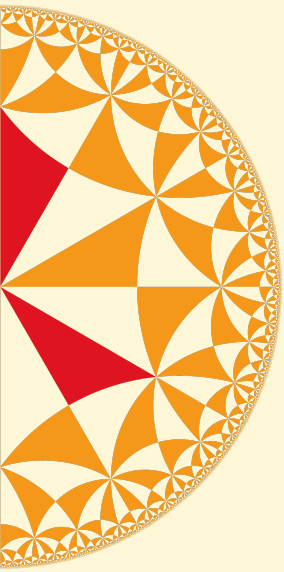
Université Grenoble Alpes



ANNALES DE L'INSTITUT FOURIER

Shalom Eliahou & Eshita Mazumdar

Optimal Bounds on the Growth of Iterated Sumsets in Abelian Semigroups

Article à paraître, mis en ligne le 5 février 2025, 19 p.

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
Article à paraître
Mis en ligne le 5 février 2025.

OPTIMAL BOUNDS ON THE GROWTH OF ITERATED SUMSETS IN ABELIAN SEMIGROUPS

by Shalom ELIAHOU & Eshita MAZUMDAR (*)

Abstract. — We provide optimal upper bounds on the growth of iterated sumsets $hA = A + \cdots + A$ for finite subsets A of abelian semigroups. More precisely, we show that the new upper bounds recently derived from Macaulay's theorem in commutative algebra are best possible, i.e., are actually reached by suitable subsets of suitable abelian semigroups. Our constructions, in a multiplicative setting, are based on certain specific monomial ideals in polynomial algebras and on their deformation into appropriate binomial ideals via Gröbner bases.

Résumé. — Nous obtenons des bornes supérieures optimales sur la croissance des sommes itérées $hA = A + \cdots + A$ de sous-ensembles finis A de semigroupes abéliens. Plus précisément, nous montrons que les nouvelles bornes supérieures récemment obtenues via le Théorème de Macaulay en algèbre commutative sont les meilleures possibles, autrement dit sont effectivement atteintes par des sous-ensembles appropriés de semigroupes abéliens appropriés. Nos constructions, dans un langage multiplicatif, sont basées sur certains idéaux monomiaux spécifiques dans des algèbres de polynômes et sur leurs déformations en idéaux binomiaux convenables via des bases de Gröbner.

1. Introduction

Let A be a nonempty finite subset of an abelian semigroup $(G, +)$. Estimating the growth of the iterated sumsets $hA = \underbrace{A + \cdots + A}_{h}$ as h increases is a core problem in additive combinatorics. Khovanskii [7, 8] showed that $|hA|$ is asymptotically polynomial in h. See also [13, 14]. But not much is known about this polynomial and, for h small, the behavior of $|hA|$ may

Keywords: Additive combinatorics, Plünnecke inequality, Standard graded algebra, Hilbert function, Binomial representation, Lexideal, Gröbner basis.
2020 *Mathematics Subject Classification:* 11P70, 05E40, 11B13, 13P25.
(*) This research was supported in part by the International Centre for Theoretical Sciences (ICTS) in Bangalore during a visit for the program - Workshop on Additive Combinatorics (Code: ICTS/wac2020/02).

wildly vary with A, even when $|A|$ is fixed. A classical estimate, originally derived using graph theory, is given by Plünnecke's inequality [17], namely

$$|hA| \leqslant |iA|^{h/i} \tag{1.1}$$

for all $1 \leqslant i \leqslant h$. See [5, 12, 16, 19] for in-depth treatments of this and related inequalities. We recently improved (1.1) by deriving it from Macaulay's 1927 theorem on the growth of Hilbert functions of standard graded algebras [3]. Macaulay's theorem involves a certain operation $a \mapsto a^{\langle h \rangle}$ on positive integers related to *binomial representations*. In short, if $a = \sum_{j=1}^{h} \binom{a_j}{j}$ with decreasing integers $a_h > \cdots > a_1 \geqslant 0$, then $a^{\langle h \rangle} = \sum_{j=1}^{h} \binom{a_j+1}{j+1}$, and this is well-defined. See Section 2 for more details. Using this notation, here is part of our improvement to (1.1) obtained in [3].

THEOREM 1.1. — *Let A be a nonempty finite subset of an abelian semigroup G. Set $d_h = |hA|$ for all h. Then $d_0 = 1$ and*

$$d_{h+1} \leqslant d_h^{\langle h \rangle} \tag{1.2}$$

for all $h \geqslant 1$.

Example 1.2. — For comparison purposes, let $A \subset \mathbb{Z}$ be a subset such that $|6A| = 1000$. While Plünnecke's inequality (1.1) yields

$$|5A| \geqslant 317, \quad |7A| \leqslant 3162,$$

inequality (1.2) yields the much sharper – and nearly optimal – bounds

$$|5A| \geqslant 511, \quad |7A| \leqslant 1827. \tag{1.3}$$

See Example 2.3 below for the derivation of $|7A| \leqslant 1827$ from $|6A| = 1000$ and (1.2).

Our purpose in this paper is to prove that the upper bounds in Theorem 1.1 are best possible. That is, if $(d_i)_{i \geqslant 0}$ is any sequence of positive integers such that $d_0 = 1$ and $d_{i+1} \leqslant d_i^{\langle i \rangle}$ for all $i \geqslant 1$, then there exists an abelian semigroup G and a subset $A \subseteq G$ such that

$$d_h = |hA| \tag{1.4}$$

for all $h \geqslant 0$. Our construction of such a pair G, A is in multiplicative notation and proceeds as follows. Let $n = d_1$ and $S = K[X_1, \ldots, X_n]$, the n-variable polynomial algebra over a field K with its standard grading. Then G will be a multiplicative submonoid of a quotient ring $R = S/J$, where J is an appropriate graded ideal of S. Denoting by $\pi \colon S \to R$ the quotient map, and setting $x_j = \pi(X_j)$ for $1 \leqslant j \leqslant n$, we consider the subset $A = \{x_1, \ldots, x_n\}$ of R and its h-fold iterated product sets $A^h = A \cdots A$.

The problem then amounts to uncover a suitable ideal J of S so as to realize, for this subset A of S/J, the equality $d_h = |A^h|$ for all h. For an almost sharp realization, a specific monomial ideal $J = L$ establishing the converse part of Macaulay's theorem suffices. A sharp realization is then achieved by deforming L into a binomial ideal $\widehat{L}$ via a Gröbner basis construction so as to preserve the Hilbert function of S/L.

The contents of this paper are as follows. Section 2 provides some background on binomial representations, Macaulay's theorem and lexideals. In Section 3, after recalling basic facts about monomial ideals, we prove that the bounds provided by Theorem 1.1 are almost sharp in an appropriate sense. In Section 4, after recalling basic facts about Gröbner bases, we proceed to prove the full sharpness of these bounds. The analogous problem restricted to abelian groups remains open. This is briefly discussed in the concluding Section 5.

2. Background

Given sets A, B in an abelian semigroup $(G, +)$, their *sumset* is $A+B = \{a + b \mid a \in A, b \in B\}$. For $A = B$, we denote $2A = A + A$, and more generally $hA = \underbrace{A + \cdots + A}_{h}$ for all $h \geqslant 2$. Macaulay's theorem involves a certain operation $a \mapsto a^{\langle h \rangle}$ on $\mathbb{N}$ related to binomial representations, which we now recall.

2.1. Binomial representation

Proposition 2.1. — *Let $h \geqslant 1$ be a fixed integer. Then for any integer $a \geqslant 1$, there are unique integers $a_h > a_{h-1} > \cdots > a_1 \geqslant 0$ such that*

$$a = \sum_{j=1}^{h} \binom{a_j}{j}.$$

Proof. — See e.g. the relevant chapters in [1, 6, 15]. □

This expression is called the *h-binomial representation of a*. Producing it is computationally straightforward: take for a_h the largest integer such that $\binom{a_h}{h} \leqslant a$, and complete that first summand by adding to it the $(h-1)$-binomial representation of $a - \binom{a_h}{h}$. The unicity follows from the classical formula

$$\binom{n+h}{h} = \sum_{j=0}^{h} \binom{n-1+j}{j}. \tag{2.1}$$

Notation 2.2. — Let $a \geqslant h \geqslant 1$ be integers. Let $a = \sum_{j=1}^{h} \binom{a_j}{j}$ be its unique h-binomial representation. We then denote $a^{\langle h \rangle} = \sum_{j=1}^{h} \binom{a_j+1}{j+1}$. We also set $0^{\langle h \rangle} = 0$.

Note that the right-hand side $\sum_{j=1}^{h} \binom{a_j+1}{j+1}$ is a valid $(h+1)$-binomial representation of some positive integer, namely of the integer it sums to.

Example 2.3. — Let $h = 6$ and $a = 1000$. Then

$$1000 = \binom{12}{6} + \binom{8}{5} + \binom{6}{4} + \binom{4}{3} + \binom{2}{2} + \binom{0}{1},$$

whence

$$1000^{\langle 6 \rangle} = \binom{13}{7} + \binom{9}{6} + \binom{7}{5} + \binom{5}{4} + \binom{3}{3} + \binom{1}{2} = 1827.$$

This explains the upper bound in (1.3) using Theorem 1.1.

2.2. Macaulay's theorem

Let $R = \bigoplus_{i \geqslant 0} R_i$ be a standard graded algebra over a field $R_0 = K$. That is, R is a graded commutative algebra which is finitely generated by R_1 as a K-algebra. It follows that $R_i = R_1^i$, the i-fold product set of R_1, and that R_i is finite-dimensional as a vector space over K for all $i \geqslant 0$. The *Hilbert function* of R is the numerical function $i \mapsto d_i = \dim_K R_i$.

Macaulay's classical theorem gives necessary and sufficient conditions for any numerical function $i \mapsto d_i$ to be the Hilbert function of a standard graded algebra [9]. Here it is.

THEOREM 2.4 (Macaulay). — *Let $R = \bigoplus_{i \geqslant 0} R_i$ be a standard graded algebra over a field K, with Hilbert function $d_i = \dim R_i$. Then $d_0 = 1$ and*

$$d_{i+1} \leqslant d_i^{\langle i \rangle} \tag{2.2}$$

for all $i \geqslant 1$. Conversely, let $(d_i)_{i \geqslant 0}$ be a sequence of nonnegative integers such that $d_0 = 1$ and $d_{i+1} \leqslant d_i^{\langle i \rangle}$ for all $i \geqslant 1$. Then there exists a standard graded K-algebra $R = \bigoplus_{i \geqslant 0} R_i$ such that $d_i = \dim R_i$ for all $i \geqslant 0$.

With the notation of Theorem 2.4, note that if $d_i = 0$ for some $i \geqslant 2$, then $d_j = 0$ for all $j \geqslant i$, and this occurs if and only if R is finite-dimensional as a K-vector space. A more detailed version of the converse statement, needed for our present purposes, is given below.

2.3. Lexideals

For the converse part in Theorem 2.4, the desired algebra R may be constructed as a quotient of a polynomial algebra by a suitable monomial ideal (see Section 3.1), and more specifically by a *lexideal* L. Here are some details needed in the sequel.

Let $(d_i)_{i\geqslant 0}$ be a sequence of nonnegative integers such that $d_0 = 1$ and $d_{i+1} \leqslant d_i^{\langle i\rangle}$ for all $i \geqslant 1$. Set $d_1 = n$. In the polynomial algebra $S = K[X_1, \dots, X_n]$ over the field K, with its standard grading given by $\deg(X_j) = 1$ for all j, we endow the set $\mathcal{M}$ of monomials in S with the *graded lexicographic order* relative to $X_1 > \cdots > X_n$. That is, for $u = \prod_j X_j^{a_j}, v = \prod_j X_j^{b_j} \in \mathcal{M}$, we set $u > v$ if either $\deg(u) > \deg(v)$, or else $\deg(u) = \deg(v)$ and u comes before v lexicographically, i.e. the first nonzero difference $a_j - b_j$ is positive.

Example 2.5. — With this ordering, the monomials of degree 2 in $K[X_1, X_2, X_3]$ are ordered as follows:

$$X_1^2 > X_1X_2 > X_1X_3 > X_2^2 > X_2X_3 > X_3^2.$$

For all $i \geqslant 0$, we denote by $\mathcal{M}_i$ the set of monomials of degree i in S. Thus $\mathcal{M}_0 = \{1\}$, $\mathcal{M}_1 = \{X_1, \dots, X_n\}$ and $\mathcal{M}_i = \mathcal{M}_1^i$, the i-fold product set of $\mathcal{M}_1$.

DEFINITION 2.6. — *A* lexsegment *is a subset C of $\mathcal{M}_i$ for some $i \geqslant 1$ such that $C = \{u \in \mathcal{M}_i \mid u \geqslant v\}$ for some $v \in \mathcal{M}_i$. A* lexideal *L in S is a monomial ideal such that $L \cap \mathcal{M}_i$ is a lexsegment for all $i \geqslant 1$ such that $L \cap \mathcal{M}_i \neq \emptyset$.*

It is easy to verify that if $C \subseteq \mathcal{M}_i$ is a lexsegment, then $\mathcal{M}_1C \subseteq \mathcal{M}_{i+1}$ is a lexsegment as well, where $\mathcal{M}_1C = \{X_ju \mid u \in C, 1 \leqslant j \leqslant n\}$. The converse in Macaulay's theorem may be expressed in the following more detailed form. See e.g. [1, 6, 11, 15].

THEOREM 2.7. — *Let $(d_i)_{i\geqslant 0}$ be a sequence in $\mathbb{N}$ such that $d_0 = 1$ and $d_{i+1} \leqslant d_i^{\langle i\rangle}$ for all $i \geqslant 1$. Set $n = d_1$. There exists a lexideal L in $S = K[X_1, \dots, X_n]$ such that for $R = S/L = \bigoplus_{i\geqslant 0} R_i$, we have $d_i = \dim R_i$ for all $i \geqslant 0$.*

This result is constructive, implying in turn that our results, namely Theorems 3.5 and 4.12, are constructive as well. A concrete illustration is given in the extended Example 3.6 below. One key point is the following intimate link between lexsegments and the numerical operation $a \mapsto a^{\langle i\rangle}$.

LEMMA 2.8. — *Let $C \subset \mathcal{M}_i$ be a lexsegment such that $|\mathcal{M}_i \setminus C| = a$. Then $|\mathcal{M}_{i+1} \setminus \mathcal{M}_1 C| = a^{\langle i \rangle}$.*

2.4. An additive version of Macaulay's theorem

Consider the abelian semigroup $G = \mathbb{N}^n$. For $1 \leqslant i \leqslant n$, denote by e_i the ith canonical basis element of G, i.e. $e_i = (\delta_{ij})_{1 \leqslant j \leqslant n}$ where δ_{ij} is the Kronecker symbol. Let $B = \{e_1, \ldots, e_n\} \subset G$. Note that for all $h \geqslant 1$, the h-fold iterated sumset hB consists of all elements in G whose coordinate sum is equal to h. Of course, G is canonically isomorphic to the set $\mathcal{M}$ of monomials in $K[X_1, \ldots, X_n]$, viewed as a multiplicative abelian semigroup. We order G by transfering the graded lexicographic order $\leqslant$ on $\mathcal{M}$ via the canonical isomorphism induced by $X_j \leftrightarrow e_j$ for all j. The following statement is equivalent to Macaulay's Theorem 2.4.

THEOREM 2.9. — *Let $G = \mathbb{N}^n$ and $B = \{e_1, \ldots, e_n\} \subset G$. For all $h \geqslant 1$ and all subsets $A \subseteq hB$, we have*

$$|A + B| \geqslant |A^{lex} + B|,$$

where $A^{lex} \subseteq hB$ denotes the unique lexsegment of cardinality $|A^{lex}| = |A|$.

Proof. — See [11, Theorem 4.1] for an analogous statement in terms of monomial subspaces, shown there to be equivalent to Theorem 2.4. □

Macaulay's theorem is fundamental in commutative algebra and algebraic geometry, and since the 1970's in combinatorics too, thanks to the pioneering work on polytopes by McMullen [10] and Stanley [18] among others. The additive version given by Theorem 2.9 shows that Macaulay's theorem squarely belongs to additive combinatorics as well.

3. An Almost Sharp Realization

We show here that if $(d_i)_{i \geqslant 0}$ is a sequence of positive integers satisfying $d_0 = 1$ and

$$1 \leqslant d_{i+1} \leqslant d_i^{\langle i \rangle} \tag{3.1}$$

for all $i \geqslant 1$, then there exists an abelian semigroup G and a subset $A \subseteq G$ such that

$$d_h \leqslant |hA| \leqslant d_h + 1 \tag{3.2}$$

for all $h \geqslant 0$. Our proof of this almost sharp realization relies on the sufficiency condition in Macaulay's theorem, and more specifically on Theorem 2.7. To proceed, we need a few relevant facts concerning monomial ideals.

3.1. Monomial ideals

Let $S = K[X_1, \dots, X_n]$ be the n-variable polynomial algebra over the field K, endowed with its standard grading $S = \bigoplus_{i \geqslant 0} S_i$ induced by $\deg(X_j) = 1$ for all j. As earlier, we denote by $\mathcal{M}$ the set of monomials in S and by $\mathcal{M}_i = \mathcal{M} \cap S_i$ the subset of monomials of degree i for all $i \geqslant 0$.

A *monomial ideal* in $S = K[X_1, \dots, X_n]$ is an ideal J of S generated by monomials. Of course, J is a graded ideal, so that $J = \bigoplus_{i \geqslant 0} J_i$, where $J_i = J \cap S_i$. Macaulay proved that for every graded ideal I of S, there exists a monomial ideal J of S such that S/I and S/J have the same Hilbert function. See Proposition 4.2 below.

LEMMA 3.1. — *Let $J \subset S$ be a monomial ideal. Let $f \in S$. Then $f \in J$ if and only if every monomial with a nonzero coefficient in f belongs to J.*

Proof. — Easily follows from the fact that J is spanned by monomials in $\mathcal{M}$ and that $\mathcal{M}$ is a K-basis of S. □

PROPOSITION 3.2 (Macaulay, [9]). — *Let $J \subset S$ be a monomial ideal. Let $\pi\colon S \to S/J$ be the quotient map. Then the family $\mathcal{F} = \{\pi(u) \mid u \in \mathcal{M} \setminus J\}$ is a K-basis of S/J.*

Proof. — The family $\mathcal{F}$ spans S/J, since $\mathcal{M}$ spans S and $\pi(\mathcal{M} \cap J) = \{0\}$. And $\mathcal{F}$ is free, for if $f = \sum_{u \in \mathcal{M} \setminus J} \lambda_u u$ and $\pi(f) = 0$, then $f \in \ker(\pi) = J$. Lemma 3.1 then implies $\lambda_u = 0$ for all $u \in \mathcal{M} \setminus J$, i.e. $f = 0$. □

Even though we have already encountered iterated product sets above, we formally recall the notation here.

Notation 3.3. — Let G be an abelian semigroup in multiplicative notation. For any subset $A \subseteq G$, we denote by $A^h = \underbrace{A \cdots A}_{h}$ its h-fold iterated product set.

We need one more auxiliary result.

PROPOSITION 3.4. — *Let J be a monomial ideal in S. Let $R = S/J = \bigoplus_{i\geqslant 0} R_i$ and let $\pi\colon S \to R = S/J$ be the quotient map. Let $x_j = \pi(X_j)$ for all j and set $A = \{x_1, \ldots, x_n\} \subset R$. Then for all $h \geqslant 1$, we have*

$$|A^h| = \begin{cases} \dim R_h & \text{if } J_h = \{0\}, \\ \dim R_h + 1 & \text{if not,} \end{cases} \tag{3.3}$$

where $J_i = S_i \cap J$ for all i.

Proof. — We have $J = \bigoplus_{i\geqslant 0} J_i$, and J_i has for vector subspace basis $\mathcal{M}_i \cap J$ for all $i \geqslant 0$. Since $A = \pi(\mathcal{M}_1)$, and since $\mathcal{M}_h = \mathcal{M}_1^h$ for all $h \geqslant 1$, we have

$$A^h = \pi(\mathcal{M}_h) \tag{3.4}$$

for all $h \geqslant 1$. Since $J = \ker(\pi)$, we have

$$\pi(\mathcal{M}_h) = \begin{cases} \pi(\mathcal{M}_h \setminus J_h) & \text{if } \mathcal{M}_h \cap J_h = \emptyset, \\ \pi(\mathcal{M}_h \setminus J_h) \sqcup \{0\} & \text{if not.} \end{cases} \tag{3.5}$$

It follows from Proposition 3.2 that

$$\dim R_h = |\mathcal{M}_h \setminus J_h| = |\pi(\mathcal{M}_h \setminus J_h)|. \tag{3.6}$$

Combining (4.8), (3.5) and (3.6) yields the claimed formula (3.3). □

3.2. First construction

Combining the above results with the sufficiency part of Macaulay's theorem, we obtain an almost sharp realization of d_h as $|hA|$ for some subset A of some abelian semigroup.

THEOREM 3.5. — *Let $(d_i)_{i\geqslant 0}$ be a sequence of nonnegative integers such that $d_0 = 1$ and $d_{i+1} \leqslant d_i^{\langle i\rangle}$ for all $i \geqslant 1$. Then there exists an abelian semigroup G and $A \subseteq G$ such that $d_h \leqslant |hA| \leqslant d_h + 1$ for all $h \geqslant 0$.*

Proof. — Set $n = d_1$. By Macaulay's theorem, there exists a standard graded algebra $R = \bigoplus_{i\geqslant 0} R_i$ such that $d_i = \dim R_i$ for all $i \geqslant 0$. By Theorem 2.7, one may take $R = S/L$, where $S = K[X_1, \ldots, X_n]$ with its standard grading, and L is a suitable lexideal in S. Let $\pi\colon S \to R$ be the quotient map. For the required abelian semigroup, in multiplicative notation, we may take $G = (R, \cdot)$ or, more economically, $G = \pi(\mathcal{M})$. Set $x_j = \pi(X_j)$ for all j and $A = \{x_1, \ldots, x_n\} \subset G$. It then follows from Proposition 3.4 that $|A^h| \in \{d_h, d_h + 1\}$ for all $h \geqslant 0$, as desired. □

Given a sequence $(d_i)_{i\geqslant 0}$ satisfying the conditions of Theorem 3.5, the following extended example shows how to explicitly construct a pair G, A satisfying the conclusion of this theorem.

Example 3.6. — Let $(d_0, d_1, d_2, d_3, d_4, d_5, \dots) = (1, 5, 13, 25, 42, 63, \dots)$. Then $d_{i+1} \leqslant d_i^{\langle i\rangle}$ for $1 \leqslant i \leqslant 4$. Indeed, we have

$$d_1 = 5 = \binom{5}{1} \longrightarrow d_1^{\langle 1\rangle} = \binom{6}{2} = 15;$$

$$d_2 = 13 = \binom{5}{2} + \binom{3}{1} \longrightarrow d_2^{\langle 2\rangle} = \binom{6}{3} + \binom{4}{2} = 26;$$

$$d_3 = 25 = \binom{6}{3} + \binom{3}{2} + \binom{2}{1} \longrightarrow d_3^{\langle 3\rangle} = \binom{7}{4} + \binom{4}{3} + \binom{3}{2} = 42;$$

$$d_4 = 42 = \binom{7}{4} + \binom{4}{3} + \binom{3}{2} \longrightarrow d_4^{\langle 4\rangle} = \binom{8}{5} + \binom{5}{4} + \binom{4}{3} = 65.$$

Hence the differences $d_i^{\langle i\rangle} - d_{i+1}$ assume the following nonnegative values, as claimed:

$$d_1^{\langle 1\rangle} - d_2 = 2, \quad d_2^{\langle 2\rangle} - d_3 = 1, \quad d_3^{\langle 3\rangle} - d_4 = 0, \quad d_4^{\langle 4\rangle} - d_5 = 2. \tag{3.7}$$

Set $n = d_1 = 5$ and $S = K[X_1, \dots, X_5]$. We now use (3.7) to construct a lexideal $L \subset S$ such that the quotient $R = S/L = \bigoplus_{i\geqslant 0} R_i$ satisfies $\dim R_i = d_i$ for $0 \leqslant i \leqslant 5$. To do so, it suffices to exhibit a minimal system of monomial generators $\mathcal{G}$ satisfying the following requirements:

(1) $|\mathcal{G} \cap \mathcal{M}_{i+1}| = d_i^{\langle i\rangle} - d_{i+1}$ for all $1 \leqslant i \leqslant 4$,
(2) the resulting ideal $L = (\mathcal{G})$ is a lexideal.

The first condition arises from Lemma 2.8. Using these constraints as a construction tool, we obtain the following solution:

$$\mathcal{G} = \{X_1^2, X_1X_2, X_1X_3^2, X_1X_3X_4^3, X_1X_3X_4^2X_5\}.$$

As required, we do have $|\mathcal{G}\cap\mathcal{M}_2| = d_1^{\langle 1\rangle} - d_2 = 2$, $|\mathcal{G}\cap\mathcal{M}_3| = 1$, $|\mathcal{G}\cap\mathcal{M}_4| = 0$, $|\mathcal{G}\cap\mathcal{M}_5| = 2$, and $L\cap\mathcal{M}_i$ is a lexsegment for all $i \geqslant 2$. Let $\pi\colon S \to R = S/L$ be the quotient map. Again, the sought-for semigroup may be taken as $G = (R, \cdot)$, or more simply $G = \pi(\mathcal{M})$. Set $x_j = \pi(X_j)$ for $1 \leqslant j \leqslant 5$, and $A = \{x_1, \dots, x_5\} \subset G$. Then

$$|A| = d_1, \quad |A^h| = d_h + 1$$

for all $2 \leqslant h \leqslant 5$, as desired. For instance, for $h = 2$ we have $x_1^2 = x_1x_2 = 0$ in G, and

$$A^2 = \{0\} \sqcup \{x_1x_3, x_1x_4, x_1x_5, x_2^2, x_2x_3, x_2x_4, x_2x_5, x_3^2, x_3x_4, x_3x_5, x_4^2, x_4x_5, x_5^2\},$$

so that $|A^2| = 14 = d_2 + 1$.

4. Main Result

In order to show that the bounds given by Theorem 1.1 are best possible, we now aim for a sharp realization. That is, given any sequence $(d_i)_{i\geqslant 0}$ of positive integers satisfying $d_0 = 1$ and

$$1 \leqslant d_{i+1} \leqslant d_i^{\langle i \rangle}$$

for all $i \geqslant 1$, we shall construct an abelian semigroup G and a subset $A \subseteq G$ such that

$$d_h = |hA|$$

for all $h \geqslant 0$. Note that the condition $d_h \geqslant 1$ for all h is necessary here, since $|hA| \geqslant 1$ for any nonempty subset A of a semigroup $(G, +)$. To that end, we shall deform the lexideal $L \subset S$, used above for our almost sharp realization, into a binomial ideal $\widehat{L} \subset S$ with the same Hilbert function as L, i.e. such that $\dim \widehat{L} \cap S_i = \dim L \cap S_i =$ for all i. The latter constraint can be achieved with a Gröbner basis construction.

4.1. Gröbner bases

We recall here the few relevant facts on Gröbner bases needed for our constructions, and refer to [4, 6, 15] for more details. Again, let $\mathcal{M}$ denote the set of monomials in $K[X_1, \ldots, X_n]$. The notion of Gröbner basis is relative to a given ordering of $\mathcal{M}$. Here we only consider the graded lexicographic ordering $\leqslant$ on $\mathcal{M}$ relative to $X_1 > \cdots > X_n$ as defined in Section 2.3.

Denote $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$. For any $u, v \in \mathcal{M}$, let $\gcd(u, v) \in \mathcal{M}$ denote their greatest common divisor. We further need the following notation and definitions.

Notation 4.1. — For a nonzero polynomial $f \in K[X_1, \ldots, X_n]$, we denote by $\mathrm{in}(f) \in \mathcal{M}$ its *leading monomial* with respect to the given ordering on $\mathcal{M}$, and by $\mathrm{lc}(f) \in K^*$ its *leading coefficient*, i.e. the coefficient of $\mathrm{in}(f)$ in f. The *leading term* of f is

$$\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{in}(f).$$

For a proper ideal $I \subsetneq K[X_1, \ldots, X_n]$, we denote by $\mathrm{in}(I)$ the monomial ideal generated by the set $\{\mathrm{in}(f) \mid f \in I \setminus \{0\}\}$.

The importance of the ideal $\mathrm{in}(I)$ stems from the following property.

PROPOSITION 4.2 (Macaulay, [9]). — *Let I be a proper graded ideal in $S = K[X_1, \dots, X_n]$. Then the graded algebras*

$$S/I \text{ and } S/\mathrm{in}(I)$$

have the same Hilbert function.

DEFINITION 4.3. — *A finite set $\{g_1, \dots, g_s\} \subset K[X_1, \dots, X_n] \setminus K$ of nonconstant polynomials is a* Gröbner basis *if, for any nonzero element f of the ideal $I = (g_1, \dots, g_s)$, we have $\mathrm{in}(f) \in (\mathrm{in}(g_1), \dots, \mathrm{in}(g_s))$; equivalently, $\mathrm{in}(f)$ is divisible by $\mathrm{in}(g_i)$ for some $1 \leqslant i \leqslant s$. We then say that $\{g_1, \dots, g_s\}$ is a Gröbner basis of I.*

Note that every proper ideal $I \subsetneq K[X_1, \dots, X_n]$ admits a Gröbner basis; this follows from the fact that $K[X_1, \dots, X_n]$ is noetherian, whence $\mathrm{in}(I)$ is finitely generated. A key property of Gröbner bases is the following direct consequence of Proposition 4.2.

COROLLARY 4.4. — *Let $\{g_1, \dots, g_s\} \subset K[X_1, \dots, X_n] \setminus K$ be a Gröbner basis, with g_j homogeneous for all j. Then the graded algebras*

$$S/(g_1, \dots, g_s) \text{ and } S/(\mathrm{in}(g_1), \dots, \mathrm{in}(g_s))$$

have the same Hilbert function.

Proof. — Let $I = (g_1, \dots, g_s)$. Then I is a graded ideal since the g_j are homogeneous for all j. Moreover, $\mathrm{in}(I) = (\mathrm{in}(g_1), \dots, \mathrm{in}(g_s))$ since $\{g_1, \dots, g_s\}$ is a Gröbner basis by hypothesis. We conclude with Proposition 4.2. □

Buchberger developed an algorithm to construct Gröbner bases for any proper ideal of $K[X_1, \dots, X_n]$, including a stopping criterion to recognize them. Here are the relevant details for the sequel.

DEFINITION 4.5. — *Let $f, g, h \in K[X_1, \dots, X_n]$ with f, h nonzero. We say that f* properly reduces to g with respect to h *if $\mathrm{in}(h)$ divides $\mathrm{in}(f)$ in $\mathcal{M}$, and if g is obtained by eliminating the leading term of f with that of h, i.e.*

$$g = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(h)} h.$$

We write $f \xrightarrow{h} g$ when this occurs. In particular, if $f \xrightarrow{h} g$, then either $g = 0$ or else $\mathrm{in}(g) < \mathrm{in}(f)$.

DEFINITION 4.6. — *More generally, let $H \subset K[X_1, \dots, X_n]$ be a set of nonconstant polynomials, and let $f, g \in K[X_1, \dots, X_n]$ with $f \neq 0$. We say that f* properly reduces to *g with respect to H, and we write $f \xrightarrow{H} g$, if there is a sequence of proper reductions from f to g of the form*

$$f = f_0 \xrightarrow{h_1} f_1 \xrightarrow{h_2} \dots \xrightarrow{h_\ell} f_\ell = g$$

with $h_1, \dots, h_\ell \in H$.

A key ingredient in Buchberger's algorithm is the notion of *S-polynomial*.

DEFINITION 4.7. — *Let $f, g \in K[X_1, \dots, X_n] \setminus K$. Let*

$$v = \gcd(\mathrm{in}(f), \mathrm{in}(g)) \in \mathcal{M}.$$

The S-polynomial *of f, g is*

$$S(f, g) = \frac{\mathrm{lt}(g)}{v} f - \frac{\mathrm{lt}(f)}{v} g.$$

THEOREM 4.8 (Buchberger's criterion). — *A set $H = \{f_1, \dots, f_r\}$ of polynomials in $K[X_1, \dots, X_n] \setminus K$ is a Gröbner basis if and only if $S(f_i, f_j) \xrightarrow{H} 0$ for all $1 \leqslant i < j \leqslant r$.*

4.2. A Gröbner basis of binomials

We construct here a Gröbner basis made of certain homogeneous binomials, i.e. of differences $u - v$ of monomials u, v of same degree. As above, $\mathcal{M}$ is the set of monomials in $K[X_1, \dots, X_n]$, endowed with the graded lexicographic order $\leqslant$, and $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$.

Notation 4.9. — For $u \in \mathcal{M}^*$, we denote by $\min(u)$ the smallest index $i \geqslant 1$ such that X_i divides u, and by $\max(u)$ the largest index $j \geqslant 1$ such that X_j divides u.

For instance, for $u = X_2^4 X_3 X_5^3$, we have $\min(u) = 2$ and $\max(u) = 5$.

DEFINITION 4.10. — *Let $\varphi \colon \mathcal{M}^* \to \mathcal{M}^*$ be the map defined for all $u \in \mathcal{M}^*$ by*

$$\varphi(u) = u X_n / X_{\min(u)}.$$

Note that if $\min(u) < n$, then $u > \varphi(u)$ and hence $\mathrm{in}(u - \varphi(u)) = u$. For instance, for $u = X_2^4X_3X_5^3$ again, taken here as an element of $K[X_1, \dots, X_5]$, i.e. with $n = 5$, we have

$$\varphi(u) = X_2^3X_3X_5^4$$

and, as stated, $X_2^4X_3X_5^3 > X_2^3X_3X_5^4$ in $\mathcal{M}_5$.

PROPOSITION 4.11. — *Let $u_1, \dots, u_r \in \mathcal{M}^*$ satisfy $\min(u_i) \leqslant n-1$ for all i. Then the set of binomials*

$$H_r = \{u_i - \varphi(u_i) \mid 1 \leqslant i \leqslant r\}$$

is a Gröbner basis.

Proof. — The case $r = 1$ is trivial. Let $r = 2$, and let $u_1, u_2 \in \mathcal{M}^*$ satisfy $\min(u_1), \min(u_2) \leqslant n-1$. With Theorem 4.8 in mind, we will show that

$$S(u_1 - \varphi(u_1), u_2 - \varphi(u_2)) \xrightarrow{H_2} 0. \tag{4.1}$$

Without loss of generality, we may assume $u_1 > u_2$ and $\min(u_1) = 1$. Let $i = \min(u_2)$. Thus $i \in \{1, \dots, n-1\}$ by hypothesis. Write $u_1 = X_1v_1$ and $u_2 = X_iv_2$ with $v_1, v_2 \in \mathcal{M}$ and $\min(v_1) \geqslant 1$, $\min(v_2) \geqslant i$. Then

$$\begin{aligned} u_1 - \varphi(u_1) &= (X_1 - X_n)v_1, \\ u_2 - \varphi(u_2) &= (X_i - X_n)v_2. \end{aligned}$$

Let now $v = \gcd(v_1, v_2) \in \mathcal{M}$.

- Assume first $i = 1$. Then $X_1v = \gcd(u_1, u_2)$, and we have

$$\begin{aligned} S(u_1 - \varphi(u_1), u_2 - \varphi(u_2)) &= S((X_1 - X_n)v_1, (X_1 - X_n)v_2) \\ &= (X_1 - X_n)v_1v_2/v - (X_1 - X_n)v_2v_1/v \\ &= 0. \end{aligned}$$

- Assume now $i \geqslant 2$. Then

$$\begin{aligned} S(u_1 - \varphi(u_1), u_2 - \varphi(u_2)) &= S((X_1 - X_n)v_1, (X_i - X_n)v_2) \\ &= (X_1 - X_n)X_iv_1v_2/v - (X_i - X_n)X_1v_2v_1/v \\ &\xrightarrow{u_1 - \varphi(u_1)} X_1X_nv_2v_1/v - X_iX_nv_1v_2/v \\ &\xrightarrow{u_2 - \varphi(u_2)} X_n^2v_2v_1/v - X_n^2v_1v_2/v \\ &= 0. \end{aligned}$$

By Buchberger's criterion in Theorem 4.8, the set H_2 is a Gröbner basis, as desired. For $r \geqslant 3$, the analog of formula (4.1) remains valid for any pair $u_i - \varphi(u_i), u_j - \varphi(u_j)$ with $1 \leqslant i < j \leqslant r$. Hence, by Buchberger's criterion again, the set H_r is a Gröbner basis, and the proof is complete. □

4.3. Sharp realization

We are now in a position to prove our main result in this paper.

THEOREM 4.12. — *Let $(d_i)_{i\geqslant 0}$ be a sequence of positive integers such that $d_0 = 1$ and $1 \leqslant d_{i+1} \leqslant d_i^{\langle i\rangle}$ for all $i \geqslant 1$. Then there exists an abelian semigroup G and $A \subseteq G$ such that $d_h = |hA|$ for all $h \geqslant 0$.*

Proof. — Set $n = d_1$ and $S = K[X_1, \ldots, X_n] = \bigoplus_{i\geqslant 0} S_i$ with its standard grading. By Theorem 2.7, there exists a lexideal $L \subseteq S$ such that, for $R = S/L = \bigoplus_{i\geqslant 0} R_i$, we have

$$d_i = \dim R_i$$

for all $i \geqslant 0$. Denoting $L_i = L \cap S_i$, we have $L = \bigoplus_{i\geqslant 0} L_i$ and $R_i = S_i/L_i$ for all i. In particular, since $n = d_1 = \dim R_1$, we have $L_1 = \{0\}$.

Claim 1. — For all $u \in \mathcal{M} \cap L$, we have

$$\min(u) \leqslant n - 1. \tag{4.2}$$

For otherwise, let $u \in \mathcal{M} \cap L$ be such that $\min(u) = n$. Therefore $u = X_n^k$ for some $k \geqslant 1$. This implies $L \supset \mathcal{M}_k$ since $X_n^k = \min(\mathcal{M}_k)$ and $L \cap \mathcal{M}_k$ is a lexsegment. Hence $R_k = \{0\}$, contradicting $d_k \geqslant 1$. This proves the claim.

Let $\mathcal{G} \subset \mathcal{M} \cap L$ be the minimal system of monomial generators of L, so that $L = (\mathcal{G})$. Of course $\mathcal{G}$ is finite and consists of all monomials in L which are not the product of two monomials in L. Denote $\mathcal{G}_i = \mathcal{G} \cap S_i = \mathcal{G} \cap \mathcal{M}_i$ for all $i \geqslant 1$. We have $\mathcal{G}_1 = \emptyset$ since $L_1 = \{0\}$.

Since L is a lexideal, it is a *stable* monomial ideal. As such, its minimal system of generators $\mathcal{G}$ may be characterized as follows [2]: for all $u \in \mathcal{M} \cap L$, there is a unique monomial factorisation

$$u = vw$$

with $v, w \in \mathcal{M}$ such that

$$\begin{cases} v \in \mathcal{G}, \\ \max(v) \leqslant \min(w). \end{cases} \tag{4.3}$$

Using the map $\varphi\colon \mathcal{M}^* \to \mathcal{M}^*$ of Definition 4.10, denote

$$\widehat{\mathcal{G}} = \{u - \varphi(u) \mid u \in \mathcal{G}\}.$$

It follows from (4.2) and the definition of φ that $u > \varphi(u)$ for all $u \in \mathcal{G}$. Set $\widehat{L} = (\widehat{\mathcal{G}})$, the homogeneous binomial ideal of S generated by $\widehat{\mathcal{G}}$. Denote by

$$\pi\colon S \longrightarrow R = S/L = \bigoplus_{i\geqslant 0} R_i,$$
$$\widehat{\pi}\colon S \longrightarrow \widehat{R} = S/\widehat{L} = \bigoplus_{i\geqslant 0} \widehat{R}_i$$

the respective quotients and quotient maps of S. Applying Proposition 4.11 to $\widehat{\mathcal{G}}$, as allowed by (4.2), it follows that $\widehat{\mathcal{G}}$ is a Gröbner basis of $\widehat{L}$. Therefore, by Corollary 4.4, the Hilbert functions of L and $\widehat{L}$ are the same. That is, for all $i \geqslant 0$, we have

$$\dim(\widehat{R}_i) = \dim(R_i) = d_i. \tag{4.4}$$

Claim 2. — For all $u \in \mathcal{M} \cap L$, we have

$$\varphi(u) \equiv u \bmod \widehat{L}. \tag{4.5}$$

Indeed, consider the unique monomial decomposition $u = vw$ with $v \in \mathcal{G}$ provided by (4.3). Hence $\min(u) = \min(v)$, implying

$$\varphi(u) = \varphi(vw) = \varphi(v)w$$

by definition of φ. Therefore

$$u - \varphi(u) = vw - \varphi(vw) = vw - \varphi(v)w = (v - \varphi(v))w.$$

Since $v - \varphi(v) \in \widehat{\mathcal{G}}$, this proves (4.5).

Claim 3. — For all $u \in \mathcal{M} \cap L$, there is a least exponent $\ell \geqslant 1$ such that

$$\varphi^\ell(u) \in \mathcal{M} \setminus L, \tag{4.6}$$

where $\varphi^\ell = \underbrace{\varphi \circ \cdots \circ \varphi}_{\ell}$. Indeed, at each application of φ, the exponent of X_n increases by 1 while the degree remains constant. And $X_n^k \in \mathcal{M} \setminus L$ for all k by (4.2). This proves the claim.

Claim 4. — We have $\widehat{\pi}(\mathcal{M}) = \widehat{\pi}(\mathcal{M} \setminus L)$. That is, for all $u \in \mathcal{M}$, there exists $w \in \mathcal{M} \setminus L$ such that

$$u \equiv w \bmod \widehat{L}. \tag{4.7}$$

Indeed, if $u \in \mathcal{M} \setminus L$, take $w = u$. If $u \in \mathcal{M} \cap L$, let $w = \varphi^\ell(u) \in \mathcal{M} \setminus L$ with ℓ minimal as given by (4.6). We have

$$u - \varphi^\ell(u) = \sum_{i=0}^{\ell-1} (\varphi^i(u) - \varphi^{i+1}(u)).$$

By minimality of ℓ with respect to (4.6), we have $\varphi^i(u) \in \mathcal{M} \cap L$ for all $0 \leqslant i \leqslant \ell - 1$. Hence, since $v \equiv \varphi(v) \bmod \widehat{L}$ for all $v \in \mathcal{M} \cap L$ by (4.5), it follows that

$$u \equiv \varphi^\ell(u) \bmod \widehat{L}.$$

This shows that (4.7) holds with $w = \varphi^\ell(u) \in \mathcal{M} \setminus L$, as desired. This settles the claim.

Finally, let $A = \widehat{\pi}(\mathcal{M}_1) \subset \widehat{R}$. Then for all $h \geqslant 0$, we have

$$A^h = \widehat{\pi}(\mathcal{M}_h) = \widehat{\pi}(\mathcal{M}_h \setminus L_h) \tag{4.8}$$

since $\mathcal{M}_h = \mathcal{M}_1^h$. Moreover, $\widehat{\pi}(\mathcal{M} \setminus L)$ is a K-basis of $\widehat{R}$. This follows from the facts that $\widehat{\pi}(\mathcal{M} \setminus L)$ spans $\widehat{R}$, that $\pi(\mathcal{M} \setminus L)$ is a K-basis of R by Proposition 3.2, and by (4.4). We conclude that

$$|A^h| = \dim(\widehat{R}_h) = \dim(R_h) = d_h$$

for all $h \geqslant 0$, as desired. □

Example 4.13. — Revisiting Example 3.6, let $(d_0, d_1, d_2, d_3, d_4, d_5, \dots) = (1, 5, 13, 25, 42, 63, \dots)$. Let $S = K[X_1, \dots, X_5]$, and let $L \subset S$ be the lexideal with minimal monomial generating set

$$\mathcal{G} = \{X_1^2, X_1X_2, X_1X_3^2, X_1X_3X_4^3, X_1X_3X_4^2X_5\}.$$

Using the map φ from Definition 4.10, let $\widehat{\mathcal{G}} = \{u - \varphi(u) \mid u \in \mathcal{G}\}$. Then

$$\widehat{\mathcal{G}} = \{X_1^2 - X_1X_5, X_1X_2 - X_2X_5, X_1X_3^2 - X_3^2X_5, X_1X_3X_4^3 - X_3X_4^3X_5, \\ X_1X_3X_4^2X_5 - X_3X_4^2X_5^2\}.$$

This is a Gröbner basis by Proposition 4.11. Let $\widehat{L} = (\widehat{\mathcal{G}})$. Denote by $\widehat{\pi}\colon S \to \widehat{R} = S/\widehat{L}$ the quotient map, set $x_j = \widehat{\pi}(X_j)$ for $1 \leqslant j \leqslant 5$, and $A = \{x_1, \dots, x_5\} \subset \widehat{R}$. Then by Theorem 4.12, we have

$$|A^h| = d_h$$

for all $0 \leqslant h \leqslant 5$, as desired.

5. Concluding Remarks

Theorem 4.12 provides optimal upper bounds on the growth of iterated sumsets relative to all abelian semigroups. However, restricted to abelian *groups* only, the analogous problem remains open.

As recalled in Theorem 1.1, we have shown in [3] that the arithmetic conditions $d_{i+1} \leqslant d_i^{\langle i \rangle}$ for all i are satisfied by all sequences $(d_i)_{i \geqslant 0}$ occuring as $d_h = |hA|$ for all h, with A a nonempty finite subset of an abelian semigroup G. But the arithmetic conditions $d_{i+1} \leqslant d_i^{\langle i \rangle}$ for all i do not imply that this sequence is nondecreasing. Yet relative to groups, and in contrast with semigroups in general, monotonicity is a necessary condition, since

$$|hA| \leqslant |(h+1)A| \tag{5.1}$$

for all finite subsets A of groups and for all h. On the other hand, this monotonicity condition is far from being sufficient. For instance, consider the eventually constant sequence

$$(d_0, d_1, d_2, d_3, \dots) = (1, 3, 3, 4, 4, 4, \dots)$$

with $d_i = 4$ for all $i \geqslant 3$. The conditions $d_{i+1} \leqslant d_i^{\langle i \rangle}$ for all $i \geqslant 1$ are satisfied here. Yet this sequence cannot be of the form $(|hA|)_{h \geqslant 0}$ for a subset A of a group G. For if $|A| = |2A| = 3$, then A is a translate of a subgroup of order 3, whence $|hA| = 3$ for all $h \geqslant 1$. This follows from the following well known lemma, whose short proof we recall for convenience.

LEMMA 5.1. — *Let A be a nonempty finite subset of a group $(G, +)$. Then $|hA| = |(h+1)A|$ for some $h \geqslant 0$ if and only if A is a translate of a subgroup of G of cardinality $|hA|$. In particular, $|hA| = |h'A|$ for all $h' \geqslant h$.*

Proof. — Without loss a generality, we may assume that A contains 0. Let $B = hA$, where $h \geqslant 0$ satisfies $|hA| = |(h+1)A|$. Then $|hA| = |h'A|$ for all $h' \geqslant h$, and in fact $hA = h'A$ for all $h' \geqslant h$ since $hA \subseteq h'A$ as A contains 0. It follows that B is a finite subset of G satisfying $0 \in B$ and $2B = B$. Hence, for all $b \in B$, there exists $c \in B$ such that $b + c = 0$. It follows that B is both stable under addition and taking opposites. Hence it is a subgroup of G. □

Besides the problem of finding an analog of Theorem 4.12 restricted to abelian groups, the following general problem is completely open.

PROBLEM. — *Characterize the nondecreasing sequences $(d_i)_{i \geqslant 0}$ of positive integers arising as iterated sumsets cardinalities in abelian groups, i.e. such that there exists an abelian group G and a nonempty finite subset $A \subseteq G$ such that $d_h = |hA|$ for all $h \geqslant 0$.*

BIBLIOGRAPHY

[1] W. Bruns & J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, 1993, xii+403 pages.

[2] S. Eliahou & M. Kervaire, "Minimal resolutions of some monomial ideals", *J. Algebra* **129** (1990), no. 1, p. 1-25.

[3] S. Eliahou & E. Mazumdar, "Iterated sumsets and Hilbert functions.", *J. Algebra* **593** (2022), p. 274-294.

[4] R. Fröberg, *An introduction to Gröbner bases*, Pure and Applied Mathematics, John Wiley & Sons, 1997, x+177 pages.

[5] A. Geroldinger & I. Z. Ruzsa, *Combinatorial number theory and additive group theory. With a foreword by Javier Cilleruelo, Marc Noy and Oriol Serra (Coordinators of the DocCourse)*, Advanced Courses in Mathematics – CRM Barcelona, Birkhäuser, 2009, xii+330 pages.

[6] J. Herzog & T. Hibi, *Monomial ideals*, Graduate Texts in Mathematics, vol. 260, Springer, 2011, xvi+305 pages.

[7] A. G. Khovanskiĭ, "The Newton polytope, the Hilbert polynomial and sums of finite sets", *Funkts. Anal. Prilozh.* **26** (1992), no. 4, p. 57-63, 96.

[8] ———, "Sums of finite sets, orbits of commutative semigroups and Hilbert functions", *Funkts. Anal. Prilozh.* **29** (1995), no. 2, p. 36-50, 95.

[9] F. S. Macaulay, "Some Properties of Enumeration in the Theory of Modular Systems", *Proc. Lond. Math. Soc.* **26** (1927), p. 531-555.

[10] P. McMullen, "The numbers of faces of simplicial polytopes", *Isr. J. Math.* **9** (1971), p. 559-570.

[11] J. Mermin & I. Peeva, "Hilbert functions and lex ideals", *J. Algebra* **313** (2007), no. 2, p. 642-656.

[12] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, vol. 165, Springer, 1996, xiv+293 pages.

[13] ———, "Growth of sumsets in abelian semigroups", *Semigroup Forum* **61** (2000), no. 1, p. 149-153.

[14] M. B. Nathanson & I. Z. Ruzsa, "Polynomial growth of sumsets in abelian semigroups", *J. Théor. Nombres Bordeaux* **14** (2002), no. 2, p. 553-560.

[15] I. Peeva, *Graded syzygies*, Algebra and Applications, vol. 14, Springer, 2011, xii+302 pages.

[16] G. Petridis, "The Plünnecke–Ruzsa inequality: an overview", in *Combinatorial and additive number theory – CANT 2011 and 2012*, Springer Proceedings in Mathematics & Statistics, vol. 101, Springer, 2014, p. 229-241.

[17] H. Plünnecke, "Eine zahlentheoretische Anwendung der Graphentheorie", *J. Reine Angew. Math.* **243** (1970), p. 171-183.

[18] R. P. Stanley, "Hilbert functions of graded algebras", *Adv. Math.* **28** (1978), no. 1, p. 57-83.

[19] T. Tao & V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, 2006, xviii+512 pages.

Manuscrit reçu le 29 octobre 2021,
révisé le 15 avril 2023,
accepté le 2 octobre 2023.

Shalom ELIAHOU
LMPA-ULCO, Calais (France)
eliahou@univ-littoral.fr

Eshita MAZUMDAR
Ahmedabad University (India)
eshita.mazumdar@ahduni.edu.in