Canad. J. Math. Vol. 75 (1), 2023 pp. 322–340
http://dx.doi.org/10.4153/S0008414X21000687

On multiplicative energy of subsets of varieties

Ilya D. Shkredov

Abstract. We obtain a nontrivial upper bound for the multiplicative energy of any sufficiently large subset of a subvariety of a finite algebraic group. We also find some applications of our results to the growth of conjugates classes, estimates of exponential sums, and restriction phenomenon.

1 Introduction

In papers [4, 5, 7, 10, 11, 17, 19, 20, 25] and in many others, the authors study the growth properties of rather general subsets A of different groups $\mathbf{G}$ (basically, of Lie type). One of the difficulties concerning growth of A is that, in principle, A can live in a subvariety of $\mathbf{G}$ (see [10, 11, 17]). In this paper, we restrict ourselves to the case when A indeed belongs to a subvariety and consider the most natural combinatorial problem connecting growth of A, namely, the basic question about obtaining upper bounds for the *multiplicative energy* (see, e.g., [35]) of A

$$\mathsf{E}(A) := |\{(a,b,c,d) \in A^4 \ : \ ab^{-1} = cd^{-1}\}|.$$

Our result is the following.

Theorem 1 *Let $\mathbf{G}$ be a finite algebraic group over $\mathbb{F}_q$, $V \subseteq \mathbf{G}$ be a variety, and Γ be a maximal algebraic subgroup such that a coset of Γ is contained in V. Then, for any $A \subseteq V$, $|A| \geq |\Gamma|^{1+\varepsilon}$, and all sufficiently large q, one has*

$$\mathsf{E}(A) \ll |A|^{3-\delta}, \tag{1.1}$$

where $\delta = \delta(\varepsilon, \dim(V)) > 0$ and the implied constant in (1.1) depends on $\dim(V), \deg(V), \dim(\mathbf{G}), \deg(\mathbf{G})$, and dimension n of $\mathbb{F}_q^n \supseteq \mathbf{G}$.

In particular, bound (1.1) takes place for a variety V iff V does not contain a coset of an algebraic subgroup of size $\Omega(|V|)$.

Now, we consider a particular case of Theorem 1 when our variety V belongs to a finite Chevalley group and $A \subseteq V$ is a rather large set. It is possible to show that bound (1.1) can be significantly improved for such A in the sense that A must be uniformly distributed among any sets with small product and not just subgroups (see the discussion in Proposition A.1).

Received by the editors January 31, 2021; revised July 3, 2021; accepted December 13, 2021.
Published online on Cambridge Core January 13, 2022.
This work is supported by the Russian Science Foundation under grant 19-11-00001.
AMS subject classification: **11B30**, 11B75, 11B99, 05B99, 20G15, 42B05.
Keywords: Multiplicative energy, varieties, restriction phenomenon.

Theorem 2 *Let $\mathbf{G}_r(\mathbb{F}_q)$ be a finite Chevalley group with rank r and odd q, and let $\Pi \le \mathbf{G}_r(\mathbb{F}_q)$ be its maximal (by size) parabolic subgroup. Also, let $V \subset \mathbf{G}_r(\mathbb{F}_q)$ be a variety which does not coincide with all shifts of conjugates of Π. Then, for any $A \subseteq V$ and $|A| \ge |\Pi| q^{-1+c}$, $c > 0$, one has*

$$\| \sum_{g \in A} \rho(g) \|_o \le |A|^{1-\delta}, \tag{1.2}$$

where $\delta = \delta(c, r) > 0$, $\| \cdot \|_o$ is the operator norm, and ρ is any nontrivial unitary representation of $\mathbf{G}_r(\mathbb{F}_q)$.

It is interesting that all our conditions in Theorems 1 and 2 concerning intersection of A with subgroups are formulated in terms of V but not A. In a similar way, we do not require that A is a generating set of $\mathbf{G}$. It differs our result from Larsen–Pink machinery (see [5, 11, 17, 25]).

Theorem 1 has a naturally looking algebraic consequence (see rigorous formulation in Section 4).

Corollary 3 *Suppose that $\mathbf{G}$ is a finite algebraic group and $V \subseteq \mathbf{G}$ is a variety. Put*

$$t(V) := \max_{x \in \mathbf{G},\, \Gamma \le \mathbf{G}} \{|\Gamma| \,:\, x\Gamma \subseteq V\},$$

and

$$t_a(V) := \max_{x \in \mathbf{G},\, \Gamma \le \mathbf{G}} \{|\Gamma| \,:\, x\Gamma \subseteq V,\ \Gamma \text{ is an algebraic subgroup}\}.$$

Then, $t(V) = O(t_a(V))$.

In Corollary 3, we assume that q (or $|\mathbf{G}|$) tends to infinity and the implied constant in big-O depends on $\dim(V), \deg(V), \dim(\mathbf{G}), \deg(\mathbf{G})$, and the dimension of the ground affine space.

We obtain several applications of Theorem 1. In the first one, we take our variety V be a Zariski closure of conjugate class C of a finite algebraic group. In [19, 20], the authors obtain that for any such C, one has $|CC| \gg \min\{|C|^{2-o(1)}, |\mathbf{G}|\}$. We prove that in certain cases, one has $|AA| \gg |A|^{1+c}$, $c > 0$, for *any* sufficiently large subset A of C.

Of course, Theorem 2 is based on a purely noncommutative phenomenon of growth in groups, and, say, estimate (1.2) does not hold in $\mathbb{F}_q^n$. Nevertheless, in Section 5, we obtain a purely commutative application to the so-called *restriction* problems (see the fundamental book [34] and papers [2, 3, 33]). Here, we have dealt with the restriction phenomenon in finite fields (see [21] and good survey [14]). Let us recall some definitions. Now, our group $\mathbf{G} = \mathbb{F}_q^n$, and $\mathbf{G}$ acts on $\mathbf{G}$ via shifts. For any function $g : \mathbf{G} \to \mathbb{C}$, consider its Fourier transform

$$\hat{g}(\xi) := \sum_{x \in \mathbf{G}} g(x) e(-x \cdot \xi),$$

as well as the inverse Fourier transform of a function $f : V \to \mathbb{C}$,

$$(f d\sigma)^\vee(x) := \frac{1}{|V|} \sum_{\xi \in V} f(\xi) e(x \cdot \xi),$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

where $e(-x\cdot\xi)$ is an additive character on $\mathbf{G}$. Put

$$\|f\|_{L^q(V,d\sigma)} := \left(\frac{1}{|V|}\sum_{\xi\in V}|f(\xi)|^q\right)^{\frac{1}{q}} \qquad \text{and} \qquad \|g\|_{L^q(\mathbf{G})} := \left(\sum_{x\in\mathbf{G}}|g(x)|^q\right)^{\frac{1}{q}}.$$

The finite-field restriction problem [21] for our variety V seeks exponent pairs (q,r) such that one has the inequality

$$\|(fd\sigma)^\vee\|_{L^r(\mathbf{G})} \le R^*(q\to r)\|f\|_{L^q(V,d\sigma)}$$

t $R^*(q\to r)$ independent of the size of the finite field. In papers [13, 14, 18, 21, 36], the authors consider some particular varieties as cones, paraboloids, and spheres. Our result is weaker, but on the other hand, we have dealt with an almost arbitrary variety V. We think that this is the first result of such generality in the restriction theory over finite fields.

Theorem 4 *Let $V\subseteq\mathbb{F}_q^n$ be a variety and $d=\dim(V)$. Suppose that V does not contain any line. Then, $R^*(\frac{4}{3-c}\to 4)\ll 1$, where $c=c(d)>0$.*

Let us say a few words about the proofs. To estimate the multiplicative energy $\mathsf{E}(A)$, $A\subseteq V$, we consider the shifts $A_g := A\cap Ag\subseteq V\cap Vg$ and use the formula $\mathsf{E}(A)=\sum_g|A_g|^2$. The main idea is that for "typical" g, the intersection $V\cap Vg$ is a variety of a strictly less dimension than $\dim(V)$, and hence we can use induction, considering $(A_g)_h = A\cap Ag\cap Ah\cap Agh\subseteq(V_g)_h$, $((A_g)_h)_t\subseteq((V_g)_h)_t$, and so on. Our induction procedure can be expressed using the language of the so-called *Gowers norms* (see [6], because these norms are defined in terms of the considered intersections $(((A_{g_1})_{g_2})\dots)_{g_k}$). Also, we need to connect the multiplicative energy $\mathsf{E}(A)$ and Gowers norms of A in a direct way, and we do this using some combinatorial tools (see Section 3 and paper [28]). Hence, to obtain bound (1.1), it is sufficient to estimate the Gowers norms of A. In the proof, we separate abelian and nonabelian cases, because the dependence of δ on $\dim(V)$ and ε in (1.1) is rather concrete and is much better in the case of an abelian group $\mathbf{G}$ than for a general group $\mathbf{G}$. Also, we show that "nontypical" elements g exist iff there is a coset of a large algebraic subgroup in V. To avoid such situations, we need the condition $|A|\ge|\Gamma|^{1+\varepsilon}$ in our Theorem 1.

2 Definitions

Let $\mathbf{G}$ be a group with the identity 1. Given two sets $A,B\subset\mathbf{G}$, define the *product set* of A and B as

$$AB := \{ab\ :\ a\in A,\ b\in B\}.$$

In a similar way, we define the higher product sets, e.g., A^3 is AAA. Let $A^{-1} := \{a^{-1}\ :\ a\in A\}$. As usual, having two subsets A,B of a group $\mathbf{G}$, denote by

$$\mathsf{E}(A,B) = |\{(a,a_1,b,b_1)\in A^2\times B^2\ :\ a^{-1}b=a_1^{-1}b_1\}|,$$

the *common energy* of A and B. Clearly, $\mathsf{E}(A,B)=\mathsf{E}(B,A)$, and by the Cauchy–Schwarz inequality,

$$\mathsf{E}(A,B)|A^{-1}B|\ge|A|^2|B|^2. \tag{2.1}$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

In a little more general way, define

$$\mathsf{E}^L_k(A) = |\{(a_1,\dots,a_k,b_1,\dots,b_k) \in A^{2k} \ : \ a_1^{-1}b_1 = \dots = a_k^{-1}b_k\}|,$$

and, similarly,

$$\mathsf{E}^R_k(A) = |\{(a_1,\dots,a_k,b_1,\dots,b_k) \in A^{2k} \ : \ a_1b_1^{-1} = \dots = a_kb_k^{-1}\}|.$$

For $k=2$, we have $\mathsf{E}^L_k(A) = \mathsf{E}^R_k(A)$, but for larger k, it is not the case. If there is no difference between $\mathsf{E}^L_k(A)$ and $\mathsf{E}^R_k(A)$, then we write just $\mathsf{E}_k(A)$. In this paper, we use the same letter to denote a set $A \subseteq \mathbf{G}$ and its characteristic function $A : \mathbf{G} \to \{0,1\}$.

First of all, we recall some notions and simple facts from the representation theory (see, e.g., [23] or [27]). For a finite group $\mathbf{G}$, let $\widehat{\mathbf{G}}$ be the set of all irreducible unitary representations of $\mathbf{G}$. It is well known that size of $\widehat{\mathbf{G}}$ coincides with the number of all conjugate classes of $\mathbf{G}$. For $\rho \in \widehat{\mathbf{G}}$, denote by d_ρ the dimension of this representation. Thus, $\mathbf{G}$ is a quasi-random group in the sense of Gowers (see [7]) iff $d_\rho \geq |\mathbf{G}|^\varepsilon$, where $\varepsilon > 0$ and ρ is any nontrivial irreducible unitary representation of $\mathbf{G}$. We write $\langle\cdot,\cdot\rangle$ for the corresponding Hilbert–Schmidt scalar product $\langle A,B\rangle = \langle A,B\rangle_{HS} := \mathrm{tr}(AB^*)$, where A,B are any two matrices of the same sizes. Put $\|A\| = \sqrt{\langle A,A\rangle}$. Finally, it is easy to check that for any matrices A,B, one has $\|AB\| \leq \|A\|_o\|B\|$ and $\|A\|_o \leq \|A\|$, where the operator l^2-norm $\|A\|_o$ is just the maximal singular value of A.

For any function $f : \mathbf{G} \to \mathbb{C}$ and $\rho \in \widehat{\mathbf{G}}$, define the matrix $\widehat{f}(\rho)$, which is called the Fourier transform of f at ρ by the formula

$$\widehat{f}(\rho) = \sum_{g\in\mathbf{G}} f(g)\rho(g). \tag{2.2}$$

Then, the inverse formula takes place

$$f(g) = \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \langle \widehat{f}(\rho), \rho(g^{-1})\rangle, \tag{2.3}$$

and the Parseval identity is

$$\sum_{g\in\mathbf{G}} |f(g)|^2 = \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{f}(\rho)\|^2. \tag{2.4}$$

The main property of the Fourier transform is the convolution formula

$$\widehat{f * g}(\rho) = \widehat{f}(\rho)\widehat{g}(\rho), \tag{2.5}$$

where the convolution of two functions $f,g : \mathbf{G} \to \mathbb{C}$ is defined as

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

Given a function $f : \mathbf{G} \to \mathbb{C}$ and a positive integer k, we write $f^{(k)} = f^{(k-1)} * f$ for the kth convolution of f. Now, let $k \geq 2$ be an integer and $f_j : \mathbf{G} \to \mathbb{C}$, $j \in [2k]$ be any functions. Denote by $\mathcal{C}$ the operator of convex conjugation. As in [31], define

$$\mathsf{T}_k(f_1,\dots,f_{2k}) = \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \langle \prod_{j=1}^{k} \mathcal{C}^j\widehat{f}_j(\rho), \prod_{j=k+1}^{2k} \mathcal{C}^j\widehat{f}_j(\rho)\rangle. \tag{2.6}$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Put $\mathsf{T}_k(f) = \mathsf{T}_k(f,\dots,f)$. For example, we have, clearly, $\mathsf{T}_2(A) = \mathsf{E}(A)$. It is easy to see that $\mathsf{T}_k^{1/2k}(f)$ defines a norm of a function f (see [31]). This fact follows from the following inequality [31, Lemma 10]:

$$\mathsf{T}_k^{2k}(f_1,\dots,f_{2k}) \le \prod_{j=1}^{2k} \mathsf{T}_k(f_j). \tag{2.7}$$

In particular, $\mathsf{E}(A, A^{-1}) \le \mathsf{E}(A)$.

Now, let us say a few words about varieties. Having a field $\mathbb{F}$, define an (affine) variety in $\mathbb{F}^n$ to be the set of the form

$$V = \{(x_1,\dots,x_n) \in \mathbb{F}^n \ : \ p_j(x_1,\dots,x_n) = 0 \ \text{for all } j\},$$

where $p_j \in \mathbb{F}[x_1,\dots,x_n]$. Let us recall some basic properties of varieties. General theory of varieties and schemes can be found, e.g., in [8]. The union of any finite number of varieties is, clearly, a variety, and the intersection of any number of varieties is a variety as well. Having a set X, we denote by $\mathrm{Zcl}(X)$ a minimal (by inclusion) variety, containing X. A variety over an algebraically closed field $\mathbb{F}$ is *irreducible* if it is not the union of two proper subvarieties. Every variety has a unique (up to inclusion) decomposition into finitely many irreducible components [8]. The *dimension* of V is

$$\dim(V) = \max\{n \ : \ V \supseteq X_n \supset X_{n-1} \supset \dots \supset X_0 \ne \varnothing\},$$

where X_j are irreducible subvarieties of V. We will frequently use the simple fact that if $V_1 \subseteq V_2$ are two varieties and V_2 is irreducible, then either $V_1 = V_2$, or $\dim(V_1) < \dim(V_2)$. A variety is *absolutely irreducible* if it is irreducible over $\overline{\mathbb{F}}$. In this paper, we consider just these varieties.

We define the *degree* of any irreducible variety V with $\dim(V) = d$ as in [9], namely,

$$\deg(V) = \sup\{|L \cap V| < \infty \ : \ L \text{ is } (n-d)\text{-dimensional affine subspace in } \mathbb{F}^n\}.$$

For an arbitrary variety V, we denote $\deg(V)$ to be the sum of the degrees of its irreducible components. Recall the generalized Bézout theorem (see [9, Theorem 1]): for any varieties U, V, one has

$$\deg(U \cap V) \le \deg(U)\deg(V). \tag{2.8}$$

The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. If we want to underline the dependence on a parameter M, then we write $\ll_M$ and $\gg_M$. All logarithms are to base 2. Sometimes, we allow ourselves to lose logarithmic powers of $|\mathbb{F}|$. In this situation, we write $\lesssim$ and $\gtrsim$ instead of $\ll$ and $\gg$.

3 On noncommutative Gowers norms

Let $\mathbf{G}$ be a group and $A \subseteq \mathbf{G}$ be a finite set. Let $\|A\|_{\mathcal{U}^k}$ be the Gowers nonnormalized kth-norm [6] of the characteristic function of A (in multiplicative form; see, say, [28]):

$$\|A\|_{\mathcal{U}^k} = \sum_{x_0,x_1,\dots,x_k \in \mathbf{G}} \prod_{\vec{\varepsilon} \in \{0,1\}^k} A\left(x_0 x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}\right),$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

where $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k)$. For example,

$$\|A\|_{\mathcal{U}^2} = \sum_{x_0,x_1,x_2 \in \mathbf{G}} A(x_0)A(x_0x_1)A(x_0x_2)A(x_0x_1x_2) = \mathsf{E}(A)$$

is the energy of A, and $\|A\|_{\mathcal{U}^1} = |A|^2$. For any $\vec{s} = (s_1, \dots, s_k) \in \mathbf{G}^k$, put

$$A_{\vec{s}}(x) = \prod_{\vec{\varepsilon} \in \{0,1\}^k} A\left(xs_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}\right), \tag{3.1}$$

and similar for an arbitrary function $f : \mathbf{G} \to \mathbb{C}$, namely,

$$f_{\vec{s}}(x) = \prod_{\vec{\varepsilon} \in \{0,1\}^k} \mathcal{C}^{\varepsilon_1 + \dots + \varepsilon_k} f\left(xs_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}\right),$$

where $\mathcal{C}$ is the operator of the conjugation. For example, $A_s(x) = A(x)A(xs)$ or, in other words, $A_s = A \cap (As^{-1})$. Then, obviously,

$$\|A\|_{\mathcal{U}^k} = \sum_{\vec{s}} |A_{\vec{s}}|. \tag{3.2}$$

Also, note that

$$\|A\|_{\mathcal{U}^{k+1}} = \sum_{\vec{s}} |A_{\vec{s}}|^2. \tag{3.3}$$

Moreover, the induction property for Gowers norms holds (it follows from the definitions or see [6])

$$\|A\|_{\mathcal{U}^{k+1}} = \sum_{s \in A^{-1}A} \|A_s\|_{\mathcal{U}^k}, \tag{3.4}$$

e.g., in particular,

$$\|A\|_{\mathcal{U}^3} = \sum_{s \in A^{-1}A} \mathsf{E}(A_s).$$

The Gowers norms enjoy the following weak commutativity property. Namely, let $k = n + m$ and $\vec{s} = (s_1, \dots, s_k) = (\vec{u}, \vec{v})$, where the vectors $\vec{u}, \vec{v}$ have lengths n and m, correspondingly. We have

$$\|A\|_{\mathcal{U}^k} = \sum_{\vec{s}} \sum_{x} \prod_{\vec{\varepsilon} \in \{0,1\}^k} A\left(xs_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}\right)$$

$$= \sum_{\vec{u},\vec{v}} \sum_{x} \prod_{\vec{\eta} \in \{0,1\}^m} \prod_{\vec{\omega} \in \{0,1\}^n} A\left(u_1^{\eta_1} \dots u_m^{\eta_m} x v_1^{\omega_1} \dots v_n^{\omega_n}\right). \tag{3.5}$$

In particular, $\|A^{-1}\|_{\mathcal{U}^k} = \|A\|_{\mathcal{U}^k}$ and $\|gA\|_{\mathcal{U}^k} = \|Ag\|_{\mathcal{U}^k} = \|A\|_{\mathcal{U}^k}$ for any $g \in \mathbf{G}$. To obtain (3.5), just make the changing of variables $u_j x = x\tilde{u}_j$ for $j \in [m]$.

It was proved in [6] that ordinary Gowers kth-norms of the characteristic function of any subset of an abelian group $\mathbf{G}$ are connected to each other. In [28], the author shows that the connection for the nonnormalized norms does not depend on the size of the group $\mathbf{G}$. Here, we formulate a particular case of Proposition 35 from [28], which relates $\|A\|_{\mathcal{U}^k}$ and $\|A\|_{\mathcal{U}^2}$ (see Remark 36 here).

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Lemma 1 *Let A be a finite subset of a commutative group $\mathbf{G}$. Then, for any integer $k \ge 1$, one has*

$$\|A\|_{\mathcal{U}^{k+1}} \ge \frac{\|A\|_{\mathcal{U}^k}^{(3k-2)/(k-1)}}{\|A\|_{\mathcal{U}^{k-1}}^{2k/(k-1)}}.$$

In particular,

$$\|A\|_{\mathcal{U}^k} \ge \mathsf{E}(A)^{2^k-k-1}|A|^{-(3\cdot 2^k-4k-4)}.$$

Actually, one can derive Lemma 1 from Lemma 2, but to prove this more general result, we need an additional notation and arguments.

Given two functions $f, g : \mathbf{G} \to \mathbb{C}$ and an integer $k \ge 0$, consider the "scalar product"

$$\langle f, g\rangle_k := \sum_{\vec{s},t}\sum_x f_{\vec{s}}(x)\overline{g_{\vec{s}}(xt)} = \overline{\langle g, f\rangle_k},$$

where $\vec{s} = (s_1, \dots, s_k)$. For example, $\langle A, B\rangle_1 = \mathsf{E}(A, B)$, $\langle A, B\rangle_0 = |A||B|$, $\langle A, A\rangle_k = \|A\|_{\mathcal{U}^{k+1}}$, and $\langle A, 1\rangle_k = |\mathbf{G}|\|A\|_{\mathcal{U}^k}$ (for finite group $\mathbf{G}$). Clearly, $\langle f, g\rangle_0 = (\sum_x f(x))\left(\overline{\sum_x g(x)}\right)$, but for $k \ge 1$, it is easy to see that $\langle f, g\rangle_k \ge 0$, because $\langle f, g\rangle_k = \sum_{\vec{s}_*, s_k} |(f_{\vec{s}_*} * \tilde{\bar{g}}_{\vec{s}_*})(s_k)|^2 \ge 0$, where $\vec{s}_* = (s_1, \dots, s_{k-1})$, and $\tilde{g}(x) := g(x^{-1})$. Also, note that

$$\langle A, B\rangle_k = \sum_{\vec{s}} |A_{\vec{s}}||B_{\vec{s}}| = \sum_{\vec{s}_*}\sum_{s_k} |A_{\vec{s}_*} \cap A_{\vec{s}_*}s_k||B_{\vec{s}_*} \cap B_{\vec{s}_*}s_k|. \tag{3.6}$$

Lemma 2 *Let $\mathbf{G}$ be a commutative group and $f, g : \mathbf{G} \to \mathbb{C}$ be functions. Then, for any integer $k \ge 1$, one has*

$$\langle f, g\rangle_k^{3+1/k} \le \langle f, g\rangle_{k-1}^2 \langle f, g\rangle_{k+1} \|f\|_{\mathcal{U}^k}^{1/k} \|g\|_{\mathcal{U}^k}^{1/k}, \tag{3.7}$$

and hence for an arbitrary $k \ge 2$ and any sets $A, B \subseteq \mathbf{G}$, the following holds:

$$\mathsf{E}(A, B) \le (|A||B|)^{\frac{3}{2} - \frac{\beta(k+2)}{2}} \langle A, B\rangle_k^{\beta}, \tag{3.8}$$

where $\beta = \beta(k) \in [4^{-k}, 2^{-k+1}]$.
For any (not necessary commutative) group $\mathbf{G}$, if $\|A\|_{\mathcal{U}^k} \le |A|^{k+1-c}$, where $c > 0$, then $\mathsf{E}(A) \le |A|^{3-c_*}$ with $c_* = c_*(c, k) > 0$.

Proof We have

$$\sigma := \langle f, g\rangle_k = \sum_{\vec{s},t}\sum_x f_{\vec{s}}(x)\overline{g_{\vec{s}}(xt)}, \tag{3.9}$$

and our first task to estimate the size of the set of $(\vec{s}, t)$ in the last formula. Basically, we consider two cases. If the summation in (3.9) is taken over the set

$$Q := \{\vec{s} : \sum_t g_{\vec{s}}(t) \ge \sigma(2k\|f\|_{\mathcal{U}^k})^{-1}\}, \tag{3.10}$$

then it gives us $(1 - 1/2k)$ proportion of σ. Cardinality of the set Q can be estimated as

$$|Q| \cdot \sigma(2k\|f\|_{\mathcal{U}^k})^{-1} \le \|g\|_{\mathcal{U}^k},$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

and hence $|Q| \le 2k\|f\|_{U^k}\|g\|_{U^k}\sigma^{-1}$. Now, we fix any $j \in [k]$ (without any loss of generality, we can assume that $j = 1$), put $\vec{s}_* = (s_2, \dots, s_k)$, and consider

$$Q_1 := \{(\vec{s}_*, t) \ : \ \sum_{s_1} f_{\vec{s}_*}(s_1)\overline{g_{\vec{s}_*}(ts_1)} \ge \sigma(2k\langle f, g\rangle_{k-1})^{-1}\}. \tag{3.11}$$

Using the changing of the variables as in (3.5) (here we appeal to the commutativity of the group **G**) and arguing as above, we have

$$|Q_1| \cdot \sigma(2k\langle f, g\rangle_{k-1})^{-1} \le \sum_{\vec{s}_*, t}\sum_{s_1} f_{\vec{s}_*}(s_1)\overline{g_{\vec{s}_*}(ts_1)}\langle f, g\rangle_{k-1}.$$

Again, if the summation in (3.9) is taken over the set Q_1, then it gives us $(1 - 1/2k)$ proportion of σ. Hence, by the standard projection results (see, e.g., [1]), we see that the summation in (3.9) is taken over a set $\mathcal{S}$ of vectors $(\vec{s}, t)$ of size at most

$$|\mathcal{S}| \le ((2k)^{k+1}\|f\|_{U^k}\|g\|_{U^k}\sigma^{-(k+1)})^{1/k}\langle f, g\rangle_{k-1}^2. \tag{3.12}$$

The proof below is rather technical in the commutative case. If the reader is interested in the general case, then it is possible to avoid all calculations before (3.17), where much simpler arguments are presented to estimate the size of the set $\mathcal{S}$.

Returning to (3.12) and using the Cauchy–Schwarz inequality, we get

$$2^{-4}\sigma^2 \le |\mathcal{S}|\sum_{\vec{s},t}\left|\sum_x f_{\vec{s}}(x)\overline{g_{\vec{s}}(xt)}\right|^2 \le ((2k)^{k+1}\|f\|_{U^k}\|g\|_{U^k}\sigma^{-(k+1)})^{1/k}\langle f, g\rangle_{k-1}^2\langle f, g\rangle_{k+1},$$

and we have (3.7) up to a constant depending on k. Using the tensor trick (see, e.g., [35]), we obtain the result with the constant one.

To prove inequality (3.8), we see by induction and formula (3.7) that one has, for $l \le k$,

$$\langle A, B\rangle_l \le \langle A, B\rangle_0^{\alpha_0(l,k)}\prod_{j=1}^{k-1}(\|A\|_{U^j}\|B\|_{U^j})^{\alpha_j(l,k)} \cdot \langle A, B\rangle_k^{\beta_k(l,k)},$$

where $\alpha_j(l, k), \beta_j(l, k)$ are some nonnegative functions. In principle, in view of (3.7), these functions can be calculated via some recurrences, but we restrict ourselves giving just crude bounds for them. We are interested in $l = 1$ and k is a fixed number, and hence we write

$$\mathsf{E}(A, B) = \langle A, B\rangle_1 \le \langle A, B\rangle_0^{\alpha_0}\prod_{j=1}^{k-1}(\|A\|_{U^j}\|B\|_{U^j})^{\alpha_j} \cdot \langle A, B\rangle_k^{\beta}.$$

By homogeneity, we get

$$2 = \alpha_0 + \sum_{j=1}^{k-1}\alpha_j 2^j + 2^k\beta. \tag{3.13}$$

In particular, $\beta \le 2^{-k+1}$. Further taking $A = B$ equals a subgroup, we obtain one more equation

$$3 = 2\alpha_0 + 2\sum_{j=1}^{k-1}\alpha_j(j + 1) + (k + 2)\beta. \tag{3.14}$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Using trivial inequalities $\|A\|_{\mathcal{U}^j} \le |A|^{j+1}$, $\|B\|_{\mathcal{U}^j} \le |B|^{j+1}$ and formula (3.14), we derive

$$\mathsf{E}(A,B) \le (|A||B|)^{\alpha_0+\sum_{j=1}^{k-1}\alpha_j(j+1)}\langle A,B\rangle_k^{\beta} = (|A||B|)^{\frac{3}{2}-\frac{\beta(k+2)}{2}}\langle A,B\rangle_k^{\beta},$$

as required. Actually, if there is a nontrivial upper bound for $\|A\|_{\mathcal{U}^j}$ (and it will be so in the next section), then the last estimate can be improved in view of Lemma 1. Furthermore, our task is to obtain a good lower bound for β. Put $\omega_j := 3 + 1/j > 3$, $j \in [k-1]$. Using (3.7), we get

$$\prod_{j=1}^{k-1}\langle A,B\rangle_j^{\omega_j x_j} \le S\prod_{j=1}^{k-1}\left(\langle A,B\rangle_{j-1}^2\langle A,B\rangle_{j+1}\right)^{x_j}, \tag{3.15}$$

where S is a quantity depending on $\|A\|_{\mathcal{U}^j}$, $\|B\|_{\mathcal{U}^j}$, which we do not specify, and let x_j be some positive numbers, which we will choose (indirectly) later. For $2 \le j \le k-2$, put

$$x_{j-1} + 2x_{j+1} = \omega_j x_j. \tag{3.16}$$

Then, we obtain from (3.15)

$$\langle A,B\rangle_1^{4x_1}\langle A,B\rangle_{k-1}^{\omega_{k-1}x_{k-1}} \le S\langle A,B\rangle_1^{2x_2}\langle A,B\rangle_k^{x_{k-1}}\langle A,B\rangle_{k-1}^{x_{k-2}}.$$

Now, choosing $x_{k-2} = \omega_{k-1}x_{k-1}$, we see that $\beta = x_{k-1}/(4x_1 - 2x_2)$, and it remains to estimate x_{k-1} in terms of x_1, x_2. But for all j, one has $\omega_j \le 4$, hence $x_{k-1} \ge 4^{-1}x_{k-2}$, and similarly, from $x_{j-1} + 2x_{j+1} = \omega_j x_j$, $2 \le j \le k-2$, we get $x_j \ge 4^{-1}x_{j-1}$, and hence $x_{k-1} \ge 4^{-(k-1)}x_1$. Furthermore, summing (3.16) over $2 \le j \le k-2$ and putting $T = \sum_{j=1}^{k-1} x_j$, we obtain

$$T - x_{k-1} - x_{k-2} + 2T - 2x_1 - 2x_2 = \sum_{j=2}^{k-2}\omega_j x_j \ge 3T - 3x_1 - 3x_{k-1},$$

and hence

$$x_1 - 2x_2 \ge x_{k-2} - 2x_{k-1} = (\omega_{k-1} - 2)x_{k-1} > 0. \tag{3.17}$$

In particular, it gives $x_j > 0$ for all $j \in [k-1]$, and thus indeed $\beta \ge 4^{-k}$.

Now, suppose that $\mathbf{G}$ is an arbitrary group and $\|A\|_{\mathcal{U}^k} \le |A|^{k+1-c}$, but $\mathsf{E}(A) \ge |A|^3/K$, where $K \ge 1$ is a parameter. By the noncommutative Balog–Szemerédi–Gowers theorem (see [22, Theorem 32] or [35, Proposition 2.43 and Corollary 2.46]), there is $a \in A$ and $A_* \subseteq a^{-1}A$, $|A_*| \gg_K |A|$ such that $|A_*^3| \ll_K |A_*|$. We can apply the previous argument to the set A_* and obtain an estimate similar to Lemma 1

$$|A|^{k+1-c} \ge \|A\|_{\mathcal{U}^k} \ge \|A_*\|_{\mathcal{U}^k} \gg_K \mathsf{E}(A_*)^{2^{k-2}}|A_*|^{-(3\cdot 2^{k-2}-k-1)}$$

$$\gg_K \mathsf{E}(A)^{2^{k-2}}|A|^{-(3\cdot 2^{k-2}-k-1)}. \tag{3.18}$$

Indeed, to bound $\mathsf{E}(A_*)$ via $\|A_*\|_{\mathcal{U}^{k+2}}$ using the argument as in the proof above, we need to estimate the size of the set $\mathcal{S}_k$ at each step k. But clearly, $|\mathcal{S}_k| \le |A_*A_*^{-1}|^{k+1} \ll_K |A_*|^{k+1}$, and hence, by induction, we obtain $\mathsf{E}^{2^k}(A_*) \ll_K |A_*|^{3\cdot 2^k-k-3}\|A_*\|_{\mathcal{U}^{k+2}}$, as required. Finally, from (3.18), it follows that $K^{C(k)} \gg |A|^c$, where $C(k)$ is a constant depending on k only. This completes the proof. ∎

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

A closer look to the proof (see, e.g., definition (3.11)) shows that for $k = 1$, estimate (3.7) of Lemma 1 takes place for any class functions f, g. Nevertheless, for larger k, this argument does not work.

4 The proof of the main result

Let $\mathbf{G}$ be an algebraic group in an affine or projective space of dimension n over the field $\mathbb{F}_q$, and let $V \subseteq \mathbf{G}$ be a variety, $d = \dim(V)$, and $D = \deg(V)$. If V is absolutely irreducible, then by Lang and Weil [16], we know that

$$\big||V| - q^d\big| \le (d-1)(d-2)q^{d-1/2} + A(n,d,D)q^{d-1}, \tag{4.1}$$

where $A(n,d,D)$ is a certain constant. By sufficiently large q, we mean that $q \ge q_0(n,d,D,\ \dim(\mathbf{G}), \deg(\mathbf{G}))$ and all constants below are assumed to depend on $n, d, D, \dim(\mathbf{G}), \deg(\mathbf{G})$. In particular, for an absolutely irreducible variety V, one has $q^d \ll |V| \ll q^d$. One can think about $\mathbf{G}$ and V as varieties defined over $\mathbb{Q}$ by absolutely irreducible polynomials. Then, by the Noether theorem [24], we know that $\mathbf{G}$ and V reduce mod p to some absolutely irreducible varieties defined over p, $p \notin S(\mathbf{G}, V)$, where $S(\mathbf{G}, V)$ is a certain finite set of the primes.

Finally, for any set $W \subseteq \mathbf{G}$, consider the quantity

$$t = t(W) := \max_{x \in \mathbf{G},\ \Gamma \le \mathbf{G}} \{|\Gamma| \ :\ x\Gamma \subseteq W,\ \Gamma \text{ is an algebraic subgroup}\}. \tag{4.2}$$

Now, we are ready to estimate different energies of varieties in terms of the quantity $t(V)$. We are also able to give a nontrivial bound for any sufficiently large subset of V (see inequality (4.5)). The proof relies on Lemma 2, and this lemma works better in the abelian case allowing to find concrete $\delta = \delta(d,\varepsilon)$ in (1.1) for an abelian group $\mathbf{G}$.

Theorem 1 *Let $\mathbf{G}$ be an algebraic group, $V \subseteq \mathbf{G}$ be a variety, $d = \dim(V)$, $D = \deg(V)$, and $t = t(V)$. Then, for any positive integer k and all sufficiently large q, one has*

$$\mathsf{E}_k(V) \ll_{d,D} \frac{|V|^{k+1}}{q^{k-1}} + t|V|^k. \tag{4.3}$$

In particular, if V is absolutely irreducible and V is not a coset of a subgroup, then $\mathsf{E}_k(V) \ll_{d,D} |V|^{k+1-\frac{1}{d}}$.

Similarly, one has

$$\|V\|_{\mathcal{U}^k} \ll_{d,D} |V|^{k+1} q^{-\frac{k(k-1)}{2}} + |V|^2 t^{k-1} + |V|^2 \sum_{j=1}^{k-2} |V|^j t^{k-1-j} q^{-\frac{j(1+j)}{2}}, \tag{4.4}$$

and for any $A \subseteq V$, the following holds:

$$\|A\|_{\mathcal{U}^{d+1}} \ll_{d,D} t|A|^{d+1}. \tag{4.5}$$

Proof First of all, consider the case of an absolutely irreducible V. For any $g \in \mathbf{G}$, we have either $\dim(V \cap gV) < \dim(V)$, or g belongs to the stabilizer $\mathrm{Stab}(V)$ of V. It is well known that any stabilizer under any action of an algebraic group is an algebraic subgroup (but not necessary irreducible). Clearly, $\mathrm{Stab}(V) \subseteq v^{-1}V$ for any $v \in V$, and hence either V is a coset of an (algebraic) subgroup, and hence there is nothing

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

to prove, or $\dim(\mathrm{Stab}(V)) < \dim(V)$. The degree of the variety $gV \cap V$ is at most $\deg^2(V)$ by inequality (2.8). Similarly, because our topological space is a Noetherian one (see, e.g., [8, p. 5]) and $\mathrm{Stab}(V) = \bigcap_{v\in V} v^{-1}V$, it follows that the cardinality of $\mathrm{Stab}(V)$ can be estimated in terms of d and D thanks to (4.1). Hence, all parameters of all appeared varieties are controlled by d, D, n (and, possibly, by $\dim(\mathbf{G}), \deg(\mathbf{G})$). Using the Lang–Weil formula (4.1), we obtain for sufficiently large q that $q^d/2 \le |V| \le 2q^d$, say, further $|\mathrm{Stab}(V)| \ll q^{d-1}$, and, similarly, for any $g \notin \mathrm{Stab}(V)$, one has $|V \cap gV| \ll q^{d-1}$. Hence,

$$\mathsf{E}_k(V) = \sum_{g\in\mathbf{G}} |V \cap gV|^k = \sum_{g\notin \mathrm{Stab}(V)} |V \cap gV|^k + \sum_{g\in \mathrm{Stab}(V)} |V \cap gV|^k \tag{4.6}$$

$$\ll (q^{d-1})^{k-1} \sum_{g\in\mathbf{G}} |V \cap gV| + q^{d-1}|V|^k \ll (q^{d-1})^{k-1}|V|^2 + q^{d-1}|V|^k \ll |V|^{k+1-\frac{1}{d}}. \tag{4.7}$$

Now, to obtain (4.3), we apply the same argument but before we need to consider V as a union of its irreducible components $V = \bigcup_{j=1}^s V_j$. Clearly, $s \le \deg(V)$. Take any $g \in \mathbf{G}$, and consider $V \cap gV = \bigcup_{i,j=1}^s (V_i \cap gV_j)$. If, for all $i, j \in [s]$, one has $\dim(V_i \cap gV_j) < \dim V$, then for such g, we can repeat the previous calculations in (4.6)–(4.7). Consider the set of the remaining g, and denote this set by B. For any $g \in B$, there is $i, j \in [s]$ such that $\dim(V_i \cap gV_j) = \dim(V)$. In particular, $\dim(V_i) = \dim(V_j) = \dim(V)$ and $V_i \cap gV_j = V_i = gV_j$ by irreducibility of V_i, V_j. Suppose that for the same pair (i, j), there is another $g_* = g_*(i, j) \in B$ such that $g_*V_j = V_i$. Then, $g_*^{-1}g \in \mathrm{Stab}(V_j)$. It follows that $g \in g_*\mathrm{Stab}(V_j)$, and hence the set B belongs to $\bigcup_{i,j=1}^s g_*(i, j)\mathrm{Stab}(V_j)$ plus at most $s^2 \le \deg^2(V)$ points. Hence, we need to add to the computations in (4.6)–(4.7) the term

$$s^2(t+1)|V|^k \le \deg(V)^2(t+1)|V|^k \ll t|V|^k,$$

as required.

To prove bound (4.4), let us obtain a generalization of (4.3). Put $\mathsf{E}_k^{(l)} = \mathsf{E}_k^{(l)}(V) := \sum_{\vec{s}} |V_{\vec{s}}|^k$, where $\vec{s} = (s_1, \dots, s_l)$ and $V_{\vec{s}}$ as in (3.1). Write $\vec{s} = (\vec{s}_*, s_l)$. Because $\mathsf{E}_k^{(l)} = \sum_{\vec{s}_*} \mathsf{E}_k(V_{\vec{s}_*})$, it follows that by the obtained estimate (4.3),

$$\mathsf{E}_k^{(l)} \ll \sum_{\vec{s}_*} \left(\frac{|V_{\vec{s}_*}|^{k+1}}{q^{k-1}} + t(V_{\vec{s}_*})|V_{\vec{s}_*}|^k \right) \ll q^{-(k-1)}\mathsf{E}_{k+1}^{(l-1)} + t\mathsf{E}_k^{(l-1)}. \tag{4.8}$$

Here, we have used the fact that the function t on a subset of V does not exceed $t(V)$. Furthermore, inequality (4.8) gives by induction

$$\mathsf{E}_k^{(l)} \ll |V|^k \sum_{j=0}^{l} q^{-\frac{j(2k+j-3)}{2}} |V|^j t^{l-j}. \tag{4.9}$$

Now, applying inequality (4.3) with the parameter $k = 2$ and using the notation $\vec{s} = (\vec{s}_*, s_l)$ again, we get

$$\|V\|_{\mathcal{U}^{l+1}} = \sum_{\vec{s}} |V_{\vec{s}}|^2 = \sum_{\vec{s}_*} \mathsf{E}(V_{\vec{s}_*}) \ll \sum_{\vec{s}_*} \left(\frac{|V_{\vec{s}_*}|^3}{q} + t|V_{\vec{s}_*}|^2 \right) = q^{-1}\mathsf{E}_3^{(l-1)} + t\mathsf{E}_2^{(l-1)}.$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Hence, in view of (4.9), we derive

$$\|V\|_{\mathcal{U}^{l+1}} \ll |V|^2 \sum_{j=0}^{l-1} |V|^j t^{l-1-j} (|V| q^{-\frac{j(3+j)}{2}-1} + t q^{-\frac{j(1+j)}{2}})$$

$$\ll |V|^2 t^l + |V|^{l+2} q^{-\frac{l^2+l}{2}} + |V|^2 \sum_{j=1}^{l-1} |V|^j t^{l-j} q^{-\frac{j(1+j)}{2}}.$$

Finally, take any $A \subseteq V$. As above, put $\vec{s} = (s_1, \dots, s_d) = (\vec{s}_*, s_d)$. We have $A_{\vec{s}} \subseteq V_{\vec{s}}$. Furthermore, by (3.6),

$$\|A\|_{\mathcal{U}^{d+1}} = \sum_{\vec{s}} |A_{\vec{s}}|^2 = \sum_{\vec{s}_*} \mathsf{E}(A_{\vec{s}_*}) = \sum_{\vec{s}_*} \sum_{s_d} |A_{\vec{s}_*} \cap A_{\vec{s}_* s_d}|^2. \tag{4.10}$$

Take any vector $\vec{z} = (z_1, \dots, z_l)$, $l < d$, and consider the decomposition of the variable $V_{\vec{z}}$ onto irreducible components $V_{\vec{z}}(j)$. As before, define the set $B(\vec{z})$ of all $g \in \mathbf{G}$ such that there are $V_{\vec{z}}(i)$, $V_{\vec{z}}(j)$ with $V_{\vec{z}}(i) = g V_{\vec{z}}(j)$. Then, arguing as above, we have $|B(\vec{z})| \ll t$. Using formula (4.10), we get

$$\|A\|_{\mathcal{U}^{d+1}} \ll t \sum_{\vec{s}_*} |A_{\vec{s}_*}|^2 + \sigma = t \|A\|_{\mathcal{U}^d} + \sigma, \tag{4.11}$$

where for all $\vec{s}$ in σ, we have $\dim(V_{\vec{s}}) = 0$. Hence,

$$\|A\|_{\mathcal{U}^{d+1}} \ll t \|A\|_{\mathcal{U}^d} + \sum_{\vec{s}} |A_{\vec{s}}| \ll t|A|^{d+1} + |A|^{d+1} \ll t|A|^{d+1}. \tag{4.12}$$

This completes the proof. ∎

Once again, the bounds above depend on d, D, as well as on $\dim(\mathbf{G})$, $\deg(\mathbf{G})$ and on the dimension of the ground affine space.

Remark 2 The quantity $\|V\|_{\mathcal{U}^k}$ can be written in different ways as $\sum_{s_1,\dots,s_k} |V_{s_1,\dots,s_k}|^2$, $\sum_{s_1,\dots,s_{k-1}} \mathsf{E}(V_{s_1,\dots,s_{k-1}})$, and so on. Taking variables s_j running over the maximal coset belonging to V, we see that all terms with t in (4.4) are needed.

Corollary 3 *Let $\mathbf{G}$ be an abelian algebraic group, $V \subseteq \mathbf{G}$ be a variety, $d = \dim(V)$, and $D = \deg(V)$. Then, for all sufficiently large q and any $A \subseteq V$, one has*

$$\mathsf{E}(A) \ll_{d,D} |A|^3 \left(\frac{t}{|A|}\right)^{(2^{d+1}-d-5)^{-1}} \quad \text{for } d \geq 2 \quad \text{and} \quad \mathsf{E}(A) \ll_{d,D} |A|^2 t, \text{ for } d = 1. \tag{4.13}$$

In particular, for any $A \subseteq V$ with $|A| \geq t^{1+c}$, $c > 0$, there is $\delta = \delta(d, c) > 0$ such that

$$\mathsf{E}(A) \ll_{d,D} |A|^{3-\delta}. \tag{4.14}$$

Bound (4.14) takes place in any algebraic group. Moreover, let $B \subseteq \mathbf{G}$ be an arbitrary set. Then,

$$\mathsf{E}(A, B) \ll_{d,D} \left(\frac{t}{|A|}\right)^{\beta} \cdot |A|^{\frac{3}{2}-\frac{\beta d}{2}} |B|^{\frac{3}{2}+\frac{\beta d}{2}}, \tag{4.15}$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

where $\beta = \beta(d) \in [4^{-d}, 2^{-d+1}]$, *and for any* $k \ge 1$, *one has either* $\mathsf{T}_k(A) \le |A|^{2k-1-c\beta/4}$ *or*

$$\mathsf{T}_{k+1}(A) \ll_{d,D} |A|^2 \mathsf{T}_k(A) \cdot |A|^{-c\beta/4}. \tag{4.16}$$

Proof Let $d \ge 2$. By Theorem 1, we have $\|A\|_{\mathcal{U}^{d+1}} \ll t|A|^{d+1}$. Using the second part of Lemma 1 with $k = d+1$, we obtain

$$\mathsf{E}(A) \ll |A|^3 \left(\frac{t}{|A|}\right)^{(2^k-k-4)^{-1}} = |A|^3 \left(\frac{t}{|A|}\right)^{(2^{d+1}-d-5)^{-1}}.$$

If $d = 1$, then the arguments of the proof of Theorem 1 (see, e.g., (4.12)) give us

$$\mathsf{E}(A) \ll t|A|^2 + \sum_s |A_s| \ll t|A|^2.$$

For an arbitrary algebraic group, use the last part of Lemma 2.

To derive (4.15), we can suppose that $|B| \ge |A|$, because otherwise the required bound

$$\mathsf{E}(A,B)^2 \le \mathsf{E}(A)\mathsf{E}(B) \le \left(\frac{t}{|A|}\right)^{\beta} |A|^3|B|^3 \le \left(\frac{t}{|A|}\right)^{\beta} \cdot |A|^{3-\beta d}|B|^{3+\beta d}$$

takes place for $\beta = (2^{d+1} - d - 5)^{-1}$, $d \ge 2$ (and similar for $d = 1$; see estimate (4.13)). Furthermore, let $|B| \ge |A|$. Then, we use Lemma 2 with $k = d$, combining with Theorem 1 (see formulae (3.6), (4.11), and (4.12)) and the assumption $|A| \le |B|$ to obtain

$$\begin{aligned}\mathsf{E}(A,B) &\le (|A||B|)^{\frac{3}{2}-\frac{\beta(d+2)}{2}} \langle A,B\rangle_d^{\beta} \ll (|A||B|)^{\frac{3}{2}-\frac{\beta(d+2)}{2}} \left(\|B\|_{\mathcal{U}^d} + t\langle A,B\rangle_{d-1}\right)^{\beta} \\ &\le (|A||B|)^{\frac{3}{2}-\frac{\beta(d+2)}{2}} \left(|B|^{d+1} + t|A||B|^d\right)^{\beta} \ll (|A||B|)^{\frac{3}{2}-\frac{\beta(d+2)}{2}} t^{\beta}|B|^{\beta(d+1)} \\ &= t^{\beta}|A|^{\frac{3}{2}-\frac{\beta(d+2)}{2}}|B|^{\frac{3}{2}+\frac{\beta d}{2}},\end{aligned}$$

and (4.15) follows. Finally, to get (4.16), we use the dyadic pigeonhole principle and the fact that $\mathsf{T}^{1/2k}(f)$ defines a norm of f to find the number $\Delta > 0$ and the set P such that $P = \{x \in \mathbf{G} : \Delta < A^{(k)}(x) \le 2\Delta\}$ and $\mathsf{T}_{k+1}(A) \lesssim \Delta^2\mathsf{E}(A,P)$. Thus (we assume that $c \le 1$),

$$\mathsf{T}_{k+1}(A) \lesssim (t/|A|)^{\beta}|A|^{\frac{3}{2}-\frac{\beta d}{2}} (\Delta^2|P|)^{\frac{1}{2}-\frac{d\beta}{2}} (\Delta|P|)^{1+d\beta} \le |A|^{-\frac{c\beta}{2}}|A|^{\frac{3+2k}{2}-\frac{\beta d}{2}+\beta k d} \cdot \mathsf{T}_k^{\frac{1}{2}-\frac{d\beta}{2}}(A).$$

Suppose that $\mathsf{T}_k(A) \ge |A|^{2k-1-\varepsilon}$, where $\varepsilon \le c\beta/4$. In view of the last inequality and $\beta \le 2^{-d+1}$, one has

$$|A|^{-\frac{c\beta}{2}}|A|^{\frac{3+2k}{2}-\frac{\beta d}{2}+\beta k d} \cdot \mathsf{T}_k^{\frac{1}{2}-\frac{d\beta}{2}}(A) \le |A|^{2-\varepsilon}\mathsf{T}_k(A).$$

This completes the proof. ∎

Remark 4 As it was said in the proof of Lemma 2, the bound for $\mathsf{E}(A,B)$, $A \subseteq V$, where V is our variety and $B \subseteq \mathbf{G}$ is an arbitrary set, can be improved, because we have a nontrivial upper bound for $\|A\|_{\mathcal{U}^l}$, $2 \le l \le d+1$. Thus, bounds (4.15) and (4.16)

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

can be improved slightly. Also, inequalities (4.15) and (4.16) say, basically, that either $|A^3|$ is much larger than $|A|$ or $|A^3|$ is larger than $|A^2|$.

Theorem 1 and Corollary 3 imply the following criterion.

Corollary 5 *Let* $\mathbf{G}$ *be a finite simple group,* $V \subseteq \mathbf{G}$ *be a variety,* $d = \dim(V)$*, and* $D = \deg(V)$*. Suppose that* $t(V) = o(|V|)$*. Then, there is* $\delta = \delta(d, n) > 0$ *such that for any* $A \subseteq V$*,* $|A| \gg |V|$*, the following holds:*

$$\mathsf{E}(A) \ll_{d,D} |A|^{3-\delta}. \tag{4.17}$$

Clearly, if $t(V) \gg |V|$, then (4.17) does not hold, and hence Corollary 5 is indeed a criterion. Also, it gives a lower bound for δ of the form $\delta \gg 1/d$. Recall that our current dependence on d in (4.17) has an exponential nature.

5 Applications

In [19, 20], the authors obtain the following results on growth of normal sets.

Theorem 1 *Let* $\mathbf{G}$ *be a finite simple group and* $N \subseteq \mathbf{G}$ *be a normal set. Then, there is* $n \ll \log|\Gamma|/\log|N|$ *such that* $N^n = \mathbf{G}$*. Moreover, for any* $\varepsilon > 0$*, there is* $\delta = \delta(\varepsilon) > 0$ *such that any normal set* N *with* $|N| \le |\mathbf{G}|^{\delta}$ *satisfies* $|NN| \ge |N|^{2-\varepsilon}$*.*

From Corollary 3, we obtain a result on the growth of an *arbitrary* subset of a conjugate class.

Corollary 2 *Let* $\mathbf{G}$ *be a finite connected semisimple algebraic group, and let* $C \subseteq \mathbf{G}$ *be a conjugate class. Also, let* $A \subseteq C$ *be an arbitrary set with* $|A| \ge t(\mathrm{Zcl}(C))^{1+\varepsilon}$*. Then, for a certain* $\delta > 0$ *depending on dimension of* C*, one has* $\mathsf{E}(A) \ll_{\deg(\mathrm{Zcl}(C))} |A|^{3-\delta}$*. In particular,* $|AA| \gg_{\deg(\mathrm{Zcl}(C))} |A|^{1+\delta}$*.*

Proof It is well known (see, e.g., [12, pp. 15 and 17]) that for any conjugate class C, its Zariski closure $\mathrm{Zcl}(C)$ equals C and possibly other conjugate classes of strictly lower dimension, as well as that $C = C(x)$ is a variety iff $x \in \mathbf{G}$ is a semisimple element. Now, the result follows from a direct application of Corollary 3 where the implied constants depend on $\deg(\mathrm{Zcl}(C))$, $\dim(C)$, $\dim(\mathbf{G})$, $\deg(\mathbf{G})$, and the dimension of the ground affine space. This completes the proof. ∎

One can see that $t(C) \le |C|^{1-c_*}$ for a certain $c_* > 0$ via the general bound on such intersections with generating sets (see [17]) or, alternatively, from some modifications of Theorem 1 (see [19, 20]). Thus, Corollary 2 takes place for all large subsets of conjugate classes.

Question. Is it true that for any $A \subseteq C$, where C is a conjugate class such that $|A| \ge |C|^{1-o(1)}$, say, one has $A^n = \mathbf{G}$, where n is a function on $\log|\mathbf{G}|/\log|A|$? For $n \ll \log|\mathbf{G}|/\log|A|$? For $C = C(x)$, where x is a semisimple element?

Now, we are ready to obtain a nontrivial upper bound for any sufficiently large subset of a Chevalley group living in a variety differ from the maximal parabolic subgroup.

Theorem 3 *Let* $\mathbf{G}_r(\mathbb{F}_q)$ *be a finite Chevalley group with rank* r *and odd* q *and* $\Pi \le \mathbf{G}_r(\mathbb{F}_q)$ *be its a maximal (by size) parabolic subgroup. Also, let* $V \subset \mathbf{G}_r(\mathbb{F}_q)$ *be a variety*

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

differ from all shifts of conjugates of Π. *Then, for any* $A \subseteq V$ *and* $|A| \geq |\Pi|q^{-1+c}$, $c > 0$, *one has*

$$\|\widehat{A}(\rho)\|_o \leq |A|^{1-\delta}, \tag{5.1}$$

where $\delta = \delta(c, r) > 0$ *and* ρ *is any nontrivial representation of* $\mathbf{G}_r(\mathbb{F}_q)$.

Proof Because by the assumption $|A| \geq |\Pi|q^{-1+c}$, it follows that $|V| \geq |\Pi|q^{-1+c}$ and hence V is rather large. Also, one can see that, trivially, $|A| \geq |\Pi|q^{-1+c} \gg q^{1+c}$. Furthermore, by [30, Lemma 8], we know that Π is the maximal (by size) subgroup of $\mathbf{G}(\mathbb{F}_q)$, and for all other subgroups $\Gamma \leq \mathbf{G}(\mathbb{F}_q)$, one has $|\Gamma| \leq q^{-1}|\Pi|$ (Γ is not conjugate to Π, of course). In particular, in view of (4.1),

$$t(V) \leq \max_{x,y \in \mathbf{G}_r(\mathbb{F}_q)} \{q^{-1}|\Pi|, |V \cap x\Pi y|\} \ll |V|q^{-c_*},$$

where $c_* = \min\{c, 1\}$. Take any subgroup H differ from all conjugates of Π. Also, let $x \in \mathbf{G}_r(\mathbb{F}_q)$ be an arbitrary element. Our task is to estimate the above size of the intersection $A_* := A \cap xH \subseteq V$. By Corollary 5 and estimate (2.1), we have

$$|A_*|^{1+\delta} \ll |A_*^{-1}A_*| \leq |H| \leq |\Pi|q^{-1} \leq |A|q^{-c},$$

and hence, in particular, $|A_*| \ll |A|^{(1+\delta)^{-1}}$ (actually, in this place of the proof, we can assume a weaker condition on size of A). By a similar argument and estimate (4.1), we derive that

$$|A \cap x\Pi y| \leq |V \cap x\Pi y| \ll |\Pi|q^{-1} \leq |A|q^{-c},$$

and hence for *any* proper subgroup $\Gamma \subset \mathbf{G}_r(\mathbb{F}_q)$ and for all $x \in \mathbf{G}_r(\mathbb{F}_q)$, one has $|A \cap x\Gamma| \ll |A|q^{-c/2}$ (we use $|A| \gg q$ and assume that $\delta \leq c$). In particular, A is a generating set of $\mathbf{G}_r(\mathbb{F}_q)$. Combining this observation with the fact (see [15]) that Chevalley groups are quasi-random in the sense of Gowers [7], we obtain desired estimate (5.1) (see, e.g., [10, 11], [29, Sections 8 and 10]). This completes the proof. ∎

Now, we obtain an application of Corollary 3 to some questions about the restriction phenomenon. Recall that in this setting, our group $\mathbf{G}$ is $\mathbf{G} = \mathbb{F}^n$, $\mathbb{F}$ is a finite field, $V \subseteq \mathbb{F}^n$ is a variety, and $\mathbf{G}$ acts on $\mathbf{G}$ via shifts. For any function $g : \mathbb{F}^n \to \mathbb{C}$, consider the commutative analogue of (2.2)

$$\hat{g}(\xi) := \sum_{x \in \mathbb{F}^n} g(x)e(-x \cdot \xi),$$

as well as the inverse Fourier transform of a function $f : V \to \mathbb{C}$,

$$(fd\sigma)^\vee(x) := \frac{1}{|V|} \sum_{\xi \in V} f(\xi)e(x \cdot \xi),$$

where $e(x \cdot \xi) = e^{2\pi i(x_1\xi_1 + \dots + x_n\xi_n)/\mathrm{char}(\mathbb{F})}$ for $x = (x_1, \dots, x_n)$, $\xi = (\xi_1, \dots, \xi_n)$. Thus, a "Lebesgue L^q-norm" of f on V is defined as

$$\|f\|_{L^q(V,d\sigma)} := \left(\frac{1}{|V|} \sum_{\xi \in V} |f(\xi)|^q\right)^{\frac{1}{q}},$$

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

while for a function g, it is

$$\|g\|_{L^q(\mathbb{F}^n)} := \left(\sum_{x\in\mathbb{F}^n} |g(x)|^q\right)^{\frac{1}{q}}.$$

The finite-field restriction problem [21] for our variety V seeks exponent pairs (q,r) such that one has the inequality

$$\|(fd\sigma)^\vee\|_{L^r(\mathbb{F}^n)} \le R^*(q\to r)\|f\|_{L^q(V,d\sigma)}$$

or, equivalently,

$$\|\widehat{g}\|_{L^{q'}(V,d\sigma)} \le R^*(q\to r)\|g\|_{L^{r'}(\mathbb{F}^n)}$$

takes place with a constant $R^*(q\to r)$ independent of the size of the finite field. As before, we use the notation $\lesssim$ and $\gtrsim$ instead of $\ll$ and $\gg$, allowing ourselves to lose logarithmic powers of $|\mathbb{F}|$.

Using the arguments of the proofs of [21, Lemma 5.1 and Proposition 5.2], we obtain the following result.

Theorem 4 *Let $V\subseteq\mathbb{F}^n$ be a variety and $d=\dim(V)$. Suppose that V does not contain any line. Then, $R^*(\frac{4}{3-c}\to 4)\ll 1$, where $c=c(d)>0$.*

Proof According to our assumption that V does not contain any line, we see that the parameter $t(V)$ equals 1. Hence, by Corollary 3, we know that $\mathsf{E}(A)\ll|A|^{3-c}=|A|^{\kappa}$, where $c=c(d)>0$. Put $q=4/\kappa$, and we want to obtain a good bound for $R^*(q\to 4)$. We want to obtain an estimate of the form (see the proofs of [21, Lemma 5.1 and Proposition 5.2])

$$\sum_x (f\,V * f\,V)^2(x) \lesssim \left(\sum_{x\in V}|f(x)|^q\right)^{4/q},$$

where f is an arbitrary function (we can freely assume that f is positive). Using the dyadic pigeonhole principle, we need to prove the last bound for any $f=A$ with $A\subseteq V$, and this is equivalent to

$$\mathsf{E}(A)\lesssim |A|^{4/q}=|A|^{3-c}.$$

This completes the proof. ∎

Notice that if the variety V contains subspaces of positive dimension, then there is no any restriction-type result as in Theorem 4 in such generality (see, e.g., [21, Section 4]).

A Appendix

Now, we obtain an analogue of the Weyl criterion for noncommutative case. In this situation, ordinary abelian intervals or progressions correspond to some structural nonabelian objects as subgroups. In particular, the first part of the Proposition A.1 below is applicable for subgroups H of our group $\mathbf{G}$. Of course, such results should be known, but it is difficult to find them in the literature, and we include Proposition A.1 and its converse for the completeness.

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Proposition A.1 *Let $\varepsilon \in (0,1]$ be a real number, $\mathbf{G}$ be a finite group, and $A \subseteq \mathbf{G}$ be a set such that for any nontrivial irreducible representation ρ, one has*

$$\|\widehat{A}(\rho)\|_o \le \varepsilon |A|. \tag{A.1}$$

Then, for any $H, H_* \subseteq \mathbf{G}$, $1 \in H_*$ with $|HH_*| \le |H| + K|H_*|$, one has

$$\left| |A \cap H| - \frac{|A||H|}{|\mathbf{G}|} \right| \le 2K|H_*| + \varepsilon |A| \sqrt{|H|/|H_*| + K}. \tag{A.2}$$

Proof Put $\Pi = HH_*$. Then, for any $x \in H$, the following holds $H(x) = |H_*|^{-1}(\Pi * H_*^{-1})(x)$. Hence,

$$\|H(x) - |H_*|^{-1}(\Pi * H_*^{-1})(x)\|_1 \le |HH_*| - |H| \le K|H_*|,$$

and thus in view of formulae (2.4) and (2.5), we obtain

$$\begin{aligned} |A \cap H| &= |H_*|^{-1} \sum_x A(x)(\Pi * H_*^{-1})(x) + \mathcal{E} \\ &= \frac{|A||\Pi|}{|\mathbf{G}|} + \frac{1}{|H_*||\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}},\, \rho \ne 1} d_\rho \langle \widehat{A}(\rho), \widehat{\Pi}(\rho) \widehat{H}_*^*(\rho) \rangle + \mathcal{E}, \end{aligned}$$

where $|\mathcal{E}| \le K|H_*|$. Applying condition (A.1), the Cauchy–Schwarz inequality, and formula (2.4) again, we get

$$\begin{aligned} \left| |A \cap H| - \frac{|A||H|}{|\mathbf{G}|} \right| &\le K|H_*| + \frac{K|A||H_*|}{|\mathbf{G}|} + \varepsilon |A| |\Pi|^{1/2} |H_*|^{-1/2} \\ &\le 2K|H_*| + \varepsilon |A| \sqrt{|H|/|H_*| + K}. \end{aligned}$$

This completes the proof. ∎

The inverse statement to Proposition A.1 also takes place, but it requires some notation, and, actually, our argument gives an effective bound if the dimension of the corresponding representation ρ is small. Following [26, Section 17], define the Bohr sets in a (nonabelian) group $\mathbf{G}$.

Definition A.2 Let Γ be a collection of some unitary representations of $\mathbf{G}$ and $\delta \in (0,2]$ be a real number. Put

$$\mathrm{Bohr}(\Gamma, \delta) = \{g \in \mathbf{G} \,:\, \|\gamma(g) - I\|_o \le \delta \,, \forall \gamma \in \Gamma\}.$$

The number $|\Gamma|$ is called the *dimension* of $\mathrm{Bohr}(\Gamma, \delta)$. If $\Gamma = \{\rho\}$, then we write just $\mathrm{Bohr}(\rho, \delta)$ for $\mathrm{Bohr}(\{\rho\}, \delta)$. A Bohr set $\mathrm{Bohr}(\rho, \delta)$ is called to be *regular* if

$$||\mathrm{Bohr}(\rho, (1+\kappa)\delta)| - |\mathrm{Bohr}(\rho, \delta)|| \le 100 d_\rho^2 |\kappa| \cdot |\mathrm{Bohr}(\rho, \delta)|,$$

whenever $|\kappa| \le 1/(100 d_\rho^2)$.

Even in the abelian case, it is easy to see that not each Bohr set is regular (see, e.g., [35, Section 4.4]). Nevertheless, it can be showed (see, e.g., [32]) that one can find a regular Bohr set decreasing the parameter δ slightly.

Lemma A.3 *Let $\delta \in [0, 1/2]$ be a real number and ρ be a unitary representation. Then, there is $\delta_1 \in [\delta, 2\delta]$ such that $\mathrm{Bohr}(\rho, \delta_1)$ is regular.*

https://doi.org/10.4153/S0008414X21000687 Published online by Cambridge University Press

Let us remark an universal lower bound for the size of any Bohr set (see [26, Lemma 17.3], [32, Proposition 28] for the case of multidimensional Bohr sets).

Lemma A.4 *Let $\delta \in (0,2]$ be a real number and $Bohr(\rho,\delta) \subseteq \mathbf{G}$ be a one-dimensional Bohr set. Then,*

$$|Bohr(\rho,\delta)| \geq (c\delta)^{d_\rho^2} \cdot |\mathbf{G}|,$$

where $c > 0$ is an absolute constant.

Now, suppose that for a set $A \subseteq \mathbf{G}$, one has $|A| = \delta|\mathbf{G}|$ and $\|\widehat{A}(\rho)\|_o \geq \varepsilon|A|$. Put $f(x) = f_A(x) = A(x) - \delta$. Take a regular Bohr set $B = \mathrm{Bohr}(\rho,\delta)$, $\delta = \varepsilon/4$, and let $B_* = \mathrm{Bohr}(\rho,\kappa\delta)$, where $|\kappa| \leq 1/(100d_\rho^2)$ is a certain number. Then, by the definition of Bohr sets, we have

$$\begin{aligned}\varepsilon|A| \leq \|\widehat{A}(\rho)\|_o &= |B|^{-1}\|\sum_h \sum_g f(g)B(gh^{-1})\rho(g)\|_o \\ &= |B|^{-1}\|\sum_h \sum_g f(g)B(gh^{-1})\rho(h)\|_o + \mathcal{E},\end{aligned}$$

where $|\mathcal{E}| \leq 2\delta|A|$. Thus,

$$\varepsilon|A|/2 \leq |B|^{-1}\sum_h \left|\sum_g f(g)B(gh^{-1})\right|,$$

and hence in view of Lemma A.4, we find $h \in \mathbf{G}$ with

$$\frac{|A||B|}{|\mathbf{G}|} + \varepsilon|A|\exp(-O(d_\rho^2\log(1/\delta))) \leq |A \cap Bh|.$$

On the other hand, by the regularity of B, one has $|BB_*| \leq |B|(1 + 100d_\rho^2|\kappa|)$. It implies that Proposition A.1 can be reversed indeed.

Acknowledgment I thank Nikolai Vavilov for useful discussions. I deeply thank Brendan Murphy for his idea to study energies of subsets of various varieties. Also, I thank the anonymous reviewers for their careful reading of our manuscript and their many insightful comments and suggestions.

References

[1] B. Bollobás and A. Thomason, *Projections of bodies and hereditary properties of hypergraphs*. Bull. Lond. Math. Soc. **27**(1995), 417–424.
[2] J. Bourgain, *Some new estimates on oscillatory integrals*. In: C. Fefferman, R. Fefferman, and S. Wainger (eds.), *Essays in Fourier analysis in honor of E. M. Stein*, Princeton University Press, 1995, pp. 83–112.
[3] J. Bourgain, *Harmonic analysis and combinatorics: how much may they contribute to each other?* In: *Mathematics: Frontiers and perspectives*, IMU/Amer. Math. Society, 2000, pp. 13–32.
[4] J. Bourgain, A. Gamburd, and P. Sarnak, *Affine linear sieve, expanders, and sum–product*. Invent. Math. **179**(2010), no. 3, 559–644.
[5] E. Breuillard, B. Green, and T. Tao, *Approximate subgroups of linear groups*. Geom. Funct. Anal. **21**(2011), no. 4, 774–819.
[6] W. T. Gowers, *A new proof of Szemerédi's theorem*. Geom. Funct. Anal. **11** (2001), 465–588.
[7] W. T. Gowers, *Quasirandom groups*. Probab. Comput. **17**(2008), no. 3, 363–387.

[8] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, 52, Springer Science & Business Media, New York, 2013.
[9] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*. Theoret. Comput. Sci. **24**(1983), 239–277.
[10] H. Helfgott, *Growth and generation in SL_2 $(\mathbb{Z}/p\mathbb{Z})$*. Ann. of Math. (2) **167**(2008), no. 2, 601–623.
[11] H. Helfgott, *Growth in groups: ideas and perspectives*. Bull. Amer. Math. Soc. (N.S.) **52**(2015), no. 3, 357–413.
[12] J. E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Mathematical Surveys and Monographs, 43, American Mathematical Society, Providence, RI, 2011.
[13] A. Iosevich and D. Koh, *Extension theorems for spheres in the finite field setting*. Forum Math. **22**(2010), no.3, 457–483.
[14] A. Iosevich, D. Koh, and M. Lewko, *Finite field restriction estimates for the paraboloid in high even dimensions*. J. Funct. Anal. **278**(2020), 108450.
[15] V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*. J. Algebra **32**(1974), 418–443.
[16] S. Lang and A. Weil, *Number of points of varieties in finite fields*. Amer. J. Math. **76**(1954), 819–827.
[17] M. J. Larsen and R. Pink, *Finite subgroups of algebraic groups*. J. Amer. Math. Soc. **24**(2011), no. 4, 1105–1158.
[18] M. Lewko, *Finite field restriction estimates based on Kakeya maximal operator estimates*. J. Eur. Math. Soc. (JEMS) **21**(2019), no. 12, 3649–3707.
[19] M. W. Liebeck, G. Schul, and A. Shalev, *Rapid growth in finite simple groups*. Trans. Amer. Math. Soc. **369**(2017), no. 12, 8765–8779.
[20] M. W. Liebeck and A. Shalev, *Diameters of finite simple groups: sharp bounds and applications*. Ann. of Math. (2) **154**(2001), 383–406.
[21] G. Mockenhaupt and T. Tao, *Restriction and Kakeya phenomena for finite fields*. Duke Math. J. **121**(2004), no. 1, 35–74.
[22] B. Murphy, *Upper and lower bounds for rich lines in grids*. Amer. J. Math. **143** (2021), no. 2, 577–611.
[23] M. A. Naimark, *Theory of group representations*, Fizmatlit, Moscow, 2010.
[24] E. Noether, *Ein algebraisches Kriterium für absolute Irreduzibilität*. Math. Ann. **85**(1922), 26–40.
[25] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*. J. Amer. Math. Soc. **29**(2016), no. 1, 95–146.
[26] T. Sanders, *A quantitative version of the non-abelian idempotent theorem*. Geom. Funct. Anal. **21**(2011), no. 1, 141–221.
[27] J. P. Serre, *Représentations linéaires des groupes finis*, Collections Méthodes, Hermann, Paris, 1967.
[28] I. D. Shkredov, *Energies and structure of additive sets*. Electron. J. Combin. **21**(2014), no. 3, #P3.44, 1–53.
[29] I. D. Shkredov, *On asymptotic formulae in some sum–product questions*. Trans. Moscow Math. Soc. **79**(2018), 271–334; English transl. Trans. Moscow Math. Soc. (2018), 231–281.
[30] I. D. Shkredov, *Growth in Chevalley groups relatively to parabolic subgroups and some applications*. Preprint, 2020. arXiv:2003.12785
[31] I. D. Shkredov, *Modular hyperbolas and bilinear forms of Kloosterman sums*. J. Number Theory **220**(2021), 182–211.
[32] I. D. Shkredov, *On the spectral gap and the diameter of Cayley graphs*. Proc. Steklov Inst. Math. **314**(2021), 307–324.
[33] E. M. Stein, *Some problems in harmonic analysis*. In: *Harmonic analysis in Euclidean spaces*, Proceedings of Symposia in Pure Mathematics, XXXV Part I, Williams College, Williamstown, MA, 1978, pp. 3–20.
[34] E. M. Stein, *Harmonic analysis*, Princeton University Press, Princeton, NJ, 1993.
[35] T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, UK, 2006.
[36] A. Volobuev, Preprint.

Department of Number Theory, Steklov Mathematical Institute, ul. Gubkina, 8, Moscow 119991, Russia
e-mail: ilya.shkredov@gmail.com