Iterated sumsets and Hilbert functions

Shalom Eliahou

Université du Littoral Côte d'Opale, Calais

New York Number Theory Seminar

(on Zoom)

July 10, 2020

Introduction

[With Eshita Mazumdar. Preprint (2020) on arXiv.]

Let $A, B \subseteq G$ where G is an abelian group, e.g. $G = \mathbb{Z}$. Denote

$$A + B = \{a + b \mid a \in A, b \in B\},$$

the **sumset** of A, B. For $A = B$, denote

$$2A = A + A.$$

For $h \geq 2$, denote

$$hA = A + (h-1)A,$$

the h-fold **iterated sumset** of A. Of course, $0A = \{0\}$ and $1A = A$.

Problem (typical in Additive Combinatorics)

If A is finite, how does the sequence $|hA|$ grow with h?

Specifically here, if $|hA|$ is given, what can one say about $|(h \pm 1)A|$?

Theorem (Plünnecke, 1970)

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 $1 \leq i \leq h$.

This is one **Plünnecke inequality** derived using graph theory.

Note. These estimates are equivalent to the main case $i = h - 1$, i.e.

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

Our approach

- Model the sequence $|hA|$ with the **Hilbert function** of a standard graded algebra $R(A)$.
- Apply **Macaulay's theorem** on the growth of Hilbert functions.

It allows us to recover and strengthen Plünnecke's estimate.

An example

Let $A \subset \mathbb{Z}$ satisfy $|5A| = 100$. Plünnecke's inequality yields

$$\begin{aligned} |4A| &\geq 100^{4/5} \approx 39.8 \\ |6A| &\leq 100^{6/5} \approx 251.18 \end{aligned}$$

Hence

$$\begin{aligned} |4A| &\geq 40 \\ |6A| &\leq 251 \end{aligned}$$

Can one do better? Yes. Our approach yields

$$\begin{aligned} |4A| &\geq 61 \\ |6A| &\leq 152 \end{aligned}$$

How?

Hilbert functions

A **standard graded algebra** is a quotient $R = K[X_1, \dots, X_n]/J$, where K is a field, $\deg X_i = 1$ for all i, and J is a homogeneous ideal. So $R = \oplus_{i \geq 0} R_i$, with $R_0 = K$ and $R_i R_j = R_{i+j}$ for all i, j.

The **Hilbert function** of the standard graded algebra $R = \oplus_{i \geq 0} R_i$ is the map $i \mapsto d_i = \dim_K R_i \ \ \forall i \geq 0$.

• What characterizes such numerical functions $i \mapsto d_i$?

Macaulay's classical theorem (1927) provides a **complete answer**.

• For instance, if $\dim R_1 = n$, then $\dim R_2 \leq (n+1)n/2$. That is,

$$d_1 = \binom{n}{1} \implies d_2 \leq \binom{n+1}{1+1}.$$

Binomial representation

Let $a, i \geq 1$ be positive integers. There is a **unique expression**

$$a = \sum_{k=1}^{i} \binom{a_k}{k} = \binom{a_i}{i} + \binom{a_{i-1}}{i-1} + \cdots + \binom{a_1}{1}$$

with decreasing integers $a_i > a_{i-1} > \cdots > a_1 \geq 0$. We then define

$$a^{\langle i \rangle} = \sum_{k=1}^{i} \binom{a_k + 1}{k+1}.$$

Example

$$100^{\langle 5 \rangle} = 152.$$

Example: $100^{\langle 5 \rangle} = 152$

Let $a = 100$, $i = 5$. The 5th binomial representation of 100 is

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

Hence

$$\begin{aligned} 100^{\langle 5 \rangle} &= \binom{9}{6} + \binom{8}{5} + \binom{5}{4} + \binom{4}{3} + \binom{3}{2} \\ &= 152. \end{aligned}$$

From this we shall deduce: if $|5A| = 100$ then $|6A| \leq 152$.

Macaulay's theorem, first half

Macaulay's theorem characterizes the Hilbert functions of standard graded algebras. Here is a **necessary condition**.

Theorem (1/2)

Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra over a field K, with Hilbert function $d_i = \dim_K R_i$. Then for all $i \geq 1$, we have

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

Example

Assume $\dim R_5 = 100$, i.e. $d_5 = 100$. Macaulay states $d_6 \leq d_5^{\langle 5 \rangle}$. Now $100^{\langle 5 \rangle} = 152$ as seen above. Hence

$$\dim R_6 \leq 152.$$

Macaulay's theorem, full version

Remarkably, that necessary condition is also **sufficient**.

Theorem (Macaulay, 1927)

*A numerical function $i \mapsto d_i$ is the Hilbert function of a standard graded algebra **if and only if** $d_0 = 1$ and $d_{i+1} \leq d_i^{\langle i \rangle}$ for all $i \geq 1$.*

Example

Let $(d_0, d_1, d_2, d_3, d_4, d_5, d_6) = (1, 5, 15, 33, 61, 100, 152)$. Then $d_{i+1} \leq d_i^{\langle i \rangle}$ for all $i = 1, \ldots, 5$. By Macaulay's theorem, there exists a standard graded algebra $R = \oplus_{i \geq 0} R_i$ such that $\dim R_i = d_i$ for $i = 0, \ldots, 6$. For instance, take

$$R = K[X_1, \ldots, X_5]/(X_5^3, X_4 X_5^2, X_3^3 X_5^2).$$

A glimpse inside the box

1. Denote M_d = set of monomials of degree d in $X_1, \ldots, X_n$.
2. Order M_d **lexicographically**: $X_1^d > X_1^{d-1}X_2 > X_1^{d-1}X_3 > \cdots > X_n^d$.
3. A **lexsegment** in M_d is $L = \{v \in M_d \mid v \geq u\}$ for some $u \in M_d$.
4. Denote $\mathcal{M} = \{X_1, \ldots, X_n\}$. If $A \subseteq M_d$ then $\mathcal{M}A \subseteq M_{d+1}$.
5. If $L \subseteq M_d$ is a lexsegment, then so is $\mathcal{M}L$.
6. Lexsegments have minimal growth: Let $A, L \subseteq M_d$ such that $|L| = |A|$ and L is a lexsegment. Then $|\mathcal{M}A| \geq |\mathcal{M}L|$.
7. For $A \subseteq M_d$, denote $\overline{A} = M_d \setminus A$, its complement.
8. Let $L \subseteq M_d$ be a lexsegment. If $|\overline{L}| = a$ then $|\overline{\mathcal{M}L}| = a^{\langle d \rangle}$.

The algebra $R(A)$

Let G be an abelian group and K a commutative field. Let $A \subset G$ be finite nonempty. We associate to A a standard graded K-algebra

$$R = R(A) = \oplus_{h \geq 0} R_h$$

whose Hilbert function $\dim_K R_h$ exactly models the sequence $|hA|$ for $h \geq 0$.

• Consider the **group algebra** $K[G]$ of G. Its canonical 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 $S = K[G][X]$, the one-variable polynomial algebra over $K[G]$.

• A natural K-basis for S is the set

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

• The product of any two basis elements is given by

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

for all $g_1, g_2 \in G$ and all $n_1, n_2 \in \mathbb{N}$.

• We define the **degree** of a basis element as

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

for all $g \in G$ and all $n \in \mathbb{N}$.

• Thus $S = \oplus_{h \geq 0} S_h$ is a graded K-algebra, where for all $h \geq 0$, S_h is the K-vector space with basis the set $\{t^g X^h \mid g \in G\}$.

Definition

Set $A = \{a_1, \ldots, a_n\}$. *We define* $R(A)$ *to be the* K*-subalgebra of* S *spanned by the set* $\{t^{a_1}X, \ldots, t^{a_n}X\}$. *That is,*

$$R(A) = K[t^{a_1}X, \ldots, t^{a_n}X].$$

• Since $R(A)$ is finitely generated over K by elements of degree 1, it is a standard graded algebra.

• We then have $R = \oplus_{h \geq 0} R_h$, where R_h is the K-vector space with basis the set $\{t^b X^h \mid b \in hA\}$.

▷ For instance, $R_2 = \langle t^{a_i + a_j} X^2 \mid 1 \leq i \leq j \leq n \rangle$.

• It follows that

$$\dim R_h = |hA|$$

for all $h \geq 0$.

Example revisited

Let $A \subset \mathbb{Z}$ satisfy $|5A| = 100$. Let $R = R(A) = \oplus_{h \geq 0} R_h$ be the associated standard graded algebra, with $\dim R_h = |hA|$ for all $h \geq 0$.

• So $\dim R_5 = 100$. Macaulay implies $|6A| = \dim R_6 \leq 100^{\langle 5 \rangle} = 152$.

• Claim: $\dim R_4 = |4A| \geq 61$. Assume for a contradiction $\dim R_4 \leq 60$. Now

$$60 = \binom{7}{4} + \binom{6}{3} + \binom{3}{2} + \binom{2}{1},$$

whence $60^{\langle 4 \rangle} = 98$. Macaulay would then imply

$$\dim R_5 \leq 60^{\langle 4 \rangle} = 98,$$

a contradiction. This proves the claim. **Summary:**

When $\vert 5A\vert = 100$	$\vert 4A\vert \geq$	$\vert 6A\vert \leq$
Plünnecke	40	251
Macaulay	61	152

Optimality

- Are the bounds $|4A| \geq 61, |6A| \leq 152$ optimal, at least over $\mathbb{Z}$?
- Probably not, but they are **close to it**. For instance, let

$$A = \{0, 1, 5, 8, 49\}.$$

Then $|5A| = 100$ as required, and $|4A| = 63, |6A| = 145$.

We conjecture that this is **best possible** over $\mathbb{Z}$.

Conjecture

Let $A \subset \mathbb{Z}$ satisfy $|5A| = 100$. Then

$$\begin{aligned} |4A| &\geq 63, \\ |6A| &\leq 145. \end{aligned}$$

Recovering Plünnecke's estimate

Let $A \subset \mathbb{Z}$ be finite with $|A| \geq 2$. Let $h \geq 2$.

Theorem (Plünnecke, 1970)

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

We recover this estimate as follows.

Theorem (E.-Mazumdar, 2020+)

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

where $\theta(x,h) \geq 1$ is a well-defined real number depending on $|hA|, h$.

For that, we need a condensed version of Macaulay's theorem. It involves $\binom{x}{h}$ for $x \in \mathbb{R}$.

Binomial coefficients as functions

For $h \in \mathbb{N}$ and $x \in \mathbb{R}$, denote as usual

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

Lemma

Let $h \geq 1$ be an integer. Then the map $y \mapsto \binom{y}{h}$ is an increasing bijection from $[h-1, \infty)$ to $[0, \infty)$. Hence $y_1 \leq y_2 \iff \binom{y_1}{h} \leq \binom{y_2}{h}$.

This is a direct consequence of Rolle's theorem.

Corollary

Let $h \geq 1$ be a positive integer. Let $z \in [0, \infty)$. Then there exists a unique real number $x \geq h-1$ such that $z = \binom{x}{h}$. If $z \geq 1$ then $x \geq h$.

A condensed version

(For smoother applications of Macaulay's theorem)

Theorem (E. 2018)

Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra. Let $i \geq 1$. Let $x \geq i-1$ be the unique real number such that $\dim R_i = \binom{x}{i}$. Then

$$\dim R_{i-1} \geq \binom{x-1}{i-1}, \quad \dim R_{i+1} \leq \binom{x+1}{i+1}.$$

Notation

For an integer $h \geq 1$ and a real number $x \geq h$, we denote

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

We can now prove our main result, namely:

Theorem

Let $h \geq 2$. Then $|(h-1)A| \geq \theta(x,h)|hA|^{(h-1)/h}$, where $x \geq h$ is the unique real number such that $|hA| = \binom{x}{h}$. Moreover, $\theta(x,h) \geq 1$.

Proof.

Condensed Macaulay directly implies $|(h-1)A| \geq \binom{x-1}{h-1}$. Now $\binom{x-1}{h-1} = \frac{h}{x}\binom{x}{h}$, since

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

Proof (continued).

Hence

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

Taking hth roots, we get $|(h-1)A| \geq \theta(x,h)|hA|^{(h-1)/h}$, as desired.

It remains to show $\theta(x,h) \geq 1$.

Proof (continued).

Equivalently, let us show $\theta(x,h)^h \geq 1$:

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

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

- In fact, we actually strengthen Plünnecke's estimate:

Proposition

For all $h \in \mathbb{N}$, $x \in \mathbb{R}$ such that $x > h \geq 2$, one has $1 < \theta(x,h) < e$.

Proof by elementary manipulations, using $\displaystyle\frac{h^h}{h!} < \sum_{k \in \mathbb{N}} \frac{h^k}{k!} = e^h$.

Proposition (Asymptotic behavior)

Let $h \geq 2$ be an integer. Then for x large,

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

In particular,

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

The proof uses the following

Approximation formulas, including Stirling's

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

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

Proposition

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

Indeed, Stirling's formula implies $\theta(n, \lfloor n/2 \rfloor) \approx 2\left(\frac{2}{\pi n}\right)^{1/n}.$

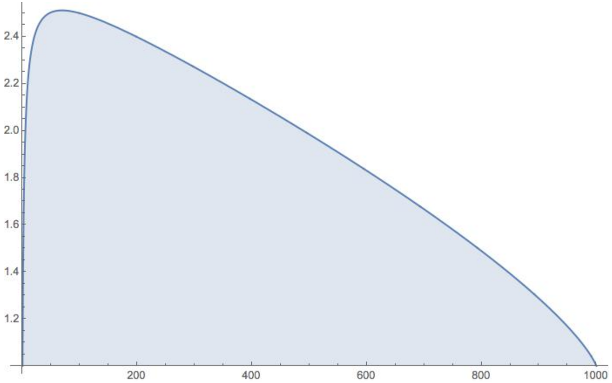

Figure: Values of $\theta(1000, h)$ for $h = 1, \ldots, 1000$

Numerical behavior of improvement factor $\theta(x, h)$

$\theta(x, 3)$	$>$	1.5	$x \geq 12$	
$\theta(48, 2)$	$>$	2		
$\theta(x, 6)$	$>$	2	$x \geq 1210$	
$\theta(1210, h)$	$>$	2		$h \in [6, 595]$
$\theta(x, h)$	$>$	2.70	$x \geq 200000$	$h \in [1200, 1300]$
$\theta(x, h)$	$>$	2.71	$x \geq 1100000$	$h \in [2600, 3700]$

Theoretical and numerical evidence suggest:

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

Some references

- S. Eliahou, Wilf's conjecture and Macaulay's theorem, J. Eur. Math. Soc. 20 (2018) 2105–2129.
- S. Eliahou and E. Mazumdar, Iterated sumsets and Hilbert functions, arXiv:2006.08998 [math.AC].
- J. Herzog and T. Hibi, Monomial ideals. Graduate Texts in Mathematics, vol. 260, Springer, London, 2011.
- F.S. Macaulay, Some properties of enumeration in the theory of modular systems, Proc. Lond. Math. Soc. 26 (1927) 531–555.
- M.B. Nathanson, Additive Number Theory, Inverse Problems and the Geometry of Sumsets. Graduate Texts in Mathematics, vol. 165, Springer, New York, 1996.
- H. Plünnecke, Eine zahlentheoretische Anwendung der Graphentheorie, J. Reine Angew. Math. 243 (1970) 171–183.
- T. Tao and V. Vu, Additive combinatorics. Cambridge Studies in Advanced Maths, 105. Cambridge University Press, 2006.

Thank you for your attention!