SUMSETS AND VERONESE VARIETIES

LIENA COLARTE-GÓMEZ, JOAN ELIAS, AND ROSA M. MIRÓ-ROIG

ABSTRACT. In this paper, to any subset $\mathcal{A} \subset \mathbb{Z}^n$ we explicitly associate a unique monomial projection $Y_{n,d_{\mathcal{A}}}$ of a Veronese variety, whose Hilbert function coincides with the cardinality of the t-fold sumsets $t\mathcal{A}$. This link allows us to tackle the classical problem of determining the polynomial $p_{\mathcal{A}} \in \mathbb{Q}[t]$ such that $|t\mathcal{A}| = p_{\mathcal{A}}(t)$ for all $t \geq t_0$ and the minimum integer $n_0(\mathcal{A}) \leq t_0$ for which this condition is satisfied, i.e. the so-called *phase transition* of $|t\mathcal{A}|$. We use the Castelnuovo–Mumford regularity and the geometry of $Y_{n,d_{\mathcal{A}}}$ to describe the polynomial $p_{\mathcal{A}}(t)$ and to derive new bounds for $n_0(\mathcal{A})$ under some technical assumptions on the convex hull of $\mathcal{A}$; and vice versa we apply the theory of sumsets to obtain geometric information of the varieties $Y_{n,d_{\mathcal{A}}}$.

1. INTRODUCTION

In additive number theory, a *t-fold sumset* $t\mathcal{A} \subset \mathbb{Z}^n$ is the set of sums of t non necessarily different elements of a finite non empty subset $\mathcal{A} \subset \mathbb{Z}^n$. A classical problem concerning sumsets consists of determining the behaviour of the cardinality function $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ as t grows. A central result of Khovanskii [23] shows that there exists a polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$, of degree at most n, such that $\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t)$ for t sufficiently large. He also determines the leading coefficient of $p_{\mathcal{A}}(t)$ in terms of the volume of the convex hull associated to the subset $\mathcal{A} \subset \mathbb{Z}^n$ and the index of the additive subgroup in $\mathbb{Z}^n$ generated by the difference set $\mathcal{A} - \mathcal{A} \subset \mathbb{Z}^n$. Notwithstanding, Khovanskii's result sheds no light on the polynomial $p_{\mathcal{A}}(t)$, excepting the leading coefficient, nor the phase transition of $\varphi_{\mathcal{A}}(t)$. In view of these considerations, many contributions have been made to these topics as one can see, for instance, in [4, 8, 9, 13, 14, 15, 24, 27, 28, 29].

Most of the results regarding the polynomial $p_{\mathcal{A}}(t)$ and the phase transition $n_0(\mathcal{A})$ are based on the study of the structure of t-fold sumsets $t\mathcal{A}$ as sets of lattice points, being particularly useful for finite subsets of integers. The case $\mathcal{A} \subset \mathbb{Z}$ can be reduced to finite subsets $\mathcal{A} = \{0, a_1, \ldots, a_k\} \subset \mathbb{Z}$ with $0 < a_1 < \cdots < a_k$ and $\mathrm{GCD}(a_1, \ldots, a_k) = 1$. The structure of the $t-$fold sumset $t\mathcal{A}$ is completely determined for t sufficiently large and it produces upper bounds for $n_0(\mathcal{A})$ (see, for instance, [4, 9, 13, 28]). On the other hand, Khovanskii's result assures that $p_{\mathcal{A}}(t) = a_k t + b \in \mathbb{Z}[t]$. However, when dealing with subsets $\mathcal{A} \subset \mathbb{Z}^n$ in arbitrary dimension $n \geq 2$, the structure of t-fold sumsets $t\mathcal{A}$ is considerably more complex (see [8, 14, 15]), and it becomes less effective to determine $p_{\mathcal{A}}(t)$ or to produce, in general, a suitable bound for $n_0(\mathcal{A})$. That being said, the authors of [8] give a complete solution for subsets $\mathcal{A} \subset \mathbb{Z}^n$ of $n+2$ elements and such that the different set $\mathcal{A} - \mathcal{A}$

generates $\mathbb{Z}^n$. The structure of the $t-$fold sumsets $t\mathcal{A}$ has played a significant role on establishing bounds for $n_0(\mathcal{A})$ when the convex hull of the subset $\mathcal{A} \subset \mathbb{Z}^n$ is an $n-$simplex. Overall, the polynomial $p_\mathcal{A}(t)$ and its coefficients remain less understood.

In this paper, we stress the link between sumsets and the geometry of projective varieties, outlined for instance in [9, 22, 26]. Our aim is twofold. First, to any finite subset $\mathcal{A} \subset \mathbb{Z}^n$, we explicitly associate a unique projective toric variety $Y_{n,d_\mathcal{A}}$ in $\mathbb{P}^{|\mathcal{A}|-1}$ whose Hilbert function $\mathrm{HF}_{Y_{n,d_\mathcal{A}}}(t)$ coincides with the cardinality function $\varphi_\mathcal{A}(t)$ for any $t \geq 0$. The variety $Y_{n,d_\mathcal{A}}$ turns out to be a *monomial projection of a Veronese variety* (see Section 2). This identification and the geometric knowledge of monomial projections of Veronese varieties allows us to go ahead with the study of the polynomial $p_\mathcal{A}(t)$ and to provide bounds for the phase transition $n_0(\mathcal{A})$ of subsets $\mathcal{A} \subset \mathbb{Z}^n$ in arbitrary dimension $n \geq 2$. Second, we make use of the theory of sumsets to derive new geometric information about the varieties $Y_{n,d_\mathcal{A}}$ and, in particular of the so called $RL-$variety (see Section 5). This relationship between additive number theory and projective geometry will allow us to go back and forth and to use algebraic and geometric results on monomial projections of Veronese varieties to recover and improve results on additive combinatorics and vice versa.

Since the cardinality of a t-fold sumset is invariant under translations, we can assume that $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$. We set $d_\mathcal{A} := \min\{d \in \mathbb{Z}_{\geq 0} \mid \sum_{i=1}^n a_i \leq d, \forall a = (a_1, \ldots, a_n) \in \mathcal{A}\}$ and we define:

$$\Omega_{n,d_\mathcal{A}} := \{x_0^{d_\mathcal{A}-a_1-\cdots-a_n} x_1^{a_1} \cdots x_n^{a_n} \mid a = (a_1, \ldots, a_n) \in \mathcal{A}\} = \{m_1, \ldots, m_{|\mathcal{A}|}\},$$

a set of monomials of degree $d_\mathcal{A}$ in $R = \mathbb{K}[x_0, \ldots, x_n]$. Moreover, applying a suitable translation, we can also assume that $\mathrm{GCD}(m_1, \ldots, m_{|\mathcal{A}|}) = 1$. We denote by $Y_{n,d_\mathcal{A}}$ the variety image of the rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^{|\mathcal{A}|-1}$ defined by the parameterization $(m_1 : \ldots : m_{|\mathcal{A}|})$. We establish that the homogeneous coordinate ring $A(Y_{n,d_\mathcal{A}})$ of $Y_{n,d_\mathcal{A}}$ is isomorphic to the semigroup ring of monomials $\mathbb{K}[\Omega_{n,d_\mathcal{A}}]$, which in turn gives a description of $A(Y_{n,d_\mathcal{A}})$ and the homogeneous ideal $\mathrm{I}(Y_{n,d_\mathcal{A}})$ of $Y_{n,d_\mathcal{A}}$ in terms of $\mathcal{A}$ (Section 3). As a result of these facts, we deduce that $\varphi_\mathcal{A}(t) = \mathrm{HF}_{Y_{n,d_\mathcal{A}}}(t)$ for any $t \geq 0$ (Proposition 3.3). Consequently, $\varphi_\mathcal{A}(t)$ is a polynomial in $\mathbb{Q}[t]$ for t sufficiently large and, hence, $p_\mathcal{A}(t)$ is the Hilbert polynomial of the monomial projection $Y_{n,\mathcal{A}}$. Both facts provide further information on $\varphi_\mathcal{A}(t)$ and $p_\mathcal{A}(t)$ ((3) and (4)). For instance, a new geometric description of the leading coefficient of $p_\mathcal{A}(t)$ (Proposition 3.10) and a complete solution for any subset $\mathcal{A}$ of $n+1$ and $n+2$ elements, respectively, associated to an $n-$dimensional monomial projection $Y_{n,d_\mathcal{A}}$ (Proposition 3.7), recovering the corresponding results in [8]. In this setting, $n_0(\mathcal{A})$ translates into the *regularity* of the Hilbert function $\mathrm{HF}_{Y_{n,d_\mathcal{A}}}(t) = \varphi_\mathcal{A}(t)$, thus the Castelnuovo–Mumford regularity $\mathrm{reg}(Y_{n,d_\mathcal{A}})$ of $A(Y_{n,d_\mathcal{A}})$, which we denote by $\mathrm{reg}(\mathcal{A})$, bounds $n_0(\mathcal{A}) \leq \mathrm{reg}(\mathcal{A}) + 1$ (see [3] for the definition and basic properties of the Castelnuovo-Mumford regularity). Taking advantage of this fact and the results of [19, 20], we provide new estimations for $n_0(\mathcal{A})$ when the convex hull of $\mathcal{A}$ is an $n-$simplex with vertexes $0, (d_\mathcal{A}, 0 \ldots, 0), \ldots, (0, \ldots, 0, d_\mathcal{A})$, or equivalently when $\mathbb{K}[\Omega_{n,d_\mathcal{A}}]$ is the semigroup ring of a simplicial affine semigroup (Theorems 4.5, 4.6 and 4.11).

The arguments developed so far do not consider any further particularity of the subset $\mathcal{A}$. In this sense, the bounds established for the phase transition $n_0(\mathcal{A})$ are often very far from the actual value of $n_0(\mathcal{A})$. Motivated by this fact, in the last part of this paper we introduce $GT-$subsets and

$GT-$sumsets (Definition 5.2). They form a family of t-fold sumsets uniquely determined by a linear system of congruences. The algebraic structure of $GT-$sumsets $t\mathcal{A}$ as solutions of a linear system of congruences allows to significantly improve the bound for $n_0(\mathcal{A})$ (Proposition 5.3). In addition, they provide a good field to delve into the polynomial $p_{\mathcal{A}}(t)$, which is completely determined in several interesting cases (Propositions 5.4 and 5.5). Finally, we apply this new approach and recent results on sumsets to compute the degree and the Hilbert polynomial of $RL-$varieties (Proposition 5.6), a family of rational smooth projective varieties introduced in [7] and intrinsically related to $GT-$subsets whose geometry is barely known.

The content of this paper is organized as follows. In Section 2, we gather the basic definitions and notations needed in the body of this article. Given a finite subset $\mathcal{A} \subset \mathbb{Z}^n$, we introduce the notion of t-fold sumsets $t\mathcal{A} \subset \mathbb{Z}^n$ and the cardinality function $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$. We recall Khovanskii's result on the polynomial growth of $\varphi_{\mathcal{A}}(t)$, i.e. the existence of a polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ such that $\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t)$ for t sufficiently large, along to the so called *phase transition* $n_0(\mathcal{A})$ of $\varphi_{\mathcal{A}}$ and illustrating examples. Afterwards, we introduce Veronese varieties $X_{n,d} \subset \mathbb{P}^{\binom{n+d}{n}-1}$ and *monomial projections* $Y_{n,d}$ of $X_{n,d}$, which play a central role through this work.

In Section 3, to any subset $\mathcal{A} \subset \mathbb{Z}^n$, we explicitly associate a monomial projection $Y_{n,d_{\mathcal{A}}}$ of the Veronese variety $X_{n,d_{\mathcal{A}}}$ whose Hilbert function agrees with the cardinality function $\varphi_{\mathcal{A}}(t)$. This link allows us, on one hand, to describe the homogeneous coordinate ring $A(Y_{n,d_{\mathcal{A}}})$ and the homogeneous ideal $\mathrm{I}(Y_{n,d_{\mathcal{A}}})$ of $Y_{n,d_{\mathcal{A}}}$ in terms of the t-fold sumsets $t\mathcal{A}$ and, on the other hand, to interpret the function $\varphi_{\mathcal{A}}(t)$ and the polynomial $p_{\mathcal{A}}(t)$ in terms of the variety $Y_{n,d_{\mathcal{A}}}$ (Proposition 3.3). Through this identification, we obtain further information on the general structure of $p_{\mathcal{A}}(t)$ and we provide a combinatorial and a geometric formula for the leading coefficient of $p_{\mathcal{A}}(t)$ (Proposition 3.10 and (7)). Using purely geometric techniques, we determine $p_{\mathcal{A}}(t)$ and $n_0(\mathcal{A})$ when $\mathcal{A}$ contains $n+1$ and $n+2$ elements and $Y_{n,d_{\mathcal{A}}}$ is an $n-$dimensional projective variety, recovering some of the results in [8].

In Section 4, we focus our attention on subsets $\mathcal{A} \subset \mathbb{Z}^n$ whose associated convex hull $\mathrm{conv}(\mathcal{A})$ is an $n-$simplex (Definition 4.1) and we gather the bounds known so far for $n_0(\mathcal{A})$ in this case (Theorem 4.2 and Proposition 4.3). Using the Castelnuovo–Mumford regularity $\mathrm{reg}(\mathcal{A})$ of $A(Y_{n,d_{\mathcal{A}}})$, we provide improved bounds for $n_0(\mathcal{A})$ under some technical assumptions on the convex hull of $\mathcal{A}$ (Theorems 4.5, 4.6 and 4.11). We end this section with Example 4.12 where we compare our results with previous bounds for the phase transition $n_0(\mathcal{A})$.

In Section 5, we focus our attention on how far are the bounds for $n_0(\mathcal{A})$ from its real value. We introduce the notions of $GT-$subsets and $GT-$sumsets (Definition 5.2), they are uniquely determined by the $\mathbb{Z}_{\geq 0}^{n+1}-$solutions of linear systems of congruences. We show that this algebraic property allows to improve significantly the bound for $n_0(\mathcal{A})$ (Proposition 5.3) and, in several cases, to actually compute the polynomial $p_{\mathcal{A}}(t)$ (Propositions 5.4 and 5.5). Finally, we use the connection between sumsets and geometry to estimate the Castelnuovo–Mumford regularity and to compute the degree and the Hilbert Polynomial of $RL-$varieties (Theorem 5.6), a family of smooth rational monomial projections of $X_{n,d_{\mathcal{A}}}$ introduced in [7]. $RL-$varieties are actually monomial projections

image of embeddings of $\mathbb{P}^n$. Using this fact along with the combinatorial structure of the subset defining them, in [7] it is determined the cohomology of the normal bundle of any $RL-$variety.

Notation. Throughout this paper $\mathbb{K}$ will be an algebraically closed field of characteristic zero and we set $R := \mathbb{K}[x_0, \ldots, x_n]$. Let $A = \sum_{i \geq 0} A_i$ be an standard $\mathbb{K} = A_0$ algebra, i.e. $A = \mathbb{K}[A_1]$. We denote by HF_A the Hilbert function of A, i.e. $\mathrm{HF}_A(i) = \dim_\mathbb{K} A_i$ for all $i \geq 0$. It is well known that there exists a rational coefficient polynomial HP_A, the Hilbert polynomial of A, such that $\mathrm{HP}_A(i) = \mathrm{HF}_A(i)$ for $i \gg 0$.

Given integers $n, d \geq 1$, we define the $d-th$ binomial expansion of n as

$$n = \binom{m_d}{d} + \cdots + \binom{m_e}{e}$$

where $m_d > \cdots > m_e \geq e \geq 1$ are uniquely determined integers (see [3, Lemma 4.2.6]). We write

$$n^{<d>} = \binom{m_d + 1}{d + 1} + \cdots + \binom{m_e + 1}{e + 1}.$$

2. PRELIMINARIES

In this section, we gather the main notations, definitions and results we use in this paper. The reader can look at [10, 11, 27] for more details.

2.1. **Sumsets.** Let $n \geq 1$ be an integer and $\mathcal{A} \subset \mathbb{Z}^n$ a non-empty finite subset. For any $t \in \mathbb{N}$, a t-fold sumset $t\mathcal{A}$ is defined as follows:

$$t\mathcal{A} = \{a_1 + \cdots + a_t \mid a_i \in \mathcal{A} \text{ for all } 1 \leq i \leq t\}.$$

As usual, we set $0\mathcal{A} = \{0\}$. A longstanding problem in additive combinatorics is to determine the cardinality $|t\mathcal{A}|$ of the t-fold sumset $t\mathcal{A}$ as t grows. To this end, we introduce the *cardinality function*

$$\varphi_\mathcal{A} : \mathbb{N} \longrightarrow \mathbb{N}, \qquad t \mapsto |t\mathcal{A}|.$$

Proposition 2.1. *([23, Theorem 1]) Let $\mathcal{A} \subset \mathbb{Z}^n$ be a non empty finite subset. There exists a polynomial $p_\mathcal{A}(t) \in \mathbb{Q}[t]$ such that $\varphi_\mathcal{A}(t) = p_\mathcal{A}(t)$ for t sufficiently large. The* phase transition *of the cardinality function $\varphi_\mathcal{A}(t)$ is defined as*

$$n_0(\mathcal{A}) := \min\{n_0 \in \mathbb{Z}_{\geq 0} \mid \varphi_\mathcal{A}(t) = p_\mathcal{A}(t), \forall t \geq n_0\}.$$

The coefficients of the polynomial $p_\mathcal{A}(t)$ and the value of $\varphi_\mathcal{A}(t)$ for small t are barely known. Another interesting problem is to determine the phase transition $n_0(\mathcal{A})$ of $\varphi_\mathcal{A}$. The case $n = 1$ has lately received a lot of attention and our goal is to address the general case, i.e. $n \geq 1$. First, we deal with arbitrary subsets $\mathcal{A} \subset \mathbb{Z}^n$ and, later in Section 5, we restrict our attention to suitable subsets ($GT-$subsets) to improve previous results.

Let us start with easy examples which show that the behaviour of $|t\mathcal{A}|$ for small t, the coefficients of $p_\mathcal{A}(t)$ and the phase transition strongly depend on the structure of $\mathcal{A}$.

Example 2.2. (i) We consider the subset $\mathcal{A}^1 = \{(0,0),(3,0),(2,2),(0,1)\} \subset \mathbb{Z}^2$. We have $|\mathcal{A}^1| = 4$, $|2\mathcal{A}^1| = 10$, $|3\mathcal{A}^1| = 20$, $|4\mathcal{A}^1| = 35$ and $|t\mathcal{A}^1| = 4t^2 - 16t + 36$ for all $t \geq 5$. Therefore, the phase transition is 5.

(ii) We consider now the set $\mathcal{A}^2 = \{(0,0),(2,0),(2,2),(0,1)\} \subset \mathbb{Z}^2$. We have $|\mathcal{A}^2| = 4$, $|2\mathcal{A}^2| = 10$, $|3\mathcal{A}^2| = 19$, $|4\mathcal{A}^2| = 31$ and $|t\mathcal{A}^2| = \frac{3}{2}(t^2 + t) + 1$ for $t \geq 0$. Therefore, the phase transition is 0.

Notice that $|\mathcal{A}^1| = |\mathcal{A}^2|$, and $\mathcal{A}^1$, $\mathcal{A}^2$ differ only by one element. Nevertheless, the behaviour of the $t-$fold sumsets $|t\mathcal{A}^1|$ and $|t\mathcal{A}^2|$ and the phase transition drastically change. This phenomenon will be explained geometrically in next sections.

Next goal is to identify $p_{\mathcal{A}}(t)$ with the Hilbert polynomial of a suitable monomial projection $Y_{n,d}$ of the Veronese variety $X_{n,d}$; and use the geometry of Veronese varieties and their monomial projections to determine upper bounds for the phase transition as well as for identifying certain coefficients of $p_{\mathcal{A}}(t)$. For sake of completeness we recall below the basic facts on Veronese varieties.

2.2. **Veronese varieties.** We fix integers $n, d \geq 1$ and we set $N_{n,d} := \binom{n+d}{n}$. We consider the set $\mathcal{M}_{n,d} = \{m_0, \ldots, m_{N_{n,d}-1}\} \subset R$ of *all* monomials of degree d in R, ordered lexicographically. The *Veronese variety* $X_{n,d} \subset \mathbb{P}^{N_{n,d}-1}$ is defined as the image of the Veronese embedding of $\mathbb{P}^n$

$$\nu_{n,d} : \mathbb{P}^n \longrightarrow \mathbb{P}^{N_{n,d}-1}$$

which sends a point $p = (x_0 : \cdots : x_n) \in \mathbb{P}^n$ to $\nu_{n,d}(p) = (m_0(p) : \cdots : m_{N_{n,d}-1}(p)) \in \mathbb{P}^{N_{n,d}-1}$ (for further details see, for instance, [17]).

We take new variables $w_0, \ldots, w_{N_{n,d}-1}$ and we set $S := \mathbb{K}[w_0, \ldots, w_{N_{n,d}-1}]$. The homogeneous ideal $\mathrm{I}(X_{n,d}) \subset S$ of the Veronese variety $X_{n,d} \subset \mathbb{P}^{N_{n,d}-1}$ is the homogeneous binomial prime ideal generated by all binomials of degree 2 of the form:

$$(1) \qquad\qquad w_i w_j - w_\ell w_k \quad \text{such that} \quad m_i m_j = m_\ell m_k.$$

Example 2.3. We take an integer $d \geq 1$ and we set $S = \mathbb{K}[w_0, \ldots, w_d]$. The *rational normal curve of degree* d is the Veronese curve $X_{1,d} \subset \mathbb{P}^d$. It is the image of the morphism

$$\nu_{1,d} : \mathbb{P}^1 \longrightarrow \mathbb{P}^d, \quad \nu_{1,d}(x_0 : x_1) = (x_0^d : x_0^{d-1}x_1 : \cdots : x_0 x_1^{d-1} : x_1^d).$$

The homogeneous ideal $\mathrm{I}(X_{1,d}) \subset S$ of $X_{1,d}$ is the binomial prime ideal generated by the $\binom{d}{2}$ quadrics obtained from the 2×2 minors of the matrix

$$\begin{pmatrix} w_0 & w_1 & \cdots & w_{d-1} \\ w_1 & w_2 & \cdots & w_d \end{pmatrix}.$$

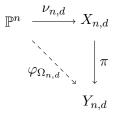These quadrics correspond to the 2×2 minors of the matrix of rank 1

$$\begin{pmatrix} x_0^d & x_0^{d-1}x_1 & \cdots & x_0 x_1^{d-1} \\ x_0^{d-1}x_1 & x_0^{d-2}x_1 & \cdots & x_1^d \end{pmatrix}.$$

An easy computation shows that the Hilbert polynomial of $X_{1,d}$ is:

$$\mathrm{HF}_{X_{1,d}}(t) := \dim(S/\mathrm{I}(X_{1,d}))_t = td + 1 = \mathrm{HP}_{X_{1,d}}(t) \text{ for all } t \geq 0.$$

Given a subset $\Omega_{n,d} = \{m_{i_0}, \ldots, m_{i_{\mu_{n,d}-1}}\} \subseteq \mathcal{M}_{n,d}$ of $\mu_{n,d} = |\Omega_{n,d}|$ monomials, we denote by

$$\varphi_{\Omega_{n,d}} : \mathbb{P}^n \dashrightarrow \mathbb{P}^{\mu_{n,d}-1}$$

the rational map defined by $\Omega_{n,d}$ which sends a point $p = (x_0 : \cdots : x_n) \in \mathbb{P}^n$ to $\varphi_{\Omega_{n,d}}(p) = (m_{i_0}(p) : \cdots : m_{i_{\mu_{n,d}-1}}(p)) \in \mathbb{P}^{\mu_{n,d}-1}$. We say that $Y_{n,d} := \overline{\varphi_{\Omega_{n,d}}(\mathbb{P}^n)} \subset \mathbb{P}^{\mu_{n,d}-1}$ is the *monomial projection of the Veronese variety $X_{n,d}$ parameterized by $\Omega_{n,d}$.* So, we have the commutative diagram:

$$
\begin{array}{ccc}
\mathbb{P}^n & \xrightarrow{\ \nu_{n,d}\ } & X_{n,d} \\
& {\scriptstyle \varphi_{\Omega_{n,d}}} \searrow & \downarrow {\scriptstyle \pi} \\
& & Y_{n,d}
\end{array}
$$

where π is the projection of the Veronese variety $X_{n,d} \subset \mathbb{P}^{N_{n,d}-1}$ from the linear subspace generated by the coordinate points $(0 : \cdots : 0 : 1 : 0 : \cdots : 0) \in \mathbb{P}^{N_{n,d}-1}$ with 1 in position i such that $m_i \notin \Omega_{n,d}$ to the linear subspace $V(w_{m_i}, \ m_i \notin \Omega_{n,d}) \cong \mathbb{P}^{\mu_{n,d}-1} \subset \mathbb{P}^{N_{n,d}-1}$. In particular, $Y_{n,d} \subset \mathbb{P}^{\mu_{n,d}-1}$ is called a *simple* (resp. *double*) monomial projection if $\Omega_{n,d}$ is obtained from $\mathcal{M}_{n,d}$ by deleting only one monomial (resp. two monomials).

Example 2.4. We take $n = 1$, $d = 4$ and $\Omega_{1,4} = \{x_0^4, x_0^3 x_1, x_0 x_1^3, x_1^4\} \subset \mathbb{K}[x_0, x_1]$. The simple monomial projection $Y_{1,4} \subset \mathbb{P}^3$ parameterized by $\Omega_{1,4}$ is the rational quartic in $\mathbb{P}^3$ obtained as the monomial projection of the rational normal curve $X_{1,4}$ of degree 4 in $\mathbb{P}^4 = \mathrm{Proj}(\mathbb{K}[w_0, w_1, w_2, w_3, w_4])$ from the coordinate point $(0 : 0 : 1 : 0 : 0)$ to the hyperplane $V(w_2) \subset \mathbb{P}^4$.

3. Sumsets and monomial projections of Veronese varieties

The goal of this section is to associate to *any* finite subset $\mathcal{A} \subset \mathbb{Z}^n$ a monomial projection $Y_{n,d_{\mathcal{A}}}$ of the Veronese variety $X_{n,d_{\mathcal{A}}}$ whose Hilbert function $\mathrm{HF}_{Y_{n,d_{\mathcal{A}}}}(t)$ models the cardinality function $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ and, hence, allows to conclude that there is a polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ of degree the dimension of $Y_{n,d_{\mathcal{A}}}$ such that $\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t)$ for t sufficiently large.

Definition 3.1. For any integer $n \geq 1$ and any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$, we denote by $d_{\mathcal{A}}$ the minimum of the integers $\delta \geq 0$ such that any element $a = (a_1, \ldots, a_n) \in \mathcal{A}$ satisfies $|a| = a_1 + \cdots + a_n \leq \delta$. We define $Y_{n,d_{\mathcal{A}}} \subset \mathbb{P}^{|\mathcal{A}|-1}$ the monomial projection of the Veronese variety $X_{n,d_{\mathcal{A}}} \subset \mathbb{P}^{N_{n,d_{\mathcal{A}}}-1}$ parameterized by the set of monomials

$$\Omega_{n,d_{\mathcal{A}}} = \{x_0^{d_{\mathcal{A}}-|a|} x_1^{a_1} \cdots x_n^{a_n} \mid a \in \mathcal{A}\}.$$

For simplicity, we use the notation $Y_{n,d_{\mathcal{A}}}$, notwithstanding the reader has to be aware of the fact that $Y_{n,d_{\mathcal{A}}}$ depends on $\mathcal{A}$ and not just on $d_{\mathcal{A}}$.

Remark 3.2. Given a finite subset $\mathcal{A} \subset \mathbb{Z}^n$, there is a unique translation $\tau : \mathbb{Z}^n \to \mathbb{Z}^n$ such that $\tau(\mathcal{A}) \subset \mathbb{Z}_{\geq 0}^n$ and $\mathrm{GCD}(m \in \Omega_{n,d_{\tau(\mathcal{A})}}) = 1$. In fact, τ is the translation defined by $-C$ where the

i-th component of C is the minimum of the i-th components of the elements $a \in \mathcal{A}$. We have:

$$\varphi_{\mathcal{A}}(t) = |t\mathcal{A}| = |t\tau(\mathcal{A})| = \varphi_{\tau(\mathcal{A})}(t)$$

for all $t \geq 0$. Hence, without loss of generality we will assume in the sequel that $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ and $\mathrm{GCD}(m \in \Omega_{n,d_{\mathcal{A}}}) = 1$.

Given an integer $n \geq 1$ and a finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$, we consider $\Omega_{n,d_{\mathcal{A}}} = \{m_1, \ldots, m_{|\mathcal{A}|}\} \subset R$ the set of monomials determined by $\mathcal{A}$. We take $w_1, \ldots, w_{|\mathcal{A}|}$ new variables and $S = \mathbb{K}[w_1, \ldots, w_{|\mathcal{A}|}]$. The homogeneous ideal $\mathrm{I}(Y_{n,d_{\mathcal{A}}}) \subset S$ of $Y_{n,d_{\mathcal{A}}}$ is the kernel of the epimorphism

$$\rho : S \to \mathbb{K}[\Omega_{n,d_{\mathcal{A}}}], \quad \rho(w_i) = m_i, \; i = 1, \ldots, |\mathcal{A}|.$$

It is a binomial prime ideal of S generated by ([21, pag 335]):

(2)
$$\left\{ \prod_{i=1}^{|\mathcal{A}|} w_i^{\alpha_i} - \prod_{i=1}^{|\mathcal{A}|} w_i^{\beta_i} \;\middle|\; \prod_{i=1}^{|\mathcal{A}|} m_i^{\alpha_i} = \prod_{i=1}^{|\mathcal{A}|} m_i^{\beta_i}, \; \alpha_i, \beta_i \in \mathbb{Z}_{\geq 0} \right\}$$

and the homogeneous coordinate ring $A(Y_{n,d_{\mathcal{A}}}) := S/\mathrm{I}(Y_{n,d})$ of $Y_{n,d_{\mathcal{A}}}$ is isomorphic to $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$.

To simplify, we denote by $\mathrm{HF}_{\mathcal{A}}$ the Hilbert function of $A(Y_{n,d_{\mathcal{A}}})$ (see [3, Chapter 4] for further details). Recall that for any integer $t \geq 0$, $\mathrm{HF}_{\mathcal{A}}(t)$ equals to $\dim_{\mathbb{K}} A(Y_{n,d_{\mathcal{A}}})_t = \dim_{\mathbb{K}} \mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]_{td}$. Moreover, we have:

Proposition 3.3. *For any integer $n \geq 1$ and any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$, it holds:*

(1) $\mathrm{HF}_{\mathcal{A}}(t) = \varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ *for all $t \geq 0$.*
(2) [3, Theorem 4.1.3] *There exists a polynomial $\mathrm{HP}_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ of degree $r = \dim(Y_{n,d_{\mathcal{A}}}) \leq n$, the Hilbert polynomial of $Y_{n,d_{\mathcal{A}}}$, such that $\mathrm{HP}_{\mathcal{A}}(t) = p_{\mathcal{A}}(t)$ for t sufficiently large.*

The *degree* $\deg(Y_{n,d_{\mathcal{A}}})$ of $Y_{n,d_{\mathcal{A}}}$ is defined algebraically as $r!$ times the leading coefficient of $\mathrm{HP}_{\mathcal{A}}(t)$. It corresponds geometrically to the number of points of intersection of $Y_{n,d_{\mathcal{A}}}$ with a sufficiently general linear subspace of $\mathbb{P}^{|\mathcal{A}|-1}$ of dimension $|\mathcal{A}| - r - 1$ (see, for instance, [18, Chapter I §7]). This perspective provides that for t large enough, $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ is a polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ of degree r and, hence, a geometrical interpretation of its leading coefficient $\frac{\deg(Y_{n,d_{\mathcal{A}}})}{r!}$. In addition, the phase transition $n_0(\mathcal{A})$, known also as the regularity of the Hilbert function, is bounded by the Castelnuovo-Mumford regularity $\mathrm{reg}(\mathcal{A})$ plus one (see also [3] for further details).

The numerical functions $H : \mathbb{N} \longrightarrow \mathbb{N}$ that are Hilbert functions of standard $\mathbb{K}$-algebras were characterized by Macaulay, [3]. Indeed, given a numerical function $H : \mathbb{N} \longrightarrow \mathbb{N}$ the following conditions are equivalent:

(i) There exists a $\mathbb{K}$-algebra A such that $H = \mathrm{HF}_A$,
(ii) $H(0) = 1$ and $H(t+1) \leq H(t)^{<t>}$ for all $t \geq 1$.

Hence, for any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$, the growth of the cardinality function $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ satisfies:

(3)
$$\varphi_{\mathcal{A}}(t+1) \leq \varphi_{\mathcal{A}}(t)^{<t>} \quad \text{for all } t \geq 1.$$

The polynomials $p(t) \in \mathbb{Q}[t]$ that are Hilbert polynomials are characterized as those admitting a Gotzmann development (see [12] and [16]). Recall that $p(t) \in \mathbb{Q}[t]$ admits a Gotzmann development if $p = 0$ or there exist integers $a_1 \geq \cdots \geq a_s \geq 0$ such that

$$(4) \qquad p(t) = \binom{t + a_1}{a_1} + \binom{t + a_2 - 1}{a_2} + \cdots + \binom{t + a_s - (s-1)}{a_s}.$$

Moreover, this representation is unique. From [2, Theorem 4.4] we have that the following conditions are equivalent:

    (i) $p(t) \in \mathbb{Q}[t]$ is the Hilbert polynomial of a standard $\mathbb{K}$-algebra A

    (ii) $p(t)$ admits a Gotzmann development.

The integer s is an upper bound of the Castelnuvo-Mumford regularity $\mathrm{reg}(A)$ of A (see [3]). In general this bound is far to be optimal. In fact, the Eisenbud-Goto conjecture claims that if A is an integral $\mathbb{K}$-algebra then

$$\mathrm{reg}(A) \leq \deg(A) - \mathrm{codim}(A) + 1.$$

Although this bound has been disproved ([25]), it is true for several types of rings covering some of the considered in this paper, see [30] and the references therein. See also Section 4 for further results on the phase transition of finite sets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$.

Since $Y_{n, d_{\mathcal{A}}}$ is a monomial projection of the n-dimensional Veronese variety $X_{n, d_{\mathcal{A}}}$, its dimension is bounded by n and its degree by the degree $d_{\mathcal{A}}^n$ of $X_{n, d_{\mathcal{A}}}$. However, the following examples show that both the dimension and the degree of the variety $Y_{n, d_{\mathcal{A}}}$ can be smaller than those of the Veronese variety $X_{n, d_{\mathcal{A}}}$.

Example 3.4. (i) We take integers $n, d \geq 1$ and $\mathcal{A} = \{(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^n \mid a_1 + \cdots + a_n \leq d\}$. We have $d_{\mathcal{A}} = d$, $|\mathcal{A}| = N_{n,d}$ and we observe that $\Omega_{n, d_{\mathcal{A}}}$ is the set of all monomials of degree d in R. Therefore, $Y_{n, d_{\mathcal{A}}}$ is the Veronese variety $X_{n,d} \subset \mathbb{P}^{N_{n,d}-1}$.

(ii) We take $n = 2$ and $\mathcal{A} = \{(0,0), (1,0), (0,1), (2,0), (0,2), (3,0), (2,1), (1,2), (0,3)\} \subset \mathbb{Z}_{\geq 0}^2$. We have $d_{\mathcal{A}} = 3$, $|\mathcal{A}| = 9$ and the associated monomial projection $Y_{2,3} \subset \mathbb{P}^8$ of the Veronese surface $X_{2,3} \subset \mathbb{P}^9$ is the surface parameterized by $\Omega_{2,3} = \{x_0^3, x_0^2 x_1, x_0^2 x_2, x_0 x_1^2, x_0 x_2^2, x_1^3, x_1^2 x_2, x_1 x_2^2, x_2^3\}$. It is a simple monomial projection of $X_{2,3}$.

(iii) We take $n = 2$ and $\mathcal{A} = \{(3,1), (2,2), (1,3), (0,4)\} \subset \mathbb{Z}_{\geq 0}^2$. We have $d_{\mathcal{A}} = |\mathcal{A}| = 4$ and the associated monomial projection $Y_{2,4} \subset \mathbb{P}^3$ of $X_{2,4} \subset \mathbb{P}^{14}$ is a curve parameterized by $\Omega_{2,4} = \{x_1^3 x_2, x_1^2 x_2^2, x_1 x_2^3, x_2^4\}$.

(iv) We come back to Examples 2.2 (i) and (ii). We take $\mathcal{A}^1 = \{(0,0), (3,0), (2,2), (0,1)\} \subset \mathbb{Z}_{\geq 0}^2$. We have $d_{\mathcal{A}^1} = |\mathcal{A}^1| = 4$ and the associated monomial projection $Y_{2,4}^1 \subset \mathbb{P}^3$ of $X_{2,4} \subset \mathbb{P}^{14}$ is the surface of degree 8 parameterized by $\Omega_{2,4}^1 = \{x_0^4, x_0^3 x_2, x_0 x_1^3, x_1^2 x_2^2\}$. If we fix coordinates w_0, w_1, w_2, w_3 in $\mathbb{P}^3$, the equation of $Y_{2,4}^1$ is: $w_0^5 w_3^3 - w_2^2 w_1^6$ (see (2)). We slightly modify $\mathcal{A}^1$ and we take $\mathcal{A}^2 = \{(0,0), (2,0), (2,2), (0,1)\} \subset \mathbb{Z}_{\geq 0}^2$. We have $d_{\mathcal{A}^2} = |\mathcal{A}^2| = 4$ and the associated monomial projection $Y_{2,4}^2 \subset \mathbb{P}^3$ of $X_{2,4} \subset \mathbb{P}^{14}$ is the cubic surface parameterized by $\Omega_{2,4}^2 = \{x_0^4, x_0^3 x_2, x_0^2 x_1^2, x_1^2 x_2^2\}$. It has equation: $w_0^2 w_3 - w_2 w_1^2$ (see (2)).

From now onward, we restrict our attention to finite subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ associated to $n-$dimensional monomial projections $Y_{n,d_{\mathcal{A}}}$ of $X_{n,d_{\mathcal{A}}}$. This restriction is quite natural and well controlled since we have the following, [23],

Proposition 3.5. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite set. Then, the associated variety $Y_{n,d_{\mathcal{A}}}$ has dimension n if and only if $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ has maximal rank.*

Remark 3.6. We also have a geometrical version of Proposition 3.5. Indeed, by [1, Pag. 186], given $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ a finite set, then the associated variety $Y_{n,d_{\mathcal{A}}} \subset \mathbb{P}^{|\mathcal{A}|-1}$ has dimension n if and only if $\mathrm{rank}((\partial m_i/\partial x_j))_{\substack{i=1,\dots,|\mathcal{A}| \\ j=0,\dots,n}} = n+1$, where $\{m_i\}_{i=1,\dots,|\mathcal{A}|}$ are the monomials parameterizing $Y_{n,d_{\mathcal{A}}}$.

It immediately follows that for any finite set $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ associated to an $n-$dimensional monomial projection $Y_{n,d_{\mathcal{A}}}$ of $X_{n,d_{\mathcal{A}}}$ we have $|\mathcal{A}| \geq n+1$. Our first goal is to study $\varphi_{\mathcal{A}}(t) = |t\mathcal{A}|$ for small values of $|\mathcal{A}|$, i.e. $|\mathcal{A}| = n+1$ and $|\mathcal{A}| = n+2$ and, to provide easier and new proofs of known formulae. To this purpose, we need to fix some notation. We denote by $\mathrm{conv}(\mathcal{A})$ the convex hull of A and let $[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]$ be the index of of the subgroup $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ in $\mathbb{Z}^n$. It holds:

Proposition 3.7. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite set associated to an $n-$dimensional projective variety $Y_{n,d_{\mathcal{A}}}$ of degree d.*

(i) *If $|\mathcal{A}| = n+1$ then*

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \binom{t+n}{n} \text{ for all } t \geq 0.$$

In particular, $n_0(\mathcal{A}) = 0$.

(ii) *If $|\mathcal{A}| = n+2$, then $n_0(\mathcal{A}) = d - n - 1$ and*

$$\varphi_{\mathcal{A}}(t) = \begin{cases} \binom{t+n+1}{n+1} & \text{if } 0 \leq t < d - n - 1 \\ \binom{t+n+1}{n+1} - \binom{t-d+n+1}{n+1} & \text{if } t \geq d - n - 1. \end{cases}$$

Moreover, we have

$$d = \deg(Y_{n,d_{\mathcal{A}}}) = n! \frac{\mathrm{vol}(\mathrm{conv}(\mathcal{A}))}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]}.$$

Proof. (i) By hypothesis $\mathcal{A}$ defines a rational map $\psi : \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ and the closure $Y_{n,d_{\mathcal{A}}}$ of its image is an n-dimensional subvariety of $\mathbb{P}^n$. Therefore, $Y_{n,d_{\mathcal{A}}} = \mathbb{P}^n$ and

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \mathrm{HF}_R(t) = \binom{t+n}{n} \text{ for all } t \geq 0.$$

(ii) In this case, $\mathcal{A}$ defines a rational map $\psi : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n+1}$ and the closure $Y_{n,d_{\mathcal{A}}}$ of its image is a hypersurface of degree d of $\mathbb{P}^{n+1}$ defined by $\mathrm{I}(Y_{n,d_{\mathcal{A}}}) = (F)$. Using the exact sequence

$$0 \longrightarrow S(-d) \xrightarrow{\times F} S \longrightarrow S/\mathrm{I}(Y_{n,d_{\mathcal{A}}}) \longrightarrow 0,$$

where $\times F : S(-d) \to S$ denotes the multiplication map by F and $S = \mathbb{K}[w_0, \ldots, w_{n+1}]$, we get the claim. The last equality follows from the fact that in [23] and [24] it is established that if $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ has maximal rank, then the leading coefficient of the polynomial $p_{\mathcal{A}}(t) = \varphi_{\mathcal{A}}(t)$ is

$$\frac{\mathrm{vol}(\mathrm{conv}(\mathcal{A}))}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]}.$$

$\square$

Remark 3.8. Notice that if $|\mathcal{A}| = n + 2$ and $\mathcal{A} - \mathcal{A}$ generates $\mathbb{Z}^n$ we easily recover [8, Theorem 1.2]:

$$\varphi_{\mathcal{A}}(t) = \begin{cases} \binom{t+n+1}{n+1} & \text{if } 0 \leq t \leq n!\,\mathrm{vol}(\mathrm{conv}(\mathcal{A})) - n - 2 \\ \binom{t+n+1}{n+1} - \binom{t-n!\,\mathrm{vol}(\mathrm{conv}(\mathcal{A}))+n+1}{n+1} & \text{if } t \geq n!\,\mathrm{vol}(\mathrm{conv}(\mathcal{A})) - n - 1. \end{cases}$$

In particular, $n_0(\mathcal{A}) = n!\,\mathrm{vol}(\mathrm{conv}(\mathcal{A})) - n - 1$.

To explicitly determine the function $\varphi_{\mathcal{A}}(t)$, the coefficients of the polynomial $p_{\mathcal{A}}(t)$ and the phase transition $n_0(\mathcal{A})$ of $\varphi_{\mathcal{A}}(t)$ for arbitrary finite subsets $\mathcal{A} \subset \mathbb{Z}^n$ with more than $n + 2$ elements is out of reach. In the remaining part of this section, we will focus our attention on the leading coefficient of the polynomial $p_{\mathcal{A}}(t)$.

So far we have a description of the degree $\deg(Y_{n,d_{\mathcal{A}}})$ of $Y_{n,d_{\mathcal{A}}}$ in terms of the set $\mathcal{A}$ and the difference set $\mathcal{A} - \mathcal{A}$. By [23] and [24], if $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ has maximal rank, then

$$(5) \qquad\qquad \deg(Y_{n,d_{\mathcal{A}}}) = n!\frac{\mathrm{vol}(\mathrm{conv}(\mathcal{A}))}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]}.$$

On the other hand, since $Y_{n,d_{\mathcal{A}}}$ is a toric variety, $\deg(Y_{n,d_{\mathcal{A}}})$ can also be described combinatorially as follows. From now on, given a finite subset $\mathcal{A} \subset \mathbb{Z}^n$, we set

$$(6) \qquad\qquad \overline{\mathcal{A}} = \{(d_{\mathcal{A}} - |a|, a_1, \ldots, a_n) \mid a \in \mathcal{A}\} \subset \mathbb{Z}^{n+1}_{\geq 0}.$$

We denote by M the $(n + 1) \times |\mathcal{A}|$ matrix whose columns correspond to the points of $\overline{\mathcal{A}}$. By [31, Theorem 2.13 and 4.5], we have:

$$(7) \qquad\qquad \deg(Y_{n,d_{\mathcal{A}}}) = \frac{r!\,\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}}))}{\Delta_r}$$

where $r = \mathrm{rk}(M)$, $\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}}))$ is the volume of the convex hull of $\overline{\mathcal{A}} \cup \{0\}$ and Δ_r is the greatest common divisor of all the non-zero $r \times r$ minors of M.

Expressions (5) and (7) provide two different ways to determine the degree of $Y_{n,d_{\mathcal{A}}}$ in terms of subsets. Both involve the volume of convex polyhedrons and the *Smith normal form* of certain matrix (see, for instance, [31]). Let us see some examples where we compute the Hilbert function and polynomial and, hence, the degree of $Y_{n,d_{\mathcal{A}}}$.

Example 3.9. (i) We take integers $n, d \geq 1$ and $\mathcal{A} = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0} \mid a_1 + \cdots + a_n \leq d\}$. Then, $\overline{\mathcal{A}} = \{(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}_{\geq 0} \mid a_0 + \cdots + a_n = d\}$ and the associated monomial projection is the Veronese variety $X_{n,d}$. It is straightforward to see that $\mathrm{rk}(M) = n+1$ and $\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}})) = \frac{d^{n+1}}{(n+1)!}$. To

compute Δ_{n+1} in this case, it is enough to find the *Smith normal form* of M (see [31]). Notice that the transpose matrix M^t of M contains n rows corresponding to $f_i = (d-1,\dots,1,\dots,0)$ with 1 in position ith, $i = 1,\dots,n$. Consider the submatrix M_a of M^t whose rows are $a, f_1, \dots, f_n$ with $a = (a_0, \dots, a_n) \in \overline{\mathcal{A}} \setminus \{f_1, \dots, f_n\}$. Then, by doing the elementary row operation $a - a_1 f_1 - \dots - a_n f_n$, we can transform the row a as $(|a| - d(a_1 + \dots + a_n), 0, \dots, 0)$. Since $|a|$ is a multiple of d and, in particular, $(d, 0, \dots, 0) \in \overline{\mathcal{A}}$, we obtain that the Smith normal form of M is $\mathrm{diag}(1, \dots, 1, d, 0, \dots, 0)$. Therefore, $\Delta_{n+1} = d$ and we get $\deg(X_{n,d}) = d^n$. On the other hand, for $t \geq 0$ we have

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \binom{n+dt}{n},$$

so $n_0(\mathcal{A}) = 0$ and the leading coefficient of $p_{\mathcal{A}}(t)$ is $\frac{d^n}{n!}$.

(ii) We take $n = 2$ and $\mathcal{A} = \{(0,0), (1,0), (0,1), (2,0), (0,2), (3,0), (2,1), (1,2), (0,3)\}$. Then, $|\mathcal{A}| = 9$, $d_{\mathcal{A}} = 3$ and the associated monomial projection $Y_{2,3} \subset \mathbb{P}^8$ of the Veronese surface $X_{2,3} \subset \mathbb{P}^9$ is the surface parameterized by $\Omega_{2,3} = \{x_0^3, x_0^2 x_1, x_0^2 x_2, x_0 x_1^2, x_0 x_2^2, x_1^3, x_1^2 x_2, x_1 x_2^2, x_2^3\}$. We have $\overline{\mathcal{A}} = \{(3,0,0), (2,1,0), (2,0,1), (1,2,0), (1,0,2), (0,3,0), (0,2,1), (0,1,2), (0,0,3)\}$. It is straightforward to check that $\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}})) = 27$ and, computing the maximal minors of M, we get $\Delta_3 = 3$. By Proposition 7, $\deg(Y_{2,3}) = 9$. On the other hand, for $t \geq 2$ we have

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \frac{9t^2 + 9t + 2}{2} = \binom{3t+2}{2},$$

so $n_0(\mathcal{A}) = 2$ and the leading coefficient of $p_{\mathcal{A}}(t)$ is $\frac{9}{2}$.

(iii) We take $n = 2$ and $\mathcal{A} = \{(0,0), (1,1), (3,0), (0,3)\}$. Then, $|\mathcal{A}| = 4$, $d_{\mathcal{A}} = 3$ and the associated monomial projection $Y_{2,3} \subset \mathbb{P}^3$ of the Veronese surface $X_{2,3} \subset \mathbb{P}^9$ is the surface parameterized by $\Omega_{2,3} = \{x_0^3, x_0 x_1 x_2, x_1^3, x_2^3\}$. We have $\overline{\mathcal{A}} = \{(3,0,0), (1,1,1), (0,3,0), (0,0,3)\}$. It is straightforward to check that $\mathrm{vol}(\mathrm{conv}(\mathcal{A})) = 27$ and, computing the maximal minors of M, we have $\Delta_3 = 9$. By Proposition 7, $\deg(Y_{2,3}) = 3$. On the other hand, for $t \geq 0$ we have

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \frac{3t^2 + 3t + 2}{2},$$

so $n_0(\mathcal{A}) = 0$ and the leading coefficient of $p_{\mathcal{A}}(t)$ is $\frac{3}{2}$.

(iv) We take $n = 2$ and $\mathcal{A} = \{(2,2), (2,0), (1,2), (0,4)\}$. Then, $|\mathcal{A}| = 4$, $d_{\mathcal{A}} = 4$ and the associated monomial projection $Y_{2,4} \subset \mathbb{P}^3$ of the Veronese surface $X_{2,4} \subset \mathbb{P}^9$ is the surface parameterized by $\Omega_{2,4} = \{x_1^2 x_2^2, x_0^2 x_1^2, x_0 x_1 x_2^2, x_2^4\}$. We have $\overline{\mathcal{A}} = \{(0,2,2), (2,2,0), (1,1,2), (0,0,4)\}$, $\mathrm{rk}(M) = 3$, $\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}})) = \frac{8}{3}$ and, computing the maximal minors of M, we get $\Delta_3 = 8$. By Proposition 7, $\deg(Y_{2,4}) = \frac{3! \cdot 8}{3 \cdot 8} = 2$. On the other hand, for $t \geq 0$ we have

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = t^2 + 2t + 1,$$

so $n_0(\mathcal{A}) = 0$ and the leading coefficient of $p_{\mathcal{A}}(t)$ is 1.

We end this section with a purely geometric approach to calculate the leading term of the polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ associated to any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$. The result is based on the following observation: we consider two finite subsets $\mathcal{A}_1 \subset \mathcal{A}_2 \subset \mathbb{Z}_{\geq 0}^n$ with $|\mathcal{A}_2| = |\mathcal{A}_1| + 1$ and

associated n-dimensional projective varieties $Y_{n,d_{\mathcal{A}_1}} \subset \mathbb{P}^{|\mathcal{A}_1|-1}$ and $Y_{n,d_{\mathcal{A}_2}} \subset \mathbb{P}^{|\mathcal{A}_2|-1} \cong \mathbb{P}^{|\mathcal{A}_1|}$. Notice that $Y_{n,d_{\mathcal{A}_1}}$ is obtained projecting $Y_{n,d_{\mathcal{A}_2}}$ from a point $p_{2,1} \in \mathbb{P}^{|\mathcal{A}_2|-1}$. Denote by $\pi_{2,1} : Y_{n,d_{\mathcal{A}_2}} \longrightarrow Y_{n,d_{\mathcal{A}_1}}$ the projection; it is a finite morphism of degree $\deg \pi_{2,1} = \#\pi_{2,1}^{-1}(x)$ where $x \in Y_{n,d_{\mathcal{A}_1}}$ is a general point. By [17, Pgs. 234-235, 259], we have:

$$(8) \quad \deg \pi_{2,1} \cdot \deg Y_{n,d_{\mathcal{A}_2}} = \begin{cases} \deg Y_{n,d_{\mathcal{A}_2}} & \text{if } p_{2,1} \notin Y_{n,d_{\mathcal{A}_1}} \\ \deg Y_{n,d_{\mathcal{A}_2}} - 1 & \text{if } p_{2,1} \in Y_{n,d_{\mathcal{A}_1}} \text{ is a smooth point} \\ \deg Y_{n,d_{\mathcal{A}_2}} - m_{2,1} & \text{if } p_{2,1} \in Y_{n,d_{\mathcal{A}_1}} \text{ is a point of multiplicity } m_{2,1}. \end{cases}$$

Iterating this process we can compute the leading term of the polynomial $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ associated to any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$. To this end, we need to fix some extra notation. Given any finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ with $r := |\mathcal{A}|$, we consider a chain

$$\mathcal{A} = \mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{N_{n,d}-r} = \mathcal{M}_{n,d} \subset \mathbb{Z}_{\geq 0}^n$$

where $|\mathcal{A}_i| = |\mathcal{A}_{i-1}| + 1$ and $\mathcal{M}_{n,d}$ denotes the set of all monomials of degree d in R. The n-dimensional rational projective variety $Y_{n,d_{\mathcal{A}_{i-1}}} \subset \mathbb{P}^{|\mathcal{A}_{i-1}|-1}$ is obtained projecting $Y_{n,d_{\mathcal{A}_i}} \subset \mathbb{P}^{|\mathcal{A}_i|-1}$ from a point $p_{i,i-1}$. Call $\pi_{i,i-1}$ such a projection. We define

$$d_{i,i-1} = \begin{cases} 0 & \text{if } p_{i,i-1} \notin Y_{n,d_{\mathcal{A}_i}} \\ 1 & \text{if } p_{i,i-1} \notin Y_{n,d_{\mathcal{A}_i}} \text{ is a smooth point} \\ m_{i,i-1} & \text{if } p_{i,i-1} \notin Y_{n,d_{\mathcal{A}_i}} \text{ is a point of multiplicity } m_{i,i-1}. \end{cases}$$

Proposition 3.10. *Let $p_{\mathcal{A}}(t) \in \mathbb{Q}[t]$ be the polynomial of a finite subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ with associated n-dimensional projective $Y_{n,d_{\mathcal{A}}}$ and let a_n be its leading coefficient. With the above notation it holds:*

$$a_n = \frac{\deg Y_{n,d_{\mathcal{A}}}}{n!} = \frac{1}{n! \prod_{i=1}^{N_{n,d}-r} \deg \pi_{i,i-1}} \Big(d^n - \sum_{i=1}^{N_{n,d}-r} \big(m_{i,i-1} \prod_{j=i+1}^{N_{n,d}-r} \deg \pi_{j,j-1} \big) \Big).$$

Proof. It immediately follows from (8) taking into account that $\deg X_{n,d} = d^n$. $\qquad\square$

Next example illustrates the above results.

Example 3.11. We consider the finite set $\mathcal{A} = \{(0,0),(3,0),(2,0),(2,2),(0,1)\} \subset \mathbb{Z}_{\geq 0}^n$ and the associated rational projective surface $Y_{2,4} \subset \mathbb{P}^4$, i.e. the surface parameterized by $\Omega_{2,4} = \{x_0^4, x_0 x_1^3, x_0^2 x_1^2, x_1^2 x_2^2, x_0^3 x_2\}$. If we fix coordinates $w_0, \dots, w_4$ in $\mathbb{P}^4$, the ideal $\mathrm{I}(Y_{2,4}) \subset S = \mathbb{K}[w_0, \dots, w_4]$ is generated by $w_2^3 - w_0 w_3^2, w_1^2 w_2 - w_0^2 w_4, w_1^2 w_3^2 - w_0 w_2^2 w_4$ and it has a minimal graded free S-resolution:

$$0 \longrightarrow S(-5)^2 \xrightarrow{d_2} S(-3)^2 \oplus S(-4) \xrightarrow{d_1} \mathrm{I}(Y_{2,4}) \longrightarrow 0,$$

where the graded S-maps d_1 and d_2 are associated to the matrices

$$\begin{pmatrix} w_2^3 - w_0 w_3^2 & w_1^2 w_2 - w_0^2 w_4 & w_1^2 w_3^2 - w_0 w_2^2 w_4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -w_0 w_3 & w_4^2 \\ w_1^2 & -w_2^2 \\ -w_2 & w_0 \end{pmatrix},$$

respectively. Therefore, we have

$$\mathrm{HP}_{Y_{2,4}}(t) = \varphi_{\mathcal{A}}(t) = |t\mathcal{A}| = 4t^2 - 2t + 3 \text{ for all } t \geq 1.$$

In particular, $Y_{2,4}$ is a degree 8 surface in $\mathbb{P}^4$. The Example 3.4 (iv) can be recovered from suitable projections of $Y_{2,4}$. Indeed, we fix the points $p_0 = (1 : 0 : 0 : 0 : 0), \ldots, p_4 = (0 : 0 : 0 : 0 : 1)$ and we denote by $\pi_i : Y_{2,4} \longrightarrow \mathbb{P}^3$ the projection of $Y_{2,4}$ to $\mathbb{P}^3$ from the point p_i, $i = 0, \cdots, 4$. It holds $\pi_2(Y_{2,4}) = Y_{2,4}^1$ and $\pi_3(Y_{2,4}) = Y_{2,4}^2$. By the above result, since $p_2 \notin Y_{2,4}$, $p_3 \in Y_{2,4}$ is a double point, $\deg \pi_2 = 1$ and $\deg \pi_3 = 2$, we obtain:

$$\deg(Y_{2,4}) = \deg(Y_{2,4}^1) = 8 \text{ and } \deg Y_{2,4}^2 = \frac{\deg(Y_{2,4}) - 2}{2} = 3.$$

The result fits well with our previous calculations (see Examples 2.2 and 3.4) and we have:

$$\mathrm{HP}_{Y_{2,4}^1}(t) = \varphi_{\mathcal{A}^1}(t) = |t\mathcal{A}^1| = 4t^2 - 16t + 36 \text{ for all } t \geq 5$$

and

$$\mathrm{HP}_{Y_{2,4}^2}(t) = \varphi_{\mathcal{A}^2}(t) = |t\mathcal{A}^2| = \frac{3}{2}(t^2 + t) + 1 \text{ for all } t \geq 0.$$

being $\mathcal{A}^1 = \{(0,0), (3,0), (2,2), (0,1)\}, \mathcal{A}^2 = \{(0,0), (2,0), (2,2), (0,1)\} \subset \mathbb{Z}_{\geq 0}^n$ the finite sets associated to $Y_{2,4}^1$ and $Y_{2,4}^2$, respectively.

We end the example with one more computation to show the casuistry we can have. Since $\pi_0 : Y_{2,4} \longrightarrow \mathbb{P}^3$ is a finite morphism of degree 1 and $p_0 \in Y_{2,4}$ a double point, we get that $Y_{2,4}^0 := \pi_0(Y_{2,4}) \subset \mathbb{P}^3$ is a surface of degree 6 parameterized by $\{x_0 x_1^3, x_0^2 x_1^2, x_1^2 x_2^2, x_0^3 x_2\}$ and the associated finite set $\mathcal{A}^0 = \{(3,0), (2,0), (2,2), (0,1)\} \subset \mathbb{Z}_{\geq 0}^n$ satisfies:

$$\mathrm{HP}_{Y_{2,4}^0}(t) = \varphi_{\mathcal{A}^0}(t) = |t\mathcal{A}^0| = 3t^2 - 6t + 11 \text{ for all } t \geq 3.$$

4. Bounds for the phase transition

In Section 3, we have studied the leading coefficient of $p_{\mathcal{A}}(t)$ and we have provided combinatorial and geometric interpretations of it. Notwithstanding, for arbitrary $n \geq 1$ and $\mathcal{A} \subset \mathbb{Z}^n$, the phase transition $n_0(\mathcal{A})$ and the polynomial $p_{\mathcal{A}}(t)$ are barely known. We will use the Castelnuovo–Mumford regularity $\mathrm{reg}(\mathcal{A})$ of $A(Y_{n,d_{\mathcal{A}}})$ to derive new bounds for $n_0(\mathcal{A})$ under some technical assumptions on $\mathcal{A}$.

Following [15] and [8], we gather a series of known bounds for the phase transition in the following setting: finite subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ whose convex hull $\mathrm{conv}(\mathcal{A})$ is an $n-$simplex. In this case, the bounds on the phase transition $n_0(\mathcal{A})$ are expressed in terms of $n, |\mathcal{A}|, \mathrm{vol}(\mathrm{conv}(\mathcal{A}))$ and a constant $K(\mathcal{A}, B)$, which depends further on $\mathcal{A}$ and its associated semigroup $\mathcal{H}(\mathcal{A}) \subset \mathbb{Z}_{\geq 0}^n$.

Definition 4.1. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset. The convex hull $\mathrm{conv}(\mathcal{A})$ of $\mathcal{A}$ is an $n-$simplex if there is a subset $B = \{v_1, \ldots, v_{n+1}\} \subset \mathcal{A}$ of $n+1$ elements such that the difference set $B - B$ generates $\mathbb{R}^n$ and $\mathrm{conv}(\mathcal{A}) = \mathrm{conv}(B)$.*

Theorem 4.2. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset with $\mathrm{conv}(\mathcal{A})$ an $n-$simplex. We have:*

$$n_0(\mathcal{A}) \leq (n+1)(n! \frac{\mathrm{vol}(\mathrm{conv}(\mathcal{A}))}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]} - |\mathcal{A}| + n) + 1.$$

If in addition $\mathbb{Z}(\mathcal{A} - \mathcal{A}) = \mathbb{Z}^n$, then

$$n_0(\mathcal{A}) \leq (n+1)! \, \mathrm{vol}(\mathrm{conv}(\mathcal{A})) - \max\{3n+1, (n+1)(|\mathcal{A}| - n) - 1\}.$$

Proof. See [15, Theorem 1.4] and [8, Theorem 1.4]. □

Assume now that $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ is a finite subset such that $0 \in \mathcal{A}$ and $\mathrm{conv}(\mathcal{A})$ is an $n-$simplex. We denote by $\mathbb{Z}(B) \subset \mathbb{Z}^n$ the subgroup generated by B and we set $\Pi_B := \{\sum_{i=1}^{n+1} \lambda_i v_i \mid 0 \leq \lambda_i < 1\}$. Given $a \in \mathcal{H}(\mathcal{A}) = \cup_{t \geq 0}(t\mathcal{A})$, the *height* of a is the minimum of the integers $t \geq 0$ such that $a \in t\mathcal{A}$, we denote it by N_a. The class of a modulo $\mathbb{Z}(B)$ can be represented by an element of $\pi_a \in \Pi_B$ and we denote by S_π the set of elements of $\mathcal{H}(\mathcal{A})$ which are congruent to π_a modulo $\mathbb{Z}(B)$. An element $a \in S_\pi$ is said to be $B-minimal$ if $a - v_i \notin \mathcal{H}(\mathcal{A})$ for any $i = 1, \ldots, n+1$. The set of all $B-minimal$ elements of $\mathcal{H}(\mathcal{A})$ is denoted by $\mathcal{S}(\mathcal{A}, B)$. Keeping this notation:

Proposition 4.3. [15, Theorem 4.1] *If $\mathcal{S}(\mathcal{A}, B)$ is finite, then*

$$n_0(\mathcal{A}) \leq (n+1)(K(\mathcal{A}, B) - 1) + 1,$$

where $K(\mathcal{A}, B) := \max\limits_{a \in \mathcal{S}(\mathcal{A}, B)} N_a$.

In next example, we compute the bounds given in Theorem 4.2 and Proposition 4.3 and we show that both bounds are far from the real value of $n_0(\mathcal{A})$.

Example 4.4. Let $2 \leq n < d$ and $0 \leq \alpha_1 \leq \cdots \leq \alpha_n < d$ be integers such that $\mathrm{GCD}(\alpha_1, \ldots, \alpha_n, d) = 1$. Set

$$\mathcal{A} = \{(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^n \mid a_1 + \cdots + a_n \leq d \text{ and } \alpha_1 a_1 + \cdots + \alpha_n a_n \equiv 0 \mod d\}.$$

We have that $d_\mathcal{A} = d$ and $\mathcal{A}$ contains 0 and the elements $de_i := (0, \ldots, d, \ldots, 0)$ with d in position ith, $i = 1, \ldots, n$. Then, $\mathcal{A}$ fulfils the hypothesis of Proposition 4.3 with $B = \{0, de_1, \ldots, de_n\}$ and $\mathrm{vol}(\mathrm{conv}(\mathcal{A})) = \frac{d^n}{n!}$. Moreover, in [5] it is proved that the set $\overline{\mathcal{A}}$ generates the semigroup

$$H = \{(a_0, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^{n+1} \mid a_0 + \cdots + a_n \equiv 0 \mod d \text{ and } \alpha_1 a_1 + \cdots + \alpha_n a_n \equiv 0 \mod d\}$$

Take $a \in \mathcal{H}(\mathcal{A})$. If $a = (a_1, \ldots, a_n) - de_i \in \mathbb{Z}_{\geq 0}^n$, then $a - de_i \in \mathcal{H}(\mathcal{A})$. Therefore, $\mathcal{S}(\mathcal{A}, B) = \{a = (a_1, \ldots, a_n) \in \mathcal{A} \mid a_i < d, i = 1, \ldots, n\}$ and, hence, $K(\mathcal{A}, B) \leq n$. Applying Proposition 4.3, we obtain that $n_0(\mathcal{A}) \leq (n+1)(n-1) + 1$. As a particular example, we take $n = 2$, $d = 5$, $\alpha_1 = 1$ and $\alpha_2 = 2$. Then, we have

$$\mathcal{A} = \{(0,0), (5,0), (3,1), (1,2), (0,5)\},$$

$d_\mathcal{A} = 5$, $|\mathcal{A}| = 5$, $B = \{(0,0), (5,0), (0,5)\}$, $\mathrm{vol}(\mathrm{conv}(\mathcal{A})) = \frac{25}{2}$ and $K(\mathcal{A}, B) = 2$. Notice that the subgroup $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ does not coincide with $\mathbb{Z}^2$. The bound for the phase transition of $\varphi_\mathcal{A}(t)$

from Theorem 4.2 is $n_0(\mathcal{A}) \leq 5$; in contrast to the lower one $n_0(\mathcal{A}) \leq 4$ from Proposition 4.3. Notwithstanding, we have that

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \frac{5t^2 + 3t + 2}{2} \text{ for all } t \geq 0$$

([5, Theorem 4.12]), so the phase transition of $\mathcal{A}$ is $n_0(\mathcal{A}) = 0$.

Next, we establish new bounds for the phase transition using the geometric approach we have developed in Section 3. The first bounds we provide for $n_0(\mathcal{A})$ are expressed in terms of $n, |\mathcal{A}|$ and $\deg(Y_{n,d_{\mathcal{A}}})$, and they can be easily compared with the previous ones using (5). The last bound we give is based on the reduction number $r(\mathcal{A})$ of $\mathbb{K}[Y_{n,d_{\mathcal{A}}}]$ which, as the constant $K(\mathcal{A}, B)$, depends further on the subset $\overline{\mathcal{A}}$.

Through the rest of this section, we consider subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ such that $\overline{\mathcal{A}} \subset \mathbb{Z}_{\geq 0}^{n+1}$ generates a *simplicial* affine semigroup $\mathcal{H}(\overline{\mathcal{A}})$, i.e. $e_0 := (d_{\mathcal{A}}, 0, \ldots, 0), \ldots, e_n := (0, \ldots, 0, d_{\mathcal{A}}) \in \overline{\mathcal{A}} \subset \mathbb{Z}_{\geq 0}^{n+1}$. The homogeneous coordinate ring $A(Y_{n,d})$ of the monomial projection $Y_{n,d}$ associated to $\mathcal{A}$ is isomorphic to $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$, which is the simplicial semigroup ring associated to the affine semigrop $\mathcal{H}(\overline{\mathcal{A}}) \subset \mathbb{Z}_{\geq 0}^{n+1}$. This is equivalent to consider subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ containing the origin $0 \in \mathbb{Z}^n$ and the elements, which we fix in the sequel, $v_1 := (d_{\mathcal{A}}, 0, \ldots, 0), \ldots, v_n := (0, \ldots, 0, d_{\mathcal{A}}) \in \mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$. The convex hull $\mathrm{conv}(\mathcal{A})$ is an $n-$simplex with vertexes $0, v_1, \ldots, v_n$ and $\mathrm{vol}(\mathrm{conv}(\mathcal{A})) = \frac{d_{\mathcal{A}}^n}{n!}$. In particular, $\mathbb{Z}(\mathcal{A} - \mathcal{A})$ has maximal rank, hence ((5) and (7)):

$$\deg(Y_{n,d_{\mathcal{A}}}) = n! \frac{\mathrm{vol}(\mathrm{conv}(\mathcal{A}))}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]} = (n+1)! \frac{\mathrm{vol}(\mathrm{conv}(\overline{\mathcal{A}}))}{\Delta_{n+1}} = \frac{d_{\mathcal{A}}^n}{[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})]}.$$

We have:

Theorem 4.5. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. If one of the following conditions yields,*

(i) $n = 1$,
(ii) $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$ *is a Cohen-Macaulay ring,*
(iii) $\deg(Y_{n,d_{\mathcal{A}}}) \leq |\mathcal{A}| - n$,
(iv) $|\mathcal{A}| - n - 1 \leq \deg(Y_{n,d_{\mathcal{A}}})/d_{\mathcal{A}}$ *or*
(v) $\deg(Y_{n,d_{\mathcal{A}}}) = d_{\mathcal{A}}^n$ *and* $d_{\mathcal{A}} \leq n$,

then

$$n_0(\mathcal{A}) \leq \deg(Y_{n,d_{\mathcal{A}}}) - |\mathcal{A}| + n + 2.$$

If $Y_{n,d_{\mathcal{A}}}$ is a smooth variety, then we have further

$$n_0(\mathcal{A}) \leq \min\{n(d_{\mathcal{A}} - 2) + 1, \deg(Y_{n,d_{\mathcal{A}}}) - |\mathcal{A}| + n + 2\}.$$

Proof. Under the hypothesis of the statement, the Eisenbud-Goto conjecture for the Castelnuovo-Mumford regularity $\mathrm{reg}(\mathcal{A})$ of $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$ holds (see [20, Corollary 3.6 and Proposition 3.7] and [19, Theorem 1.1 and Corollary 1.3]). Therefore, the proof now follows from the general fact:

$$n_0(\mathcal{A}) \leq \mathrm{reg}(\mathcal{A}) + 1.$$

$\square$

In general,

Theorem 4.6. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. Then,*

$$n_0(\mathcal{A}) \leq (d_{\mathcal{A}} - 1)(|\mathcal{A}| - n - 1) + 1.$$

Moreover, if $\deg(Y_{n,d_{\mathcal{A}}}) \geq |\mathcal{A}| - n + 1$, then

$$n_0(\mathcal{A}) \leq \min\{(n+1)(\deg(Y_{n,d_{\mathcal{A}}}) - |\mathcal{A}| + n - 1) + 3, (d_{\mathcal{A}} - 1)(|\mathcal{A}| - n - 1) + 1\}.$$

Proof. The result follows from [20, Theorem 3.2 and Theorem 3.5]. $\square$

Overall, combining Theorems 4.2, 4.5 and 4.6 we obtain finer bounds for the phase transition $n_0(\mathcal{A})$. For instance, subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ containing $\{0, v_1, \ldots, v_n\}$ and moreover any point of the form $(0, \ldots, \alpha(d_{\mathcal{A}} - 1), \ldots, \beta, \ldots, 0)$ with $\alpha, \beta \in \{0, 1\}$ give rise to a smooth monomial projection $Y_{n,d_{\mathcal{A}}}$ of the Veronese variety $X_{n,d_{\mathcal{A}}}$. In this case, $\mathbb{Z}(\mathcal{A} - \mathcal{A}) = \mathbb{Z}^n$ and we have $\deg(Y_{n,d_{\mathcal{A}}}) = d_{\mathcal{A}}^n$. Therefore,

$$n_0(\mathcal{A}) \leq \min\{d_{\mathcal{A}}^n + n(d_{\mathcal{A}}^n - 3) - 1, n(d_{\mathcal{A}} - 2) + 1, d_{\mathcal{A}}^n - |\mathcal{A}| + n + 2\},$$

which gives $\min\{n(d_{\mathcal{A}} - 2) + 1, d_{\mathcal{A}}^n - |\mathcal{A}| + n + 2\}$ whenever $d_{\mathcal{A}}^n - n - 1 \geq 1$ or $n(d_{\mathcal{A}}^n - 3) - 1 > n + 2 - |\mathcal{A}|$.

Remark 4.7 (Comparision of bounds)**.** Assume that $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ is a finite subset with $n \geq 2$ and $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. Without further assumptions, by Theorem 4.5(iii) and Theorem 4.6, we have that $n_0(\mathcal{A}) \leq (n+1)(\deg(Y_{n,\mathcal{A}}) - |\mathcal{A}| + n - 1) + 3$ which improves by $n - 1$ the bound $n_0(\mathcal{A}) \leq (n+1)(\deg(Y_{n,\mathcal{A}}) - |\mathcal{A}| + n) + 1$ given in [15] and the bound $(n+1)\deg(Y_{n,\mathcal{A}}) - 3n - 1$ given in [8] when $|\mathcal{A}| > n + 2$. On the other hand, for those subsets $\mathcal{A}$ satisfying one of the hypothesis of Theorem 4.5, we have $n_0(\mathcal{A}) \leq \deg(Y_{n,d_{\mathcal{A}}}) - |\mathcal{A}| + n + 2$ which beats the prior bounds in almost all cases and it is close to the bound $n_0(\mathcal{A}) \leq \deg(Y_{n,\mathcal{A}}) - |\mathcal{A}| + 2$ conjectured in [8]. In particular, when $Y_{n,\mathcal{A}}$ is a smooth variety we have $n_0(\mathcal{A}) \leq \min\{\deg(Y_{n,\mathcal{A}}) - |\mathcal{A}| + n - 1, n(d_{\mathcal{A}} - 2) + 1\}$. The last expressions are more difficult to compare in general. Notwithstanding, for this kind of monomial projections, it is often the case $\deg(Y_{n,\mathcal{A}}) = d_{\mathcal{A}}^n$, or equivalently $[\mathbb{Z}^n : \mathbb{Z}(\mathcal{A} - \mathcal{A})] = 1$. For instance, as we have seen before, $Y_{n,d_{\mathcal{A}}}$ is a degree $d_{\mathcal{A}}^n$ smooth variety when $\mathcal{A}$ contains any point of the form $(0, \ldots, \alpha(d_{\mathcal{A}} - 1), \ldots, \beta, \ldots, 0)$ with $\alpha, \beta \in \{0, 1\}$. In this setting, we have $n(d_{\mathcal{A}} - 2) + 1 \leq d_{\mathcal{A}}^n - |\mathcal{A}| + n - 1$. Indeed, $|\mathcal{A}| \leq \binom{n+d_{\mathcal{A}}}{n}$ and the inequality $n(d_{\mathcal{A}} - 2) + 1 \leq d_{\mathcal{A}}^n - \binom{n+d_{\mathcal{A}}}{n} + n - 1$ holds.

In [20], the authors provide bounds for $\mathrm{reg}(\mathcal{A})$ in terms of the reduction number $r(\mathcal{A})$ of $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$. We will relate $r(\mathcal{A})$ to the constant $K(\mathcal{A}, B)$, with $B = \{0, v_1, \ldots, v_n\}$, and we will provide bounds for $n_0(\mathcal{A})$ in terms of $r(\mathcal{A})$ that improve the one given in Proposition 4.3.

Definition 4.8. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. The reduction number $r(\mathcal{A})$ of the semigroup ring $\mathbb{K}[\Omega_{n,d_{\mathcal{A}}}]$ is the least positive integer r such that $(r+1)\overline{\mathcal{A}} = \{e_0, \ldots, e_n\} + r\overline{\mathcal{A}}$.*

Remark 4.9. Notice that for any $r \geq r(\mathcal{A})$, we obtain inductively that

$$(r+1)\overline{\mathcal{A}} = \{e_0, \ldots, e_n\} + r\overline{\mathcal{A}}.$$

In the next result we relate $r(\mathcal{A})$ to $K(\mathcal{A}, B)$:

Proposition 4.10. Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. Then, $r(\mathcal{A}) = K(\mathcal{A}, B)$.

Proof. To prove the result, we check the inequalities $r(\mathcal{A}) \leq K(\mathcal{A}, B)$ and $K(\mathcal{A}, B) \leq r(\mathcal{A})$. Let $r \geq K(\mathcal{A}, B)$ be an integer and $a = (a_1, \ldots, a_n) \in (r+1)\mathcal{A}$. We set $a_0 = (r+1)d_{\mathcal{A}} - a_1 - \cdots - a_n$ and we denote $\overline{a} = (a_0, a_1, \ldots, a_n) \in (r+1)\overline{\mathcal{A}}$. By hypothesis, there exists v_i such that $a - v_i \in r\mathcal{A}$. Hence, $\overline{a} \in \{e_0 + \cdots + e_n\} + r\overline{\mathcal{A}}$. So, $r(\mathcal{A}) \leq K(\mathcal{A}, B)$.

Now, let $r \geq r(\mathcal{A})$ be an integer and assume that $a \in \mathcal{S}(\mathcal{A}, B)$ has height $N_a = r + 1$, i.e. $a \in (r+1)\mathcal{A}$ is $B-$minimal and $a \notin r'\mathcal{A}$ for any $r' \leq r+1$. By hypothesis, $(r+1)\overline{\mathcal{A}} = \{e_0, \ldots, e_n\} + r\overline{\mathcal{A}}$, so $\overline{a} - e_i \in r\overline{\mathcal{A}}$ for some $0 \leq i \leq n$. Since a is $B-$minimal, it follows that $\overline{a} - e_i \notin r\overline{\mathcal{A}}$ for any $1 \leq i \leq n$. Thus, $\overline{a} - e_0 \in r\overline{\mathcal{A}}$. In particular, we obtain that $a \in r\mathcal{A}$ which contradicts the hypothesis $N_a = r + 1$. As a result, any $B-$minimal element has height $N_a \leq r(\mathcal{A})$, so $K(\mathcal{A}, B) \leq r(\mathcal{A})$. $\square$

We have:

Theorem 4.11. Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$. We have:

(i) if $r(\mathcal{A}) \leq 1$, then $n_0(\mathcal{A}) \leq 2$, and

(ii) if $r(\mathcal{A}) > 1$, then

$$n_0(\mathcal{A}) \leq \min\{(n+1)(r(\mathcal{A}) - 1) - n + 2, (n+1)r(\mathcal{A}) - \lceil \frac{(n+1)r(\mathcal{A})}{d_{\mathcal{A}}} \rceil + 1\}.$$

Proof. By Proposition 4.10 we have $r(\mathcal{A}) = K(\mathcal{A}, B)$. Hence, applying [20, Theorems 3.1 and 3.2] we get what we want. $\square$

As we have established before in Proposition 4.10, when $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ contains $\{0, v_1, \ldots, v_n\}$, we have the equality of the constants $K(\mathcal{A}, B) = r(\mathcal{A})$. In this setting, it is natural to compare the bounds for $n_0(\mathcal{A})$ which are expressed in terms of them. By Theorem 4.11 and Proposition 4.10, it holds that $n_0(\mathcal{A}) \leq (n+1)(K(\mathcal{A}, B) - 1) - n + 2$. Now by Proposition 4.3, $n_0(\mathcal{A}) \leq (n+1)(K(\mathcal{A}, B) - 1) + 1$. Accordingly, Theorem 4.11 improves at least by $n - 1$, which is always positive when $n \geq 2$, the bound for the phase transition $n_0(\mathcal{A})$ given in Proposition 4.3. Let us see a more concrete example.

Example 4.12. Continuing with Example 4.4, we take $\mathcal{A} = \{(0,0), (5,0), (3,1), (1,2), (0,5)\} \subset \mathbb{Z}_{\geq 0}^2$ and we have $d_{\mathcal{A}} = 5$, $|\mathcal{A}| = 5$, $\deg(Y_{2,5}) = 5$, $B = \{(0,0), (5,0), (0,5)\}$, $\mathrm{vol}(\mathrm{conv}(\mathcal{A})) = \frac{25}{2}$, $K(\mathcal{A}, B) = r(\mathcal{A}) = 2$. As we have seen before, the bounds from Theorem 4.2 and Proposition 4.3 are $n_0(\mathcal{A}) \leq 5$ and $n_0(\mathcal{A}) \leq 4$, respectively. Thus far, we can assure that $n_0(\mathcal{A}) \leq 4$. Since $\mathbb{K}[\Omega_{2,5}]$ is a Cohen–Macaulay ring ([5, Theorem 3.3]), by Theorem 4.5 we obtain $n_0(\mathcal{A}) \leq 4$; and by Proposition 4.11 we get $n_0(\mathcal{A}) \leq 3$, which overall improves the previous bound.

To determine $K(\mathcal{A}, B)$, or equivalently $r(\mathcal{A})$, could be cumbersome depending on the subset $\mathcal{A}$. In [15], the authors provide a bound for $K(\mathcal{A}, B)$ in terms of the *Davenport constant* of a certain group. On the other hand, for subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ with $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$, the constant $r(\mathcal{A})$ can be also bounded as follows:

Proposition 4.13. *Let $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ be a finite subset such that $\{0, v_1, \ldots, v_n\} \subset \mathcal{A}$.*

    (i) *If $\mathcal{H}(\overline{\mathcal{A}})$ contains all integral points of an i-dimensional face of $\mathrm{conv}(\overline{\mathcal{A}})$, then $r(\mathcal{A}) \leq d_{\mathcal{A}}^{n-i} + i - 1$.*

    (ii) *If an i-dimensional face of $\mathrm{conv}(\overline{\mathcal{A}})$ contains $q + i + 1$ points of $\mathcal{H}(\overline{\mathcal{A}})$, then $r(\mathcal{A}) \leq (d_{\mathcal{A}}^i - q)d_{\mathcal{A}}^{n-i}$.*

Proof. See [20, Lemma 1.2 and 1.3]. $\square$

5. GT-SUMSETS AND RL-VARIETIES

The aim of this section is to illustrate how the relationship between additive number theory and algebraic geometry allows us to go back and forth and solve interesting open problems. First, we introduce the notions of $GT-$subsets and GT-sumsets associated to linear systems of congruences. For this kind of subsets $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ and using the geometry of $Y_{n, d_{\mathcal{A}}}$, we provide a low bound for the phase transition $n_0(\mathcal{A})$ and families of examples for which the function $\varphi_{\mathcal{A}}(t)$ and polynomial $p_{\mathcal{A}}(t)$ are completely determined. Second, we present $RL-$varieties, they are monomial projections of the Veronese variety $X_{n,d}$ intrinsically related to $GT-$subsets and $GT-$sumsets. Using properties of sumsets, we are able to compute their degree and their Hilbert polynomial.

Notation 5.1. *Let $1 \leq n, d_1, \ldots, d_s$ be integers and let $M = (a_{i,j})$ be a $s \times (n+1)$ matrix of integers with $0 \leq a_{i,0}, \ldots, a_{i,n} < d_i$ and $\mathrm{GCD}(a_{i,0}, \ldots, a_{i,n}, d_i) = 1$, for each $1 \leq i \leq s$. We set $d := d_1 \cdots d_s$ and we denote by $(M, d_1, \ldots, d_s)$ the linear system of congruences*

(9)
$$\begin{cases} y_0 & + & y_1 & + & \cdots & + & y_n & \equiv & 0 \mod d \\ a_{1,0}y_0 & + & a_{1,1}y_1 & + & \cdots & + & a_{1,n}y_n & \equiv & 0 \mod d_1 \\ & & & & \vdots & & & & \\ a_{s,0}y_0 & + & a_{s,1}y_1 & + & \cdots & + & a_{s,n}y_n & \equiv & 0 \mod d_s. \end{cases}$$

For each $t \geq 1$, we denote by $(M, d_1, \ldots, d_s; t)$ the linear system:

(10)
$$\begin{cases} y_0 & + & y_1 & + & \cdots & + & y_n & = & td \\ a_{1,0}y_0 & + & a_{1,1}y_1 & + & \cdots & + & a_{1,n}y_n & \equiv & 0 \mod d_1 \\ & & & & \vdots & & & & \\ a_{s,0}y_0 & + & a_{s,1}y_1 & + & \cdots & + & a_{s,n}y_n & \equiv & 0 \mod d_s. \end{cases}$$

Definition 5.2. *Let $(M, d_1, \ldots, d_s)$ be a linear system of congruences. The $\mathbb{Z}_{\geq 0}^{n+1}-$solutions of the system $(M, d_1, \ldots, d_s; 1)$ form a finite subset $\overline{\mathcal{A}} \subset \mathbb{Z}_{\geq 0}^{n+1}$ and we define the $GT-$subset associated to $(M, d_1, \ldots, d_s)$ to be $\mathcal{A} = \{(a_1, \ldots, a_n) \mid (a_0, a_1, \ldots, a_n) \in \overline{\mathcal{A}}\} \subset \mathbb{Z}_{\geq 0}^n$.*

The set of all $\mathbb{Z}_{\geq 0}^{n+1}$−solutions of a system of congruences $(M, d_1, \ldots, d_s)$ is an affine semigroup $H \subset \mathbb{Z}_{\geq 0}^{n+1}$. By [7, Theorem 2.2.11] the associated subset $\overline{\mathcal{A}}$ minimally generates the semigroup H. Thus, for each $t \geq 1$ the GT−sumset $t\mathcal{A}$ is uniquely determined by the set of $\mathbb{Z}_{\geq 0}^{n+1}$−solutions of the system $(M, d_1, \ldots, d_s; t)$ and, hence,

$$\varphi_{\mathcal{A}}(t) = |t\mathcal{A}| = |(M, d_1, \ldots, d_s, t)|.$$

Geometrically, the coordinate ring of the monomial projection $Y_{n,d_{\mathcal{A}}}$ of the Veronese variety $X_{n,d}$ parameterized by the set $\Omega_{n,d}$ of monomials associated to the GT−subset $\mathcal{A}$ of $(M, d_1, \ldots, d_s)$ is the semigroup ring $\mathbb{K}[H]$.

In addition, the above construction can be also interpreted from invariant theory point of view. Given a system of congruences $(M, d_1, \ldots, d_s)$, we set e a dth primitive root of $1 \in \mathbb{K}$. For each $1 \leq i \leq s$ we denote $e_i = e^{d/d_i}$ and by $M_{d_i; a_{i,0}, \ldots, a_{i,n}}$ the diagonal $(n+1) \times (n+1)$ matrix $\mathrm{diag}(e_i^{a_{i,0}}, \ldots, e_i^{a_{i,n}})$. Since by hypothesis $\mathrm{GCD}(a_{i,0}, \ldots, a_{i,n}, d_i) = 1$, each matrix $M_{d_i; a_{i,0}, \ldots, a_{i,n}}$ generates a cyclic subgroup Γ_i of $\mathrm{GL}(n+1, \mathbb{K})$ of order d_i. We take $G = \Gamma_1 \oplus \cdots \oplus \Gamma_s \subset \mathrm{GL}(n+1, \mathbb{K})$, which is an abelian group of order d acting diagonally on R and we denote by $\overline{G} \subset \mathrm{GL}(n+1, \mathbb{K})$ its cyclic extension, the abelian group generated by G and the diagonal matrix $\mathrm{diag}(e, \ldots, e)$. The ring $R^{\overline{G}} = \{p \in R \mid g(p) = p, \forall g \in \overline{G}\}$ of invariants of $\overline{G}$ has a basis of monomials, precisely the monomials $x_0^{a_0} \cdots x_n^{a_n} \in R$ such that $(a_0, \ldots, a_n)$ is a $\mathbb{Z}_{\geq 0}^{n+1}$−solution of $(M, d_1, \ldots, d_s)$. By [7, Theorem 2.2.11], $\Omega_{n,d}$ is a minimal set of generators of the ring $R^{\overline{G}} = \mathbb{K}[H]$. So, for the phase transition $n_0(\mathcal{A})$ of a GT-subset we have:

Proposition 5.3. *Let $\mathcal{A}$ be the GT−subset associated to a linear system of congruences $(M, d_1, \ldots, d_s)$. Then, $n_0(\mathcal{A}) \leq n + 1$.*

Proof. By [7, Theorem 3.3.5], it holds that $\mathrm{reg}(R^{\overline{G}}) + 1 = \mathrm{reg}(\mathcal{A}) + 1 \leq n + 1$. Since $n_0(\mathcal{A}) \leq \mathrm{reg}(\mathcal{A}) + 1$, the result follows. □

The Castelnuovo–Mumford regularity $\mathrm{reg}(\mathcal{A})$ gives us a bound for the phase transition $n_0(\mathcal{A})$ for GT−sumsets which is considerable low compared to the bounds we have in Section 4. Indeed, $R^{\overline{G}} = K[H]$ is a Cohen-Macaulay ring, so we have by Theorem 4.5 that $n_0(\mathcal{A}) \leq \deg(Y_{n,d}) - |\mathcal{A}| + n + 2$. Now, by [7, Proposition 3.1.2] we have that $\deg(Y_{n,d}) \geq |\mathcal{A}| - 1$ and, hence, the claim $\deg(Y_{n,d}) - |\mathcal{A}| + n + 2 \geq n + 1$ follows. Furthermore, the structure of GT−sumsets allows to completely determine the function $\varphi_{\mathcal{A}}(t)$, the polynomial $p_{\mathcal{A}}(t)$ and the phase transition $n_0(\mathcal{A})$ in many cases. The first approach consists of counting the number of solutions of the systems $(M, d_1, \ldots, d_s; t)$. This method depends on the system $(M, d_1, \ldots, d_s)$ and it is out of reach for large values of n. Nevertheless, for $n = 2, 3$ it often leads to a complete solution. For instance,

Proposition 5.4. *Let $2 \leq n < d$ be integers and (M, d) the system of congruences:*

$$\begin{cases} y_0 + y_1 + y_2 \equiv 0 \mod d \\ a_{1,1}y_1 + a_{1,2}y_2 \equiv 0 \mod d. \end{cases}$$

We set $a' = \frac{a_{1,1}}{\mathrm{GCD}(a_{1,1},d)}$, $d' = \frac{d}{\mathrm{GCD}(a_{1,1},d)}$ and $0 < \lambda \leq d'$ the integer such that $a_{1,2} = \lambda a' + \mu d'$ with $\mu \in \mathbb{Z}$.

Then, the phase transition $n_0(\mathcal{A})$ for the $GT-$subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^2$ of (M,d) is zero and

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \frac{dt^2 + \theta(a_{1,1}, a_{1,2}, d)t + 2}{2},$$

where $\theta(a_{1,1}, a_{1,2}, d) = \mathrm{GCD}(a_{1,1}, d) + \mathrm{GCD}(\lambda, d') + \mathrm{GCD}(\lambda - \mathrm{GCD}(a_{1,1}, d), d')$.

Proof. The function $\varphi_{\mathcal{A}}(t)$ coincides with the number of solutions of the system $(M, d; t)$ and the result follows from [5, Theorem 4.12]. □

The second approach is based on the computation of the Hilbert series $\mathrm{HS}(A(Y_{n,d_{\mathcal{A}}}), z) = \sum_{t \geq 0} \varphi_{\mathcal{A}}(t) z^t$ of $Y_{n,d_{\mathcal{A}}}$ and the fact that $A(Y_{n,d_{\mathcal{A}}}) \cong R^{\overline{G}}$. The Hilbert series can be obtained from the Molien series of $\overline{G}$ as follows:

$$\mathrm{HS}(A(Y_{n,d_{\mathcal{A}}}), z^d) = \frac{1}{|\overline{G}|} \sum_{g \in \overline{G}} \frac{1}{\det(Id - zg)},$$

which is an expression that only depends on $(M, d_1, \ldots, d_s)$ (see, for instance, [3]). The expansion of the Molien series of $\overline{G}$ gives the function $\varphi_{\mathcal{A}}(t)$ and the polynomial $p_{\mathcal{A}}(t)$. For instance we have the following result, for sake of completeness we include a simple proof.

Proposition 5.5. *Let $2 \leq n < d$ be integers with d prime and (M, d) a system of congruences:*

$$\begin{cases} y_0 + y_1 + \cdots + y_n \equiv 0 \mod d \\ a_{1,1}y_1 + \cdots + a_{1,n}y_n \equiv 0 \mod d \end{cases}$$

with $0 < a_{1,1} < \cdots < a_{1,n}$. Then, the phase transition $n_0(\mathcal{A})$ for the $GT-$subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ associated to (M, d) is zero and

$$\varphi_{\mathcal{A}}(t) = p_{\mathcal{A}}(t) = \frac{1}{d}\binom{td + n}{n} + \frac{d - 1}{d}.$$

Proof. For any $t \in \mathbb{Z}_{\geq 0}$, we have that $\varphi_{\mathcal{A}}(t) = |(M, d_1, \ldots, d_s; t)|$ which is the number of monomial invariants of $\overline{G}$ of degree td. Since it coincides with the number of monomial invariants of G of degree td, it is enough to consider the expansion of the Molien series of G in degree td:

$$\frac{1}{d} \sum_{g \in G} \frac{1}{\det(Id - zg)} = \frac{1}{d} \sum_{k=0}^{d-1} \frac{1}{(1 - z)(1 - e^{ka_{1,1}}z) \cdots (1 - e^{ka_{1,n}}z)}.$$

Since d is prime and the exponents $0 < a_{1,1} < \cdots < a_{1,n} < d$, the classes of $ka_{1,1}, \ldots, ka_{1,n} \mod d$ are represented by two by two distinct integers in the set $\{0, \ldots, d - 1\}$. Using the factorization $(1 - z^d) = \prod_{j=0}^{d-1}(1 - e^j z)$, we can write it as:

$$\frac{1}{(1 - z^d)} \prod_{\substack{j \neq ka_{1,i} \mod d \\ i=0,\ldots,n}} (1 - e^j z),$$

which gives us the following expression:

$$\frac{1}{d}\left(\sum_{i=0}^{\infty}(-1)^i\binom{-(n+1)}{i}z^i+\sum_{i=0}^{\infty}(\sum_{k=1}^{d-1}\prod_{\substack{j\neq ka_{1,i} \mod d \\ i=0,\ldots,n}}(1-e^jz))z^{id}\right).$$

The expansion of the first summand at z^{td} provides $\binom{td+n}{n}$. For each $1 \leq k \leq d-1$, $\prod_{\substack{j\neq ka_{1,i} \mod d \\ i=0,\ldots,n}}(1-e^jz)$ is a polynomial in z of degree strictly smaller than d, so the second provides $d-1$ at z^{td} and the result follows. $\square$

In the last part of this paper, we will use the results of sumsets obtained so far to derive new results about $RL-$varieties; $RL-$varieties were introduced and studied in [6] and [7]. They are a family of smooth rational monomial projections of the Veronese variety $X_{n,d}$ naturally related to $GT-$subsets. Basic information as the degree of an $RL-$variety was unknown and the approach and techniques we have presently developed will allow us to obtain new information about this family of varieties and, in particular, to compute their degree and their Hilbert polynomial.

Given a system of congruences $(M, d_1, \ldots, d_s)$, the set of $\mathbb{Z}_{\geq 0}^{n+1}-$solutions $(a_0, \ldots, a_n)$ satisfying $a_0 \cdots a_n \neq 0$ is the *relative interior* relint(H) of the associated affine semigroup $H \subset \mathbb{Z}_{\geq 0}^{n+1}$. We define rl$(\overline{\mathcal{A}}) := \overline{\mathcal{A}} \cap$ relint(H), we denote by rl$(\mathcal{A}) \subset \mathbb{Z}_{\geq 0}^n$ the corresponding subset and by rl$(\Omega_{n,d})$ its associated set of monomials. The $RL-$variety rl$(Y_{n,d_\mathcal{A}})$ associated to the $GT-$subset $\mathcal{A}$ is the monomial projection of the Veronese variety $X_{n,d}$ induced by the subset rl$(\mathcal{A})^c := \{(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^n \mid a_1 + \cdots + a_n \leq d\} \setminus$ rl$(\mathcal{A})$, i.e. it is parameterized by $\mathcal{M}_{n,d} \setminus$ rl$(\Omega_{n,d})$.

Proposition 5.6. *Let $n \geq 2$ be an integer and $(M, d_1, \ldots, d_s)$ a system of congruences with $GT-$subset $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$.*

   (i) *The degree of the $RL-$variety rl$(Y_{n,d_\mathcal{A}})$ associated to $\mathcal{A}$ is d^n.*
   (ii) *The Castelnuovo–Mumford regularity* reg(rl$(\mathcal{A})^c) \leq \min\{n(d-2)+1, d^n - \binom{n+d}{n} + |rl(\mathcal{A})| + n + 2\}$.
   (iii) *The phase transition $n_0($rl$(\mathcal{A})^c) \leq n+1$, moreover, for any $t \geq n+1$ we have*

$$\varphi_{\text{rl}(\mathcal{A})^c}(t) = p_{\text{rl}(\mathcal{A})^c}(t) = \binom{td+n}{n}.$$

Proof. (i) The subset $\overline{\text{rl}(\mathcal{A})^c}$ contains $(d, 0, \ldots, 0), \ldots, (0, \ldots, 0, d)$ and any point $(0, \ldots, 1, \ldots, d-1, \ldots, 0)$. Therefore, the convex hull of rl$(\mathcal{A})^c$ is an $n-$simplex and $\mathbb{Z}($rl$(\mathcal{A})^c - rl(\mathcal{A})^c) = \mathbb{Z}^n$. Using (5), it follows that deg(rl$(Y_{n,d_\mathcal{A}})) = d^n$.

(ii) Since rl$(Y_{n,d_\mathcal{A}})$ is a smooth variety ([7, Proposition 5.1.11]), it follows from Theorem 4.5.

(iii) The statement follows from the *claim: for any $t \geq n+1$, the t-fold sumset $t\overline{\text{rl}(\mathcal{A})^c} = \{(a_0, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^{n+1} \mid a_0 + \cdots + a_n = td\}$. Indeed, let $t \geq n+1$ be an integer and $a = (a_0, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^{n+1}$ be such that $a_0 + \cdots + a_n = td$. We prove that $a \in t\overline{\text{rl}(\mathcal{A})^c}$. Notice that if some $a_i = 0$, then it is immediate that $a \in t\overline{\text{rl}(\mathcal{A})^c}$ since $\overline{\text{rl}(\mathcal{A})^c}$ contains all points

$\{(a_0, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^{n+1} \mid a_0 + \cdots + a_n = d \quad \text{and} \quad a_i = 0\}$. So, we can assume that $a_0 \geq 1, \ldots, a_n \geq 1$ and, without loss of generality, we consider $a_0 = \min\{a_0, \ldots, a_n\}$. Since $|a| = a_0 + \cdots + a_n \geq (n+1)d$, there is a_i such that $a_i \geq d$, otherwise $|a| < (n+1)d$ and we get a contradiction. We set $a_0 = t'd + k_0$ with $k_0 \in \{0, \ldots, d-1\}$ and we distinguish two cases.

<u>Case 1</u>: If $t' > 0$, then $a_1 > d$ and we can write

$$a = (a_0, d - k_0, 0, \ldots, 0) + (0, a_1 - d + k_0, a_2, \ldots, a_n) = a^1 + a^2$$

with $a^1, a^2 \in \mathbb{Z}_{\geq 0}^{n+1}$. Then we have that $|a^1| = t'd + k_0 + d - k_0 = (t'+1)d$ and $|a^2| = a_1 - d + k_0 + a_2 + \cdots + a_n = td - a_0 - d + k_0 = td - t'd - k_0 - d + k_0 = (t - t' - 1)d$. Thus $a^1, a^2 \in \mathcal{H}(\overline{\mathrm{rl}(\mathcal{A})^c})$ and, hence, $a \in t\overline{\mathrm{rl}(cA)^c}$.

<u>Case 2</u>: If $t' = 0$, then $a_0 = k_0 < d$ and, without loss of generality, we can assume that $a_1 \geq d$. Hence, we can write

$$a = (a_0, d - a_0, 0, \ldots, 0) + (0, a_1 - d + a_0, a_2, \ldots, a_n) = a^1 + a^2$$

with $a^1, a^2 \in \mathbb{Z}_{\geq 0}^{n+1}$. Arguing exactly as in Case 1, we obtain $a \in t\overline{\mathrm{rl}(cA)^c}$. $\qquad\square$

Actually, Proposition 5.6 is true for any monomial projection $Y_{n,d}$ of the Veronese variety $X_{n,d}$ in dimension $n \geq 2$ parameterized by a subset of monomials $\Omega_{n,d}$ obtained from the set of all monomials of degree d in R by deleting only monomials $x_0^{a_0} \cdots x_n^{a_n}$ with $a_0 \cdots a_n \neq 0$, i.e. by deleting only monomials having all the variables $x_0, \ldots, x_n$.

We end this section with an illustrating example.

Example 5.7. We take $n = 2$ and $\mathcal{A} = \{(0,0), (3,0), (0,3), (1,1)\}$ with $d_{\mathcal{A}} = 3$. We have that $\mathcal{A}$ is the GT−subset of the linear system of congruences:

$$\begin{cases} y_0 & + & y_1 & + & y_2 & \equiv & 0 \mod 3 \\ & & y_1 & + & 2y_2 & \equiv & 0 \mod 3. \end{cases}$$

It is straightforward to see that $\mathrm{rl}(\mathcal{A}) = \{(1,1)\}$ and $\mathrm{rl}(\mathcal{A})^c = \{(0,0), (1,0), (0,1), (2,0), (0,2), (3,0), (2,1), (1,2), (0,3)\}$. We have $|\mathrm{rl}(\mathcal{A})^c| = 9$, $d_{\mathrm{rl}(\mathcal{A})^c} = 3$ and the associated simple projection $Y_{2,3} \subset \mathbb{P}^8$ of the Veronese surface $X_{2,3} \subset \mathbb{P}^9$ parameterized by $\mathrm{rl}(\mathcal{A})^c$ is the RL−variety associated to the GT−sumset $\mathcal{A}$ (Example 3.9(ii)). By Proposition 5.6, we obtain $\deg(Y_{2,3}) = 9$ as in Example 3.9(ii). On the other hand, $\mathrm{reg}(\mathrm{rl}(\mathcal{A})^c) \leq 3$ and $n_0(\mathrm{rl}(\mathcal{A})^c) \leq 3$, which is very close to the real value $n_0(\mathrm{rl}(\mathcal{A})^c) = 2$. In addition, for all $t \geq n+1$ we have

$$\varphi_{\mathrm{rl}(\mathcal{A})^c}(t) = p_{\mathrm{rl}(\mathcal{A})^c}(t) = \binom{3t+2}{2}.$$

REFERENCES

[1] M. Beltrametti, E. Carletti, D. Gallarati and G. Monti Bragadin, *Lectures on Curves, Surfaces and Projective Varieties: A Classical View of Algebraic Geometry*. EMS Textbooks in Mathematics. European Mathematical Society (EMS), Zürich, 2009. xvi+491 pp. ISBN: 978-3-03719-064-7

[2] C. Blancafort, *Hilbert functions of graded algebras over Artinian rings* J. Pure and Appl. Algebra 125 (1998) 55-78.

[3] W. Bruns and J. Herzog. *Cohen-Macaulay rings.* Cambridge Studies in Advanced Mathematics, 39. Cambridge University Press, Cambridge, 1993.

[4] F. J. Chen, Y. G. Chen and J. D. Wu, *On the structure of the sumsets.* Discrete Math. **311:6** (2011), 408–412.

[5] L. Colarte-Gómez, E. Mezzetti and R. M. Miró-Roig, *On the arithmetic Cohen–Macaulayness of varieties parameterized by monomial Togliatti systems.* Annali di Matematica Pura ed Applicata. **200** (2021), 1757–1780.

[6] L. Colarte-Gómez and R. M. Miró-Roig, *The canonical module of GT-varieties and the normal bundle of RL-varieties.* Mediterranean Journal of Mathematics, to appear. Doi: 10.1007/s00009-021-01936-w.

[7] L. Colarte-Gómez, *Gröbner's problem and the geometry of GT−varieties.* PhD Thesis, Universitat de Barcelona, Barcelona, Spain, July of 2021.

[8] M. J. Curran and L. Goldmakher, *Khovanskii's theorem and effective results on sumset structure.* arXiv:2009.02140v3.

[9] J. Elias, *Sumsets and monomial projective curves.* Mediterranean Journal of Mathematics, to appear.

[10] G. A. Freiman, *Structure theory of set addition* Astérisque, **258** (1999), 1–33.

[11] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory.* Advances courses in Mathematics-CRM Barcelona. Birkhäuser Basel, 2009.

[12] G. Gotzmann. *Einige einfach-zusammenhängende Hilbertschemata.* Math. Z. 180 (1982), no. 3, 291–305.

[13] A. Granville and A. Walker, *A tight structure theorem for sumsets.* arXiv:2006.01041v2

[14] A. Granville and G. Shakan, *The Frobenious postage stamp problem, and beyond.* Acta Math. Hungar. **161:2** (2020), 700–718.

[15] A. Granville, G. Shakan and A. Walker, *Effective results on the size and structure of sumsets.* arXiv:2105.09181v1

[16] M. Green. *Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann.* Algebraic curves and projective geometry (Trento, 1988), 76–86, Lecture Notes in Math., 1389, Springer, Berlin, 1989.

[17] J. Harris, *Algebraic Geometry. A first course.* GTM **133** Springer-Verlag, New York, 1992

[18] R. Hartshorne, *Algebraic Geometry.* Springer-Verlag, New York, 1977.

[19] J. Herzog and T. Hibi, *Castelnuovo–Mumford regularity of simplicial semigroup rings with isolated singularity.* Proceedings of the American Mathematical Society. **131** (2003), 2641–2647.

[20] L. T. Hoa and J. Stückrad, *Castelnuovo–Mumford regularity of simplicial toric rings.* Journal of Algebra. **259** (2003), 127–146.

[21] M. Hochster, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes.* Annals of Mathematics. **96:2** (1972), 318–337.

[22] V. Jelínek and M. Klazar, *Generalizations of Khovanskii's theorems on the growth of sumsets in Abelian semigroups.* Advances in Applied Mathematics. **41** (2008), 115–132.

[23] A. G. Khovanskii, *Newton polyhedron, Hilbert polynomial, and sums of finite sets.* Funct. Anal. Its Appl. **26** (1992), 276–281.

[24] J. Lee, *Algebraic proof for the geometric structure of sumsets.* Integers **11:4** (2011), 477–486.

[25] J. McCullough and I. Peeva, *Counterexamples to the Eisenbud-Goto regularity conjecture.* J. Amer. Math. Soc. 31 (2018), no. 2, 473–496.

[26] E. Miller and B. Sturmfels, *Combinatorial commutative algebra.* Springer, New York, 2005.

[27] M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets.* Graduate Texts in Mathematics, 165, Springer-Verlag, New York (1996).

[28] M. B. Nathanson, *Sums of finite sets of integers.* Amer. Math. Monthly **79** (1972), 1010–1012.

[29] M. B. Nathanson and I. Z. Ruzsa, *Polynomial growth of sumsets in abelian semigroups.* Journal de théorie des nombres de Bordeaux, **14:2** (2002), 553–560.

[30] M.J. Nitsche *A combinatorial proof of the Eisenbud-Goto conjecture for monomial curves and some simplicial semigroup rings.* J. Algebra 397 (2014), 47–67.

[31] L. O'Carroll, F. Planas-Vilanova and R. H. Villarreal, *Degree and algebraic properties of lattice and matrix ideals.* SIAM J. Discrete Math., **28:1** (2014), 394–427.

Facultat de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via des les Corts Catalanes 585, 08007 Barcelona, Spain

Email address: `liena.colarte@ub.edu`

Facultat de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via des les Corts Catalanes 585, 08007 Barcelona, Spain

Email address: `elias@ub.edu`

Facultat de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via des les Corts Catalanes 585, 08007 Barcelona, Spain

Email address: `miro@ub.edu`