}$, we have

$$\sum_{j \in J_f} c_j(gw_j) = 0.$$

Then all the components of $\sum_{j \in J_f} c_j w_j$ are zero. Since the components of w_j's are in L and c_j's are L-linearly independent for j's in J_f, we deduce that $w_j = 0$ for every $j \in J_f$. Hence,

$$\sum_{j \in J_f} c_j(gL^{d_0}) = \bigoplus_{j \in J_f} c_j(gL^{d_0}),$$

which completes the proof of (146) by (147) and (148).

Since $A_E = g\,\mathrm{M}_{d_0}(L)g^{-1}$,

$$A_E(c_i(gL^{d_0})) = g\,\mathrm{M}_{d_0}(L)g^{-1}(c_i(gL^{d_0})) = c_i(gL^{d_0}), \tag{149}$$

which means $c_i(gL^{d_0})$ is A_E-submodule for every i. Moreover, by (149) and the fact that L^{d_0} is a simple $\mathrm{M}_{d_0}(L)$-module, we obtain that $c_i(gL^{d_0})$ is a simple A_E-module for every i. Hence, by [27, Section 2.4], the claim follows. □

In Lemma 41, we describe the subfield $L \subseteq F$ that is given by Lemma 39.

Lemma 41. *In the above setting, suppose $L \subseteq F$ is the subfield and $g \in \mathrm{GL}_{d_0}(F)$ are the ones given in Lemma 39 for $E = \mathbb{F}_p$; that means the $\mathbb{F}_p$ span of $\rho_{\mathbf{m}}(\mathrm{SL}_2(F))$ is $g\,\mathrm{M}_{d_0}(L)g^{-1}$. Then L is the unique subfield of F that has order p^k where k is the smallest period of $m_0, \dots, m_{n-1}$. This means k is the smallest positive integer such that $m_{i+k} = m_i$ for every non-negative integer $i < n - k$.*

Proof. Since $A_{\mathbb{F}_p} = g\,\mathrm{M}_{d_0}(L)g^{-1}$, L is equal to $\mathrm{Tr}(A_{\mathbb{F}_p})$. Therefore, L is the subfield of F that is generated by $\mathrm{Tr}(\rho_{\mathbf{m}}(\mathrm{SL}_2(F)))$. Since every non-central element of $\mathrm{SL}_2(F)$ is conjugate to an element of the form $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ for some $t \in F$ and the central elements are $\pm \mathrm{id}_2$, L is the subfield generated by the trace of $\rho_{\mathbf{m}}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ as t ranges in F. Let's recall that for every integer vector $\mathbf{i} := (i_0, \dots, i_{n-1})$ in $\prod_{i=0}^{n-1}[0, m_i]$, $e_{\mathbf{i}} := \prod_{j=0}^{n-1} x_j^{i_j} y_j^{m_j - i_j}$, and $e_{\mathbf{i}}$'s form an F-basis for $V_{\mathbf{m}}(F)$. We have

$$\rho_{\mathbf{m}}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}(e_{\mathbf{i}}) = \prod_{j=0}^{n-1} y_j^{i_j}(-x_j + t^{p^j} y_j)^{m_j - i_j}. \tag{150}$$

Next, we expand the right hand side of (150) to find the coefficient of $e_{\mathbf{i}}$. It is easy to see that this coefficient is

$$(-1)^{i_j}\binom{m_j - i_j}{i_j} t^{c(\mathbf{m}-2\mathbf{i})}, \tag{151}$$

where $c : \prod_{j=0}^{n-1}[-m_j, m_j] \to \mathbb{Z}$, $c(b_0, \dots, b_{n-1}) := \sum_{j=0}^{n-1} b_j p^j$. Notice that this coefficient is non-zero exactly when $m_j \geqslant 2i_j$ for every j. By (151), we obtain that

$$\mathrm{Tr}\left(\rho_{\mathbf{m}}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}\right) = \sum_{\mathbf{i}} (-1)^{i_j}\binom{m_j - i_j}{i_j} t^{c(\mathbf{m}-2\mathbf{i})} = \prod_{j=0}^{n-1} \overline{U}_{m_j}(t)^{p^j} = \prod_{j=0}^{n-1} \phi^j(\overline{U}_{m_j}(t)), \tag{152}$$

where $\phi : F \to F$, $\phi(x) := x^p$ and $\overline{U}_m(x) := \sum_{i=0}^{\lfloor m/2 \rfloor}(-1)^i\binom{m-i}{i}x^{m-2i}$ (notice that if p is not 2, then $\overline{U}_m(x) = U_m(x/2)$ where U_m is the Chebyshev polynomial of the second kind). If k is the period of $m_0, \dots, m_{n-1}$, then for every $t \in F$

$$\phi^k\left(\prod_{j=0}^{n-1} \phi^j(\overline{U}_{m_j}(t))\right) = \prod_{j=0}^{n-1} \phi^j(\overline{U}_{m_j}(t));$$

consequently, for every $t \in F$, trace of $\rho_{\mathbf{m}}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ is in the fixed points of ϕ^k. Therefore, the subfield generated by the traces of the image of $\rho_{\mathbf{m}}$ is in the unique subfield of F that has order p^k.

Next, assume that the subfield generated by the traces of the image of $\rho_{\mathbf{m}}$ has $p^{k'}$ elements. Then k' divides k and

$$\phi^{k'}\left(\prod_{j=0}^{n-1} \phi^j(\overline{U}_{m_j}(t))\right) = \prod_{j=0}^{n-1} \phi^j(\overline{U}_{m_j}(t))$$

for every $t \in F$. This implies that

$$\prod_{j=0}^{n-1-k'} \overline{U}_{m_j}(t)^{p^{k'+j}} \prod_{j=n-k'}^{n-1} \overline{U}_{m_j}(t)^{p^{k'+j-n}} = \prod_{j=0}^{n-1} \overline{U}_{m_j}(t)^{p^j} \tag{153}$$

for every $t \in F$. Since $\deg \overline{U}_m = m$, the degree of the polynomials in both the sides of the equation given in (153) is less than p^n. Consequently, (153) implies that

$$\prod_{j=0}^{n-1} \overline{U}_{m_{j-k'}}(x^{p^j}) = \prod_{j=0}^{n-1} \overline{U}_{m_j}(x^{p^j}) \tag{154}$$

as two polynomials in $\mathbb{F}_p[x]$ where the index $j-k'$ is taken modulo n. For every non-negative integer m, let $\overline{\overline{U}}_m(x)$ be $\overline{U}_m(x)$ if m is even and $\overline{U}_m(x)/x$ if m is odd. Then $\overline{\overline{U}}_m(0) = \pm 1$ for every non-negative even integer m and $\overline{\overline{U}}_m(0) = \pm\frac{m+1}{2}$ for every non-negative odd integer m, and (154) implies that

$$\prod_{j=0}^{n-1} \overline{\overline{U}}_{m_{j-k'}}(x^{p^j}) = \prod_{j=0}^{n-1} \overline{\overline{U}}_{m_j}(x^{p^j}). \tag{155}$$

Looking at both sides of (155) modulo x^p and noticing that $(m_j+1)/2 \neq 0$ in F, we deduce that $\overline{\overline{U}}_{m_0} = \overline{\overline{U}}_{m_{n-k'}}$, which implies that $m_0 = m_{n-k'}$. After canceling this common polynomial from both sides of (154) and repeating this argument, we conclude that $m_0, \dots, m_{n-1}$ is k' periodic. This means k' is at least k, which finishes the proof. □

We refer to the subfield generated by the traces of elements in the image of $\rho_{\mathbf{m}}$ as the *trace field* of $\rho_{\mathbf{m}}$.

Lemma 42. *Suppose F is a finite field of characteristic p and order $q := p^n$. Let $\mathbb{F}_p$ be the prime subfield of F. Let M be a simple $F[\mathrm{SL}_2(F)]$-module, and $1 < \dim_F M < \sqrt{p}$. Then there exists a positive integer C which only depends on $\dim_F M$ such that for every $f \in M$,*

$$\textstyle\sum_C \mathcal{O}_f - \sum_C \mathcal{O}_f = M_f, \tag{156}$$

where M_f is the $\mathbb{F}_p[\mathrm{SL}_2(F)]$-submodule of M that is generated by f and $\mathcal{O}_f$ is the $\mathrm{SL}_2(F)$-orbit of f. Moreover, there is a subfield $L := L(M)$ of F which only depends on M such that the following statements hold.

1. *M_f is an $L[\mathrm{SL}_2(F)]$-submodule of M.*
2. *$[F : L] \leqslant \dim_F M$.*
3. *$\dim_L M_f \leqslant (\dim_F M)^2$.*

Proof. If $f = 0$, there is nothing to prove. By Proposition 36, $M \simeq V_{\mathbf{m}}(F)$ for some integer vector $\mathbf{m} \in [0, p-1]^n$. So without loss of generality, we can and will assume that $M = V_{\mathbf{m}}(F)$ and f is a non-zero element of $V_{\mathbf{m}}(F)$. Therefore, by Lemma 37, either $f \notin V_{\mathbf{m}}(F)^{U^+}$ or $f \notin V_{\mathbf{m}}(F)^{U^-}$. Without loss of generality, we can and will assume that $f \notin V_{\mathbf{m}}(F)^{U^+}$. Notice that $u^+(t)$ acts on $V_{\mathbf{m}}(F)$ as a unipotent transformation. Hence, there is a positive integer $d < \deg_F V_{\mathbf{m}}(F) = \prod_{i=0}^{n-1}(m_i+1)$ such that for some $t_0 \in F$

$$h := (u^+(t_0) - I)^d \cdot f \neq 0 \quad \text{and} \quad \forall t \in F,\ (u^+(t) - I)^{d+1} \cdot f = 0.$$

Hence, h is a non-zero element of $V_{\mathbf{m}}(F)^{U^+}$. Thus, by Lemma 37, $h = c x_0^{m_0} \cdots x_{n-1}^{m_{n-1}} =: c e_{\mathbf{m}}$ for some $c \in F^\times$, and

$$c e_{\mathbf{m}} = \textstyle\sum_{j=0}^{d} (-1)^j \binom{d}{j} u^+(jt_0) \cdot f \in \sum_{2^d} \mathcal{O}_f - \sum_{2^d} \mathcal{O}_f.$$

Therefore for every $\alpha \in F^\times$,

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \cdot (c e_{\mathbf{m}}) = \alpha^k (c e_{\mathbf{m}}) = c\alpha^k e_{\mathbf{m}} \in \textstyle\sum_{2^d} \mathcal{O}_f - \sum_{2^d} \mathcal{O}_f, \tag{157}$$

where $k := m_0 + m_1 p + \cdots + m_{n-1} p^{n-1}$. Let L be the subfield of F which is generated by

$$(F^\times)^k := \{\alpha^k \mid \alpha \in F^\times\}.$$

Suppose $|L| = p^l$. Since L is a subfield of F, $n = ls$ for some integer s. Because $F^\times$ and $L^\times$ are cyclic groups, we obtain that

$$k = (1 + p^l + \cdots + p^{(s-1)l})r \tag{158}$$

for some integer r. Viewing both sides of (158) modulo p^l, we obtain that

$$m_0 + pm_1 + \cdots + p^{l-1}m_{l-1} \equiv r \pmod{p^l}. \tag{159}$$

Notice that $k < p^n$, and consequently $r < p^l$. Therefore, by (159), we deduce that

$$r = m_0 + pm_1 + \cdots + p^{l-1}m_{l-1}. \tag{160}$$

By (158), (160), and the fact that m_i's are digits of k in base p, we obtain that m_i's are l-periodic; that means

$$(m_0, \ldots, m_{l-1}) = (m_{il}, \ldots, m_{il+l-1})$$

for every integer i in $[0, s-1]$. Hence, by Lemma 41, the trace field of $\rho_{\mathbf{m}}$ is a subfield of L. On the other hand, if l' is the smallest positive integer such that $m_0, \ldots, m_{n-1}$ is l'-periodic, it is clear $(F^\times)^k$ is pointwise fixed by $\phi^{l'}$ where $\phi : F \to F$, $\phi(x) := x^p$. Hence, again by Lemma 41, $(F^\times)^k$ is a subset of the trace field of $\rho_{\mathbf{m}}$. Therefore, the field L generated by $(F^\times)^k$ is simply the trace field of $\rho_{\mathbf{m}}$.

Also notice that since m_i's are l-periodic, we obtain

$$m_0 + \cdots + m_{n-1} = s(m_0 + \cdots + m_{l-1}). \tag{161}$$

Because $\dim_F M = \prod_{i=0}^{n-1}(m_i + 1)$, at least one of the m_i's is not zero, and

$$m_0 + \cdots + m_{n-1} < \dim_F M. \tag{162}$$

By (161) and (162), we obtain that

$$[F : L] < \dim_F M. \tag{163}$$

We also notice that $L^\times$ is the unique subgroup of $F^\times$ that has order $p^l - 1$, and so

$$(F^\times)^k = (F^\times)^{\frac{p^n-1}{p^l-1}\cdot r} = (L^\times)^r. \tag{164}$$

By (162), there are at most $\dim_F M - 1$ non-zero m_i's. Consider

$$\left\{ \frac{i}{l} + \mathbb{Z} \mid m_i \neq 0 \right\} \subseteq \mathbb{R}/\mathbb{Z}, \tag{165}$$

and view $\mathbb{R}/\mathbb{Z}$ as a circle with circumference 1. The points given in (165) (location of non-zero digits) cut out at most $\dim_F M - 1$ arcs, and so one of them has length at least $\frac{1}{\dim_F M - 1}$. Therefore, there is an index i_0 such that $m_{i_0} \neq 0$ and

$$\left\{ \frac{i - i_0}{l} + \mathbb{Z} \mid m_i \neq 0 \right\} \cap \{x + \mathbb{Z} \mid 1 - \frac{1}{\dim_F M - 1} < x < 1\} = \varnothing. \tag{166}$$

Notice the restriction of ϕ to every subfield of F is an automorphism. This implies that

$$(L^\times)^r = \phi^{-i_0}((L^\times)^r) = \{x^{m_{i_0} + pm_{i_0+1} + \cdots + p^{l-1-i_0}m_{l-1} + p^{l-i_0}m_0 + \cdots + p^{l-1}m_{i_0-1}} \mid x \in L^\times\}. \tag{167}$$

Let $r' := m_{i_0} + pm_{i_0+1} + \cdots + p^{l-1-i_0}m_{l-1} + p^{l-i_0}m_0 + \cdots + p^{l-1}m_{i_0-1}$. Then by (166), we obtain that

$$r' < p^{l - \frac{l}{\dim_F M - 1} + 1}. \tag{168}$$

Now, we consider two cases to show that there is a positive integer C which only depends on $\dim_F M$ such that

$$\sum_C (F^\times)^k - \sum_C (F^\times)^k = L. \tag{169}$$

Case 1 ($l \gg_{\dim_F M} 1$). In this case, by (168), we can and will assume that $r' < |L|^{1-\frac{1}{\dim_F M}}$. Therefore, by Lemma 38, (167) (which implies $(L^\times)^r = (L^\times)^{r'}$), and (164), we deduce that there is a positive integer C which only depends on $\dim_F M$ such that

$$\sum_C (F^\times)^k - \sum_C (F^\times)^k = \sum_C (L^\times)^{r'} - \sum_C (L^\times)^{r'} = L.$$

Case 2 ($l \ll_{\dim_F M} 1$ (the complement of Case 1)). Let $\mathbb{F}_p$ be the prime field of F, and notice that for every $x \in \mathbb{F}_p$,

$$x^r = x^{m_0+\cdots+m_{l-1}} \in (L^\times)^r.$$

Since $\dim_F M < p^{1/2}$, we can use the Waring problem modulo primes (see [6]), and obtain that every element of $\mathbb{F}_p$ can be written as a sum of at most $\lfloor \frac{m_0+\cdots+m_{l-1}}{2} \rfloor + 1$ elements of

$$(\mathbb{F}_p^\times)^{m_0+\cdots+m_{l-1}} := \{\alpha^{m_0+\cdots+m_{l-1}} \mid \alpha \in \mathbb{F}_p^\times\}.$$

By (162) and the previous argument, we deduce that for $C' = \lfloor \dim_F M/2 \rfloor + 1$

$$\mathbb{F}_p \subseteq \sum_{C'} (L^\times)^r - \sum_{C'} (L^\times)^r. \tag{170}$$

The assumption of Case 2 implies that there is a positive integer $C'' := C''(\dim_F M)$ which only depends on $\dim_F M$ such that $l \leqslant C''$. Then by (170), we conclude that

$$L = \sum_{C'C''} (L^\times)^r - \sum_{C'C''} (L^\times)^r = \sum_{C'C''} (F^\times)^k - \sum_{C'C''} (F^\times)^k.$$

In either case, we showed that (169) holds. By (157) and (169), we deduce that

$$cLe_{\mathbf{m}} \subseteq \sum_{2^d C} \mathcal{O}_f - \sum_{2^d C} \mathcal{O}_f. \tag{171}$$

On the other hand, by Corollary 40 and Lemma 41, the $\mathbb{F}_p[\mathrm{SL}_2(F)]$-submodule $M_{e_{\mathbf{m}}}$ generated by $e_{\mathbf{m}}$ is a vector space over L that is of dimension at most $(\dim_F M)^2$. Hence, by (171),

$$cM_{e_{\mathbf{m}}} \subseteq \sum_{2^d C(\dim_F M)^2} \mathcal{O}_f - \sum_{2^d C(\dim_F M)^2} \mathcal{O}_f \subseteq M_f. \tag{172}$$

By Corollary 40, M_f is a completely reducible $\mathbb{F}_p[\mathrm{SL}_2(F)]$-module. Hence there is an $\mathbb{F}_p[\mathrm{SL}_2(F)]$-submodule N of M_f such that $M_f = N \oplus cM_{e_{\mathbf{m}}}$. Hence, f can be written as a sum of $f_{\mathrm{new}} \in N$ and $f_{\mathrm{achieved}} \in cM_{e_{\mathbf{m}}}$. Therefore,

$$f_{\mathrm{new}} \in \sum_{2^d C(\dim_F M)^2+1} \mathcal{O}_f - \sum_{2^d C(\dim_F M)^2} \mathcal{O}_f.$$

Repeating this previous process, we have

$$c_{\mathrm{new}} M_{e_{\mathbf{m}}} \subseteq \sum_{2^d C(\dim_F M)^2} \mathcal{O}_{f_{\mathrm{new}}} - \sum_{2^d C(\dim_F M)^2} \mathcal{O}_{f_{\mathrm{new}}} \subseteq M_{f_{\mathrm{new}}} \subseteq N.$$

Hence,

$$cM_{e_{\mathbf{m}}} \oplus c_{\mathrm{new}} M_{e_{\mathbf{m}}} \subseteq \sum_{C_1} \mathcal{O}_f - \sum_{C_1} \mathcal{O}_f.$$

By Corollary 40, this process ends in at most $\dim_F M$ iterations. This means that there is a positive integer $\overline{C}$ which only depends on $\dim_F M$ such that

$$M_f = \sum_{\overline{C}} \mathcal{O}_f - \sum_{\overline{C}} \mathcal{O}_f,$$

which finishes proof of (156).

As it is discussed earlier in the argument, by Corollary 40 and Lemma 41, M_f is an $L[\mathrm{SL}_2(F)]$-submodule of M where L is the trace subfield associated with the representation $\rho_{\mathbf{m}}$. By (163), $[F:L] < \dim_F M$, and by Corollary 40, $\dim_L M_f \leqslant (\dim_F M)^2$, which finishes the proof. □

Lemma 43. *Suppose F is a finite field of characteristic p, m is an integer less than $\sqrt{p}$, and $\rho : (\underline{\mathrm{SL}}_2)_F \to (\underline{\mathrm{GL}}_m)_F$ is a group homomorphism. Let $M := F^m$ and view it as an $F[\mathrm{SL}_2(F)]$-module via ρ, where $F[\mathrm{SL}_2(F)]$ is the group ring of $\mathrm{SL}_2(F)$ over the ring F. Suppose no non-zero element of M is invariant under $\mathrm{SL}_2(F)$. Then, M is a completely reducible $F[\mathrm{SL}_2(F)]$-module and there exists a positive integer C which only depends on m such that for every $x \in M$,*

$$\sum_C \mathcal{O}_x - \sum_C \mathcal{O}_x = M_x, \tag{173}$$

where $\mathcal{O}_x$ is the $\mathrm{SL}_2(F)$-orbit of x and M_x is the $\mathbb{F}_p[\mathrm{SL}_2(F)]$-submodule generated by x.

Proof. By [17, Theorem A], M is a completely reducible $F[\mathrm{SL}_2(F)]$-module. Hence, it is also a completely reducible $\mathbb{F}_p[\mathrm{SL}_2(F)]$-module. This implies that M_x is also completely reducible. To prove (173), we proceed by induction on the dimension of M over F. Without loss of generality, we can and will assume that M is generated by x as an $F[\mathrm{SL}_2(F)]$-module. If M is a simple $F[\mathrm{SL}_2(F)]$-module, (173) follows from Lemma 42. Otherwise, there are proper submodules N and N' of M such that $M = N \oplus N'$ and N is a simple $F[\mathrm{SL}_2(F)]$-module. Hence, x can be written as $x_N + x_{N'}$ for some $x_N \in N$ and $x_{N'} \in N'$. Then, by Lemma 42, there is a positive integer C' which only depends on $\dim_F N < m-1$ such that

$$M_{x_N} = \sum_{C'} \mathcal{O}_{x_N} - \sum_{C'} \mathcal{O}_{x_N}. \tag{174}$$

Let $\mathrm{pr}_N : M \to N$ be the projection to the N-component. By (174), we have that

$$M_{x_N} = \mathrm{pr}_N\Big(\sum_{C'} \mathcal{O}_x - \sum_{C'} \mathcal{O}_x\Big) \subseteq \mathrm{pr}_N(M_x). \tag{175}$$

Since pr_N is not an isomorphism , by (175), there is a non-zero element $y \in \ker \mathrm{pr}_N$ which is in

$$\sum_{3C'} \mathcal{O}_x - \sum_{3C'} \mathcal{O}_x.$$

Notice that $\ker p_N = N'$, and so by the induction hypothesis, there is an integer C'' which only depends on $\dim_F N' < m-2$ such that

$$M_y = \sum_{C''} \mathcal{O}_y - \sum_{C''} \mathcal{O}_y \subseteq \sum_{3C'C''} \mathcal{O}_x - \sum_{3C'C''} \mathcal{O}_x. \tag{176}$$

Because M_x is a completely reducible $\mathbb{F}_p[\mathrm{SL}_2(F)]$-module, there is a submodule N'' such that

$$M_x = N \oplus M_y \oplus N''.$$

Notice that by (174) and (176), we have

$$M_{x_N} \oplus M_y = \mathrm{pr}_{N \oplus M_y}\Big(\sum_{3C'C''+C'} \mathcal{O}_x - \sum_{3C'C''+C'} \mathcal{O}_x\Big).$$

By repeating this process at most $(\dim_F M)/2$ times, we get to the entire M, and the claim follows. □

Proposition 44. *Suppose F is a finite field of characteristic p, m is an integer less than $\sqrt{p}$, $\mathbb{H}$ is a semisimple group defined over F, and $\rho : \mathbb{H} \to (\underline{\mathrm{GL}}_m)_F$ is a group homomorphism. Let $\mathbb{H}(F)^+$ be the subgroup generated by the p-elements of $\mathbb{H}(F)$. Let $M := F^m$, and view it as an $F[\mathbb{H}(F)^+]$-module via ρ, where $F[\mathbb{H}(F)^+]$ is the group ring of $\mathbb{H}(F)^+$. Suppose no non-zero element of M is invariant under*

$\mathbb{H}(F)^+$. *Then,* M *is a completely reducible* $F[\mathbb{H}(F)^+]$*-module and there exists a positive integer* C *which only depends on* m *such that for every* $x \in M$*,*

$$\sum_C \mathcal{O}_x - \sum_C \mathcal{O}_x = M_x, \tag{177}$$

where $\mathcal{O}_x$ *is the* $\mathbb{H}(F)^+$*-orbit of* x *and* M_x *is the* $\mathbb{F}_p[\mathbb{H}(F)^+]$*-submodule generated by* x*.*

Proof. Let $\widetilde{\mathbb{H}}$ be the simply-connected cover of $\mathbb{H}$, and $\iota : \widetilde{\mathbb{H}} \to \mathbb{H}$ be the corresponding central isogeny. Then $\iota(\widetilde{\mathbb{H}}(F)) = \mathbb{H}(F)^+$, and so without loss of generality, we can and will assume that $\mathbb{H}$ is simply-connected and $\mathbb{H}(F)^+ = \mathbb{H}(F)$.

Since $\mathbb{H}$ is a simply-connected semisimple group defined over F and F is a finite field, there are simply-connected, F-almost simple, quasi-split groups $\mathbb{H}_i$ defined over F such that $\mathbb{H}$ is a direct product of $\mathbb{H}_i$'s. Because $\mathbb{H}_i$ is quasi-split and simply-connected over a finite field F, $\mathbb{H}_i \times_F \widetilde{F}$ splits for some cyclic extension $\widetilde{F}/F$ of degree at most 3. Looking at the action of the Galois group $\mathrm{Gal}(\widetilde{F}/F)$ on the Dynkin diagram of $\mathbb{H}_i \times_F \widetilde{F}$, we deduce that either there is an embedding of $(\mathrm{SL}_2)_F$ into $\mathbb{H}_i$ or there is an embedding of the unitary group of the hermitian form given by

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

into $\mathbb{H}_i$. In the latter case, again there is an embedding of $(\mathrm{SL}_2)_F$ into $\mathbb{H}_i$. Since $\mathbb{H}_i$ is F-almost simple, it is generated by the conjugates of a non-central subgroup. Hence, $\mathbb{H}$ has finitely many copies $\mathbb{L}_j$'s of $(\mathrm{SL}_2)_F$ which generate $\mathbb{H}$; and because $\mathbb{H}$ is simply-connected, $\mathbb{L}_j(F)$'s generate $\mathbb{H}(F)$. By [17, Theorem A], M is a completely reducible $F[\mathbb{H}(F)^+]$-module (and similarly $F[\mathbb{L}_j(F)]$-module for every j). Therefore, there is an $F[\mathbb{L}_j(F)]$-submodule M_j which does not have any non-zero $\mathbb{L}_j(F)$-invariant vector and

$$M = M^{\mathbb{L}_j(F)} \oplus M_j, \tag{178}$$

where $M^{\mathbb{L}_j(F)}$ is the set of $\mathbb{L}_j(F)$-fixed points of M. By Lemma 42, for every j, there is a subfield L_j such that every $\mathbb{F}_p[\mathbb{L}_j(F)]$-submodule of M is a vector space over L_j and $[F : L_j] \leqslant \dim_F M$. Let

$$L := \bigcap \{E \subseteq F \mid E \text{ subfield of } F, [F : E] \leqslant \dim_F M\}.$$

Hence, $L \subseteq L_j$ for every j, $[F : L] \leqslant (\dim_F M)!$, and for every j, an $\mathbb{F}_p[\mathbb{L}_j(F)]$-submodule of M is a vector space over L.

Since $\mathbb{H}(F)$ has no non-zero fixed points in M and $\mathbb{L}_j(F)$'s generate $\mathbb{H}(F)$, for every non-zero $x \in M$, there is j such that $x \notin M^{\mathbb{L}_j(F)}$. Therefore, $\mathrm{pr}_{M_j}(x) \neq 0$. Thus, by Lemma 43, for some positive integer C_1 which only depends on $\dim_F M$ such that

$$\mathbb{F}_p[\mathbb{L}_j(F)] \cdot \mathrm{pr}_{M_j}(x) \subseteq \sum_{C_1} \mathbb{L}_j(F) \cdot \mathrm{pr}_{M_j}(x) - \sum_{C_1} \mathbb{L}_j(F) \cdot \mathrm{pr}_{M_j}(x). \tag{179}$$

Therefore, by (179), we deduce that

$$L \,\mathrm{pr}_{M_j}(x) \subseteq \sum_{C_1} \mathbb{L}_j(F) \cdot x - \sum_{C_1} \mathbb{L}_j(F) \cdot x \subseteq \sum_{C_1} \mathcal{O}_x - \sum_{C_1} \mathcal{O}_x. \tag{180}$$

Because the dimension of M as an L-vector space is bounded by a function of $\dim_F M$, by (180) we obtain that there is a positive integer C_2 which only depends

on $\dim_F M$ such that

$$M_{\mathrm{pr}_{M_j}(x)} \subseteq \sum_{C_2} \mathcal{O}_x - \sum_{C_2} \mathcal{O}_x. \tag{181}$$

Let $x_1 := \mathrm{pr}_{M_j}(x)$. Since M is a completely reducible $\mathbb{F}_p[\mathbb{H}(F)]$-module, there is a submodule N of M_x such that

$$M_x = M_{x_1} \oplus N.$$

If $N = 0$, we are done. If not, $\mathrm{pr}_N(x) \neq 0$. So repeating the above argument this time for $\mathrm{pr}_N(x)$, we can find $x_2 \in N$ such that

$$M_{x_2} \subseteq \sum_{C_2} \mathcal{O}_{\mathrm{pr}_N(x)} - \sum_{C_2} \mathcal{O}_{\mathrm{pr}_N(x)} = \mathrm{pr}_N\Big(\sum_{C_2} \mathcal{O}_x - \sum_{C_2} \mathcal{O}_x\Big). \tag{182}$$

By (181) and (182), we obtain that

$$M_{x_1} \oplus M_{x_2} \subseteq \sum_{2C_2} \mathcal{O}_x - \sum_{2C_2} \mathcal{O}_x.$$

Because the dimension of M as an L-vector space is bounded by a function of $\dim_F M$, the above process terminates in at most $O_{\dim_F M}(1)$. This means that there is a positive integer C which only depends on $\dim_F M$ such that

$$M_x = \sum_C \mathcal{O}_x - \sum_C \mathcal{O}_x.$$

□

Here is an important consequence of Proposition 44.

Proposition 45. *Suppose $\mathbb{H} \subseteq (\underline{\mathrm{GL}}_n)_{\mathbb{Q}}$ is a connected semisimple simply-connected $\mathbb{Q}$-group and $\rho : \mathbb{H} \to (\underline{\mathrm{GL}}_m)_{\mathbb{Q}}$ is a group homomorphism such that $\mathbb{Q}^m$ does not have a non-zero $\mathbb{H}(\mathbb{Q})$-fixed point. Let $\underline{H}$ be the Zariski-closure of $\mathbb{H}$ in $(\underline{\mathrm{GL}}_n)_{\mathbb{Z}}$, and $\underline{M}$ be the group scheme given by $\mathbb{Z}^m$. Then there are positive integers q_0 and C depending on $\mathbb{H}$ and ρ such that the following statements hold.*

1. *$\underline{H}_{\mathbb{Z}[1/q_0]} := \underline{H} \times_{\mathbb{Z}} \mathbb{Z}[1/q_0]$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/q_0])$, and for every prime p which does not divide q_0, $\underline{H}_{\mathbb{F}_p}$ is a connected semisimple simply-connected algebraic group defined over $\mathbb{F}_p$.*
2. *The group homomorphism ρ has an extension to a group homomorphism from $\underline{H}_{\mathbb{Z}[1/q_0]}$ to $(\underline{\mathrm{GL}}_m)_{\mathbb{Z}[1/q_0]}$ (that we still denote by ρ).*
3. *For every prime p not dividing q_0 and every finite field F of characteristic p, $\underline{M}(F)$ is a completely reducible $\mathbb{Z}[\underline{H}(F)]$-module where $\underline{H}(F)$ acts on $\underline{M}(F)$ via ρ.*
4. *For an integer i in $[1, k]$, suppose p_i is a prime which does not divide q_0 and F_i is a finite field of characteristic p_i. Then for every $x \in \underline{M}(\prod_{i=1}^k F_i)$,*

$$M_x = \sum_C \mathcal{O}_x - \sum_C \mathcal{O}_x,$$

where M_x is the $\mathbb{Z}[\underline{H}(\prod_{i=1}^k F_i)]$-module generated by x and $\mathcal{O}_x$ is the $\underline{H}(\prod_{i=1}^k F_i)$-orbit of x.

Proof. For Parts (1)–(3) see [17, Theorem A] and [14, Lemma 64, Lemma 65]. In [14, Lemma 65], Part (3) is proved only for $F = \mathbb{F}_p$. The complete reducibility of $\underline{M}(F)$ follows from [17, Theorem A] and the fact that $\underline{H}(F)^+ = \underline{H}(F)$ as $\underline{H}_{\mathbb{F}_p}$ is simply-connected. By the argument given in the last paragraph of the proof of [14, Lemma 65], $\underline{H}(\mathbb{F}_p)$ does not have a non-zero fixed point in $\underline{M}(F)$.

Suppose $x := (x_1, \dots, x_k) \in \underline{M}(\prod_{i=1}^k F_i)$. By Proposition 44 and the fact that $\underline{H}(F_i)^+ = \underline{H}(F_i)$, there is a positive integer C which only depends on $\dim \mathbb{H}$ and m such that

$$M_{x_i} = \sum_C \mathcal{O}_{x_i} - \sum_C \mathcal{O}_{x_i} \tag{183}$$

for every i where M_{x_i} is the $\mathbb{F}_{p_i}[\underline{H}(F_i)]$-submodule generated by x_i and $\mathcal{O}_{x_i}$ is the $\underline{H}(F_i)$-orbit of x_i. Notice that, we enlarge q_0 to make sure that all the primes less than or equal to $\sqrt{m}$ divide q_0, and so $p_i \nmid q_0$ implies that $p_i > \sqrt{m}$.

Part (4) follows from (183) and

$$M_x = \prod_{i=1}^k M_{x_i} \quad \text{and} \quad \mathcal{O}_x = \prod_{i=1}^k \mathcal{O}_{x_i}.$$

□

8. Perfect groups, their almost simple factors, and spectral gap

Suppose $\mathbb{G} \subseteq (\underline{\mathrm{GL}}_n)_{\mathbb{Q}}$ is a connected, simply-connected perfect group. It is well-known that the unipotent radical of $\mathbb{G} \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ descends to a unipotent subgroup $\mathbb{U}$ of $\mathbb{G}$. Since $\mathbb{G}$ is perfect, connected, and simply connected, $\mathbb{G}/\mathbb{U}$ is a perfect, connected, simply-connected reductive group. Because the derived subgroup of a reductive group is semisimple, we obtain that $\mathbb{G}/\mathbb{U}$ is a connected simply-connected semisimple $\mathbb{Q}$-group. By a result of Mostow, the short exact sequence

$$1 \to \mathbb{U} \to \mathbb{G} \to \mathbb{G}/\mathbb{U} \to 1$$

splits. Hence, there is a connected, simply-connected, semisimple subgroup $\mathbb{H}$ of $\mathbb{G}$, and a normal unipotent subgroup $\mathbb{U}$ of $\mathbb{G}$ such that $\mathbb{G}$ is isomorphic to $\mathbb{H} \ltimes \mathbb{U}$ where $\mathbb{H}$ acts on $\mathbb{U}$ by conjugation. Since $\mathbb{U}$ is a connected unipotent subgroup of $(\underline{\mathrm{GL}}_n)_{\mathbb{Q}}$, there is $g \in \mathrm{GL}_n(\mathbb{Q})$ such that $g\mathbb{U}g^{-1}$ is a subgroup of $(\underline{\mathrm{Uni}}_n^+)_{\mathbb{Q}}$. Hence, after conjugating $\mathbb{G}$, we can and will assume that $\mathbb{U}$ is a subgroup of $(\underline{\mathrm{Uni}}_n^+)_{\mathbb{Q}}$. This discussion justifies the following assumptions:

(A1) $\mathbb{H} \subseteq (\mathrm{GL}_n)_{\mathbb{Q}}$ is a connected, simply-connected, semisimple group.

(A2) $\mathbb{U}$ is a closed subgroup of $(\underline{\mathrm{Uni}}_n^+)_{\mathbb{Q}}$ which is normalized by $\mathbb{H}$ (and $\mathbb{H} \cap \mathbb{U} = \{1\}$).

(A3) $\mathbb{G} := \mathbb{H} \ltimes \mathbb{U}$ is a perfect group.

Notice that if $\mathbb{G}$ is perfect, then so is $\mathbb{G}/[\mathbb{U}, \mathbb{U}] \simeq \mathbb{H} \ltimes \mathbb{U}^{\mathrm{ab}}$. By an argument similar to the proof of Lemma 21, we see that the converse holds as well (see [14, Lemma 65]). By Proposition 29, $\mathbb{U}^{\mathrm{ab}}$ is isomorphic to the $\mathbb{Q}$-vector group $(\underline{V})_{\mathbb{Q}}$ given by

$$V := \mathrm{Lie}(\mathbb{U})(\mathbb{Q})^{\mathrm{ab}} := \mathrm{Lie}(\mathbb{U})(\mathbb{Q})/[\mathrm{Lie}(\mathbb{U})(\mathbb{Q}), \mathrm{Lie}(\mathbb{U})(\mathbb{Q})];$$

moreover, since the given isomorphism in Proposition 29 is based on the logarithmic map, it is an $\mathbb{H}$-equivariant map where $\mathbb{H}$ acts on $(\underline{V})_{\mathbb{Q}}$ via the adjoint action of $\mathbb{H}$ on $\mathrm{Lie}\,\mathbb{U}$. Since $\mathbb{H} \ltimes \mathbb{U}^{\mathrm{ab}}$ is perfect (and $\mathbb{H}(\mathbb{Q})$ is Zariski-dense in $\mathbb{H}$), no non-zero element of V is invariant under $\mathbb{H}(\mathbb{Q})$.

Let $\underline{G}$, $\underline{H}$, and $\underline{U}$ be the Zariski-closure of $\mathbb{G}$, $\mathbb{H}$, and $\mathbb{U}$, respectively, in $(\underline{\mathrm{GL}}_n)_{\mathbb{Z}}$. By the *spreading out* results ([16, Theorem 9.7.7 and Theorem 12.2.4]; see also Proposition 29 and [14, Theorem 40]), there is a positive integer q_0 such that $\underline{G}_{\mathbb{Z}[1/q_0]}$, $\underline{H}_{\mathbb{Z}[1/q_0]}$, and $\underline{U}_{\mathbb{Z}[1/q_0]}$ are smooth and the fibers $\underline{G}_{\mathbb{Z}/p\mathbb{Z}}$, $\underline{H}_{\mathbb{Z}/p\mathbb{Z}}$, and $\underline{U}_{\mathbb{Z}/p\mathbb{Z}}$ are connected algebraic groups defined over $\mathbb{Z}/p\mathbb{Z}$ and they are of dimension $\dim \mathbb{G}$,

$\dim \mathbb{H}$, and $\dim \mathbb{U}$, respectively, for every prime p which does not divide q_0. Furthermore, we have a splitting short exact sequence

$$1 \to \underline{U}_{\mathbb{Z}[1/q_0]} \to \underline{G}_{\mathbb{Z}[1/q_0]} \to \underline{H}_{\mathbb{Z}[1/q_0]} \to 1.$$

Moreover, we can and will assume that q_0 satisfies properties given by Proposition 29. Let $\mathfrak{u}$ be $\mathrm{Lie}((\underline{U})_{\mathbb{Z}[1/q_0]})(\mathbb{Z}[1/q_0])$ and

$$\mathfrak{u}^{\mathrm{ab}} := \mathfrak{u}/[\mathfrak{u},\mathfrak{u}].$$

Let $\rho : \underline{H} \to \underline{\mathrm{GL}}(\underline{\mathfrak{u}}^{\mathrm{ab}})$ be the group homomorphism that is given by the natural action of $\underline{H}(B)$ on $\mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} B$ for every $\mathbb{Z}[1/q_0]$-algebra B.

Suppose $p_1, \dots, p_k$ are primes that do not divide q_0 and $F_1, \dots, F_k$ are finite fields of characteristic $p_1, \dots, p_k$, respectively. Let

$$G := \underline{G}_{\mathbb{Z}[1/q_0]}(\prod_{i=1}^{k} F_i),\ H := \underline{H}_{\mathbb{Z}[1/q_0]}(\prod_{i=1}^{k} F_i),\ \text{and}\ U := \underline{U}_{\mathbb{Z}[1/q_0]}(\prod_{i=1}^{k} F_i). \tag{184}$$

Since $\mathbb{H}$ is simply-connected, there are connected, simply-connected, $\mathbb{Q}$-almost simple groups $\mathbb{H}_1, \dots, \mathbb{H}_s$ such that

$$\mathbb{H} = \mathbb{H}_1 \oplus \cdots \oplus \mathbb{H}_s.$$

Let $\underline{H}_i$ be the closure of $\mathbb{H}_i$ in $(\underline{\mathrm{GL}}_n)_{\mathbb{Z}}$. As before, choosing q_0 with large enough prime factors we can and will assume that $(\underline{H}_i)_{\mathbb{Z}[1/q_0]}$ is smooth and

$$(\underline{H})_{\mathbb{Z}[1/q_0]} = (\underline{H}_1)_{\mathbb{Z}[1/q_0]} \oplus \cdots \oplus (\underline{H}_s)_{\mathbb{Z}[1/q_0]}.$$

Let $H_{j,i} := (\underline{H}_j)_{\mathbb{Z}[1/q_0]}(F_i)$ for every j. Changing q_0, if needed, we can and will assume that $p_i > \sqrt{\dim \mathbb{U}}$ and we get a splitting short exact sequence

$$1 \to U \to G \to \underbrace{\bigoplus_{j=1}^{s} \bigoplus_{i=1}^{k} H_{j,i}}_{H} \to 1. \tag{185}$$

Theorem 46. *Suppose G, H, $H_{j,i}$'s, and U are as in the setting laid out in the previous couple of paragraphs (in particular, see* (184) *and* (185)*). Suppose $Z := (X_{1,1}, \dots, X_{s,k}, Y)$ is a symmetric random-variable with values in G where $X_{j,i}$ is a random-variable with values in $H_{j,i}$ and Y is a random-variable with values in U. Assume the range of Z generates G. Suppose c_0 and α_0 are positive numbers such that for every integer j in $[1,s]$ and i in $[1,k]$,*

$$\mathcal{L}(X_{j,i}) \geqslant c_0 \quad \textit{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$, where the implied constant depends on $\dim \mathbb{G}$, k (number of fields), and α_0.

In addition to Theorem 46, we can study random-walks in $\underline{G}(\mathbb{Z}/q_{\mathrm{s}}^{v_0}\mathbb{Z})$ where $\underline{G}$ is as above, v_0 is a fixed positive integer, and q_{s} is a square-free positive integer such that $\gcd(q_{\mathrm{s}}, q_0) = 1$. Suppose p_i's are distinct prime factors of q_{s}. Let $q := q_{\mathrm{s}}^{v_0}$, $U_q := \underline{U}(\mathbb{Z}/q\mathbb{Z})$, $G_q := \underline{G}(\mathbb{Z}/q\mathbb{Z})$, $H_q := \underline{H}(\mathbb{Z}/q\mathbb{Z})$, $H_{j,i} := \underline{H}_j(\mathbb{Z}/p_i^{v_0}\mathbb{Z})$, and $\overline{H}_{j,i} := \underline{H}_j(\mathbb{Z}/p_i\mathbb{Z})$ (notice that we are using the same notation $H_{j,i}$ as in Theorem 46, but

considering the context is different this should not cause any confusion). Then we get the following short exact sequences

$$1 \to U_q \to G_q \to \underbrace{\bigoplus_{j=1}^{s} \bigoplus_{i=1}^{k} H_{j,i}}_{H_q} \to 1, \tag{186}$$

and for every i and j

$$1 \to H_{j,i}[p_i] \to H_{j,i} \xrightarrow{\pi_{p_i}} \overline{H}_{j,i} \to 1, \tag{187}$$

where π_{p_i} is the residue modulo p_i map and $H_{j,i}[p_i]$ is its kernel.

Theorem 47. *Suppose G_q, H_q, $H_{j,i}$'s, and U_q are as in the setting in the previous paragraph (in particular (186) and (187)). Suppose $Z := (X_{1,1}, \dots, X_{s,k}, Y)$ is a symmetric random-variable with values in G_q where $X_{j,i}$ is a random-variable with values in $H_{j,i}$ and Y is a random-variable with values in U_q. Assume the range of Z generates G. Suppose c_0 and α_0 are positive numbers such that for every integer j in $[1, s]$ and i in $[1, k]$,*

$$\mathcal{L}(\pi_{p_i}(X_{j,i})) \geqslant c_0 \quad \text{and} \quad \mathbb{P}(Z = z) \geqslant \alpha_0$$

for every z in the range of Z. Then $\mathcal{L}(Z) \gg \min\{c_0, 1\}$ where the implied constant depends on $\dim \mathbb{G}$, k (number of prime factors), α_0, and v_0 (the power of prime factors).

8.1. **Semisimple groups and dealing with non-log-balanced factors.** To prove Theorem 46, we start with obtaining a spectral gap for $(X_1, \dots, X_s)$; this means passing from (almost) simple groups of bounded rank to their products (see Proposition 50). To do this, we need the following variant of Proposition 2.

Lemma 48. *Suppose X is a symmetric random-variable with values in a finite group G. Assume the range of X generates G. Let μ be the probability law of X. Suppose $\pi_0 : G \to \mathrm{GL}(V_{\pi_0})$ is a unitary irreducible representation of G, f_0 is in the space $\mathcal{H}_{\pi_0}$ of matrix coefficients of π; that means*

$$\mathcal{H}_{\pi_0} := \{x \mapsto \langle \pi_0(x) f_1, f_2 \rangle \mid f_1, f_2 \in V_{\pi_0}\},$$

$\|f_0\|_2 = 1$, and $\mu * f_0 = \lambda(\mu) f_0$. Suppose c is a positive number and $\deg \pi_0 \geqslant |G|^c$. If

$$H_2(X^{(\ell_0)}) \geqslant \left(1 - \frac{c}{2}\right) \log |G|$$

for some integer $\ell_0 \leqslant C \log |G|$, then

$$\mathcal{L}(X) \geqslant \frac{c}{4C}.$$

Proof. Let us recall that for every function $g \in L^2(G)$ and $\pi \in \widehat{G}$, the Fourier inverse $\widehat{g}$ of g is defined as

$$\widehat{g}(\pi) := \frac{1}{|G|} \sum_{x \in G} g(x) \pi(x)^*.$$

Then, for every $g_1, g_2 \in L^2(G)$ and $\pi \in \widehat{G}$, we have

$$\widehat{g_1 * g_2}(\pi) = |G| \widehat{g}_2(\pi) \widehat{g}_1(\pi). \tag{188}$$

Hence, by the Parseval theorem, for every positive integer ℓ, we have

$$\begin{aligned}\lambda(\mu)^{2\ell} =&\|\mu^{(\ell)} * f_0\|_2^2 = |G| \sum_{\pi\in\widehat{G}} \deg\pi \|\widehat{\mu^{(\ell)} * f_0}(\pi)\|_{\mathrm{HS}}^2\\ =&|G|^3 \sum_{\pi\in\widehat{G}} \deg\pi \|\widehat{f}_0(\pi)\widehat{\mu^{(\ell)}}(\pi)\|_{\mathrm{HS}}^2, \qquad (189)\end{aligned}$$

where $\|x\|_{\mathrm{HS}} := (\mathrm{Tr}(x^*x))^{1/2}$ is the Hilbert-Schmidt norm of x. Since $f_0 \in \mathcal{H}_{\pi_0}$, $\widehat{f}_0(\pi) = 0$ for every $\pi \neq \pi_0$. Therefore, by (189) and (192), we obtain that

$$\begin{aligned}\lambda(\mu)^{2\ell} =&|G|^3 \deg\pi_0 \, \|\widehat{f}_0(\pi_0)\widehat{\mu^{(\ell)}}(\pi_0)\|_{\mathrm{HS}}^2\\ =&\frac{|G|}{\deg\pi_0}(|G|\deg\pi_0\|\widehat{f}_0(\pi_0)\|_{\mathrm{HS}}^2)(|G|\deg\pi_0\|\widehat{\mu^{(\ell)}}(\pi_0)\|_{\mathrm{HS}}^2)\\ \leqslant&\frac{|G|}{\deg\pi_0}\|f_0\|_2^2\|\mu^{(\ell)}\|_2^2 \leqslant |G|^{1-c}\|\mu^{(\ell)}\|_2^2. \qquad (190)\end{aligned}$$

Applying the function $(-\log)$ to both the sides of the inequality given in (190), we deduce that

$$2\ell_0\mathcal{L}(\mu) \geqslant H_2(X^{(\ell_0)}) - (1-c)\log|G|.$$

Since $\ell_0 \leqslant C\log|G|$ and $H_2(X^{(\ell_0)}) \geqslant (1-\frac{c}{2})\log|G|$, we conclude that

$$\mathcal{L}(X) \geqslant \frac{c}{4C}.$$

□

In several steps in the proof of Theorem 46, we are working with a product of groups that are not necessarily *log-balanced*; that means we do not have a control on the ratio of the logarithm of their orders. Lemma 49 helps us reduce to the case with a log-balanced condition.

Lemma 49. *Suppose c is a positive number, $G_1, \dots, G_k$ are c-quasi-random groups, and $|G_i| \geqslant 2^{4/c}$ for every i. Let $G := \prod_{i=1}^k G_i$. For every subset I of $\{1,\dots,k\}$, let $G_I := \prod_{i\in I} G_i$ and*

$$b_I := \min\left\{\frac{\log|G_i|}{\log|G_I|} \mid i \in I\right\}.$$

Suppose $X := (X_1,\dots,X_k)$ is a symmetric random-variable with values in G. Suppose there is a function $f : (\mathbb{R}^+)^3 \to (0,1)$ which is increasing with respect to the first and the third factors, decreasing with respect to the second factor, and for every non-empty subset I of $\{1,\dots,k\}$ we have

$$\mathcal{L}(X_I) \geqslant f(c,|I|,b_I),$$

where $X_I := (X_i)_{i\in I}$. Then

$$\mathcal{L}(X) \geqslant \frac{f(c,k,c/(4k))}{12}.$$

Proof. Suppose μ is the probability law of X; that means for every $x \in G$, $\mu(x) := \mathbb{P}(X = x)$. Let's recall that $T_\mu : L^2(G) \to L^2(G)$ is $T_\mu(f) := f * \mu$, $\lambda(\mu) := \|T_\mu|_{L^2(G)^\circ}\|_{\mathrm{op}}$, and $\mathcal{L}(X) = -\log\lambda(\mu)$. For every unitary irreducible representation $\pi : G \to \mathrm{GL}(V_\pi)$ of G, let $\mathcal{H}_\pi$ be the space of *matrix coefficients* of π; that means

$$\mathcal{H}_\pi := \{x \mapsto \langle\pi(x)f_1, f_2\rangle \mid f_1, f_2 \in V_\pi\}.$$

Let $\widehat{G}$ be the set of unitary irreducible representations of G up to equivalency. By the Peter-Weyl theorem, $L^2(G) = \bigoplus_{\pi\in\widehat{G}} \mathcal{H}_\pi$ and if $\pi_1 \neq \pi_2$, then $\mathcal{H}_{\pi_1}$ is orthogonal to $\mathcal{H}_{\pi_2}$. Moreover, $\mathcal{H}_\pi$'s are irreducible $G \times G$-subspaces of $L^2(G)$, where

$$((x_1, x_2) \cdot f)(x) = f(x_1^{-1} x x_2),$$

for every $x_1, x_2, x \in G$. Hence, there is a non-trivial $\pi_0 \in \widehat{G}$ and $f_0 \in \mathcal{H}_{\pi_0}$ such that

$$T_\mu(f_0) = \lambda(\mu) f_0 \quad \text{and} \quad \|f_0\|_2 = 1. \tag{191}$$

Let

$$I := \{i \in [1, k] \mid G_i \not\subseteq \ker \pi_0\}.$$

Then by (191), $\mathcal{L}(X) = \mathcal{L}(X_I)$. Since passing to a subset of G_i's does not change the set of assumptions, without loss of generality, we can and will assume that $I = \{1, \dots, k\}$. This implies that

$$\pi = \pi_1 \otimes \cdots \otimes \pi_k$$

for some non-trivial unitary irreducible representation π_i of G_i. Because G_i's are c-quasi-random

$$\deg \pi = \prod_{i=1}^{k} \deg \pi_i \geqslant \prod_{i=1}^{k} |G_i|^c = |G|^c. \tag{192}$$

Thus, by Lemma 48, if for some positive integer C which depends only on the given parameters and some positive integer $\ell \leqslant C \log |G|$,

$$H_2(X^{(\ell)}) \geqslant \left(1 - \frac{c}{2}\right) \log |G|, \qquad \text{(Target entropy)} \tag{193}$$

then

$$\mathcal{L}(X) \geqslant \frac{c}{4C}. \tag{194}$$

Next, we look for a *large* quotient of G, which consists of roughly *log-balanced* factors. Let x_i be $\frac{\log |G_i|}{\log |G|}$. After rearranging the factors, if needed, we can and will assume that x_i's are decreasing. Suppose k_0 is the smallest positive integer such that

$$x_1 + \cdots + x_{k_0} > 1 - \frac{c}{4}. \tag{195}$$

Notice that since x_i's add up to 1, there is such a positive integer k_0. This implies that

$$x_1 + \cdots + x_{k_0 - 1} \leqslant 1 - \frac{c}{4}. \tag{196}$$

By (196) and the fact that $(k - k_0 + 1)x_{k_0} \geqslant x_{k_0} + \cdots + x_k$, we obtain that

$$1 - \frac{c}{4} + (k - k_0 + 1)x_{k_0} \geqslant (x_1 + \cdots + x_{k_0 - 1}) + (x_{k_0} + \cdots + x_k) = 1.$$

Hence

$$x_{k_0} \geqslant \frac{c}{4(k - k_0 + 1)} \geqslant \frac{c}{4k}. \tag{197}$$

Let $I_0 := \{1, \dots, k_0\}$. Notice that, by (197), $b_{I_0} \geqslant \frac{c}{4k}$. Therefore,

$$\mathcal{L}(X_{I_0}) \geqslant f(c, k, c/(4k)). \tag{198}$$

Let ℓ_0 be the smallest positive integer such that

$$\ell_0 \mathcal{L}(X_{I_0}) \geqslant 2 \log |G_{I_0}|. \tag{199}$$

By (198) and (199), we have that

$$\ell_0 \leqslant \frac{3}{f(c,k,c/(4k))} \log |G_{I_0}|. \tag{200}$$

By (199) and a similar argument as how we derived (40), we deduce that

$$\left| \mathbb{P}(X_{I_0}^{(\ell_0)} = x) - \frac{1}{|G_{I_0}|} \right| \leqslant \frac{1}{|G_{I_0}|^2} \tag{201}$$

for every $x \in G_{I_0}$. Therefore

$$\begin{aligned} H_2(X^{(\ell_0)}) \geqslant & H_2(X_{I_0}^{(\ell_0)}) \geqslant -\log\Bigg(\sum_{x \in G_{I_0}} (|G_{I_0}|^{-1} + |G_{I_0}|^{-2})^2 \Bigg) \\ & = \log |G_{I_0}| - 2\log(1 + |G_{I_0}|^{-1}) \geqslant \log |G_{I_0}| - 2. \end{aligned} \tag{202}$$

By (202) and (195), we obtain that

$$H_2(X^{(\ell_0)}) \geqslant \left(1 - \frac{c}{4}\right) \log |G| - 2. \tag{203}$$

Since $|G| \geqslant 2^{4/c}$, by (203) it follows that

$$H_2(X^{(\ell_0)}) \geqslant \left(1 - \frac{c}{2}\right) \log |G|. \tag{204}$$

Now that we reached to the *target entropy* in logarithmic steps, by (200) and (194), we conclude that,

$$\mathcal{L}(X) \geqslant \frac{c f(c,k,c/(4k))}{12}.$$

□

Proposition 50. *Suppose $F_1, \dots, F_m$ are finite fields and $\mathbb{H}_i$ is a connected, simply-connected, absolutely almost simple F_i-group for every i. Suppose $\dim \mathbb{H}_i \leqslant d_0$ for every i. Let $H_i := \mathbb{H}_i(F_i)$ and*

$$H := H_1 \oplus \cdots \oplus H_m.$$

Assume that $|F_i| \gg_{d_0} 1$. Suppose $X = (X_1, \dots, X_m)$ is a symmetric random-variable with values in H whose range generates H. Suppose c_0 and α_0 are positive numbers such that $\mathcal{L}(X_i) \geqslant c_0$ for every i and $\mathbb{P}(X = x) \geqslant \alpha_0$ for every x in the range of X. Then

$$\mathcal{L}(X) \gg \min\{c_0, 1\},$$

where the implied constant depends only on α_0, d_0, and m.

Proof. By [22], there is a positive number c which depends only on d_0 such that H_i is c-quasi-random for every i. For every subset I of $\{1, \dots, m\}$, let $H_I := \bigoplus_{i \in I} H_i$, $X_I := (X_i)_{i \in I}$, and

$$b_I := \min\left\{ \frac{\log |H_i|}{\log |H_I|} \mid i \in I \right\}.$$

By induction on the number of factors, Theorem 12, Proposition 25, and Proposition 26, we deduce that for every d_0 and α_0 there is a function $f_{d_0,\alpha_0} : (\mathbb{R}^+)^3 \to (0,1)$ which is increasing with respect to the first and the third components, decreasing with respect to the second component, and

$$\mathcal{L}(X_{I_0}) \geqslant f_{d_0,\alpha_0}(c, m, b_I) \min\{c_0, 1\}.$$

Then by Lemma 49,

$$\mathcal{L}(X) \geqslant \frac{f_{d_0,\alpha_0}(c,m,c/(4m))}{12}\min\{c_0,1\}.$$

□

8.2. **Proof of Theorem 46. Perfect to simple factors: Finite fields.** By (185), we have the following short exact sequence

$$1 \to U/\gamma_2(U) \to G/\gamma_2(U) \to H \to 1.$$

By Proposition 28, Proposition 29, and the preparatory discussion at the beginning of the section, there is an H-equivariant isomorphism from U^{ab} to $\mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} (\prod_{i=}^{k} F_i)$, and the action of $\mathbb{H} = (\underline{H})_{\mathbb{Q}}$ on $(\underline{\mathfrak{u}^{\mathrm{ab}}})_{\mathbb{Q}}$ does not have a non-zero fixed point. Hence, by Proposition 45, there is a positive integer C' such that for every $x \in U^{\mathrm{ab}}$,

$$M_x = \sum_C \mathcal{O}_x - \sum_C \mathcal{O}_x, \tag{205}$$

where M_x is the $\mathbb{Z}[H]$-module generated by x and $\mathcal{O}_x$ is the H-orbit of x. This means the pair of groups H and U^{ab} satisfy (G6).

Notice that for every i, the following is a short exact sequence

$$1 \to \underline{\mathfrak{u}^{\mathrm{ab}}}(F_i) \to \underline{G}(F_i)/\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]}(F_i)) \to \underline{H}(F_i) \to 1.$$

By Proposition 25, there is a positive number c depending only on $d_0 := \dim \mathbb{G}$ such that $\overline{H}_i := \underline{H}(F_i)$ is c-quasi-random, and by (205), the pair of groups $\overline{H}_i$ and $A_i := \underline{\mathfrak{u}^{\mathrm{ab}}}(F_i)$ satisfy (G6). The pair of groups $\overline{H}_i$ and A_i also satisfy (G5) with a constant which only depends on $\dim \mathbb{G}$. Hence, by Lemma 17, there exists a positive number $\overline{c}$ which depends only on d_0 such that

$$\overline{G}_i := \underline{G}(F_i)/\gamma_2(\underline{U}_{\mathbb{Z}[1/q_0]}(F_i))$$

is $\overline{c}$-quasi-random for every i. Let $\overline{G} := \prod_{i=1}^{k} \overline{G}_i$, and notice that $\overline{G}$ is naturally isomorphic to $G/\gamma_2(U)$. Let $\overline{Z} := \pi_{\gamma_2(U)}(Z)$ where $\pi_{\gamma_2(U)} : G \to \overline{G}$ is the natural quotient map.

For every subset I of $\{1,\dots,k\}$, let $\overline{G}_I := \prod_{i\in I} \overline{G}_i$, $\overline{Z}_I := \mathrm{pr}_I(\overline{Z})$ where $\mathrm{pr}_I : \overline{G} \to \overline{G}_I$ is the natural projection, and

$$\overline{b}_I := \min\left\{ \frac{\log|\overline{G}_i|}{\log|\overline{G}_I|} \mid i \in I \right\}.$$

By Theorem 15 and Proposition 25, for every d_0 and α_0, there is a function $f_{d_0,\alpha_0} : (\mathbb{R}^+)^3 \to (0,1)$ which is decreasing with respect to the first and the third components, decreasing with respect to the second component, and

$$\mathcal{L}(\overline{Z}_I) \geqslant f_{d_0,\alpha_0}(\overline{c},|I|,\overline{b}_I)\min\{c_0,1\}. \tag{206}$$

Hence, by Lemma 49, we deduce that

$$\mathcal{L}(\overline{Z}) \geqslant \frac{f_{d_0,\alpha_0}(\overline{c},k,\overline{c}/(4k))}{12}\min\{c_0,1\}. \tag{207}$$

Notice that choosing q_0 with enough prime factors, we can and will assume that $|\overline{G}_i| \geqslant 2^{4/\overline{c}}$ for every i.

By Proposition 28, for every positive integer i, we have

$$\gamma_i(U) = \prod_{j=1}^{k} \gamma_i(\underline{U}_{F_j})(F_j). \tag{208}$$

By (208), U is a finite nilpotent group whose nilpotency class is bounded by d_0. Moreover,

$$L(U) := \bigoplus_{i=1}^{d_0} \gamma_i(U)/\gamma_{i+1}(U) = \prod_{j=1}^{k} \left(\bigoplus_{i=1}^{d_0} \gamma_i(\underline{U}_{F_j})(F_j)/\gamma_{i+1}(\underline{U}_{F_j})(F_j) \right). \tag{209}$$

By (209), $L(U)$ is an $\prod_{j=1}^{k} F_j$-algebra. Furthermore, by $\underline{U}_{\mathbb{F}_{p_i}}(F_i) = \underline{U}_{\mathbb{Z}[1/q_0]}(F_i)$ and Proposition 29

$$U^{\mathrm{ab}} \simeq \mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} (\prod_{j=1}^{k} F_j);$$

and so U^{ab} is generated by at most d_0 elements as an $\prod_{j=1}^{k} F_j$-module. Hence, U satisfies (G7) and (G8) with parameters that depend only on d_0.

For every i, let $G_i := \underline{G}(F_i)$. As we discussed earlier, $\overline{G}_i = G_i/\gamma_2(\underline{U}_{F_i})(F_i)$ is $\overline{c}$-quasi-random for some positive number $\overline{c}$ which depends only on d_0. For a subset I of $\{1, \dots, k\}$, let $G_I := \prod_{i \in I} G_i$ and

$$b_I := \min\left\{ \frac{\log |G_i|}{\log |G_I|} \mid i \in I \right\}.$$

Then G_I is cb_I-quasi-random. For every non-empty subset I of $\{1, \dots, k\}$, let $Z_I := \mathrm{pr}_I(Z)$ where $\pi_I : G \to G_I$ is the natural projection. By Proposition 19 and (207), for every d_0 there is a function $f_{d_0} : (\mathbb{R}^+)^3 \to (0,1)$ which is increasing with respect to the first and the third components, decreasing with respect to the second component, and

$$\mathcal{L}(Z_I) \geqslant f_{d_0}(\overline{c}, |I|, b_I) \frac{f_{d_0,\alpha_0}(\overline{c}, k, \overline{c}/(4k))}{12} \min\{c_0, 1\} \tag{210}$$

for every non-empty subset I of $\{1, \dots, k\}$. Therefore, by Lemma 49, we deduce that

$$\mathcal{L}(Z) \geqslant \frac{f_{d_0}(\overline{c}, k, \overline{c}/(4k))}{12} \frac{f_{d_0,\alpha_0}(\overline{c}, k, \overline{c}/(4k))}{12} \min\{c_0, 1\},$$

which finishes the proof.

8.3. **Proof of Theorem 47. Perfect to simple factors: Bounded number of prime factors.** For every positive integer r, let $U_r := \underline{U}(\mathbb{Z}/r\mathbb{Z})$, $G_r := \underline{G}(\mathbb{Z}/r\mathbb{Z})$, and $H_r := \underline{H}(\mathbb{Z}/r\mathbb{Z})$. For every divisor d of r, let π_d be the residue map modulo d from G_r to G_d, and let $G_r[d] := \ker \pi_d$. Then the following is a short exact sequence,

$$1 \to G_q[q_{\mathrm{s}}] \to G_q \to G_{q_{\mathrm{s}}} \to 1; \tag{211}$$

moreover, by the Chinese remainder theorem,

$$G_q = \bigoplus_i G_{p_i^{v_0}} \quad \text{and} \quad G_q[q_{\mathrm{s}}] = \bigoplus_i G_{p_i^{v_0}}[p_i].$$

It is well-known (and easy to check) that for every integer $v < v_0$ and every index i,

$$[G_{p_i^{v_0}}[p_i^v], G_{p_i^{v_0}}[p_i]] \subseteq G_{p_i^{v_0}}[p_i^{v+1}].$$

Hence, $G_q[q_{\mathrm{s}}]$ is a nilpotent group with nilpotency class at most v_0-1. In fact, by [25, Lemma 1.8], for every positive integer $j \leqslant v_0$, we have that

$$\gamma_j(G_{p_i^{v_0}}[p_i]) = G_{p_i^{v_0}}[p_i^j] \quad \text{and} \quad G_{p_i^{v_0}}[p_i^j]/G_{p_i^{v_0}}[p_i^{j+1}] \simeq \mathfrak{g} \otimes_{\mathbb{Z}[1/q_0]} (\mathbb{Z}/p_i\mathbb{Z}), \tag{212}$$

where $\mathfrak{g} := \mathrm{Lie}(\underline{G}_{\mathbb{Z}[1/q_0]})(\mathbb{Z}[1/q_0])$. Notice that this claim is true only for large enough primes p_i, and by assuming that q_0 has enough prime divisors we can and will insure this property. We should also point out that the mentioned result in [25] is written only for the semisimple case, but the same argument implies the perfect case (see [10, Lemma 39] and [9, Section 2.9]). Therefore,

$$L(G_q[q_{\mathrm{s}}]) = \bigoplus_{j=1}^{v_0} \gamma_j(G_q[q_{\mathrm{s}}])/\gamma_{j+1}(G_q[q_{\mathrm{s}}]) \simeq \mathfrak{g} \otimes_{\mathbb{Z}[1/q_0]} t(\mathbb{Z}/q_{\mathrm{s}}\mathbb{Z})[t]/\langle t^{v_0}\rangle. \tag{213}$$

By (213), we obtain that the nilpotent group $G_q[q_{\mathrm{s}}]$ satisfies (G7) and (G8) with parameters that depend only on v_0 and $\dim \mathbb{G}$.

By (212), we also deduce that there is a short exact sequence of the form

$$1 \to \mathfrak{g} \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/q_{\mathrm{s}}\mathbb{Z} \to G_q/\gamma_2(G_q[q_{\mathrm{s}}]) \to G_{q_{\mathrm{s}}} \to 1, \tag{214}$$

and $G_q/\gamma_2(G_q[q_{\mathrm{s}}]) \simeq G_{q_{\mathrm{s}}^2}$.

We identify G_q with $\prod_i G_{p_i^{v_0}}$, and for every subset I of $\{1,\dots,k\}$, let

$$\mathrm{pr}_I : G_q \to \prod_{i\in I} G_{p_i^{v_0}}$$

be the natural projection.

For every subset I of $\{1,\dots,k\}$, let b_I be the *log-balanced* factor of $G_{p_i^{v_0}}$'s; that means

$$b_I := \min_{i\in I} \frac{\log|G_{p_i^{v_0}}|}{\log|G_{q_{\mathrm{s}}^{v_0}}|}.$$

By [10, Proposition 19], $\prod_{i\in I} G_{p_i^{v_0}}$ is c_I-quasi-random where c_I is a positive number which depends only on $\dim \mathbb{G}, v_0$ and b_I. Moreover, by the same result, we have that there is a positive number c which depends only on $\dim \mathbb{G}$ and v_0 such that $G_{p_i^{v_0}}$ is c-quasi-random for every i. Let $q_I := \prod_{i\in I} p_i^{v_0}$ and $q_{I,\mathrm{s}} := \prod_{i\in I} p_i$. By (214), we have that the following is a short exact sequence

$$1 \to \mathfrak{g} \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/q_{I,\mathrm{s}}\mathbb{Z} \to G_q/\gamma_2(G_{q_I}[q_{I,\mathrm{s}}]) \to G_{q_{I,\mathrm{s}}} \to 1. \tag{215}$$

By Proposition 19, we obtain that there is a function $g : \mathbb{R}^+ \to (0,1)$ which is increasing and for every non-empty subset I of $\{1,\dots,k\}$, we have

$$\mathcal{L}(Z_I) \geqslant g(c_I)\mathcal{L}(\pi_{q_{I,\mathrm{s}}^2}(Z_I)) \geqslant g(c_I)\mathcal{L}(\pi_{q_{\mathrm{s}}^2}(Z)),$$

where $Z_I := \mathrm{pr}_I(Z)$. Hence, by Lemma 49, we conclude that there is a function $\overline{g}$ of $\dim \mathbb{G}$, v_0, and k such that

$$\mathcal{L}(Z) \geqslant \overline{g}(\dim \mathbb{G}, v_0, k)\mathcal{L}(\pi_{q_{\mathrm{s}}^2}(Z)). \tag{216}$$

Next, notice that by [10, Equation (8) in Lemma 13] the following is a splitting short exact sequence when all the prime factors p_i's are large enough:

$$1 \to U_{q_{\mathrm{s}}^2} \to G_{q_{\mathrm{s}}^2} \to H_{q_{\mathrm{s}}^2} \to 1. \tag{217}$$

Moreover, by Proposition 28, $U_{q_{\mathrm{s}}^2}$ is a nilpotent group with nilpotency class at most $\dim \mathbb{U}-1$, and $L(U_{q_{\mathrm{s}}^2})$ satisfies (G8) with a parameter which only depends on $\dim \mathbb{U}$.

Hence, by a similar argument as above, using Proposition 19 and Lemma 49, we obtain that

$$\mathcal{L}(\overline{Z}) \gg \mathcal{L}(\pi_{\gamma_2(U_{q_s^2})}(\overline{Z})), \tag{218}$$

where $\pi_{\gamma_2(U_{q_s^2})} : G_{q_s^2} \to G_{q_s^2}/\gamma_2(U_{q_s^2})$ is the natural quotient map, the implied constant is a positive number which depends only on $\dim \mathbb{G}$, v_0, and k, and $\overline{Z} := \pi_{q_s^2}(Z)$. Notice that by Proposition 29 and (217),

$$G_{q_s^2}/\gamma_2(U_{q_s^2}) \simeq U_{q_s^2}^{\mathrm{ab}} \rtimes H_{q_s^2} \simeq (\mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/q_s^2\mathbb{Z}) \rtimes H_{q_s^2}.$$

By [25, Lemma 1.8] (see [10, Lemma 39] and [9, Section 2.9]), we have that the following is a short exact sequence

(219)

$$1 \to (\mathfrak{u}^{\mathrm{ab}} \oplus \mathfrak{h}) \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/q_s\mathbb{Z} \to G_{q_s^2}/\gamma_2(U_{q_s^2}) \xrightarrow{\pi} (\mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/q_s\mathbb{Z}) \rtimes H_{q_s} \to 1,$$

where $\mathfrak{h} := \mathrm{Lie}(\underline{H}_{\mathbb{Z}[1/q_0]})(\mathbb{Z}[1/q_0])$.

We can finish the proof similar to the previous step: starting with the log-balanced case, using Theorem 15, and then applying Lemma 49.

For every subset I of $\{1, 2 \dots, k\}$, let b_I be the *log-balanced* factor of $G_{p_i^2}/\gamma_2(U_{p_i^2})$; that means

$$b_I := \min_{i \in I} \frac{\log |G_{p_i^2}/\gamma_2(U_{p_i^2})|}{\log |G_{q_s^2}/\gamma_2(U_{q_s^2})|}.$$

It is worth mentioning that

$$G_{q_s^2}/\gamma_2(U_{q_s^2}) \simeq \prod_{i=1}^{k} G_{p_i^2}/\gamma_2(U_{p_i^2}).$$

For every subset I of $\{1, \dots, k\}$, let

$$\overline{A}_I := \prod_{i \in I} (\mathfrak{u}^{\mathrm{ab}} \oplus \mathfrak{h}) \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/p_i\mathbb{Z}, \quad \overline{H}_I := \prod_{i \in I} (\mathfrak{u}^{\mathrm{ab}} \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Z}/p_i\mathbb{Z}) \rtimes H_{p_i},$$

and

$$\overline{G}_I := \prod_{i \in I} G_{p_i^2}/\gamma_2(U_{p_i^2}).$$

We also let $\overline{Z}_I := \mathrm{pr}_I(\pi_{\gamma_2(U_{q_s^2})}(\overline{Z}))$ where $\pi_I : \overline{G}_{\{1,\dots,k\}} \to \overline{G}_I$ is the natural projection.

By [10, Proposition 19], $\overline{G}_I$ is c_I-quasi-random for a positive number c_I which depends only on $\dim \mathbb{G}$ and b_I. In particular, there is a positive number c which depends on $\dim \mathbb{G}$ such that $\overline{G}_{\{i\}}$ is c-quasi-random for every $i \in \{1, \dots, k\}$.

Notice that the action of $\mathbb{H}(\mathbb{Q})$ on $(\mathfrak{u}^{\mathrm{ab}} \oplus \mathfrak{h}) \otimes_{\mathbb{Z}[1/q_0]} \mathbb{Q}$ does not have a non-zero fixed point as $\mathbb{G}$ is perfect and $\mathbb{H}$ is semisimple. Therefore, by Proposition 44, we have that the pair of groups $\overline{H}_I$ and $\overline{A}_I$ satisfy (G6) with a parameter that depends only on $\dim \mathbb{G}$. They also satisfy (G5) with a parameter depending only on $\dim \mathbb{G}$. Hence, by Theorem 15, there is a function $g : (\mathbb{R}^+)^2 \to (0, 1)$ such that for every subset I of $\{1, \dots, k\}$,

$$\mathcal{L}(\overline{Z}_I) \geqslant g(\dim \mathbb{G}, c_I)\mathcal{L}(\pi(\overline{Z}_I)) \geqslant g(\dim \mathbb{G}, c_I)\mathcal{L}(\pi(\overline{Z}_{\{1,\dots,k\}})).$$

Thus by Lemma 49, we deduce that there is a function $\overline{g}$ of $\dim \mathbb{G}$ and k such that

$$\mathcal{L}(\pi_{\gamma_2(U_{q_s^2})}(\overline{Z})) \geqslant \overline{g}(\dim \mathbb{G}, k)\mathcal{L}(\pi(\overline{Z}_{\{1,\dots,k\}})). \tag{220}$$

On the other hand, by Theorem 46,

$$\mathcal{L}(\pi(\overline{Z}_{\{1,\dots,k\}})) \gg \min\{1, c_0\}, \tag{221}$$

where the implied constant depends on $\dim \mathbb{G}$, k, and α_0. By (216), (220), and (221), we conclude that

$$\mathcal{L}(Z) \gg \min\{c_0, 1\},$$

where the implied constant depends on $\dim \mathbb{G}$, k, v_0, and α_0.

Acknowledgment

Special thanks are due to the anonymous referee for their thorough report, which helped us make the necessary revisions.

References

[1] Noga Alon, Alexander Lubotzky, and Avi Wigderson, *Semi-direct product in groups and zig-zag product in graphs: connections and applications (extended abstract)*, 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), IEEE Computer Soc., Los Alamitos, CA, 2001, pp. 630–637. MR1948752

[2] Jean Bourgain and Alex Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) **167** (2008), no. 2, 625–642, DOI 10.4007/annals.2008.167.625. MR2415383

[3] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57, DOI 10.1007/s00039-004-0451-1. MR2053599

[4] R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2) **42** (1941), 556–590, DOI 10.2307/1968918. MR4042

[5] Emmanuel Breuillard and Alex Gamburd, *Strong uniform expansion in* $\mathrm{SL}(2, p)$, Geom. Funct. Anal. **20** (2010), no. 5, 1201–1209, DOI 10.1007/s00039-010-0094-3. MR2746951

[6] S. Chowla, H. B. Mann, and E. G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh., Trondheim **32** (1959), 74–80. MR125077

[7] Michel Demazure and Peter Gabriel, *Introduction to algebraic geometry and algebraic groups*, North-Holland Mathematics Studies, vol. 39, North-Holland Publishing Co., Amsterdam-New York, 1980. Translated from the French by J. Bell. MR563524

[8] Persi Diaconis and Laurent Saloff-Coste, *Comparison techniques for random walk on finite groups*, Ann. Probab. **21** (1993), no. 4, 2131–2156. MR1245303

[9] Alireza Salehi Golsefidy, *Super-approximation, I:* $\mathfrak{p}$*-adic semisimple case*, Int. Math. Res. Not. IMRN **23** (2017), 7190–7263, DOI 10.1093/imrn/rnw208. MR3802123

[10] Alireza Salehi Golsefidy, *Super-approximation, II: the p-adic case and the case of bounded powers of square-free integers*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 7, 2163–2232, DOI 10.4171/JEMS/883. MR3959861

[11] Alireza Salehi Golsefidy, *Sum-product phenomena:* $\mathfrak{p}$*-adic case*, J. Anal. Math. **142** (2020), no. 2, 349–419, DOI 10.1007/s11854-020-0139-y. MR4205786

[12] Keivan Mallahi-Karai, Amir Mohammadi, and Alireza Salehi Golsefidy, *Locally random groups*, Michigan Math. J. **72** (2022), 479–527, DOI 10.1307/mmj/20217213. MR4460261

[13] Golsefidy, A. S. and S. Srinivas. 2024. *Random walks on direct product of groups*, J. Eur. Math. Soc. (JEMS), Accepted for publication.

[14] A. Salehi Golsefidy and Péter P. Varjú, *Expansion in perfect groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891, DOI 10.1007/s00039-012-0190-7. MR3000503

[15] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387, DOI 10.1017/S0963548307008826. MR2410393

[16] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II* (French), Inst. Hautes Études Sci. Publ. Math. **24** (1965), 231. MR199181

[17] Robert M. Guralnick, *Small representations are completely reducible*, J. Algebra **220** (1999), no. 2, 531–541, DOI 10.1006/jabr.1999.7963. MR1717357

[18] Bertram Huppert and Norman Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften, vol. 242, Springer-Verlag, Berlin-New York, 1982. AMD, 44. MR650245

[19] I. Martin Isaacs, *Character theory of finite groups*, Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423 (57 #417)]. MR1280461

[20] Martin Kassabov, *Symmetric groups and expander graphs*, Invent. Math. **170** (2007), no. 2, 327–354, DOI 10.1007/s00222-007-0065-y. MR2342639

[21] Emmanuel Kowalski, *An introduction to expander graphs*, Cours Spécialisés [Specialized Courses], vol. 26, Société Mathématique de France, Paris, 2019. MR3931316

[22] Vicente Landazuri and Gary M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443, DOI 10.1016/0021-8693(74)90150-1. MR360852

[23] Martin W. Liebeck and Aner Shalev, *Diameters of finite simple groups: sharp bounds and applications*, Ann. of Math. (2) **154** (2001), no. 2, 383–406, DOI 10.2307/3062101. MR1865975

[24] Elon Lindenstrauss and Péter P. Varjú, *Spectral gap in the group of affine transformations over prime fields* (English, with English and French summaries), Ann. Fac. Sci. Toulouse Math. (6) **25** (2016), no. 5, 969–993, DOI 10.5802/afst.1518. MR3582116

[25] Alexander Lubotzky, *Subgroup growth and congruence subgroups*, Invent. Math. **119** (1995), no. 2, 267–295, DOI 10.1007/BF01245183. MR1312501

[26] A. Lubotzky and B. Weiss, *Groups and expanders*, Expanding graphs (Princeton, NJ, 1992), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 10, Amer. Math. Soc., Providence, RI, 1993, pp. 95–109, DOI 10.1090/dimacs/010/08. MR1235570

[27] Richard S. Pierce, *Associative algebras*, Studies in the History of Modern Science, vol. 9, Springer-Verlag, New York-Berlin, 1982. Graduate Texts in Mathematics, 88. MR674652

[28] Aner Shalev, *Word maps, conjugacy classes, and a noncommutative Waring-type theorem*, Ann. of Math. (2) **170** (2009), no. 3, 1383–1416, DOI 10.4007/annals.2009.170.1383. MR2600876

[29] T. A. Springer, *Linear algebraic groups*, 2nd ed., Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2009. MR2458469

[30] Robert Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56. MR155937

[31] Péter P. Varjú, *Expansion in $SL_d(\mathcal{O}_K/I)$, I square-free*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 1, 273–305, DOI 10.4171/JEMS/302. MR2862040

Department of Mathematics, University of California, San Diego, California 92093-0112

Email address: golsefidy@ucsd.edu

Department of Mathematics, University of California, San Diego, California 92093-0112

Email address: scsriniv@ucsd.edu