ISSN 0012-9593

quatrième série - tome 54 *fascicule 3* *mai-juin 2021*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Martin BAYS & Emmanuel BREUILLARD

Projective geometries arising from Elekes-Szabó problems

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

Responsable du comité de rédaction / *Editor-in-chief*

Yves de Cornulier

Publication fondée en 1864 par Louis Pasteur

Continuée de 1872 à 1882 par H. Sainte-Claire Deville
de 1883 à 1888 par H. Debray
de 1889 à 1900 par C. Hermite
de 1901 à 1917 par G. Darboux
de 1918 à 1941 par É. Picard
de 1942 à 1967 par P. Montel

Comité de rédaction au 1er juin 2021

S. Boucksom, G. Caron, G. Chenevier, F. Deglise, A. Ducros, B. Fayad, G. Giacomin, D. Häfner, D. Harari, C. Imbert, S. Morel, P. Shan, J. Szeftel, S. Vũ Ngọc, G. Williamson

Rédaction / *Editor*

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.
Tél. : (33) 1 44 32 20 88. Fax : (33) 1 44 32 20 80.
Email : annales@ens.fr

Édition et abonnements / *Publication and subscriptions*

Société Mathématique de France
Case 916 - Luminy
13288 Marseille Cedex 09
Tél. : (33) 04 91 26 74 64. Fax : (33) 04 91 41 17 51
Email : abonnements@smf.emath.fr

Tarifs

Abonnement électronique : 437 euros.
Abonnement avec supplément papier :
Europe : 600 €. Hors Europe : 686 € ($ 985). Vente au numéro : 77 €.

© 2021 Société Mathématique de France, Paris

En application de la loi du 1er juillet 1992, il est interdit de reproduire, même partiellement, la présente publication sans l'autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie (20, rue des Grands-Augustins, 75006 Paris).
All rights reserved. No part of this publication may be translated, reproduced, stored in a retrieval system or transmitted in any form or by any other means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the publisher.

ISSN 0012-9593 (print) 1873-2151 (electronic)

Directeur de la publication : Fabien Durand
Périodicité : 6 nos / an

Ann. Scient. Éc. Norm. Sup.
4e série, t. 54, 2021, p. 627 à 681

PROJECTIVE GEOMETRIES ARISING FROM ELEKES-SZABÓ PROBLEMS

BY Martin BAYS AND Emmanuel BREUILLARD

ABSTRACT. – We generalize the Elekes-Szabó theorem to arbitrary arity and dimension and characterize the complex algebraic varieties without power saving. The characterization involves certain algebraic subgroups of commutative algebraic groups endowed with an extra structure arising from a skew field of endomorphisms. We also extend the Erdős-Szemerédi sum-product phenomenon to elliptic curves. Our approach is based on Hrushovski's framework of pseudo-finite dimensions and the abelian group configuration theorem.

RÉSUMÉ. – Nous généralisons le théorème de Elekes-Szabó au cas d'un produit cartésien quelconque de variétés de dimension arbitraire et nous caractérisons les sous-variétés algébriques complexes sans gain d'exposant. La caractérisation fait intervenir certains sous-groupes algébriques de groupes algébriques commutatifs munis d'une structure supplémentaire associée à un corps gauche d'endomorphismes. Nous étendons aussi le phénomène somme-produit de Erdős-Szemerédi au cas des courbes elliptiques. Notre approche est fondée sur le formalisme des dimensions pseudo-finies de Hrushovski et sur la version abélienne du théorème de la configuration de groupe.

1. Introduction

Let $V \subset \mathbb{C}^n$ be an irreducible algebraic set over $\mathbb{C}$, let $N \in \mathbb{N}$, and let $X_i \subset \mathbb{C}$ with $|X_i| \leq N$, $i = 1, \ldots, n$. Then it is easy to see that

$$|V \cap \prod_{i=1}^{n} X_i| \leq O_V(N^{\dim V}).$$

Indeed, this follows inductively from the observation that there exists an algebraic subset $W \subset V$ of lesser dimension and a co-ordinate projection of the complement $V \setminus W \to \mathbb{C}^{\dim V}$ with fibers of finite size bounded by a constant.

Say V *admits no power-saving* if the exponent $\dim V$ is optimal, i.e., if for no $\epsilon > 0$ do we have a bound $|V \cap \prod_{i=1}^{n} X_i| \leq O_{V,\epsilon}(N^{\dim V - \epsilon})$ as the X_i vary among finite subsets of $\mathbb{C}$ of size $\leq N$.

0012-9593/03/© 2021 Société Mathématique de France. Tous droits réservés
doi:10.24033/asens.2467

In an influential paper Elekes and Szabó [9] classified the varieties which admit no power-saving in the case $n = 3$. In order to state their main theorem, we first need the following definition:

Definition 1.1. – A *generically finite algebraic correspondence* between irreducible algebraic varieties V and V' is a closed irreducible subvariety of the product $\Gamma \subset V \times V'$ such that the projections $\pi_V(\Gamma) \subset V$ and $\pi_{V'}(\Gamma) \subset V'$ are Zariski dense, and $\dim(\Gamma) = \dim(V) = \dim(V')$.

Suppose $W_1, \dots, W_n$ and $W'_1, \dots, W'_n$ are irreducible algebraic varieties, and $V \subset \prod_{i=1}^n W_i$ and $V' \subset \prod_{i=1}^n W'_i$ are irreducible subvarieties. Then we say V and V' are in *co-ordinatewise correspondence* if there is a generically finite algebraic correspondence $\Gamma \subset V \times V'$ and a permutation $\sigma \in \mathrm{Sym}(n)$ such that for each i, the closure of the projection $(\pi_i \times \pi'_{\sigma i})(\Gamma) \subset W_i \times W'_{\sigma i}$ is a generically finite algebraic correspondence (between the closure of $\pi_i(V)$ and the closure of $\pi'_{\sigma i}(V')$).

Theorem 1.2 (Elekes-Szabó [9]). – *An irreducible surface $V \subset \mathbb{C}^3$ admits no power-saving if and only if either*

(i) *$V \subset \mathbb{C}^3$ is in co-ordinatewise correspondence with the graph $\Gamma = \{(g, h, g + h) : g, h \in G\} \subset G^3$ of the group operation of a 1-dimensional connected complex algebraic group G,*

(ii) *or V projects to a curve, i.e.,* $\dim(\pi_{ij}(V)) = 1$ *for some $i \neq j \in \{1, 2, 3\}$.*

Here we generalize these results to arbitrary n and $V \subset \mathbb{C}^n$.

Definition 1.3. – An irreducible algebraic set $V \subset \mathbb{C}^n$ is *special* if it is in co-ordinatewise correspondence with a product $\prod_i H_i \leq \prod_i G_i^{n_i}$ of connected subgroups H_i of powers $G_i^{n_i}$ of 1-dimensional complex algebraic groups, where $\sum_i n_i = n$.

We prove:

Theorem 1.4. – *An irreducible algebraic set $V \subset \mathbb{C}^n$ admits no power-saving if and only if it is special.*

The case of Theorem 1.4 with $V \subset \mathbb{C}^3$ and $\dim(V) = 2$ is precisely Theorem 1.2. Indeed it is easy to verify that V is special if and only if it is either of the form (i) or of the form (ii). The latter occurs exactly when the special subgroup $H \leq G^3$ can be taken to be a diagonal subgroup $\{x_i = x_j\}$, while the curve $\pi_{ij}(V)$ gives the correspondence.

The case $V \subset \mathbb{C}^4$ with $\dim(V) = 3$ is a consequence of the results of [26].

A slightly stronger version of the case $V \subset \mathbb{C}^n$ with $\dim(V) = n - 1$, asking also for some uniformity in the power-saving (c.f. Remark 1.14), was conjectured by de Zeeuw in [36, Conjecture 4.3].

The case $V \subset \mathbb{C}^4$ with $\dim(V) = 2$ solves [36, Problem 4.4].

Example 1.5. – $V := \{(x, y, z, w) \in \mathbb{C}^4 : xzw = 1 = yz^2w^2\}$ is special because it is a subgroup of $(\mathbb{C}^*)^4$, and geometric progressions witness that it admits no power-saving: setting $X = \{2^k : -M \leq k \leq M\}$, we find $|V \cap X^4| \geq \Omega(M^2) \geq \Omega(|X|^2)$.

EXAMPLE 1.6. – Let $E \subset \mathbb{P}^2(\mathbb{C})$ be an elliptic curve, say defined by $\{y^2 = x(x-1)(x-\lambda)\}$. Then taking x co-ordinates yields a surface $V \subset \mathbb{C}^3$ in co-ordinatewise correspondence with the graph $\Gamma_+ \subset E^3$ of the elliptic curve group law, and arithmetic progressions in E witness that V admits no power-saving. This demonstrates the necessity of taking correspondences in the definition of special.

To demonstrate the necessity of taking products, suppose $E' \subset \mathbb{P}^2(\mathbb{C})$ is another elliptic curve. Then taking x co-ordinates yields a 4-dimensional subvariety $W \subset \mathbb{C}^6$ in co-ordinatewise correspondence with the product $\Gamma_+ \times \Gamma_{+'} \subset E^3 \times E'^3$ of the graphs of the two group laws, and again arithmetic progressions witness that W admits no power-saving. But if E' is not isogenous to E, then W is not in co-ordinatewise correspondence with a subgroup of a power of a single elliptic curve (see Fact 2.13).

In fact we obtain a more general result, with arbitrary varieties in place of the complex co-ordinates. Again, this generalizes the corresponding result of [9], who considered the case of a subvariety V of $\mathbb{C}^d \times \mathbb{C}^d \times \mathbb{C}^d$ of dimension $2d$ and with dominant projections to pairs of co-ordinates, and showed that V must be in correspondence with the graph of multiplication of some algebraic group G. In [6] it was noted that this group must be commutative. Theorem 1.11 below gives a complete classification of the subvarieties without power saving, showing in particular that the groups involved must be commutative. To state the result, we first introduce the following definition.

DEFINITION 1.7. – Let W be a complex variety. Let $C, \tau \in \mathbb{N}$ with $C \geq \tau$. A finite subset $X \subset W$ is in *coarse* (C, τ)*-general position* in W if for any proper irreducible complex closed subvariety $W' \subsetneq W$ of complexity at most C, we have $|W' \cap X| \leq |X|^{\frac{1}{\tau}}$. When $C = \tau$ we will simply say that X is τ*-cgp* in W.

The notion of the complexity of a subvariety of a fixed variety is defined in full generality in 2.1.10 below. In the case that W is affine, $W' \subset W$ has complexity at most C if it can be defined as the zero set of polynomials of degree at most C.

Let W_i, $i = 1, \ldots, n$, be irreducible complex varieties each of dimension d, and let $V \subset \prod_{i=1}^n W_i$ be an irreducible subvariety.

Now let $C, \tau \in \mathbb{N}$ and consider finite subsets $X_i \subset W_i$ with $|X_i| \leq N^d$, $N \in \mathbb{N}$, and with each X_i in coarse (C, τ)-general position in W_i. As a straightforward consequence of coarse general position, if $\tau > d$ and C is sufficiently large depending on V only, we will see in Lemma 7.1 that we have a trivial bound

$$|V \cap \prod_{i=1}^n X_i| \leq O_V(N^{\dim(V)}).$$

We say that $V \subset \prod_i W_i$ *admits a power-saving by* $\epsilon > 0$ if for some $C, \tau \in \mathbb{N}$ depending on V only, this bound can be improved to $|V \cap \prod_{i=1}^n X_i| \leq O_{V,\epsilon}(N^{\dim(V)-\epsilon})$. We say V *admits no power-saving* if it does not admit a power-saving by ϵ for any $\epsilon > 0$.

It is easy to see that if V admits no power-saving, then $\dim(V)$ must be an integral multiple of d (see Lemma 7.1). In Theorem 1.11 below we give a complete classification of the varieties with no power-saving. To this end we introduce as earlier a notion of special varieties, which generalizes the previous definition and is slightly more involved.