Iterated sumsets and Hilbert functions

Shalom Eliahou, Eshita Mazumdar

Iterated sumsets and Hilbert functions

Shalom Eliahou* and Eshita Mazumdar†

Abstract

Let A be a finite subset of an abelian group $(G, +)$. Let $h \geq 2$ be an integer. If $|A| \geq 2$ and the cardinality $|hA|$ of the h-fold iterated sumset $hA = A + \cdots + A$ is known, what can one say about $|(h-1)A|$ and $|(h+1)A|$? It is known that

$$|(h-1)A| \geq |hA|^{(h-1)/h},$$

a consequence of Plünnecke's inequality. Here we improve this bound with a new approach. Namely, we model the sequence $|hA|_{h\geq 0}$ with the Hilbert function of a standard graded algebra. We then apply Macaulay's 1927 theorem on the growth of Hilbert functions, and more specifically a recent condensed version of it. Our bound implies

$$|(h-1)A| \geq \theta(x,h)\,|hA|^{(h-1)/h}$$

for some factor $\theta(x,h) > 1$, where x is the unique real number larger than h such that $|hA| = \binom{x}{h}$. Moreover, we show that $\theta(x,h)$ asymptotically tends to $e \approx 2.718$ as $|A|$ grows and h lies in a suitable range varying with $|A|$.

Keywords: Plünnecke's inequality; Standard Graded Algebra; Macaulay's Theorem; Stirling's formula.

MSC2020: 05E40, 11P70, 13P25

1 Introduction

Let A be a nonempty finite subset of an abelian group $(G, +)$. For any $h \in \mathbb{N}_+ = \{1, 2, \dots\}$, we denote by hA the h-fold iterated sumset of A, i.e.

$$hA = A + \cdots + A = \{x_1 + \cdots + x_h \mid x_i \in A \text{ for all } 1 \leq i \leq h\}.$$

As usual, for $h = 0$ we set $hA = \{0\}$. A classical problem in additive combinatorics is to determine the sequence of cardinalities $|hA|$ as h grows.

*LMPA-ULCO, Calais, France. Email: eliahou(at)univ-littoral.fr

†Stat-Math Unit, ISI Bengaluru. Email: eshita_vs(at)isibang.ac.in

Asymptotically, it is known that $|hA|$ is eventually polynomial in h. See e.g. [7, 8, 12]. But the behavior of $|hA|$ for small h may wildly depend on the structure, or lack thereof, of A. For instance, if A is a subset of $\mathbb{Z}$ such that $|A| = n$, then

$$hn - h + 1 \leq |hA| \leq \binom{n+h-1}{h},$$

with both bounds attained in suitable cases: arithmetic progressions for the lower bound, and so-called B_h-sets for the upper bound. The latter is best understood by noting that this binomial coefficient counts the number of monomials of degree h in $|A|$ commuting variables. See e.g. [17, Sections 2.1 and 4.5] or [4, Section 3.2].

Here we address the following question. If $h \geq 2$ and $|hA|$ is known, what estimates of $|(h-1)A|$ and $|(h+1)A|$ can one derive? One available estimate, given by Plünnecke's inequality and based on graph theory [14], is as follows:

$$|(h-1)A| \geq |hA|^{(h-1)/h}. \tag{1}$$

See also [6, 12, 17]. In this paper, we derive this bound from a completely different approach, and actually obtain a sharper one. We do so by modeling the sequence $|hA|_{h\geq 0}$ with the Hilbert function of a suitable graded algebra $R = R(A)$. That is, we construct a graded algebra $R = \oplus_{h\geq 0} R_h$ over a field $R_0 = \mathbb{K}$ with the property

$$\dim_{\mathbb{K}} R_h = |hA|$$

for all $h \geq 0$. Remarkably, Hilbert functions of standard graded algebras were completely characterized in 1927 in a classical theorem due to Macaulay [10]. Using a recent condensed version of it [3], we shall improve (1) as follows. Denote

$$\theta(x,h) = \frac{h}{x}\binom{x}{h}^{1/h}$$

for $x \in \mathbb{R}$ and $h \in \mathbb{N}$. If $|A| \geq 2$, our improved bound implies

$$|(h-1)A| \geq \theta(x,h)|hA|^{(h-1)/h} \tag{2}$$

for the unique real number $x > h$ such that $|hA| = \binom{x}{h}$, thereby ensuring $\theta(x,h) > 1$. In fact, for x large enough and suitable values of h, the improvement factor $\theta(x,h)$ approaches $e \approx 2.718$, the basis of the natural logarithm. This occurs, for instance, for $x \geq 10^6$ and $h = 3000$. See also Section 6.4, where strong evidence suggests that $\lim_{x\to\infty} \theta(x, \lfloor x^{1/2} \rfloor) = e$.

More modestly, the factor $\theta(x,h)$ exceeds 2 already for $x \geq 50$ and $h = 12$, in which case $\theta(x,12) > 2.013$. In practice, this means that if A is a set of integers such that $|12A| \geq 121{,}400{,}000{,}000$, then

$$|11A| \geq 2.013\,|12A|^{11/12} \geq 29{,}130{,}000{,}000.$$

See Section 6.3 for more details on the wide occurrence of the case $\theta(x,h) \geq 2$. Three general remarks are in order here.

Remark 1.1. Our results are stated for finite subsets of an abelian group G, but they hold more generally if G is a commutative semigroup, as in [13] for instance.

Remark 1.2. Commutative algebra has already been applied to estimate the growth of iterated sumsets. In particular, the Hilbert polynomial of graded modules has been used to determine the asymptotic behavior of the function $h \mapsto |hA|$, and more generally of the function $(h_1, \ldots, h_r) \mapsto |B + h_1A_1 + \cdots + h_rA_r|$. See [7, 8, 13, 12]. However, to the best of our knowledge, the only previous application of Macaulay's theorem to additive combinatorics is in [3], where the above-mentioned condensed version is established and applied to yield an asymptotic solution of Wilf's conjecture on numerical semigroups.

Remark 1.3. Another way of comparing $|hA|$ with $|(h-1)A|$ has been made, at least for $A \subset \mathbb{Z}$, by seeking to bound the difference $|hA| - |(h-1)A|$ from below rather than the quotient $|hA|/|(h-1)A|$ from above [9]. In the study of the difference $|hA| - |(h-1)A|$, a main tool is Kneser's theorem, whereas for the quotient $|hA|/|(h-1)A|$, it is Plünnecke's inequality as mentioned above, and now Macaulay's theorem as argued here.

There is a vast literature on Plünnecke's inequality, its applications to additive combinatorics and its successive refinements. Besides dedicated chapters in [6, 12, 17], see also for instance the nice survey [15] and its many references.

The contents of this paper are as follows. In Section 2, we construct a graded algebra $R(A)$ whose Hilbert function exactly models the sequence $|hA|_{h\geq 0}$. We also give a presentation of $R(A)$ by generators and relations. In Section 3, we recall Macaulay's theorem on Hilbert functions and the recent condensed version that we shall use. We prove our main result in Section 4 and apply it to the specific example $|5A| = 100$. In that example, Plünnecke's inequality implies $|4A| \geq 40$ and $|6A| \leq 251$. Our method yields much sharper and almost optimal bounds, namely $|4A| \geq 61$ and $|6A| \leq 152$. In Section 5, we derive the bound given by Plünnecke's inequality from our result and improve it by some factor $\theta(x,h) > 1$. The numerical behavior of that factor is studied in Section 6. We conclude the paper in Section 7 with two related questions.

2 The graded algebra $R(A)$

Let us start by recalling some basic terminology.

Definition 2.1. *A* standard graded algebra *is a commutative algebra R over a field $\mathbb{K}$ endowed with a vector space decomposition $R = \oplus_{i\geq 0} R_i$ such that $R_0 = \mathbb{K}$, $R_i R_j \subseteq R_{i+j}$ for all $i, j \geq 0$, and which is generated as a $\mathbb{K}$-algebra by finitely many elements in R_1.*

It follows from the definition that each R_i is a finite-dimensional vector space over $\mathbb{K}$. Moreover, the fact that R is generated by R_1 implies that $R_i R_j = R_{i+j}$ for all $i, j \geq 0$.

Definition 2.2. *Let $R = \oplus_{i\geq 0} R_i$ be a standard graded algebra. The* Hilbert function *of R is the map $i \mapsto d_i$ associating to each $i \in \mathbb{N}$ the dimension*

$$d_i \;=\; \dim_{\mathbb{K}} R_i$$

of R_i as a vector space over $\mathbb{K}$.

In particular, we have $d_0 = 1$, and R is generated as a $\mathbb{K}$-algebra by any d_1 linearly independent elements of R_1.

2.1 Construction of $R(A)$

Here we associate a standard graded algebra to a given finite subset A of an abelian group $(G, +)$. Let $\mathbb{K}$ be a commutative field. Consider the *group algebra* $\mathbb{K}[G]$ of G. Its canonical $\mathbb{K}$-basis is the set of symbols $\{t^g \mid g \in G\}$, and its product is induced by the formula

$$t^{g_1} t^{g_2} = t^{g_1+g_2}$$

for all $g_1, g_2 \in G$. Consider now $S = \mathbb{K}[G][Y]$, the one-variable polynomial algebra over $\mathbb{K}[G]$. Then S has for $\mathbb{K}$-basis the set

$$\mathcal{B} = \{t^g Y^n \mid g \in G, n \in \mathbb{N}\},$$

and the product of any two basis elements is given by

$$t^{g_1} Y^{n_1} \cdot t^{g_2} Y^{n_2} = t^{g_1+g_2} Y^{n_1+n_2}$$

for all $g_1, g_2 \in G$ and all $n_1, n_2 \in \mathbb{N}$. The *degree* of a basis element is defined as

$$\deg(t^g Y^n) = n$$

for all $g \in G$ and all $n \in \mathbb{N}$. This endows S with the structure of a graded algebra. Thus $S = \oplus_{h\geq 0} S_h$, where S_h is the $\mathbb{K}$-vector space with basis the set $\{t^g Y^h \mid g \in G\}$.

Definition 2.3. *Let $A = \{a_1, \ldots, a_n\}$ be a nonempty finite subset of the abelian group $(G, +)$. We define $R(A)$ to be the $\mathbb{K}$-subalgebra of S spanned by the set*

$$\{t^{a_1} Y, \ldots, t^{a_n} Y\}.$$

Thus $R(A)$, being finitely generated over $\mathbb{K}$ by elements of degree 1, is a standard graded algebra. We then have $R = \oplus_{h\geq 0} R_h$, where R_h is the $\mathbb{K}$-vector space with basis the set $\{t^b Y^h \mid b \in hA\}$. It follows that

$$\dim R_h = |hA| \tag{3}$$

for all $h \geq 0$.

2.2 Relators

It is of algebraic interest to determine the relations between the given generators of $R(A)$. We do so here, even though the result will not be used in the remainder of the paper.

Our present aim is thus to identify $R(A)$ as the quotient of the polynomial algebra $\mathbb{K}[X_1, \ldots, X_n]$ by a suitable homogeneous ideal I, the ideal of relations between the generators $t^{a_i} Y$.

Notation 2.4. *For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, we denote by $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ the corresponding monomial in $\mathbb{K}[X_1, \ldots, X_n]$. We denote the set of all those monomials by $M = \{X^\alpha \mid \alpha \in \mathbb{N}^n\}$.*

Let $\varphi \colon \mathbb{K}[X_1, \ldots, X_n] \to R(A)$ be the surjective morphism induced by $\varphi(X_i) = t^{a_i} Y$ for all i. On the set M, we define the equivalence relation

$$u \sim v \iff \varphi(u) = \varphi(v)$$

for all $u, v \in M$. Equivalently, let us write $u = X^\alpha, v = X^\beta$ with $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Then

$$X^\alpha \sim X^\beta \iff \left\{ \begin{array}{rcl} \sum_i \alpha_i & = & \sum_i \beta_i, \\ \sum_i \alpha_i a_i & = & \sum_i \beta_i a_i. \end{array} \right.$$

In particular, equivalent monomials have the same degree, where as usual $\deg(X^\alpha) = \sum_i \alpha_i$.

We shall need the notion of *simple polynomial* relative to $\sim$.

Definition 2.5. *Let $f \in \mathbb{K}[X_1, \ldots, X_n]$. We say that f is* simple *if $f \neq 0$ and all monomials occurring in f are equivalent under $\sim$.*

Observe that a simple polynomial is homogeneous. Indeed, equivalent monomials under $\sim$ have the same degree as observed above.

Moreover, every nonzero polynomial $g \in \mathbb{K}[X_1, \ldots, X_n]$ may be decomposed, in a unique way up to order, as the sum $g = f_1 + \cdots + f_r$ of maximal simple polynomials f_i, in the sense that for all $i \neq j$, the monomials occurring in f_i are non-equivalent under $\sim$ to those of f_j. The f_i are obtained by simply regrouping the monomials of f into maximal equivalence classes. We shall refer to the f_i as the *simple components* of f. See e.g. [2, p. 232] and [5, p. 346], where similar notions were used.

Lemma 2.6. *Let $g \in \ker(\varphi)\setminus\{0\}$. Then every simple component of g belongs to $\ker(\varphi)$.*

Proof. Let f be a simple component of g. We must show $\varphi(f) = 0$. Since f is simple, it is homogeneous of some degree h. Write $f = \sum_i \lambda_i u_i$, where $\lambda_i \in \mathbb{K} \setminus \{0\}$ for all i and where the u_i are pairwise distinct monomials. Since the u_i are pairwise equivalent under $\sim$, we have $\varphi(u_i) = t^b Y^h$ for some $b \in hA$ independent of i. Hence

$$\varphi(f) = (\sum_i \lambda_i) t^b Y^h.$$

Now, for any monomial v occurring in g but not in f, we have $\varphi(v) \neq t^b Y^h$ as v is non-equivalent to the u_i. Since $\varphi(g) = 0$, it follows that $\sum_i \lambda_i = 0$. Hence $\varphi(f) = 0$, as desired. □

Proposition 2.7. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be the ideal generated by the set $\{u - v \mid u, v \in M, u \sim v\}$. Then $\ker(\varphi) = I$.*

Proof. We have $I \subset \ker(\varphi)$ by construction. Conversely, let $0 \neq f \in \ker(\varphi)$. By Lemma 2.6, we may further assume that f is simple. Write $f = \sum_{i=1}^r \lambda_i u_i$, where $\lambda_i \in \mathbb{K}\setminus\{0\}$ for all i and where the u_i are pairwise distinct monomials. Since $\varphi(f) = 0$ and $\varphi(u_i) = \varphi(u_j)$ for all $i \neq j$, it follows that $\sum_{i=1}^r \lambda_i = 0$. Therefore $\lambda_r = -\sum_{i=1}^{r-1} \lambda_i$, and so

$$f = \sum_{i=1}^{r-1} \lambda_i (u_i - u_r).$$

Since $u_i \sim u_r$ for all i, it follows that $u_i - u_r \in I$. Hence $f \in I$, as desired. □

Corollary 2.8. *We have $R(A) \simeq \mathbb{K}[X_1, \ldots, X_n]/I$.*

Proof. By Noether's isomorphism theorem. □

3 Macaulay's theorem

We now turn to Macaulay's theorem [10] and a recent condensed version of it [3]. Macaulay's theorem gives a necessary and sufficient condition for a numerical function $\mathbb{N} \to \mathbb{N}$ to be the Hilbert function of some standard graded algebra. It rests on the so-called *binomial representations* of integers. Here is some background information.

Proposition 3.1. *Let $a \geq i \geq 1$ be positive integers. There are unique integers $a_i > a_{i-1} > \cdots > a_1 \geq 0$ such that*

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

Proof. See e.g. [1, 14]. □

This expression is called the ith *binomial representation of* a. Producing it is computationally straightforward: take for a_i the largest integer such that $\binom{a_i}{i} \leq a$, and complete $\binom{a_i}{i}$ by adding to it the $(i-1)$th binomial representation of $a - \binom{a_i}{i}$. We omit trails of 0's, if any. For instance, for $a = 10$ and $i = 3$, we abbreviate $10 = \binom{5}{3} + \binom{1}{2} + \binom{0}{1}$ as simply $10 = \binom{5}{3}$.

Notation 3.2. *Let* $a \geq i \geq 1$ *be positive integers. Let* $a = \sum_{j=1}^{i} \binom{a_j}{j}$ *be its* ith *binomial representation. We denote* $a^{\langle i \rangle} = \sum_{j=1}^{i} \binom{a_j + 1}{j+1}$ *and* $0^{\langle i \rangle} = 0$.

Note that the defining formula of $a^{\langle i \rangle}$ is a valid $(i+1)$th binomial representation of some positive integer, namely of the integer it sums to.

Here is one half of Macaulay's classical result, constraining the possible Hilbert functions of standard graded algebras [10].

Theorem 3.3. *Let* $R = \oplus_{i \geq 0} R_i$ *be a standard graded algebra over a field* $\mathbb{K}$*, with Hilbert function* $d_i = \dim_{\mathbb{K}} R_i$ *for all* $i \geq 0$*. Then*

$$d_{i+1} \ \leq \ d_i^{\langle i \rangle}. \tag{4}$$

Remarkably, the converse also holds in Macaulay's theorem, but we shall not need it here. That is, satisfying (4) for all $i \geq 0$ *characterizes* the Hilbert functions of standard graded algebras. See e.g. [1, 11, 14].

Example 3.4. *Consider the sequence*

$$(m_0, m_1, m_2, m_3, m_4, m_5, m_6) = (1, 5, 15, 33, 61, 100, 152).$$

Then $m_{i+1} \leq m_i^{\langle i \rangle}$ *for all* $i = 1, \ldots, 5$ *as readily checked. Hence there exists a standard graded algebra* $R = \oplus_{j \geq 0} R_j$ *whose values of* $\dim R_i$ *for* $i = 0, \ldots, 6$ *are exactly modeled by the sequence* $(m_0, \ldots, m_6)$*. For instance, one may take* $R = S/J$*, where* $S = \mathbb{K}[X_1, \ldots, X_5]$ *and* $J = (X_5^3, X_4 X_5^2, X_3^3 X_5^2)$.

3.1 A condensed version

We shall need the following condensed version of Macaulay's theorem, as established in [3]. For $m \in \mathbb{N}$ and $x \in \mathbb{R}$, denote as usual

$$\binom{x}{m} = \frac{x(x-1)\cdots(x-m+1)}{m!} = \prod_{i=0}^{m-1} \frac{x-i}{m-i}.$$

In particular, $\binom{x}{0} = 1$. We shall constantly need the following observations.

Lemma 3.5. *Let $i \geq 1$ be an integer. Then the map $y \mapsto \binom{y}{i}$ is an increasing continuous bijection (in fact, a homeomorphism) from $[i-1, \infty)$ to $[0, \infty)$. In particular, for any real numbers $y_1, y_2 \geq i-1$, we have*

$$y_1 \leq y_2 \iff \binom{y_1}{i} \leq \binom{y_2}{i}. \tag{5}$$

Proof. A direct consequence of Rolle's theorem. See e.g. [3, Lemma 5.6]. □

Lemma 3.6. *Let $h, d \geq 1$ be positive integers. Then there exists a unique real number $x \geq h$ such that $d = \binom{x}{h}$.*

Proof. By the above lemma, there is a unique real number $x \geq h-1$ such that $d = \binom{x}{h}$. Since $d \geq 1$, we have $\binom{x}{h} \geq \binom{h}{h}$. Hence $x \geq h$ by (5). □

Here is the condensed version of Macaulay's theorem that we shall use in the next section.

Theorem 3.7. *Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra over the field $\mathbb{K}$, with Hilbert function $d_i = \dim_{\mathbb{K}} R_i$ for $i \geq 0$. Let $h \geq 1$ be an integer. Let $x \geq h-1$ be a unique real number such that $d_h = \binom{x}{h}$. Then*

$$d_{h-1} \geq \binom{x-1}{h-1} \text{ and } d_{h+1} \leq \binom{x+1}{h+1}.$$

Proof. See [3]. □

4 Main result

Let A be a finite subset of an abelian group with $|A| \geq 2$. If $|hA|$ is known for some $h \geq 2$, what bounds can one derive on $|iA|$ for $i \neq h$?

We start with the following known answer, a direct consequence of Plünnecke's inequality. See e.g. [12, Theorem 7.5, p. 217] or [6, Theorem 1.2.3 with $m = 1$, p. 96].

Theorem 4.1. *Let A be a nonempty finite subset of an abelian group. Let $h \geq 2$ be an integer. Then $|iA| \geq |hA|^{i/h}$ for all $1 \leq i \leq h$.*

Remark 4.2. Theorem 4.1 is equivalent to its main case $i = h-1$, namely:

$$|(h-1)A| \geq |hA|^{(h-1)/h}. \tag{6}$$

Indeed, the general case is implied by (6), as shown by induction on h:

$$|iA| \overset{(6)}{\geq} (|(i+1)A|^{i/(i+1)} \overset{\text{ind.hyp.}}{\geq} (|hA|^{(i+1)/h})^{i/(i+1)} = |hA|^{i/h}.$$

Here is our main result, obtained by applying Macaulay's theorem and its condensed version to the standard graded algebra $R(A)$ defined in Section 2.

Theorem 4.3. *Let A be a nonempty finite subset of an abelian group G. Let $h \geq 2$ be an integer and $x \geq h$ the unique real number such that $|hA| = \binom{x}{h}$. Then*

$$|(h-1)A| \geq \binom{x-1}{h-1} \quad \textit{and} \quad |(h+1)A| \leq |hA|^{\langle h \rangle} \leq \binom{x+1}{h+1}.$$

Proof. Let $R = R(A)$ be the standard graded algebra associated to A as defined in Section 2. We have $R = \oplus_{h \geq 0} R_h$, where R_h denotes the homogeneous subspace of R of degree h. By (3), we have

$$|hA| = \dim R_h$$

for all $h \geq 0$. With h, x as in the hypotheses, a direct application of Theorem 3.7 yields the bounds

$$|(h-1)A| \geq \binom{x-1}{h-1} \text{ and } |(h+1)A| \leq \binom{x+1}{h+1},$$

while Theorem 3.3 yields the upper bound

$$|(h+1)A| \leq |hA|^{\langle h \rangle}.$$

For the last inequality $|hA|^{\langle h \rangle} \leq \binom{x+1}{h+1}$, see [3, Theorem 5.9]. □

Given $|hA|$, the lower bound on $|(h-1)A|$ that can be derived from Theorem 4.3 may be up to 2.71 times better, in suitable circumstances, than the one provided in (6) by Theorem 4.1. This will be shown in Sections 5 and 6. Here is a first small example demonstrating the effectiveness of Theorem 4.3.

4.1 An example

Let A be a finite set of integers such that $|5A| = 100$. The bounds given by Theorem 4.1 and derived from Plünnecke's inequality yield

$$|4A| \geq 100^{4/5} \approx 39.8, \quad |6A| \leq 100^{6/5} \approx 251.18.$$

In comparison, Theorem 4.3 yields the much sharper bounds

$$|4A| \geq 58, \quad |6A| \leq 161. \tag{7}$$

Indeed, let $x \geq 5$ be the unique real number such that $\binom{x}{5} = 100$. Then $8.69 < x < 8.7$, as follows from $\binom{8.69}{5} \approx 99.42$ and $\binom{8.7}{5} \approx 100.2$. Hence

$$|4A| \geq \binom{x-1}{4} > \binom{7.69}{4} \approx 57.2,$$
$$|6A| \leq \binom{x+1}{6} < \binom{9.7}{6} \approx 161.99.$$

This proves (7), using the condensed version of Macaulay's theorem. But using its original version, one gets still better bounds. Indeed, for the 5th binomial representation of 100, we have

$$100 = \binom{8}{5} + \binom{7}{4} + \binom{4}{3} + \binom{3}{2} + \binom{2}{1}.$$

The inequality $|(h+1)A| \le |hA|^{\langle h \rangle}$ of Theorem 4.3 then yields the following improvement of (7):

$$|4A| \ \ge \ \binom{7}{4} + \binom{6}{3} + \binom{4}{2} \ = \ 61, \tag{8}$$

$$|6A| \ \le \ \binom{9}{6} + \binom{8}{5} + \binom{5}{4} + \binom{4}{3} + \binom{3}{2} \ = \ 152. \tag{9}$$

While (9) directly follows from the inequality $|(h+1)A| \le |hA|^{\langle h \rangle}$, note that for (8), if we had $|4A| \le 60 = \binom{7}{4} + \binom{6}{3} + \binom{3}{2} + \binom{2}{1}$, that same inequality would imply $|5A| \le \binom{8}{5} + \binom{7}{4} + \binom{4}{3} + \binom{3}{2} = 100 - 2$.

Are the bounds (8), (9) optimal under the assumption $|5A| = 100$? We don't know, but they are not far from it. For instance, let $A = \{0, 1, 5, 8, 49\}$. Then $|5A| = 100$ as required, and

$$|4A| = 63, \quad |6A| = 145.$$

This example may well be optimal. That is, we conjecture that *if $A \subset \mathbb{Z}$ is any subset satisfying $|5A| = 100$, then $|4A| \ge 63$ and $|6A| \le 145$.*

As seen here, the improvement provided by Theorem 4.3 is already quite good. How good is it in general? We investigate this question in the sequel.

5 Macaulay vs Plünnecke

We first show that Theorem 4.1 based on Plünnecke's inequality, also follows from our Theorem 4.3 based on Macaulay's theorem.

Notation 5.1. *For a positive integer h and a real number $x \ge h$, we set*

$$\theta(x, h) = \frac{h}{x}\binom{x}{h}^{1/h}.$$

Theorem 5.2. *Let A be a nonempty finite subset of an abelian group G. Let $h \in \mathbb{N}, h \ge 2$. Let $x \ge h$ be the unique real number such that $|hA| = \binom{x}{h}$. Then*

$$|(h-1)A| \ge \theta(x, h)\, |hA|^{(h-1)/h}.$$

Proof. Let $x \geq h-1$ be the unique real number such that

$$|hA| = \binom{x}{h}. \tag{10}$$

Since $|hA| \geq 1$, we have $x \geq h$ by Lemma 3.6. Theorem 4.3 yields

$$|(h-1)A| \geq \binom{x-1}{h-1}. \tag{11}$$

Now

$$\binom{x-1}{h-1} = \frac{h}{x}\binom{x}{h}$$

since

$$\binom{x}{h} = \prod_{i=0}^{h-1} \frac{x-i}{h-i} = \frac{x}{h}\prod_{i=1}^{h-1} \frac{x-i}{h-i} = \frac{x}{h}\binom{x-1}{h-1}.$$

Hence

$$\begin{aligned} |(h-1)A|^h &\geq \binom{x-1}{h-1}^h \\ &= \left(\frac{h}{x}\right)^h \binom{x}{h}^h \\ &= \left(\frac{h}{x}\right)^h \binom{x}{h}\binom{x}{h}^{h-1} \\ &= \left(\frac{h}{x}\right)^h \binom{x}{h}|hA|^{h-1}. \end{aligned}$$

Therefore $|(h-1)A|^h \geq \theta(x,h)^h|hA|^{h-1}$, as desired. □

Corollary 5.3. *Theorem 4.3 implies Theorem 4.1.*

Proof. By Theorem 5.2, we only need to show $\theta(x,h) \geq 1$, or equivalently, $\theta(x,h)^h \geq 1$. Now

$$\theta(x,h)^h = \left(\frac{h}{x}\right)^h \binom{x}{h} = \prod_{i=0}^{h-1} \frac{h(x-i)}{x(h-i)}, \tag{12}$$

and $h(x-i) \geq x(h-i)$ for all $0 \leq i \leq h-1$ since $h \leq x$. □

Remark 5.4. In fact, we have $\theta(x,h) > 1$ whenever $|A| \geq 2$, $h \geq 2$. For then $|hA| \geq 2$, and since $|hA| = \binom{x}{h}$ with $x \geq h$, it follows that $x > h$, whence $h(x-1) > x(h-1)$, implying in turn $\theta(x,h)^h > 1$ by (12).

6 Behavior of $\theta(x,h)$

We now study the numerical behavior of the function $\theta(x,h)$. Denote $e \approx 2.718$, the basis of the natural logarithm. We show that $1 < \theta(x,h) < e$ whenever $x > h \geq 2$, and that $\theta(x,h)$ asymptotically goes to e in suitable circumstances. This section is more informal in nature. Numerical computations and graphics were done with *Mathematica 10* [19].

Proposition 6.1. *For all $h \in \mathbb{N}$, $x \in \mathbb{R}$ such that $x > h \geq 2$, we have*

$$1 < \theta(x,h) < e.$$

Proof. The lower bound follows from (12) and Remark 5.4. As for the upper bound, we have

$$\binom{x}{h} \leq \frac{x^h}{h!} = \frac{x^h}{h^h}\frac{h^h}{h!} < \frac{x^h}{h^h}e^h$$

since $\dfrac{h^h}{h!} < \displaystyle\sum_{k\in\mathbb{N}} \frac{h^k}{k!} = e^h$. It follows that

$$\theta(x,h) = \frac{h}{x}\binom{x}{h}^{1/h} < \frac{h}{x}\frac{x}{h}e = e. \quad \square$$

We shall also need to invoke the monotonicity of $\theta(x,h)$ in x.

Proposition 6.2. *For a fixed integer $h \geq 2$, the map $x \mapsto \theta(x,h)$ from $[h,\infty)$ to $[1,\infty)$ is strictly increasing.*

Proof. It is equivalent to show that the map $x \mapsto \theta(x,h)^h$ is strictly increasing. This easily follows from the positivity of its derivative. Details are left to the reader. $\square$

6.1 Asymptotics

We provide here, somewhat informally, a good approximation of $\theta(x,h)$ together with its asymptotic behavior as x grows. Recall Stirling's approximation of $n!$ for large n:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

On the other hand, the bounds below are valid for all $n \geq 1$:

$$\sqrt{2\pi}\, n^{n+1/2}\, e^{-n} \leq n! \leq e\, n^{n+1/2}\, e^{-n}.$$

This yields the following well known approximation of $\binom{n}{k}$ for n much larger than k, see e.g. [18]:

$$\binom{n}{k} \sim \frac{(n/k - 1/2)^k\, e^k}{\sqrt{2\pi k}}.$$

As a consequence, here is the asymptotic behavior of $\theta(x,h)$ when x grows.

Proposition 6.3. *Let $h \geq 2$ be an integer. Then*

$$\theta(x,h) \sim \frac{(1-h/(2x))\,e}{(2\pi h)^{1/(2h)}} = \frac{(2x-h)\,e}{2x(2\pi h)^{1/(2h)}}.$$

In particular,

$$\lim_{x\to\infty} \theta(x,h) = (2\pi h)^{-1/(2h)}\, e.$$

Proof. Directly follows from the above approximation of the binomial coefficients. □

6.2 When $\theta(x,h) \geq 1.5$

Our improvement factor $\theta(x,h)$ exceeds 1.5 quite early in terms of x or h. Indeed, *the smallest integer x for which $\theta(x,h) \geq 1.5$ for some integer h is* $x = 10$, specifically at $h = 4$ and 5. Even starting at $h = 3$, we have

$$\theta(x,3) \geq 1.509$$

for all $x \geq 12$.

As a quick application, let A be a subset of an abelian group G such that $|4A| \geq \binom{10}{4} = 210$. By Theorem 4.1 with Plünnecke's inequality, and the estimate $210^{3/4} \approx 55.165$, we get the lower bound

$$|3A| \geq 56.$$

Now, $\theta(x,4) \geq 1.52$ for all $x \geq 10$. It then follows from Theorem 5.2 and the estimate $55.165 \cdot 1.52 \approx 83.9$ that, in fact,

$$|3A| \geq 84.$$

Alternatively, Theorem 4.3 directly yields $|3A| \geq \binom{9}{3} = 84$.

6.3 When $\theta(x,h) \geq 2$

We now examine circumstances guaranteeing $\theta(x,h) \geq 2$, a case of interest since this is when our bound is at least twice better than (1). As it turns out, for x large, one has $\theta(x,h) \geq 2$ for almost all integers h between 6 and $\lfloor x/2 \rfloor$. We also describe cases where $\theta(x,h)$ gets very close to its upper bound e.

So, under what minimal circumstances, in terms of h or of x, do we have $\theta(x,h) \geq 2$? First note that if $y \geq h-1$ then $\theta(y,h) < \lim_{x\to\infty} \theta(x,h)$, as follows from Proposition 6.2. Moreover, $\lim_{x\to\infty} \theta(x,h_1) \leq \lim_{x\to\infty} \theta(x,h_2)$ whenever $h_1 \leq h_2$, as follows from Proposition 6.3.

That being said, consider the case $h = 5$. Since $\lim_{x\to\infty} \theta(x,5) < 1.926$ by Proposition 6.3, the values $1 \leq h \leq 5$ are excluded for the occurrence of $\theta(x,h) \geq 2$. However, already $h = 6$ qualifies, as $\lim_{x\to\infty} \theta(x,6) > 2.007$. More precisely, we have

$$\theta(x,6) \geq 2 \tag{13}$$

for all $x \geq 1210$, the least integer with that property.

If now h is allowed to grow, then $\theta(x,h) \geq 2$ may occur for much smaller values of x. Indeed, the smallest $x \in \mathbb{N}$ for which $\theta(x,h) \geq 2$ for some h is $x = 48$, namely at $h = 11$ and 12. More precisely, we have

$$\begin{aligned} &\theta(48,11) > 2.001, \quad \theta(48,12) > 2.002, \\ &\theta(48,10) < 1.997, \quad \theta(48,13) < 1.999. \end{aligned}$$

See Figure 1.

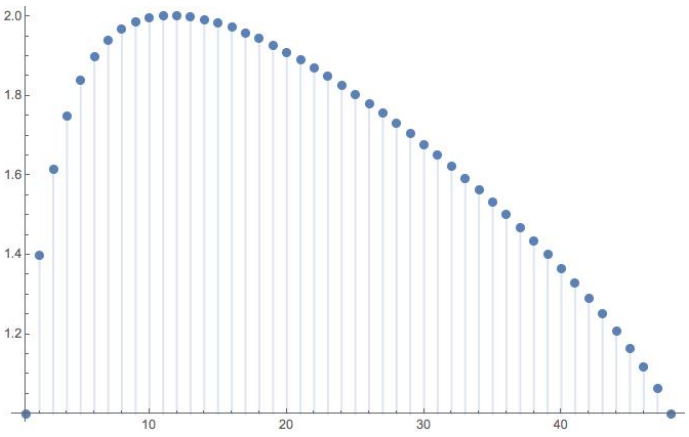

Figure 1: Values of $\theta(48,h)$ for $h = 1,\ldots,48$

In fact, when x goes to infinity, then $\theta(x,h) \geq 2$ *holds for almost all positive integers* $h \leq x/2$. Indeed, as observed in (13), we have $\theta(x,6) \geq 2$ for all $x \geq x_0 = 1210$. Now, numerical computations at x_0 yield

$$\theta(x_0,h) \geq 2 \quad \forall h \in [6, x_0/2 - 10] \cap \mathbb{N}.$$

As a further illustration, for $x_1 = 10^6$, one has

$$\theta(x_1,h) \geq 2 \quad \forall h \in [6, x_1/2 - 19] \cap \mathbb{N}.$$

This is no accident, as shown by the following result.

Proposition 6.4. *One has* $\lim_{x\to\infty} \theta(x, \lfloor x/2 \rfloor) = 2$.

Proof. Using Stirling's approximation formula of $n!$, one readily sees that

$$\theta(n, \lfloor n/2 \rfloor) \approx 2 \left(\frac{2}{\pi n}\right)^{1/n},$$

which proves the claim since $\lim_{n\to\infty}(cn)^{-1/n} = 1$ for any constant $c > 0$. $\square$

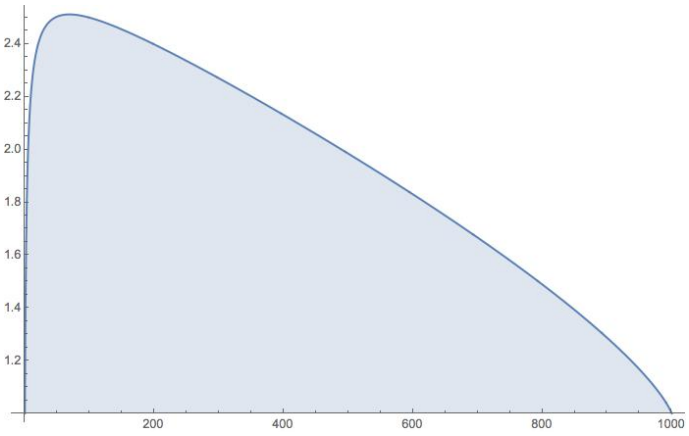

Figure 2: Values of $\theta(1000, h)$ for $h = 1, \ldots, 1000$

6.4 The highest point

For fixed x, the general shape of $\theta(x, h)$ when h runs from 1 to $\lfloor x \rfloor$ is well illustrated by Figure 1 for $x = 48$. Figure 2 displays the case $x = 1000$.

It would be desirable to determine the highest point of that curve, and in particular the integer $1 \leq h \leq x$ maximizing $\theta(x, h)$. We do not have yet a precise answer. Nevertheless, by computing derivatives of the approximation of $\theta(x, h)$ provided by Proposition 6.3, one sees that for fixed x,

$$\frac{\partial}{\partial h}\left(\frac{2x-h}{(2\pi h)^{1/(2h)}}\right) > 0 \iff 2h^2 < (2x-h)(\ln(2\pi h) - 1). \tag{14}$$

Thus, for x fixed, the sought-for integer h maximizing $\theta(x, h)$ occurs when

$$2h^2 \approx (2x-h)(\ln(2\pi h) - 1). \tag{15}$$

For instance, for $x_0 = 100$, the maximum of $\theta(x_0, h)$ is reached at $h = 18$, for which $\theta(100, 18) \approx 2.177$. Hence

$$\theta(x, 18) \geq 2.177$$

for all $x \geq 100$, as follows from Proposition 6.2.

6.5 For h fixed

In the opposite direction, for h fixed, it is easy to locate the real number $x_1 \geq h$ maximizing $\theta(x, h)$. Indeed, using (14), we find

$$x_1 \approx \frac{1}{2}\left(\frac{2h^2}{\ln(2\pi h) - 1} + h\right).$$

This suggests that

$$\lim_{x \to \infty} \theta(x, \lfloor x^{1/2} \rfloor) = e,$$

as is fully confirmed by numerical experiments. As a concrete illustration, here are instances where $\theta(x,h)$ gets very close to e:

- For all $x \geq 200000$ and all $1200 \leq h \leq 1300$, one has $\theta(x,h) \geq 2.70$.
- Similarly, for all $x \geq 1100000$ and all $2600 \leq h \leq 3700$, one has $\theta(x,h) \geq 2.71$.

7 Concluding questions

We end this paper with two related questions.

▷ How far from optimal are our new bounds? More precisely, let h, m be positive integers. Among all subsets A of $\mathbb{Z}$ such that $|hA| = m$, what is the least possible value of $|(h-1)A|$? That is, let us denote

$$\mu(h,m) = \min_{A \subset \mathbb{Z}} |(h-1)A|,$$

where A runs through all subsets subject to $|hA| = m$. How small can $\mu(h,m)$ be? We have seen that if we express $m = \binom{x}{h}$ with $x \geq h$, then

$$\mu(h,m) \geq \binom{x-1}{h-1}.$$

This is not quite optimal in general, as it follows from the condensed version of Macaulay's theorem which, while handy, comes with a little loss of information. But what about the bound given by the original Macaulay's theorem? For instance, using that bound, we have seen that $\mu(5,100) \geq 61$, and we gave an example with $|5A| = 100$ and $|4A| = 63$, namely $A = \{0,1,5,8,49\}$. Is there an improved example A reaching $|5A| = 100$ and $|4A| = 61$?

▷ Can one specialize Macaulay's theorem by characterizing the Hilbert functions of all algebras of the form $R(A)$, at least for finite subsets A of $\mathbb{Z}$? A positive answer would help tackle the former question.

Acknowledgments. This research was supported in part by the International Centre for Theoretical Sciences (ICTS) during a visit for the program - Workshop on Additive Combinatorics (Code: ICTS/wac2020/02). We are grateful to David Grynkiewicz for very useful discussions concerning this work during the ICTS Workshop.

References

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

[2] S. Eliahou, Idéaux de définition des courbes monomiales. Complete intersections (Acireale, 1983), 229–240, Lecture Notes in Math., 1092, Springer, Berlin, 1984.

[3] S. Eliahou, Wilf's conjecture and Macaulay's theorem, J. Eur. Math. Soc. 20 (2018) 2105–2129.

[4] S. Eliahou and J. Fromentin, Near-misses in Wilf's conjecture, Semigroup Forum 98 (2019) 285–298.

[5] S. Eliahou and R.H. Villarreal, On systems of binomials in the ideal of a toric variety, Proc. Amer. Math. Soc. 130 (2002) 345–351.

[6] A. Geroldinger and I.Z. Ruzsa, Combinatorial number theory and additive group theory. Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2009. xii+330 pp. ISBN: 978-3-7643-8961-1.

[7] A.G. Khovanskii, Newton Polyhedron, Hilbert Polynomial, and Sums of Finite Sets, Funct. Anal. Appl. 26 (1992) 276–281.

[8] A.G. Khovanskii, Sums of Finite Sets, Orbits of Commutative Semigroups, and Hilbert Functions, Funct. Anal. Appl. 29 (1995) 102–112.

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

[10] F.S. Macaulay, Some properties of enumeration in the theory of modular systems, Proc. Lond. Math. Soc. 26 (1927) 531–555.

[11] J. Mermin and I. Peeva, Hilbert functions and lex ideals, J. Algebra 313 (2007) 642–656.

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

[13] M.B. Nathanson, Growth of sumsets in abelian semigroups, Semigroup Forum 61 (2000) 149–153.

[14] I. Peeva, Graded syzygies. Algebra and Applications, 14. Springer-Verlag London, Ltd., London, 2011.

[15] G. Petridis, The Plünnecke-Ruzsa inequality: an overview. In Combinatorial and additive number theory—CANT 2011 and 2012, 229–241, Springer Proc. Math. Stat., 101, Springer, New York, 2014.

[16] H. Plünnecke, Eine zahlentheoretische Anwendung der Graphentheorie, J. Reine Angew. Math. 243 (1970) 171–183.

[17] T. Tao and V. Vu, Additive combinatorics. Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006. xviii+512 pp. ISBN: 978-0-521-85386-6; 0-521-85386-9.

[18] `https://en.wikipedia.org/wiki/Binomial_coefficient`.

[19] Wolfram Research, Inc., Mathematica, Version 10, Champaign, IL (2014).

Authors' addresses:

▷ Shalom Eliahou,
Univ. Littoral Côte d'Opale, UR 2597 - LMPA - Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62228 Calais, France and CNRS, FR2037, France.
`eliahou@univ-littoral.fr`

▷ Eshita Mazumdar,
Stat-Math Unit, ISI Bengaluru.
eshita_vs(at)isibang.ac.in