Mediterr. J. Math. (2022) 19:177
https://doi.org/10.1007/s00009-022-02108-0
1660-5446/22/040001-11
published online June 25, 2022

Mediterranean Journal of Mathematics

Sumsets and Projective Curves

J. Elias

Abstract. The aim of this note is to exploit a new relationship between additive combinatorics and the geometry of monomial projective curves. We associate to a finite set of non-negative integers $A = \{a_1, \dots, a_n\}$ a monomial projective curve $C_A \subset \mathbb{P}^{n-1}_{\mathbf{k}}$ such that the Hilbert function of C_A and the cardinalities of $sA := \{a_{i_1} + \cdots + a_{i_s} \mid 1 \leq i_1 \leq \cdots \leq i_s \leq n\}$ agree. The singularities of C_A determines the asymptotic behaviour of $|sA|$, equivalently the Hilbert polynomial of C_A, and the asymptotic structure of sA. We show that some additive inverse problems can be translate to the rigidity of Hilbert polynomials and we improve an upper bound of the Castelnuovo-Mumford regularity of monomial projective curves by using results of additive combinatorics.

Mathematics Subject Classification. Primary 13D40; Secondary 11B13, 14H45.

1. Introduction

Let $A = \{a_1, \dots, a_n\}$, $n \geq 2$, be a set of different non-negative integers; we assume that $a_1 < \cdots < a_n$. Given a non-negative integer $s \geq 1$ the s-fold iterated sumset of A is

$$sA = \{a_{i_1} + \cdots + a_{i_s} \mid 1 \leq i_1 \leq \cdots \leq i_s \leq n\},$$

we set $0A = \{0\}$; notice that $1A = A$.

Following Nathanson, a direct problem in additive combinatorics is a problem in which we try to determine the structure and properties of $|sA|$, $s \geq 0$, when the set A is known. On the other hand, an inverse problem in additive combinatorics is a problem in which we attempt to deduce properties of A from properties of sA, $s \geq 0$, [22].

The aim of this paper is to establish and to study a bridge between additive combinatorics and the geometry of monomial projective curves. We argue back and forth: we use results of monomial projective curves to recover

Partially supported by PID2019-104844GB-I00.

or to improve results of additive combinatorics and vice versa, see Theorems 4.3 and 4.7. In particular, we show that some inverse problems can be translate in terms of the rigidity of Hilbert polynomials, see Sects. 4 and [9].

In this paper, we have selected some significative results of the geometry of monomial projective curves and additive combinatorics; there are a huge number of results and properties of both areas to link that we will consider elsewhere, see [5].

The contents of the paper is the following. In the second section, following [8], we attach to the set A a monomial projective curve $C_A \subset \mathbb{P}^{n-1}_{\mathbf{k}}$. The Hilbert function of C_A and the cardinalities of sA, $s \geq 0$, agree. Some previous results can be found in Ref. [16].

In the section, three we use the data provided by the singularities of C_A to determine the asymptotic behaviour of $|sA|$, equivalently the Hilbert polynomial of C_A, Proposition 3.1. As a consequence we can describe the asymptotic decomposition of sA of the so-called fundamental result of additive combinatorics, Propositions 3.3 and 3.4.

The Sect. 4 is devoted to recover, by considering generic hyperplane sections of C_A, some additive inverse results and to link them with rigid polynomials and rigid properties, Proposition 4.2, Theorem 4.3. We finish the paper improving an upper bound on the Castelnuovo-Mumford regularity of C_A established in [1] using a result of Lev on the growth of $|sA|$, Theorem 4.7.

For the basic results on algebra, algebraic geometry or additive number theory we will use: [2,13,22]. The computations of this paper are performed by using Singular, [6].

Notations

In this paper $\mathbf{k}$ is an arbitrary infinite field. Let $R = \sum_{i \geq 0} R_i$ be an standard $\mathbf{k} = R_0$ algebra, i.e., $R = \mathbf{k}[R_1]$. We denote by HF_R the Hilbert function of R, i.e., $\mathrm{HF}_R(i) = \dim_{\mathbf{k}} R_i$ for all $i \geq 0$. It is known that there exists a rational coefficient polynomial HP_R, Hilbert polynomial of R, such that $\mathrm{HP}(i) = \mathrm{HF}(i)$ for $i \gg 0$.

Given a set B of non-negative integers $b_1, \dots, b_n$ we denote by $\langle b_1, \dots, b_n \rangle$ the sub-semigroup of $\mathbb{N}$ generated by B. Given a multi-index $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ we define its total order by $|\alpha| = \sum_{i=1}^n \alpha_i$ and the total order with respect to A by $|\alpha|_A = \sum_{i=1}^n a_i \alpha_i$.

2. The Bridge Between Additive Number Theory and Projective Curves

We first show that we can consider several straight simplifications on the set A and an easy property on the growth of $|sA|$, see [22],

Lemma 2.1. *Given a set of non-negative integers $A = \{a_1, \dots, a_n\}$, $n \geq 2$, with $a_1 < \cdots < a_n$, it holds:*

1. *To compute $|sA|$ we may assume that $a_1 = 0$ and $\gcd(a_2, \dots, a_n) = 1$,*
2. *under the above conditions, $|(s+1)A| \geq |sA| + n - 1$ for all $s \geq 0$.*

Proof. (1) Let us consider $A' = \{0, (a_2 - a_1)/d, \dots, (a_n - a_1)/d\}$ where $d = \gcd(a_2 - a_1, \dots, a_n - a_1)$. It is easy to see that $|sA| = |sA'|$ for all $s \geq 0$.

(2) Assume that A satisfies the conditions of (1). Since the maximum of sA is sa_n we deduce that $sa_n + a_2, \dots, sa_n + a_n \in (s+1)A \setminus sA$, so we get the claim: $|(s+1)A| \geq |sA| + n - 1$ for all $s \geq 0$.

Given a general set of non-negative integers A, the associated set A' of the proof of the previous Lemma, is called the normal form of A, see [22]. From now on we assume that a set A satisfies Lemma 2.1 (1).

Next, we recall the key construction of [8].

Definition 2.2. We denote by $R(A)$ the $\mathbf{k}$-subalgebra of $\mathbf{k}[t, w]$ generated by $t^{a_i}w$, $i = 1, \dots, n$. We consider $\mathbf{k}[t, w]$ endowed with the grading defined by $\deg(t) = 0$, $\deg(w) = 1$.

Let $\phi = \mathbf{k}[X_1, \dots, X_n] \longrightarrow \mathbf{k}[t, w]$ the degree zero $\mathbf{k}$-algebra morphism defined by $\phi(X_i) = t^{a_i}w$. We have $\mathrm{Im}(\phi) = R(A)$ and the homogeneous piece of degree s of $R(A)$, i.e. $R(A)_s$, admits the $\mathbf{k}$-basis

$$t^\alpha w^s, \quad \alpha \in sA. \tag{1}$$

From this fact we get:

Proposition 2.3. [8, Sect. 2] *For all $s \geq 0$ it holds $\mathrm{HF}_{R(A)}(s) = |sA|$.*

In the following result a system of generators of $\mathrm{Ker}(\phi)$ is computed:

Proposition 2.4. [4, Proposizione 2.2], [8, Proposition 6.4] *The kernel of ϕ is generated by the binomials $X^\alpha - X^\beta$, $\alpha, \beta \in \mathbb{N}^n$, such that $|\alpha| = |\beta|$ and $|\alpha|_A = |\beta|_A$.*

Next, we link $R(A)$ with a suitable monomial projective curve.

Definition 2.5. Given a set $A = \{a_1 = 0, a_2, \dots, a_n\}$ such that $a_1 < \cdots < a_n$ and $\gcd(a_2, \dots, a_n) = 1$ we consider the monomial curve C_A of $\mathbb{P}^{n-1}_{\mathbf{k}}$ defined by the Kernel of

$$\begin{array}{rcl} \psi\ \mathbf{k}[X_1, \dots, X_n] & \longrightarrow & \mathbf{k}[u, v] \\ X_i & \mapsto & u^{a_n - a_i}v^{a_i} \end{array}$$

If we consider the standard grading of $\mathbf{k}[u, v]$ we get that $\mathrm{Ker}(\psi) = I_A$ is a homogeneous ideal of $\mathbf{k}[X_1, \dots, X_n]$. We denote by $\mathbf{k}[C_A] := \mathbf{k}[X_1, \dots, X_n]/\mathrm{Ker}(\phi)$ the homogeneous coordinate ring of C_A. We write $\mathrm{HF}_{C_A} = \mathrm{HF}_A$ and $\mathrm{HP}_{C_A} = \mathrm{HP}_A$.

Proposition 2.6. *For all set $A = \{a_1 = 0, a_2, \dots, a_n\}$ we have that* $\mathrm{Ker}(\phi) = I_A$. *Hence $R(A) \cong \mathbf{k}[C_A]$ as graded k-algebras.*

Proof. We first prove that $\mathrm{Ker}(\phi) \subset I_A$. Let's consider a binomial $X^\alpha - X^\beta$, $\alpha, \beta \in \mathbb{N}^n$, with $|\alpha| = |\beta|$ and $|\alpha|_A = |\beta|_A$. Then

$$\psi(X^\alpha - X^\beta) = u^{a_n|\alpha| - |\alpha|_A}v^{|\alpha|_A} - u^{a_n|\beta| - |\beta|_A}v^{|\beta|_A} = 0,$$

by Proposition 2.4 we get that $\mathrm{Ker}(\phi) \subset \mathrm{Ker}(\psi) = I_A$.

Next, we prove that $I_A \subset \mathrm{Ker}(\phi)$. Let $F \in I_A$ be a polynomial, so

$$F(u^{a_n}, u^{a_n-a_2}v^{a_2}, \dots, u^{a_n-a_{n-1}}v^{a_{n-1}}, v^{a_n}) = 0.$$

If X^α, $\alpha \in \mathbb{N}^n$, is a monomial of F then

$$X^\alpha(u^{a_n}, u^{a_n-a_2}v^{a_2}, \dots, u^{a_n-a_{n-1}}v^{a_{n-1}}, v^{a_n}) = u^{a_n|\alpha|-|\alpha|_A}v^{|\alpha|_A}$$

Hence we may assume that F is a homogeneous polynomial

$$F = \sum_{i=1}^{d} \lambda_i X^{\alpha_i}$$

such that $|\alpha_i|_A = c$, $a_n|\alpha_i| = c + d$ and $\lambda_i \in \mathbf{k} \setminus \{0\}$.

Since $F(u^{a_n}, u^{a_n-a_2}v^{a_2}, \dots, u^{a_n-a_{n-1}}v^{a_{n-1}}, v^{a_n}) = 0$ we deduce that $\sum_{i=1}^{d} \lambda_i = 0$, so

$$F = \sum_{i=1}^{d-1} \lambda_i (X^{\alpha_i} - X^{\alpha_d}) \in \mathrm{Ker}(\phi).$$

Remark 2.7. We write $\mathcal{B}_A = \frac{\mathbf{k}[C_A]}{X_1\mathbf{k}[C_A]}$, notice that $\mathcal{B}_A$ is a graded algebra of dimension one since the coset of X_1 is a non-zero divisor of $\mathbf{k}[C_A]$; $\mathcal{B}_A$ is the homogeneous coordinate ring of the hyperplane section of C_A defined by $X_1 = 0$. Both algebras $\mathbf{k}[C_A]$ and $\mathcal{B}_A$ are standard algebras, i.e. generated by their homogeneous pieces of degree one, i.e. $\mathbf{k}[C_A]_1$ and $(\mathcal{B}_A)_1$, respectively. In general $\mathcal{B}_A$ is non Cohen–Macaulay as the classic example of Macaulay shows, see Example 4.8.

Example 2.8. Let us consider the set $A = \{0, 2, 4, 5, 7\}$. The associated monomial curve C_A is defined by the parameterization $(u, v) \mapsto (u^7, u^5v^2, u^3v^4, u^2v^5, v^7)$. Then the defining ideal of C_A is minimally generated by $x_2^2 - x_1x_3, x_2x_4 - x_1x_5, x_3x_4 - x_2x_5, x_2x_3^2 - x_1x_4^2, x_3^3 - x_1x_4x_5, x_4^3 - x_3^2x_5$, [6]. The Hilbert function of C_A is $\mathrm{HF}_A = \{1, 5, 12, 19, 26, 33, \dots\}$ and the Hilbert polynomial $\mathrm{HP}_A(s) = 7s - 2$.

3. Sumsets and Monomial Projective Curves

We first recall some well known results on curves applied to the projective curve C_A, [13]. The monomial projective curve C_A is rational with two eventually singular points $P_1 = (1, 0, \dots, 0), P_2 = (0, \dots, 0, 1) \in \mathbb{P}^{n-1}_{\mathbf{k}}$. In the affine open neighborhood $X_1 = 1$ of P_1 the curve C_A is defined by the parameterization $v \mapsto (v^{a_2}, \dots, v^{a_n})$; and in the open affine neighborhood $X_n = 1$ of P_2 the curve is defined by the parameterization $u \mapsto (u^{a_n}, u^{a_n-a_2}, \dots, u^{a_n-a_{n-1}})$. The point P_1 is non-singular iff $a_2 = 1$ and P_2 is non-singular iff $a_n - a_{n-1} = 1$.

We denote by $p_a(C_A)$ the arithmetic genus of C_A, i.e.,

$$\mathrm{HP}_A(0) = 1 - p_a(C_A).$$

Since C_A is rational its geometric genus is zero and

$$p_a(C_A) = \sum_{P \in \mathrm{Sing}(C_A)} \delta(C_A, P),$$

where $\delta(C_A, P)$ is the singularity order of $P \in Sing(C_A)$, i.e.

$$\delta(C_A, P) = \dim_{\mathbf{k}} \frac{\overline{\mathcal{O}_{C_A,P}}}{\mathcal{O}_{C_A,P}}$$

where the over-line stands for the integral closure of $\mathcal{O}_{C_A,P}$ in its field of fractions. Summarizing, we get

$$\mathrm{HP}_A(0) = 1 - \delta(C_A, P_1) - \delta(C_A, P_2).$$

Since C_A is a monomial curve in an affine neighbourhood of P_1 (resp. P_2) we have

$$\delta(C_A, P_1) = \mathrm{Card}(\mathbb{N} \setminus \langle a_2, \ldots, a_n \rangle)$$

and

$$\delta(C_A, P_2) = Card(\mathbb{N} \setminus \langle a_n - a_{n-1}, \ldots, a_n - a_2, a_n \rangle).$$

We know that the Hilbert polynomial $\mathrm{HP}_A(s)$ and the Hilbert function $\mathrm{HF}_A(s)$ agree for $s \gg 0$. The first integer s_0 such that $\mathrm{HF}_A(s) = \mathrm{HP}_A(s)$ for all $s \geq s_0$ is called the regularity of the Hilbert function and it is denoted by $r(C_A)$.

The Castelnuovo–Mumford regularity $\mathrm{reg}(C_A)$ of C_A, see [7], for monomial projective curves is upper bounded in terms of the set A. From [19, Proposition 5.5], see also [14],

$$\mathrm{reg}(C_A) \leq \rho(A) := 1 + \mathrm{Max}\{(a_i - a_{i-1}) + (a_j - a_{j-1}); 2 \leq i < j \leq n\}$$

since $r(C_A) \leq \mathrm{reg}(C_A)$ we get that $\mathrm{HF}_A(s) = \mathrm{HP}_A(s)$ for all $s \geq \rho(A)$.

Notice that $\rho_A \leq a_n - n + 3$. This inequality can be deduced from the upper bound of the Castelnuovo–Mumford regularity conjectured by Eisenbud and Goto and proved by Gruson–Lazarsfeld–Peskine in the case of smooth curves, [12]. If C_A is non-singular then we have a better upper bound of the Castelnuovo–Mumford regularity, [14, Theorem 2.7],

$$\mathrm{reg}(C_A) \leq 1 + \mathrm{Max}\{(a_i - a_{i-1}); 2 \leq i < j \leq n\}.$$

The following result describes the asymptotic behaviour of $|sA|$, see [11,16,23].

Proposition 3.1. *Given a set $A = \{a_1 = 0, a_2, \ldots, a_n\}$ of integers such that $a_0 < a_1 < \cdots < a_n$ with $\gcd(a_2, \ldots, a_n) = 1$ it holds*

$$|sA| = \mathrm{HF}_A(s) = sa_n + 1 - \delta(C_A, P_1) - \delta(C_A, P_2)$$

for all $s \geq \rho(A)$.

Proof. We know that C_A is a degree a_n projective curve, so

$$\mathrm{HP}_A(s) = sa_n + \mathrm{HP}_A(0) = sa_n + 1 - \delta(C_A, P_1) - \delta(C_A, P_2).$$

Since $\mathrm{HF}_A(s) = \mathrm{HP}_A(s)$ for all $s \geq \rho(A)$ and we know that $|sA| = \mathrm{HF}_A(s)$ for all $s \geq 0$, we get the claim.

Corollary 3.2. *$\mathcal{B}_A$ is a one-dimensional standard graded algebra of multiplicity a_n.*

Proof. Since X_1 is a non-zero divisor of $\mathbf{k}[C_A]$, Remark 2.7, we get the claim from the last proposition.

The often called fundamental result of additive combinatorics claims:

Proposition 3.3. [22, Theorem 1.1] *Given a set* $A = \{a_1 = 0, a_2, \ldots, a_n\}$ *of integers such that* $a_0 < a_1 < \cdots < a_n$ *with* $\gcd(a_2, \ldots, a_n) = 1$*, there exists a positive integer* σ*, non-negative integers* c_1, c_2 *and finite sets* $C_1 \subset [0, c_1 - 2]$ *and* $C_2 \subset [0, c_2 - 2]$ *such that*

$$sA = C_1 \sqcup [c_1, sa_n - c_2] \sqcup (\{sa_n\} - C_2)$$

for all $s \geq \sigma$*.*

Notice that from the above identity of sets we deduce

$$|sA| = a_n s + 1 - (c_1 - |C_1| + c_2 - |C_2|)$$

for $s \geq \sigma$. From Proposition 3.1 we get that

$$\delta(C_A, P_1) + \delta(C_A, P_2) = c_1 - |C_1| + c_2 - |C_2|.$$

Let Γ_1 be the semigroup generated by $a_1, \ldots, a_n$ and let Γ_2 be the semigroup generated by $a_n - a_{n-1}, \ldots, a_n - a_2, a_n$. Notice that Γ_i is the semigroup of the curve singularity germ (C_A, P_i), $i = 1, 2$.

Next, we determine the set C_i and the integer c_i, $i = 1, 2$, in terms of the eventual singular points of the projective curve C_A. Notice that $C_i = \emptyset$ iff P_i is a non-singular point of C_A, $i = 1, 2$.

Proposition 3.4. *Following the notations of Proposition* 3.3*, we have that,* $i = 1, 2$*,*

$$\delta(C_A, P_i) = c_i - |C_i|$$

c_i *is the conductor of* Γ_i *and* $C_i = \Gamma_i \cap [0, c_i - 2]$*.*

Proof. We only have to prove the result for $i = 1$. Notice that if $s \geq \mathrm{Max}\{\sigma, (c_1 + c_2)/a_n\}$ then

$$[c_1, c_1 + a_2] \subset sA.$$

Moreover, since $sA \subset (s+1)A$, $s \geq 1$, we have for all $s \gg 0$ that

$$[c_1, c_1 + a_2] \subset sA \cap [0, c_1 + a_2] = \Gamma_1 \cap [0, c_1 + a_2].$$

From this we get that c_1 is the conductor of Γ_1 and that

$$C_1 = \Gamma_1 \cap [0, c_1 - 2].$$

Example 3.5. We consider the set $A = \{0, 2, 4, 5, 7\}$ of Example 2.8. The decomposition of $5A$ is

$$5A = \{0, 2\} \sqcup [4, 33] \sqcup \{35\}$$

so $c_1 = 4$, $C_1 = \{0, 2\}$, $c_2 = 2$ and $C_2 = \{0\}$. In this case we have $\Gamma_1 = \{0, 2, 4, 5, \ldots\}$, $\Gamma_2 = \{0, 2, 3, \ldots\}$ and $\delta_1 = 2$, $\delta_1 = 1$.

4. Rigid Hilbert Polynomials and Additive Inverse Problems

In this section, we link the inverse problems with the rigidity of Hilbert polynomials and functions, [9,10]. In particular, we will recover several upper and lower bounds of the function $|sA|$ from some properties of the Hilbert function of C_A.

Definition 4.1. Let $H : \mathbb{N} \longrightarrow \mathbb{N}$ be a numerical function asymptotically polynomial, i.e. there exists a polynomial $p(T) \in \mathbb{Z}[T]$ such that $H(s) = p(s)$ for $s \gg 0$. Let $\mathcal{C}$ be a class of graded $\mathbf{k}$-algebras. We say that $p(T)$ is a rigid polynomial for the class $\mathcal{C}$ if for all graded $\mathbf{k}$ algebra D of $\mathcal{C}$ if $\mathrm{HP}_D = p$ then $\mathrm{HF}_D = H$, see [9].

From Lemma 2.1 (2) we get:

Proposition 4.2. [22, Theorems 1.3] *Given a set $A = \{a_1 = 0, a_2, \dots, a_n\}$ of integers such that $a_0 < a_1 < \cdots < a_n$ with $\gcd(a_2, \dots, a_n) = 1$, for all $s \geq 0$ it holds*

$$s(n-1) + 1 \leq |sA| \leq \binom{s+n-1}{s}.$$

Proof. From Lemma 2.1 (2) we deduce the left hand inequality. The right hand inequality follows from Proposition 2.6.

In the next result we get [22, Theorems 1.2, 1.6 and 1.8]; in particular we prove that $p(T) = (n-1)T+1$ is a rigid polynomial for the class of $\mathbf{k}[C_A]$ algebras and that the condition $|sA| = s(n-1)+1$, for some $s \geq 2$, is a rigid property, i.e., determines the whole Hilbert function, see [10].

Theorem 4.3. [22, Theorems 1.2, 1.6, 1.8] *Given a set $A = \{a_1 = 0, a_2, \dots, a_n\}$ of integers such that $a_0 < a_1 < \cdots < a_n$ with $\gcd(a_2, \dots, a_n) = 1$, the following conditions are equivalent:*

1. *$|sA| = s(n-1)+1+o(s)$ for infinitely many s, where $o(s)$ is an arithmetic function such that $\lim_{s\to\infty} o(s) = 0$,*
2. *$|sA| = s(n-1)+1$ for all $s \gg 0$,*
3. *$|sA| = s(n-1)+1$ for some $s \geq 2$,*
4. *$A = \{0, 1, \dots, n-1\}$,*
5. *$|sA| = s(n-1)+1$ for all $s \geq 0$.*

Proof. By Proposition 3.1 we get that (1) implies (2). On the other hand, (2) trivially implies (3).

Assume (3), i.e., $|sA| = s(n-1)+1$ for some $s \geq 2$. Notice that

$$(s-1)A \cup \{(s-1)a_n + a_2, \dots, (s-1)a_n + a_n\} \subset sA$$

and, since $(s-1)a_n$ is the maximum of $(s-1)A$, we have

$$(s-1)A \cap \{(s-1)a_n + a_2, \dots, (s-1)a_n + a_n\} = \emptyset.$$

By Proposition 4.2 we have $|(s-1)A| \geq (s-1)(n-1)+1$, so

$$(s-1)A \cup \{(s-1)a_n + a_2, \dots, (s-1)a_n + a_n\} = sA. \tag{2}$$

We know that $\mathbf{k}[C_A]_s$ has as $\mathbf{k}$-basis the monomials $t^{\alpha}w^s, \alpha \in sA$ and $X_1\mathbf{k}[C_A]_{s-1}$ is generated by $t^{\alpha+a_1}w^s, \alpha \in (s-1)A$. By (2) we have that $(s-1)A + a_1 \subset (s-1)A$ so the $\mathbf{k}$-vector space

$$(\mathcal{B}_A)_s = \frac{\mathbf{k}[C_A]_s}{X_1\mathbf{k}[C_A]_{s-1}}$$

is generated by the cosets of

$$t^{(s-1)a_n+a_i}w^s, \quad i = 2, \dots, n.$$

This fact implies that

$$X_n^{s-1}(\mathcal{B}_A)_1 = (\mathcal{B}_A)_s$$

Since the algebra $\mathcal{B}_A$ is standard we get, multiplying both sides by $(\mathcal{B}_A)_{(r-1)(s-1)}$, that

$$X_n^{(s-1)r}(\mathcal{B}_A)_1 = (\mathcal{B}_A)_{r(s-1)+1}$$

for all $r \geq 1$. Since $\dim_{\mathbf{k}}((\mathcal{B}_A)_t) = n-1$, for $t \gg 0$ we obtain, Proposition 3.2,

$$n - 1 \geq \dim_{\mathbf{k}}(\mathcal{B}_A)_{r(s-1)+1} = a_n$$

for $r \gg 0$. Hence $a_n \leq n-1$ and we get (4).

The remaining implications are easy computations.

Remark 4.4. The curve C_A for $A = \{0, \dots, n-1\}$ is the rational normal curve of $\mathbb{P}_{\mathbf{k}}^{n-1}$, i.e., the curve defined by $(u, v) \mapsto (u^{n-1}, u^{n-2}v, \dots, uv^{n-2}, v^{n-1})$.

Remark 4.5. From Lemma 2.1 (1) we get for a general set A that $|sA| = s(n-1)+1$ for all $s \geq 0$ if and only if A is a n-term arithmetic progression, i.e., $A = q_0 + q_1[0, \dots, n-1]$ for $q_0 \in \mathbb{N}$ and $q_1 \in \mathbb{N} \setminus \{0\}$.

Next we use a result on additive combinatorics in order to improve an upper bound of the Castelnuovo–Mumford regularity of rational projective curves. We first recall the following result of Lev:

Proposition 4.6. [18, Theorem 1] *Given* $A = \{a_1 = 0, a_2, \dots, a_n\}$ *with* $\gcd(a_2, \dots, a_n) = 1$, *it holds:*

$$|sA| - |(s-1)A| \geq \min\{a_n, s(n-2)+1\}$$

for all $s \geq 2$.

In the following result we improve [1, Theorem 2.7], see also [17], where an upper bound of the Castelnuovo–Mumford regularity is given for a monomial projective curve C_A under the hypothesis that A is an arithmetic sequence. We know that

$$\mathrm{HF}_{\mathcal{B}_A}(s) = \mathrm{HF}_A(s) - \mathrm{HF}_A(s-1) = |sA| - |(s-1)A|$$

so last result shows that the Hilbert function of the one-dimensional graded algebra $\mathcal{B}_A$ grows rapidly. This is the key point in the proof of the following result where we assume that $\mathbf{k}[C_A]$ is Cohen–Macaulay. See [3, 15] for several criteria implying the Cohen–Macaulayness of $\mathbf{k}[C_A]$.

Theorem 4.7. *Given* $A = \{a_1 = 0, a_2, \ldots, a_n\}$ *with* $\gcd(a_2, \ldots, a_n) = 1$. *If the two-dimensional ring* $\mathbf{k}[C_A]$ *is Cohen–Macaulay then*

$$\operatorname{reg}(\mathbf{k}[C_A]) \leq \lceil \frac{a_n - 1}{n-2} \rceil$$

Proof. We write $s_0 = \lceil \frac{a_n-1}{n-2} \rceil$. Since $\mathbf{k}[C_A]$ is Cohen–Macaulay we have $r(C_A) + 1 = \operatorname{reg}(\mathbf{k}[C_A])$ and that $\mathcal{B}_A$ is a one-dimensional Cohen–Macaulay ring. Hence we have

$$\mathrm{HF}_{\mathcal{B}_A}(s) \leq a_n$$

for all $s \geq 1$, [21, Chapter XII]. From this inequality and Proposition 4.6, we get

$$s(n-2) + 1 \leq \mathrm{HF}_{\mathcal{B}_A}(s) \leq \min \left\{ a_n, \binom{s+n-2}{s} \right\}$$

for $s = 1, \ldots, s_0 - 1$; and

$$\mathrm{HF}_{\mathcal{B}_A}(s) = a_n$$

for $s \geq s_0$, i.e. $r(\mathcal{B}_A) \leq s_0$. Since $r(C_A) + 1 = r(\mathcal{B}_A)$ we get the claim:

$$\operatorname{reg}(\mathbf{k}[C_A]) = r(C_A) + 1 = r(\mathcal{B}_A) \leq s_0.$$

Example 4.8. (Macaulay's example) In this example we consider the example of a non-singular, non-Cohen–Macaulay monomial projective curve given by Macaulay, [20]. In this case the set is $A = \{0, 1, 3, 4\}$. The monomial curve C_A associated to A is defined by the parameterization $(u, v) \mapsto (u^4, u^3v, uv^3, v^4)$. A computation with Singular [6] give us that $\mathrm{HF}_A = \{1, 4, 9, 13, 17, 21, \ldots\}$ and $\mathrm{HP}_A(s) = 4s + 1$. Since the points P_1, P_2 are non-singular points of C_A, we deduce last identity from Proposition 3.1 as well.

Example 4.9. We consider a especial case of [17, Case A]. Let us consider the set $A = \{0, 7, 8, 9, 10\}$. From [17, Theorem 2.1] we know that $\mathbf{k}[C_A]$ is Cohen–Macaulay and that $r(C_A) = 5$ that agrees with the upper bound of the Theorem 4.7. The defining ideal of C_A is minimally generated by: $x_3^2 - x_2x_4, x_3x_4 - x_2x_5, x_4^2 - x_3x_5, x_2^4 - x_1x_3x_5^2, x_2^3x_3 - x_1x_4x_5^2, x_2^3x_4 - x_1x_5^3$. A straight computation shows

$$\mathrm{HF}_A = \{|sA|, s = 0, 1, \ldots\} = \{1, 5, 12, 22, 32, 42, 52, 62, 72, \ldots\}$$

and the Hilbert polynomial of C_A is $\mathrm{HP}_A = 10s - 8$.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

[1] Bermejo, I., García-Llorente, E., García-Marco, I.: Algebraic invariants of projective monomial curves associated to generalized arithmetic sequences. J. Symbolic Comput. **81**, 1–19 (2017)

[2] Bruns, W., Herzog, J.: Cohen–Macaulay Rings, Revised Edition, Cambridge Studies in Advanced Mathematics, vol. 39. Cambridge University Press, Cambridge (1997)

[3] Cavaliere, M.P., Niesi, G.: On monomial curves and Cohen–Macaulay type. Manuscr. Math. **42**(2–3), 147–159 (1983)

[4] Cavaliere, M.P., Niesi, G.: Sulle equazioni di una curva monomiale proiettiva. Ann. Univ. Ferrara Sec. VII- Sc. Mat. **XXX** (1984)

[5] Colarte-Gómez, L., Elias, J., Miró-Roig, R.M.: Sumsets and Veronese varieties. Collectanea Mathematica (2022). https://doi.org/10.1007/s13348-022-00352-x

[6] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann, Singular 4-3-0—a computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2019). Accessed 2022

[7] Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Springer, New York (1995)

[8] S. Eliahou, E. Mazumdar, Iterated sumsets and Hilbert functions. arxiv:2006.08998v3 (2020)

[9] Elias, J.: Characterization of the Hilbert–Samuel polynomials of curve singularities. Compos. Math. **74**, 135–155 (1990)

[10] Elias, J., Valla, G.: Rigid Hilbert functions. J. Pure Appl. Algebra **71**, 19–41 (1991)

[11] J. I. García-García, D. Marín-Aragón, A. Vigneron-Tenorio, On the ideal of some sumset semigroups. arXiv:math.NT/2102.04100 (2021)

[12] Gruson, L., Lazarsfeld, R., Peskine, C.: On a theorem of Castelnuovo, and the equations defining space curves. Invent. Math. **72**(3), 491–506 (1983)

[13] Hartshorne, R.: Algebraic geometry, Graduate Texts in Mathematics, vol. 52. Springer, Berlin (1997)

[14] Hellus, M., Hoa, L.T., Stückrad, J.: Castelnuovo–Mumford regularity and the reduction number of some monomial curves. Proc. Am. Math. Soc. **138**(1), 27–35 (2010)

[15] Herzog, J., Stamate, D.I.: Cohen–Macaulay criteria for projective monomial curves via Groebner bases. Acta Math. Vietnam **44**, 51–64 (2019)

[16] Khovanskiĭ, A.G.: Sums of finite sets, orbits of commutative semigroups and Hilbert functions. Funktsional. Anal. i Prilozhen. **29**(2), 36–50 (1995). (**95**)

[17] T.T.G. Lam, On the reduction numbers and the Castelnuovo-Mumford regularity of projective monomial curves. arXiv:2103.08099 (2021)

[18] Lev, V.F.: Structure theorem for multiple addition and the Frobenius problem. J. Number Theory **58**(1), 79–88 (1996)

[19] Lvovsky, S.: On inflection points, monomial curves, and hypersurfaces containing projective curves. Math. Ann. **306**(4), 719–735 (1996)

[20] Macaulay, F.S.: The Algebraic Theory of Modular Systems. Cambridge University Press, Cambridge (1916)

[21] Matlis, E.: 1-Dimensional Cohen–Macaulay Rings, L.N.M, vol. 327. Springer, New York (1977)

[22] Nathanson, M.B.: Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics, vol. 165. Springer, New York (1996)

[23] Nathanson, M.B., Ruzsa, I.Z.: Polynomial growth of sumsets in abelian semigroups. J. Théor. Nombres Bordeaux **14**(2), 553–560 (2002)

J. Elias
Departament de Matemàtiques i Informàtica
Universitat de Barcelona (UB)
Gran Via 585
08007 Barcelona
Spain
e-mail: elias@ub.edu

Received: May 14, 2021.
Revised: November 26, 2021.
Accepted: May 25, 2022.