Wilf's conjecture and Macaulay's theorem

S. Eliahou

August 2015

Abstract

Let $S \subseteq \mathbb{N}$ be a numerical semigroup with multiplicity $m = \min(S \setminus \{0\})$, conductor $c = \max(\mathbb{N} \setminus S) + 1$ and minimally generated by e elements. Let L be the set of elements of S which are smaller than c. Wilf conjectured in 1978 that $|L|$ is bounded below by c/e. We show here that if $c \leq 3m$, then S satisfies Wilf's conjecture. Combined with a recent result of Zhai, this implies that the conjecture is asymptotically true as the genus $g(S) = |\mathbb{N} \setminus S|$ goes to infinity. One main tool in this paper is a classical theorem of Macaulay on the growth of Hilbert functions of standard graded algebras.

Keywords: Numerical semigroup; Wilf conjecture; Apéry element; graded algebra; Hilbert function; binomial representation; sumset.

MSC 2010: 05A20; 05A10; 11B75; 11D07; 20M14; 13A02.

1 Introduction

A *numerical semigroup* is a subset $S \subseteq \mathbb{N}$ closed under addition, containing 0 and of finite complement in $\mathbb{N}$. The elements of $\mathbb{N} \setminus S$ are called the *gaps* of S. The largest gap is denoted $F(S) = \max(\mathbb{N} \setminus S)$ and is called the *Frobenius number* of S. The integer $c(S) = F(S) + 1$ is known as the *conductor* of S. It satisfies $c(S) + \mathbb{N} \subseteq S$ and is minimal for that property. The number of gaps $g(S) = |\mathbb{N} \setminus S|$ is known as the *genus* of S, and the smallest nonzero element $m(S) = \min(S \setminus \{0\})$ as the *multiplicity* of S.

Every numerical semigroup S is finitely generated, i.e. is of the form

$$S = \langle a_1, \ldots, a_n \rangle = \mathbb{N}a_1 + \cdots + \mathbb{N}a_n$$

for suitable globally coprime integers $a_1, \ldots, a_n$. The least number n of generators of S is denoted $e = e(S)$ and is called the *embedding dimension* of S.

Is there a general upper bound for the density of the gaps of S in the integer interval $[0, c(S)-1]$? This question was asked by Wilf in [23] where, more precisely, he asked whether for $S = \langle a_1, \ldots, a_n \rangle$ the bound

$$\frac{|\mathbb{N} \setminus S|}{c(S)} \;\leq\; 1 - 1/n$$

might always hold[1]. This question is still widely open and is often referred to as Wilf's conjecture, in the following equivalent form. We shall denote $L(S) = S \cap [0, c(S)-1]$ thoughout, where 'L' stands for *left part* relative to the conductor.

Conjecture 1.1 (Wilf)**.** *Let S be a numerical semigroup generated by n elements. Then*

$$\frac{|L(S)|}{c(S)} \;\geq\; \frac{1}{n}.$$

The equivalence between the two formulations plainly follows from the formulas

$$|L(S)| + |\mathbb{N} \setminus S| \;=\; |\,[0, c-1]\,| \;=\; c,$$

where $c = c(S)$. Wilf gave the following example where equality holds in his conjecture:

$$S \;=\; \{0\} \cup (m + \mathbb{N}) \;=\; \{0, m, m+1, \ldots\}$$

for some integer $m \geq 2$. Indeed in this case, one has $|L(S)| = 1$, $c(S) = m$, and $e(S) = m$ since S is minimally generated by $\{m, m+1, \ldots, 2m-1\}$.

Another equality case in Wilf's conjecture is when $e(S) = 2$, i.e. for two-generated numerical semigroups $S = \langle a, b \rangle$ with $\gcd(a, b) = 1$. Indeed, nearly a century before the formulation of the conjecture, Sylvester showed in [22] that one has $c(S) = (a-1)(b-1)$ and $|L(S)| = c(S)/2$ in this case.

Finally, the last known equality case in Wilf's conjecture is the following:

$$S \;=\; m\mathbb{N} \cup (qm + \mathbb{N}) \;=\; \{0, m, 2m, \ldots, (q-1)m, qm, qm+1, qm+2, \ldots\}$$

for given integers $m, q \geq 1$. Indeed in this case, one has $|L(S)| = q$, $c(S) = qm$, and $e(S) = m$ since S is minimally generated by $\{m, qm+1, qm+2, \ldots, qm+m-1\}$. This case actually generalizes the first one by taking $q = 1$.

It is not known whether these are the only equality cases in Wilf's conjecture, but all independent computer experiments so far suggest that the above list might well be complete. See e.g. Question 8 in [14].

[1] Of course, the question is sharpest when $n = e(S)$, the embedding dimension of S.

Wilf's conjecture has been shown to hold under various hypotheses, including in [22] for $e = 2$ as mentioned above, in [8] for $e = 3$, in [7] for $|L| \leq 4$, by computer in [2] for genus $g \leq 50$ and more recently in [10] for $g \leq 60$, in [11] for $c \leq 2m$, and in [19] for $e \geq m/2$ and for $m \leq 8$.

In this paper, we extend the verification of Wilf's conjecture to all numerical semigroups S satisfying $c \leq 3m$, and in some other circumstances. The importance of the former case stems from a recent result of Zhai stating that, asymptotically as the genus $g(S)$ goes to infinity, the proportion of numerical semigroups S satisfying $c(S) \leq 3m(S)$ tends to 1 [24]. In a forthcoming paper, we will show that Wilf's conjecture holds for all numerical semigroups S satisfying $|L(S)| \leq 10$.

One key tool in the present paper is a suitable version of Macaulay's classical theorem on the growth of Hilbert functions of standard graded algebras.

Here are a few more details on the contents of this paper. Section 2 is devoted to basic notation and notions used throughout the paper. In Section 3, we study a convenient partition of a numerical semigroup S by its intersections with translates of the integer interval $[c, c+m-1]$, and we introduce the *profile* of S. A brief Section 4 gives some useful formulas in terms of Apéry elements with respect to m. Section 5 recalls some background material on standard graded algebras, Hilbert functions and Macaulay's theorem, and proposes a condensed version thereof which is well-suited to our subsequent applications to Wilf's conjecture. Section 6 is the heart of the paper, where all the material developed in the preceding sections is used to settle Wilf's conjecture in the case $2m < c \leq 3m$. A few more cases of the conjecture are then settled in the last Section 7.

Nice books are available for background information on numerical semigroups. See [17, 18].

2 More notation

In this paper we shall mostly use *integer intervals*, not real ones, except in Section 5. So, for rational numbers $x, y \in \mathbb{Q}$, we shall denote

$$\begin{aligned} [x,y] &= \{n \in \mathbb{Z} \mid x \leq n \leq y\}, \\ [x,y[&= \{n \in \mathbb{Z} \mid x \leq n < y\}. \end{aligned}$$

In particular, if $y \in \mathbb{Z}$ then $[x,y[= [x,y-1]$ and $\big|[x,y[\big| = y - x$. We shall also denote $[x,\infty[= \{n \in \mathbb{Z} \mid n \geq x\}$.

2.1 Primitives and decomposables

Let S be a numerical semigroup. We shall denote $S^* = S \setminus \{0\}$.

Definition 2.1. *We say that the element $x \in S^*$ is* decomposable *if*

$$x = x_1 + x_2$$

for some $x_1, x_2 \in S^*$, primitive *otherwise*[2]. *We denote by $D = D(S)$ the set of decomposable elements in S^*, and by $P = P(S)$ its set of primitive elements. Thus $S^* = P \dot\cup D$, the disjoint union of P and D.*

Denoting $A + B = \{a + b \mid a \in A, b \in B\}$ the *sum* of two subsets $A, B \subseteq \mathbb{Z}$, or simply $a + B$ if $A = \{a\}$, we have

$$D = S^* + S^*, \quad P = S^* \setminus D.$$

Clearly, every element $x \in S^*$ may be expressed as a finite sum of primitive elements. That is, the set P generates S as a semigroup. In fact, P is the unique *minimal generating set* of S, since every generating set of S necessarily contains P.

The finiteness of P, i.e. of the embedding dimension $e = |P|$, follows from the inclusion $P \subseteq [m, c + m[$, which itself is due to the inclusions

$$[c + m, \infty[\; = \; m + [c, \infty[\; \subseteq \; m + S^* \; \subseteq \; S^* + S^* \; = \; D.$$

Alternatively, one has $|P| \leq m$, since any two distinct primitive elements of S cannot be congruent mod m.

2.2 The associated constants q, ρ and $W(S)$

The following constants associated to S will be used throughout the paper, often tacitly so.

Notation 2.2. *Let S be a numerical semigroup. We denote by $q = q(S)$ and $\rho = \rho(S)$ the unique integers satisfying*

$$c = qm - \rho$$

with remainder $\rho \in [0, m[$. That is, we set $q = \lceil c/m \rceil$ and $\rho = qm - c$.

Example 2.3. *If $q = 1$, then $\rho = 0$, and $c = m$ since $c \geq m$ always. The semigroup structure of S is very simple in this case, namely*

$$S = \{0\} \cup [c, \infty[.$$

This case was met above already, as the first example of equality in Wilf's conjecture.

[2] Other commonly used terms for *primitive element* are *irreducible element* or *atom*.

Example 2.4. *If $q = 2$, then $m < c \leq 2m$. As mentioned above, Wilf's conjecture holds in this case as well [11]. See below for a new simpler proof.*

Thus, Wilf's conjecture holds for $q \leq 2$. In this paper, we extend this result to the much more demanding case $q = 3$.

Notation 2.5. *Let S be a numerical semigroup. We denote*

$$W(S) \ = \ e(S)|L(S)| - c(S).$$

It allows us to reformulate Wilf's conjecture in the following equivalent way.

Conjecture 2.6. *Let S be a numerical semigroup. Then $W(S) \geq 0$.*

The new results presented in this paper have been obtained via this formulation, by a successful evaluation of $W(S)$ in the cases under consideration.

3 A convenient partition

Throughout this section, S denotes a numerical semigroup with multiplicity m, conductor c and associated constants q, ρ.

3.1 The interval $[c, c+m[$

The integer interval $[c, c+m[$ of cardinality m is entirely contained in S and plays a special role in our present approach. We shall denote it by

$$I_q \ = \ [c, c+m[.$$

More generally, we shall consider the various translates of I_q by multiples of m.

Notation 3.1. *For $j \in \mathbb{Z}$, we denote by I_j the* translate *of I_q by $(j-q)m$, i.e.*

$$\begin{aligned} I_j &= I_q + (j-q)m \\ &= [c-(q-j)m, c-(q-j-1)m[\\ &= [jm-\rho, (j+1)m-\rho[. \end{aligned}$$

For instance, we have

$$I_{q-1} \ = \ [c-m, c[, \quad I_1 \ = \ [m-\rho, 2m-\rho[, \quad I_0 \ = \ [-\rho, m-\rho[.$$

As the various I_j for $j \geq q+1$ need not be distinguished here, we denote

$$I_\infty \ = \ \bigcup_{j \geq q+1} I_j \ = \ [c+m, \infty[.$$

The partition of S induced by the intervals I_j's will be used throughout.

Notation 3.2. *For all $j \geq 0$, we denote*

$$S_j \;=\; S \cap I_j \;=\; S \cap [jm - \rho, (j+1)m - \rho[.$$

Note the following straightforward properties:

$$\begin{array}{rcl} jm & \in & S_j \quad \forall j \geq 0, \\ S_0 & = & S \cap [-\rho, m-\rho[\;=\; \{0\}, \\ S_1 & \subseteq & [m, 2m-\rho[, \quad (\text{as } \min S_1 = m) \\ S_{q-1} & \subsetneq & I_{q-1}, \quad (\text{as } c-1 \in I_{q-1} \setminus S) \\ S_{q+j} & = & I_{q+j} \quad \forall j \geq 0. \end{array}$$

Lemma 3.3. *Let $L = L(S) = S \cap [0, c[$. We have*

$$\begin{array}{rcl} L & = & S_0 \,\dot\cup\, S_1 \,\dot\cup \cdots \dot\cup\, S_{q-1}, \\ |L| & = & 1 + |S_1| + \cdots + |S_{q-1}|. \end{array}$$

Proof. Straightforward from the definitions, since $L \subseteq [0, c[\subseteq \dot\bigcup_{0 \leq j \leq q-1} I_j$. □

Lemma 3.4. *We have*

$$m + S_j \;\subseteq\; S_{j+1} \quad \textit{for all } j \geq 0$$

and, in particular,

$$1 \;=\; |S_0| \;\leq\; |S_1| \;\leq\; \cdots \;\leq\; |S_{q-1}|.$$

Proof. Straightforward from the definitions. □

Proposition 3.5. *For all $i, j \geq 1$, we have a* weak grading *as follows:*

$$\begin{array}{rcrl} S_1 + S_j & \subseteq & S_{1+j} \,\cup\, S_{1+j+1} & \textit{for } j \geq 1, \\ S_i + S_j & \subseteq & S_{i+j-1} \,\cup\, S_{i+j} \,\cup\, S_{i+j+1} & \textit{for } i, j \geq 2. \end{array}$$

Proof. For $i, j \geq 1$, we have

$$(im - \rho) + (jm - \rho) \;=\; (i+j)m - 2\rho \;>\; (i+j-1)m - \rho.$$

Similarly, we have

$$((i+1)m - \rho - 1) + ((j+1)m - \rho - 1) \;<\; (i+j+2)m - \rho - 1.$$

This settles the second inclusion. Assume now $i = 1$. Since $\min S_1 = m$ and $m + S_j \subseteq S_{j+1}$, we have

$$(S_1 + S_j) \cap S_j \;=\; \emptyset.$$

The first inclusion now follows from the second one. □

When the above weak grading happens to be a true grading up to level $q-1$, more precisely if

$$S_i + S_j \;=\; S_{i+j}$$

for all $i, j \geq 0$ such that $i+j \leq q-1$, Wilf's conjecture can be shown to hold in this instance. See Theorem 7.1.

The following estimate, limiting the size of $(S_i+S_j) \cap S_{i+j-1}$ by $\rho = \rho(S)$, will play a somewhat subtle role later on.

Proposition 3.6. *For all $i, j \geq 1$, we have*

$$\begin{aligned} |(S_i+S_j) \cap S_{i+j-1}| &\leq \rho, \\ |(S_i+S_j) \cap S_{i+j+1}| &\leq m-\rho-1. \end{aligned}$$

Proof. We have

$$S_i + S_j \;\subseteq\; [(i+j)m-2\rho, (i+j+2)m-2\rho-1[.$$

It follows that

$$\begin{aligned} (S_i+S_j) \cap S_{i+j-1} &\subseteq [(i+j)m-2\rho, (i+j)m-\rho[\\ (S_i+S_j) \cap S_{i+j+1} &\subseteq [(i+j+1)m-\rho, (i+j+2)m-2\rho-1[. \quad \square \end{aligned}$$

3.2 The profile of a numerical semigroup

It is useful to record how many primitive elements there are in the various levels S_j.

Notation 3.7. *For $j \geq 1$, let*

$$\begin{aligned} P_j &= P \cap S_j, \quad p_j = |P_j|, \\ D_j &= D \cap S_j, \quad d_j = |D_j|. \end{aligned}$$

Note that $p_1 \geq 1$ since $m \in P_1$. Note also that $S_1 = P_1$, i.e. $D_1 = \emptyset$, as $x \in D$ implies $x \geq 2m$.

Definition 3.8. *The* profile *of S is the $(q-1)$-uple*

$$(p_1, \ldots, p_{q-1}) \;\in\; \mathbb{N}^{q-1}.$$

It may be shown that any $(p_1, \ldots, p_{q-1}) \in \mathbb{N}^{q-1}$ with $p_1 \geq 1$ is the profile of a suitable numerical semigroup S. For constructing such an S, one should start with $m(S) \geq p_1 + \cdots + p_{q-1}$ at the very least, but the larger the difference $m - \sum p_i$ is, the more room there is for the construction of S. For instance, one may start with $P_1 = [m, m+p_1[$, $P_2 = [2(m+p_1), 2(m+p_1)+p_2[$, and so on.

3.3 Left and right primitives

Among the primitive elements of the numerical semigroup S, we distinguish the *left ones*, namely those smaller than c, and the *right ones*, those contained in $[c, c+m[$. That is, the left primitives are the elements of $P \cap L$, and the right ones are those belonging to $P_q = P \cap I_q$. This covers all of P, since $P \subseteq [m, c+m[\subseteq L \cup I_q$.

Note that the right primitives are entirely determined by the left ones together with c, in the following sense. In $S_q = I_q$, all decomposable elements are sums of left primitives only. Thus, the right primitives are those elements in I_q which are not attained by sums of left primitives. That is, we have

$$P_q \ = \ I_q \setminus D.$$

Or equivalently,

$$S \ = \ \langle P \cap L \rangle \cup [c, \infty[, \tag{1}$$

since $P_q = P \cap [c, \infty[$. This specificity of P_q was our reason not to include its cardinality p_q in the profile $(p_1, \ldots, p_{q-1})$ of S. Incidentally, note that p_q is the *down degree* of the vertex S in the tree of all numerical semigroups. (See e.g. [2, 3, 18].)

The description of S by (1) justifies introducing a specific notation.

Notation 3.9. *For any nonempty subset $A \subseteq \mathbb{N}^*$ and $c \in \mathbb{N}^*$, we set*

$$\langle A \rangle_c \ = \ \langle A \rangle \cup [c, \infty[\ = \ \langle A \cup [c, c+m[\rangle,$$

where $m = \min A$. It is a numerical semigroup of multiplicity at most m and conductor at most c.

For example, consider the numerical semigroup

$$S \ = \ \langle 10, 15 \rangle_{23} \ = \ \langle 10, 15 \rangle \cup [23, \infty[.$$

Its left primitives are 10 and 15 and its conductor is 23. We have $q = \lceil 23/10 \rceil = 3$, and the decomposable elements in $S_3 = [23, 33[$ are 25 and 30. Therefore, the right primitives in S are 23,24,26,27,28,29,31,32. That is, we have

$$\langle 10, 15 \rangle_{23} \ = \ \langle 10, 15, 23, 24, 26, 27, 28, 29, 31, 32 \rangle.$$

Note that the conductor of the semigroup $S = \langle A \rangle_c$ may occasionally be strictly smaller than c. This happens exactly when $S' = \langle A \rangle$ is itself a numerical semigroup (equivalently, when $\gcd(A) = 1$) whose conductor $c(S')$ is strictly smaller than c. In that case, we simply have $\langle A \rangle_c \ = \ \langle A \rangle$. For instance, we have $\langle 3, 5 \rangle_{10} = \langle 3, 5 \rangle_8 = \langle 3, 5 \rangle$ with conductor 8, and $\langle 3, 5 \rangle_7 = \langle 3, 5, 7 \rangle = \langle 3 \rangle_5$ with conductor 5.

3.4 The constant $W_0(S)$

The number p_q of right primitives is involved in two terms in the formula $W(S) = |P||L| - c = |P||L| - qm + \rho$. Indeed, we have

$$\begin{aligned} |P| &= |P \cap L| + p_q, \\ m &= p_q + d_q, \end{aligned}$$

since $m = \big|[c, c+m[\big| = |I_q| = p_q + d_q$. Factoring out p_q from $W(S)$ gives rise to the following closely related constant.

Definition 3.10. *Let S be a numerical semigroup. We denote*

$$W_0(S) \;=\; |P \cap L||L| - qd_q + \rho.$$

As a side remark, note that $|P \cap L| = p_1 + \cdots + p_{q-1}$, the sum of the entries of the profile of S. By construction, we have

$$W(S) \;=\; p_q(|L| - q) + W_0(S). \tag{2}$$

Proposition 3.11. *Let S be a numerical semigroup. Then*

$$W(S) \;\geq\; W_0(S).$$

In particular, if $W_0(S) \geq 0$, then S satisfies Wilf's conjecture.

Proof. We have $|L| \geq q$ since $L \supseteq \{0, m, \ldots, (q-1)m\}$. The stated inequality now follows from (2). □

As an application, we will settle Wilf's conjecture for $q = 3$ precisely by showing that the stronger inequality $W_0(S) \geq 0$ always holds in this case.

Remark 3.12. *The inequality $W_0(S) \geq 0$ is equivalent to the fact that d_q, the number of decomposables in $I_q = [c, c+m[$, is bounded above as follows:*

$$qd_q \;\leq\; |P \cap L||L| + \rho.$$

3.5 $W_0(S)$ may be negative

While the inequality $W_0(S) \geq 0$ will be shown to hold for $q \leq 3$, it no longer holds in general for $q \geq 4$. The first counterexamples were discovered by Jean Fromentin [9], who showed by exhaustive computer search that all the $33,474,094,027,610$ numerical semigroups S of genus $g \leq 60$ do satisfy $W_0(S) \geq 0$ *except in exactly five instances*, namely

$$\langle 14,22,23\rangle_{56}\,,\;\; \langle 16,25,26\rangle_{64}\,,\;\; \langle 17,26,28\rangle_{68}\,,\;\; \langle 17,27,28\rangle_{68} \;\text{ and }\; \langle 18,28,29\rangle_{72}$$

of genus 43, 51, 55, 55 and 59, respectively. These sole counterexamples up to genus 60 all satisfy $W_0(S) = -1$, $c = 4m$ and $W(S) \geq 35$. As a corollary [10], it follows that Wilf's *conjecture is true up to genus 60.*

The case $W_0(S) < 0$ seems to be very rare indeed. An interesting problem would be to characterize all numerical semigroups S belonging to it.

3.6 The case $q = 2$

It was shown in [11] that Wilf's conjecture holds for $q = 2$, i.e. in case $m < c \leq 2m$. Here is a short proof of a slightly stronger statement.

Proposition 3.13. *Let S be a numerical semigroup with $q = 2$, i.e. with $c = 2m - \rho$ and $\rho \in [0, m-1[$. Then*

$$W_0(S) \;\geq\; \rho \;\geq\; 0.$$

Proof. Let $k = p_1$. Then $|L| = 1 + k$, since $L = S_0 \,\dot\cup\, S_1 = \{0\} \,\dot\cup\, P_1$ here. Now

$$\begin{aligned} W_0(S) - \rho &= |P \cap L||L| - 2d_2 \\ &= k(1+k) - 2d_2. \end{aligned}$$

But

$$d_2 \;\leq\; k(k+1)/2,$$

since any decomposable element in $S_2 = [c, c+m[$ is a sum of two primitives in P_1. Therefore $W_0(S) - \rho \geq 0$. □

4 Apéry elements

Throughout this section again, S denotes a numerical semigroup with multiplicity m, conductor c and associated constants q, ρ. We shall set up formulas for $|L|$ and d_q involving Apéry elements with respect to $m = m(S)$, in the spirit of those of Selmer [21].

Definition 4.1. *An* Apéry element *(with respect to m) is an element $x \in S$ such that $x - m \notin S$. We shall denote by $X \subset S$ the set of all Apéry elements of S.*

Note that a common notation for X is $\mathrm{Ap}(S,m)$. It follows from the definition that X is contained in $[0, c+m[$ and contains both extremities 0 and $c+m-1$. Moreover, we have $|X| = m$. Indeed, for every class λ mod m, there is a unique $a \in X$ of class λ, namely the smallest element of that class in S. Note also that

$$P \setminus \{m\} \;\subseteq\; X,$$

since clearly a primitive element cannot belong to $m + S$, except m itself.

Notation 4.2. *We denote by $N \subset S$ the set of non-Apéry elements, i.e. $N = S \setminus X$.*

For example, we have $m \in N$. It is clear that $S + N \subseteq N$. Note also that N and X may equivalently be described as $N = m + S$ and $X = S \setminus N$.

Notation 4.3. *For all $0 \le j \le q$, we denote*

$$X_j \ = \ X \cap S_j.$$

For instance, we have

$$X_0 \ = \ \{0\}, \quad X_1 \ = \ S_1 \setminus \{m\}, \quad X_2 \ \subseteq \ 2X_1 \dot{\cup} P_2.$$

4.1 A formula for $W_0(S)$

Here is a useful formula for $W_0(S)$ in terms of the cardinalities of the X_i's.

Notation 4.4. *For $0 \le i \le q$, we denote*

$$\alpha_i \ = \ \begin{cases} |X_i| & \text{if } i \le q-1, \\ |X_q \setminus P| & \text{if } i = q. \end{cases}$$

In particular, if $q \ge 2$, we have

$$\alpha_0 \ = \ 1, \quad \alpha_1 \ = \ p_1 - 1, \quad \alpha_i \ \ge \ p_i \quad \text{for all } \ 2 \le i \le q-1, \tag{3}$$

since all primitives except m are Apéry elements. But note that α_q only counts the *decomposable* Apéry elements in S_q, ignoring P_q. Since $|X| = m$ and since $X_q \setminus P$ may be a strict subset of X_q, we have

$$\alpha_0 + \alpha_1 + \cdots + \alpha_q \ \le \ m.$$

We now identify the left-hand sum with $d_q = |D_q|$.

Proposition 4.5. *Let S be a numerical semigroup. We have*

$$d_q \quad = \quad \sum_{i=0}^{q} \alpha_i, \tag{4}$$

$$|L(S)| \quad = \quad \sum_{i=0}^{q-1} (q-i)\alpha_i. \tag{5}$$

Proof. On the one hand, we have

$$m \ = \ |X| \ = \ \sum_{i=0}^{q} |X_i| \ = \ \sum_{i=0}^{q-1} \alpha_i + (\alpha_q + p_q).$$

On the other hand, we have $m = |S_q| = p_q + d_q$. Comparing both expressions of m yields formula (4). Now, by definition of the Apéry elements, for $1 \leq i \leq q-1$ we have

$$S_i \;=\; (m + S_{i-1}) \,\dot\cup\, X_i,$$

and hence

$$|S_i| \;=\; |S_{i-1}| + \alpha_i. \tag{6}$$

Since $|L| = |S_0| + |S_1| + \cdots + |S_{q-1}|$, it follows by a repeated application of (6) that

$$|L| \;=\; q + (q-1)\alpha_1 + \cdots + \alpha_{q-1},$$

as desired. □

Corollary 4.6. *We have*

$$W_0(S) - \rho \;=\; \Big(\sum_{i=0}^{q-1} p_i\Big)\Big(\sum_{i=0}^{q-1}(q-i)\alpha_i\Big) - q\sum_{i=0}^{q}\alpha_i.$$

Proof. Straightforward from the formula $W_0(S) - \rho = |P \cap L||L| - qd_q$ and Proposition 4.5. □

5 The Hilbert function of standard graded algebras

We now turn to standard graded algebras, Hilbert functions thereof, Macaulay's theorem, and a condensed version of it which is well-suited to our subsequent applications to Wilf's conjecture. We start by recalling a few basic definitions. In this section, the notation $[x,\infty[$ refers to the usual *real* intervals.

Definition 5.1. *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 $R_0 = \mathbb{K}$, $R_iR_j \subseteq R_{i+j}$ 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 $R_iR_j = R_{i+j}$ for all $i, j \geq 0$.

Definition 5.2. *Let $R = \oplus_{i\geq 0} R_i$ be a standard graded algebra. The* Hilbert function *of R is the map $i \mapsto h_i$ associating to each $i \in \mathbb{N}$ the dimension*

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

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

In particular, we have $h_0 = 1$, and R is generated as a $\mathbb{K}$-algebra by any h_1 linearly independent elements of R_1.

5.1 Macaulay's theorem

Macaulay's theorem rests on the so-called *binomial representations* of integers. Here is some background information about them.

Proposition 5.3. *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. [5, 16]. □

This expression is called the *i*th *binomial representation of a*.

Notation 5.4. *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 then denote $a^{\langle i \rangle} = \sum_{j=1}^{i} \binom{a_j+1}{j+1}$.*

Note that the right-hand side is a valid $(i+1)$st binomial representation of some positive integer, namely of the integer it sums to.

Here is Macaulay's classical result which constrains the possible Hilbert functions of standard graded algebras [13].

Theorem 5.5. *Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra over a field $\mathbb{K}$, with Hilbert function $h_i = \dim_{\mathbb{K}} R_i$ for all $i \geq 0$. Let i be a positive integer. Then*

$$h_{i+1} \ \leq \ h_i^{\langle i \rangle}.$$

The converse also holds in Macaulay's theorem, but we shall not need it here. That is, satisfying these inequalities for all $i \geq 1$ *characterizes* the Hilbert functions of standard graded algebras. See e.g. [5, 15, 16].

For our applications to Wilf's conjecture, we shall derive from Macaulay's theorem a condensed version of it. To this end we first need some facts concerning binomial coefficients.

5.2 Some binomial inequalities

Given $i \in \mathbb{N}$ and $x \in \mathbb{R}$, we denote as usual

$$\binom{x}{i} \ = \ \frac{x(x-1)\dots(x-i+1)}{i!}$$

if $i \geq 1$, or else 1 if $i = 0$. We shall repeatedly use the following well-known fact.

Lemma 5.6. *Let $i \geq 1$ be an integer. Then the map $x \mapsto \binom{x}{i}$ is an increasing continuous bijection (in fact, a homeomorphism) from $[i-1,\infty[$ to $[0,\infty[$.*

Proof. By Rolle's theorem, the derivative of the polynomial $f = X(X-1)\cdots(X-i+1)$ is of the form $f' = (X-\lambda_1)\cdots(X-\lambda_{i-1})$ where $j-1 < \lambda_j < j$ for all $1 \leq j \leq i-1$. Therefore f induces an increasing continuous function from $[i-1,\infty[$ onto $[0,\infty[$. □

Consequently, given $i \geq 1$ and any real number $y \geq 0$, there is a unique real number $x \geq i-1$ such that

$$y = \binom{x}{i}.$$

Moreover, for any real numbers $u, v \geq i-1$, we have

$$u < v \iff \binom{u}{i} < \binom{v}{i}. \tag{7}$$

The following result is due to Lovász [12].

Lemma 5.7. *Let $r \geq 2$ be an integer, and let $u \geq v \geq w$ be real numbers such that $v \geq r-1$ and $w \geq r-2$. Assume $\binom{u}{r} = \binom{v}{r} + \binom{w}{r-1}$. Then $\binom{u}{r-1} \leq \binom{v}{r-1} + \binom{w}{r-2}$.*

This appears as an exercise, with proof, in [12]. It is actually stated in a slightly stronger way, where $r-1$ is replaced throughout the conclusion by any integer k such that $1 \leq k \leq r-1$. But of course, the two versions are equivalent.

Proof. See [12]. The hint provided by Lovász is to use the following identity:

$$\binom{u+v+1}{m} = \sum_{k=0}^{m} \binom{u+k}{k}\binom{v-k}{m-k}.$$ □

Here is a straightforward consequence that we shall need.

Proposition 5.8. *Let $r \geq 1$ be an integer, and let $u \geq v \geq w$ be real numbers such that $v \geq r$ and $w \geq r-1$. Assume $\binom{u}{r} = \binom{v}{r} + \binom{w}{r-1}$. Then $\binom{u+1}{r+1} \geq \binom{v+1}{r+1} + \binom{w+1}{r}$.*

Proof. We first claim that the following relation holds:

$$\binom{u}{r+1} \geq \binom{v}{r+1} + \binom{w}{r}. \tag{8}$$

For otherwise, assume on the contrary that the left-hand side were strictly smaller than the right-hand side. Since the function $x \mapsto \binom{x}{r+1}$ is a strictly increasing bijection from $[r,\infty[$ to $[0,\infty[$, there would exist $z > u$ such that

$$\binom{u}{r+1} < \binom{z}{r+1} = \binom{v}{r+1} + \binom{w}{r}.$$

Lemma 5.7 would then imply

$$\binom{z}{r} \le \binom{v}{r} + \binom{w}{r-1},$$

which is absurd since by hypothesis, the right-hand side equals $\binom{u}{r}$ and $z > u$. Now, adding $\binom{u}{r}$ to (8), the hypothesis implies

$$\binom{u}{r+1} + \binom{u}{r} \ge \binom{v}{r+1} + \binom{w}{r} + \binom{v}{r} + \binom{w}{r-1}$$

which in turn, by the basic Pascal triangle identity, yields the claimed inequality. □

5.3 An upper bound on $a^{\langle i \rangle}$

We shall also need the following upper bound on $a^{\langle i \rangle}$.

Theorem 5.9. *Let $a \ge 0$, $i \ge 1$ be integers, and let $x \ge i-1$ be the unique real number such that $a = \binom{x}{i}$. Then $a^{\langle i \rangle} \le \binom{x+1}{i+1}$.*

Proof. By induction on i. For $i = 1$, we have $x = a$ and the statement directly follows from the definition. Assume now $i \ge 2$ and the statement true for $i-1$. Consider the ith binomial representation of a:

$$a = \sum_{j=1}^{i} \binom{a_j}{j} = \binom{a_i}{i} + b,$$

where

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

By definition of the operation $t \mapsto t^{\langle i \rangle}$, we have

$$a^{\langle i \rangle} = \binom{a_i+1}{i+1} + b^{\langle i-1 \rangle}.$$

Let $y \geq i-2$ be the unique real number such that $b = \binom{y}{i-1}$. Then

$$a = \binom{x}{i} = \binom{a_i}{i} + \binom{y}{i-1}. \tag{9}$$

By the induction hypothesis, we have $b^{\langle i-1 \rangle} \leq \binom{y+1}{i}$. It follows that

$$a^{\langle i \rangle} \leq \binom{a_i+1}{i+1} + \binom{y+1}{i}.$$

But now, it follows from (9) and Proposition 5.8 that

$$\binom{x+1}{i+1} \geq \binom{a_i+1}{i+1} + \binom{y+1}{i}.$$

This concludes the proof of the theorem. □

5.4 A condensed version of Macaulay's theorem

We now express Macaulay's theorem in a condensed version which is well suited to our present purposes. It is inspired by a similarly condensed version of the Kruskal-Katona theorem, due to Lovász, again given as an exercise in his book [12]. See also the book [1] of Bollobás, where it is nicely presented and where we first spotted it.

Theorem 5.10. *Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra over the field $\mathbb{K}$, with Hilbert function $h_i = \dim_{\mathbb{K}} R_i$ for all $i \geq 0$. Let $r \geq 1$ be an integer. Let $x \geq r-1$ be the unique real number satisfying $h_r = \binom{x}{r}$. Then*

$$h_{r-1} \geq \binom{x-1}{r-1} \quad \text{and} \quad h_{r+1} \leq \binom{x+1}{r+1}.$$

Proof. Let $a = h_r$. By Macaulay's Theorem 5.5 followed by Theorem 5.9, we have $h_{r+1} \leq a^{\langle r \rangle} \leq \binom{x+1}{r+1}$. Assume now, for a contradiction, that

$$h_{r-1} < \binom{x-1}{r-1}. \tag{10}$$

Let then $y \geq r-2$ be the unique real number such that $h_{r-1} = \binom{y}{r-1}$. Then $y < x-1$ by Lemma 5.6. It would then follow from the statement just proved and Lemma 5.6 that

$$h_r \leq \binom{y+1}{r} < \binom{x}{r},$$

contrary to our hypothesis. Therefore (10) is absurd and we are done. □

5.5 Averaging the Hilbert function

We conclude this section with a result on the average of initial values of the Hilbert function of a standard graded algebra, namely that for any $q \geq 1$, the average of the h_i's for $0 \leq i \leq q-1$ is bounded below by the ratio h_q/h_1. Note the similarity of the formula below with that of Remark 3.12. This will be used in Section 7 to verify one further case of Wilf's conjecture.

Theorem 5.11. *Let $R = \oplus_{i \geq 0} R_i$ be a standard graded algebra over the field $\mathbb{K}$, with Hilbert function $h_i = \dim_{\mathbb{K}} R_i$ for all $i \geq 0$. Let $q \geq 1$ be an integer. Then*

$$qh_q \;\leq\; h_1\big(1+h_1+\cdots+h_{q-1}\big).$$

Proof. Let $x \geq q-1$ be the unique real number such that $h_q = \binom{x}{q}$. By repeatedly applying Theorem 5.10 together with Lemma 5.6, we get

$$h_{q-i} \;\geq\; \binom{x-i}{q-i} \tag{11}$$

for all $0 \leq i \leq q$. Summing over all i in this range, this implies

$$\sum_{i=1}^{q} h_{q-i} \;\geq\; \sum_{i=1}^{q} \binom{x-i}{q-i}.$$

Now the sum on the right-hand side is equal to $\binom{x}{q-1}$. Therefore, we have

$$\sum_{i=1}^{q} h_{q-i} \;\geq\; \binom{x}{q-1}.$$

By the identity

$$\binom{x}{q-1} \;=\; \frac{q}{x-q+1}\binom{x}{q},$$

it follows that

$$(x-q+1)\sum_{i=1}^{q} h_{q-i} \;\geq\; q\binom{x}{q} = qh_q.$$

And finally, it follows from (11) at $i = q-1$ that $h_1 \geq x-q+1$, yielding the announced inequality. □

6 Wilf's conjecture for $q = 3$

We now settle Wilf's conjecture for numerical semigroups satisfying $q = 3$, i.e. $2m < c \leq 3m$. The profile of any such semigroup is of the form (p_1, p_2) with $p_1, p_2 \in \mathbb{N}$ and $p_1 \geq 1$. Our first step consists in reducing the verification of the conjecture to the case $p_2 = 0$. Macaulay's theorem, or its condensed version, will then be needed in the more difficult remaining step, that of settling the case of profile $(p_1, 0)$.

Notation 6.1. *For a subset $A \subseteq \mathbb{Z}$ and an integer $i \geq 1$, we shall denote by iA the ith iterated sumset*

$$iA = \underbrace{A + \cdots + A}_{i}.$$

Thus $2P_2 = P_2 + P_2$ for instance, as involved below.

6.1 Reduction to profile $(p_1, 0)$

The announced reduction is relatively straightforward, except that the constant $\rho = \rho(S)$ plays a somewhat subtle role and must be treated with sufficient care.

Proposition 6.2. *Let S be a numerical semigroup with profile (p_1, p_2). Let $S' = \langle P_1 \rangle_c = \langle P_1 \rangle \cup [c, \infty[$, so that $S' \subseteq S$ has profile $(p_1, 0)$ and same multiplicity m and conductor c as S. Then*

$$W_0(S) \geq W_0(S') - \rho.$$

Proof. Consider the decomposable elements of S in $I_q = I_3$. We have

$$D_3(S) = D_3(S') \cup \big((P_1 + P_2) \cap I_3\big) \cup \big(2P_2 \cap I_3\big).$$

Thus, if follows from Proposition 3.6 involving ρ, and the obvious sumset estimates $|2A| \leq |A|(|A|+1)/2$ and $|A+B| \leq |A||B|$ for finite subsets $A, B \subset \mathbb{Z}$, that

$$\begin{aligned} d_3(S) &\leq d_3(S') + |(P_1 + P_2) \cap I_3| + |2P_2 \cap I_3| \\ &\leq d_3(S') + p_1 p_2 + \min(\rho, p_2(p_2+1)/2). \end{aligned}$$

Plugging this inequality in the expression of $W_0(S)$, we get

$$\begin{aligned} W_0(S) &= |P \cap L||L| - 3d_3 + \rho \\ &\geq |P \cap L||L| - 3d_3(S') - 3p_1 p_2 - 3\min(\rho, p_2(p_2+1)/2) + \rho. \end{aligned}$$

Claim. For the sum of the last two terms, the following bound holds:

$$-3\min(\rho, p_2(p_2+1)/2) + \rho \geq -p_2(p_2+1). \tag{12}$$

Indeed, if $\rho \leq p_2(p_2+1)/2$, then $\min(\rho, p_2(p_2+1)/2) = \rho$, whence

$$-3\min(\rho, p_2(p_2+1)/2) + \rho \;=\; -2\rho \;\geq\; -p_2(p_2+1).$$

Similarly, if $\rho > p_2(p_2+1)/2$, then $\min(\rho, p_2(p_2+1)/2) = p_2(p_2+1)/2$, whence

$$-3\min(\rho, p_2(p_2+1)/2) + \rho \;=\; -3p_2(p_2+1)/2 + \rho \;>\; -2p_2(p_2+1)/2.$$

This establishes the claim.

Plugging (12) into the above estimate of $W_0(S)$, we get

$$W_0(S) \;\geq\; |P \cap L||L| - 3d_3(S') - 3p_1p_2 - p_2(p_2+1). \tag{13}$$

Now, we have $|P \cap L| = p_1 + p_2$ and $|L| = 1 + p_1 + (p_2 + d_2)$. It follows that

$$\begin{aligned}
|P \cap L||L| - 3d_3(S') &= (p_1+p_2)(1+p_1+p_2+d_2) - 3d_3(S') \\
&= p_2^2 + p_2(1+2p_1+d_2) + p_1(1+p_1+d_2) - 3d_3(S') \\
&= p_2^2 + p_2(1+2p_1+d_2) + W_0(S') - \rho,
\end{aligned}$$

by definition of $W_0(S')$ and since $D_2(S) = D_2(S')$. Going back to (13), the above yields

$$\begin{aligned}
W_0(S) &\geq |P \cap L||L| - 3d_3(S') - 3p_1p_2 - p_2(p_2+1) \\
&= p_2^2 + p_2(1+2p_1+d_2) + W_0(S') - \rho - 3p_1p_2 - p_2(p_2+1) \\
&= p_2(d_2 - p_1) + W_0(S') - \rho.
\end{aligned}$$

Finally, since $m + P_1 \subseteq D_2$, we have $d_2 \geq p_1$. It follows that $W_0(S) \geq W_0(S') - \rho$, as claimed. □

Consequently, in order to settle Wilf's conjecture for the case $q = 3$, it remains to prove $W_0(S') \geq \rho$ for any numerical semigroup S' with profile $(k, 0)$. This is done in Theorem 6.4 below. We start with a counting lemma whose proof relies on our condensed version of Macaulay's theorem.

6.2 Counting some Apéry elements

We shall need the following bound relating the numbers of Apéry elements in $2X_1 \cap X_2$ and in $3X_1 \cap X_3$ in a numerical semigroup S of the desired profile.

Lemma 6.3. *Assume the profile of S is $(k, 0)$. Let $x \in \mathbb{R}$ be such that $x \geq 1$ and*

$$|2X_1 \cap X_2| \;=\; \binom{x}{2}.$$

Then

$$|3X_1 \cap X_3| \;\leq\; \binom{x+1}{3}.$$

Proof. It suffices to construct a standard graded algebra R' with the property that

$$\dim R'_i \;=\; |iX_1 \cap X_i|$$

for $i = 1,2$ and then apply Macaulay's theorem or its condensed version. We now proceed to construct such an algebra R'.

By hypothesis on the profile of S, we have $P \cap L = P_1 = \{m = a_1 < a_2 < \cdots < a_k\} = \{m\} \dot\cup X_1$. Consider the standard graded algebra

$$R \;=\; \mathbb{K}[t^{a_1}u, \ldots, t^{a_k}u],$$

where the variables t and u have degree 0 and 1, respectively. Let $A = P_1$. Then, for all $i \geq 0$, we have

$$\dim R_i \;=\; |iA|.$$

Now of course, we have

$$\begin{aligned} 2A &= (2A \cap X_2) \dot\cup (2A \setminus X_2), \\ 3A &= (3A \cap X_3) \dot\cup (3A \setminus X_3). \end{aligned}$$

Moreover, since

$$2A \;=\; (m+A) \cup 2X_1 \quad \text{and} \quad (m+A) \cap X_2 \;=\; \emptyset,$$

we have $2A \cap X_2 = 2X_1 \cap X_2$. Similar properties hold for $3A \cap X_3$. Thus, we obtain the following partitions:

$$\begin{aligned} 2A &= (2X_1 \cap X_2) \;\dot\cup\; (2A \setminus X_2), \\ 3A &= (3X_1 \cap X_3) \;\dot\cup\; (3A \setminus X_3). \end{aligned}$$

Consider the ideal $J \subseteq R$ spanned by all monomials of the form

$$t^b u^2 \;\text{ and }\; t^c u^3,$$

where

$$b \in 2A \setminus X_2 \quad \text{and} \quad c \in 3A \setminus X_3.$$

Let

$$R' \;=\; R/J.$$

It is still a standard graded algebra. Regarding its Hilbert function, we claim:

$$\begin{aligned} \dim R'_2 &= |2X_1 \cap X_2|, \\ \dim R'_3 &= |3X_1 \cap X_3|. \end{aligned}$$

The first equality follows from the above partition $2A = (2X_1 \cap X_2) \dot\cup (2A \setminus X_2)$. The second one follows from the analogous partition $3A = (3X_1 \cap X_3) \dot\cup (3A \setminus X_2)$ and the following inclusion, which shows that killing the monomials $t^b u^2$ of J in the quotient R/J does not kill any monomial of the form $t^d u^3$ for $d \in X_3$:

$$A + (2A \setminus X_2) \ \subseteq\ 3A \setminus X_3. \tag{14}$$

Indeed, we have $2A \setminus X_2 \subseteq (m+S) \cup I_3$, i.e., any $z \in 2A \setminus X_2$ either is not an Apéry element or belongs to I_3. Inclusion (14) now follows from the inclusions

$$\begin{aligned} A + (m+S) &\subseteq m+S, \\ A + I_3 &\subseteq I_\infty, \end{aligned}$$

where $I_\infty = \bigcup_{j \geq 4} I_j = [c+m, \infty[$, and the fact that X_3 is disjoint from both $m+S$ and I_∞.

The lemma now follows by applying the condensed Macaulay Theorem 5.10 to the claimed respective dimensions of R'_2, R'_3. □

6.3 The case of profile $(k,0)$

Theorem 6.4. *Let $S \subset \mathbb{N}$ be a numerical semigroup with $q = 3$ and profile $(k,0)$ for some $k \geq 1$. Then $W_0(S) \geq \rho(S)$.*

Proof. By hypothesis, we have $P \cap L = P_1 = \{m\} \dot\cup X_1$. Let us denote

$$X_1 \ =\ \{a_2 < \cdots < a_k\}$$

with $m < a_2$. We may list the elements of D_3 in terms of the Apéry ones as follows:

$$D_3 \ =\ \{3m\} \dot\cup \big(2m + X_1\big) \dot\cup \big(m + X_2\big) \dot\cup X'_3,$$

where $X'_3 = X_3 \setminus P$. By Proposition 4.5, and recalling our notation $\alpha_2 = |X_2|$, $\alpha_3 = |X'_3|$, we have

$$\begin{aligned} d_3 &= k + \alpha_2 + \alpha_3, \\ |L| &= 3 + 2(k-1) + \alpha_2 \\ &= 2k + 1 + \alpha_2. \end{aligned}$$

Therefore

$$\begin{aligned} W_0(S) - \rho &= k|L| - 3d_3 \\ &= k\big(2k + 1 + \alpha_2\big) - 3(k + \alpha_2 + \alpha_3) \\ &= 2k(k-1) + k\alpha_2 - 3(\alpha_2 + \alpha_3) \\ &= 4\binom{k}{2} + k\alpha_2 - 3(\alpha_2 + \alpha_3). \end{aligned}$$

We now proceed to bound $\alpha_2 + \alpha_3 = |X_2| + |X_3'|$. Since $X_2 \subseteq 2X_1$ and $X_3' \subseteq 2X_1 \cup 3X_1$, we have

$$\begin{aligned}\alpha_2 &= |X_2| = |2X_1 \cap X_2|,\\ \alpha_3 &= |X_3'| = |2X_1 \cap X_3| + |3X_1 \cap X_3|.\end{aligned}$$

It follows that

$$\begin{aligned}\alpha_2 + \alpha_3 &= |2X_1 \cap X_2| + |2X_1 \cap X_3| + |3X_1 \cap X_3|\\ &\leq |2X_1| + |3X_1 \cap X_3|\\ &\leq \binom{k}{2} + |3X_1 \cap X_3|.\end{aligned}$$

Plugging this into the latter estimate of $W_0(S) - \rho$, we get

$$W_0(S) - \rho \geq \binom{k}{2} + k|2X_1 \cap X_2| - 3|3X_1 \cap X_3|. \tag{15}$$

Let $x \geq 1$ be the unique real number such that

$$|2X_1 \cap X_2| = \binom{x}{2}.$$

Note that $x \leq k$, since

$$|2X_1 \cap X_2| \leq |2X_1| \leq \binom{k}{2}.$$

Further, it follows from Lemma 6.3 that

$$|3X_1 \cap X_3| \leq \binom{x+1}{3}.$$

Plugging these inequalities into (15), we obtain

$$\begin{aligned}W_0(S) - \rho &\geq \binom{k}{2} + k\binom{x}{2} - 3\binom{x+1}{3}\\ &= \binom{k}{2} + k\binom{x}{2} - 3\frac{x+1}{3}\binom{x}{2}\\ &= \binom{k}{2} + (k-x-1)\binom{x}{2}.\end{aligned}$$

Since $\binom{k}{2} \geq \binom{x}{2}$ and $k \geq x$ as observed above, we conclude

$$W_0(S) - \rho \geq (k-x)\binom{x}{2} \geq 0,$$

as desired. □

Table 1: Distribution of $q = q(S)$ by genus g, for $18 \leq g \leq 25$ and $q \leq 20$.

$g \backslash q$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
18	1	4180	6935	1739	409	132	37	13	14	2	2	2	0	0	0	0	0	1		
19	1	6764	11828	2895	670	195	63	20	14	8	2	2	1	0	0	0	0	0	1	
20	1	10945	20096	4805	1085	290	103	35	14	15	2	2	2	0	0	0	0	0	0	1
21	1	17710	34069	7943	1750	453	172	46	19	15	9	2	2	2	0	0	0	0	0	0
22	1	28656	57566	13108	2806	707	249	81	32	16	16	2	2	2	1	0	0	0	0	0
23	1	46367	96949	21509	4453	1102	357	132	44	16	17	9	2	2	2	0	0	0	0	0
24	1	75024	162911	35248	7052	1741	500	221	60	26	17	18	2	2	2	2	0	0	0	0
25	1	121392	273139	57649	11149	2648	750	301	100	42	17	18	10	2	2	2	1	0	0	0

Corollary 6.5. *Wilf's conjecture holds for all numerical semigroups S satisfying $q(S) = 3$.*

Proof. Straightforward from the above result and the reduction to profile $(k,0)$ provided by Proposition 6.2, which together imply $W_0(S) \geq 0$. $\square$

As observed in the Introduction, the importance of this corollary stems from a recent result of Zhai [24] stating that, as g goes to infinity, the proportion of numerical semigroups of genus g satisfying $q = 3$ tends to 1. As a matter of illustration, here is a table showing how q is distributed for $18 \leq g \leq 25$. It clearly shows that, in this range for g, the two cases $q = 3$ and $q = 2$ together contain an overwhelming majority of numerical semigroups. This table was obtained with the GAP package `numericalsgps` [6].

Remark 6.6. *As observed by A. Sammartano after reading a preliminary version of this paper, one can show that the equality case $W(S) = 0$ in Wilf's conjecture cannot occur for $q = 3$ besides the known ones cited in the Introduction [20]. Indeed, since $W(S) = p_3(|L| - 3) + W_0(S)$ and since $W_0(S) \geq 0$ holds for $q = 3$, it follows from $W(S) = 0$ that $p_3(|L| - 3) = W_0(S) = 0$. Moreover, going through the chains of inequalities in the proofs of Proposition 6.2 and Theorem 6.4, ones sees that the equality $W_0(S) = 0$ can only occur if $\rho = p_2(p_2+1)/2$, $m + P_1 = D_2$, $|P_1 + P_2| = p_1 p_2$, $|2P_2| = p_2(p_2+1)/2$, $|2X_1 \cap X_2| = \binom{p_1}{2}$ and $|3X_1 \cap X_3| = \binom{p_1+1}{3}$. Considering all these constraints together, one can show that the profile of S either equals $(1,0)$, or $(1,1)$ provided $p_3 = 0$, both known equality cases in Wilf's conjecture.*

7 Further results

Using the present methods, we settle Wilf's conjecture in a few other cases, namely for numerical semigroups S satisfying $S_i + S_j = S_{i+j}$ whenever $i + j \leq q - 1$, for those satisfying $|L(S)| \leq 6$, and finally for those satisfying $\gcd(L(S)) \geq 2$.

7.1 The case of true grading

Theorem 7.1. *Let S be a numerical semigroup satisfying $S_i + S_j = S_{i+j}$ for all $i + j \leq q-1$. Then $W_0(S) \geq \rho \geq 0$, and hence S satisfies Wilf's conjecture.*

Proof. It follows from the hypothesis that $S_i = iS_1$ for all $1 \leq i \leq q-1$. Therefore $P \cap L = P_1 = S_1$ and $D_q \subseteq qS_1$. Now, denote $S_1 = \{a_1, a_2, \dots, a_k\}$ with $m = a_1 < a_2 < \cdots < a_k$. As in the proof of Lemma 6.3, consider the standard graded algebra

$$R \;=\; \mathbb{K}[t^{a_1}u, \dots, t^{a_k}u],$$

where the variables t and u have degree 0 and 1, respectively. As Hilbert function of R, we have

$$h_i \;=\; \dim R_i \;=\; |iS_1| \;=\; |S_i|$$

for all $0 \leq i \leq q-1$, and $h_q = \dim R_q = |qS_1|$. It follows from Theorem 5.11 that

$$qh_q \;\leq\; h_1(1 + h_1 + \cdots + h_{q-1}). \tag{16}$$

Since $W_0(S) - \rho = |P \cap L||L| - qd_q$, since $d_q = |D_q| \leq |qS_1| = h_q$, and by the formula for $|L|$ in Lemma 3.3, we have

$$\begin{aligned} W_0(S) - \rho \;&\geq\; |P \cap L||L| - qh_q \\ &=\; h_1(1 + h_1 + \cdots + h_{q-1}) - qh_q. \end{aligned}$$

Hence $W_0(S) - \rho \geq 0$ by (16), as claimed. □

Corollary 7.2. *Let S be a numerical semigroup satisfying $q \geq 4$ and*

$$P \cap L \;\subseteq\; \left[m, m + \frac{m - \rho}{q-1}\right[.$$

Then S satisfies Wilf's conjecture.

Proof. It suffices to show that S satisfies the hypotheses of Theorem 7.1. First note that

$$\left[m, m + \frac{m - \rho}{q-1}\right[\;\subseteq\; I_1.$$

Indeed, we have $m + (m - \rho)/(q-1) \leq 2m - \rho = \max I_1 - 1$, since

$$\begin{aligned} (q-1)m + (m - \rho) \;&\leq\; (q-1)m + (q-1)(m - \rho) \\ &\leq\; (q-1)(2m - \rho). \end{aligned}$$

It follows that $P \cap L = P_1$. Therefore, for all $2 \le k \le q-1$, we have $S_k = kS_1 \cap I_k$.

Consider now the following inclusions for k in this same range:

$$\begin{aligned} kS_1 &\subseteq [km, km + k(m-\rho)/(q-1)[\\ &\subseteq [km, km + (m-\rho)[\\ &\subseteq I_k. \end{aligned}$$

It follows that $S_k = kS_1$. Therefore, for any integers $1 \le i, j \le q-1$ such that $i+j \le q-1$, we have

$$S_i + S_j \;=\; iS_1 + jS_1 \;=\; (i+j)S_1 \;=\; S_{i+j},$$

and we are done. □

Example 7.3. *Let S be a numerical semigroup with $m = 1000$ and $c = 4000$. Assume further that all left primitives of S are contained in $[1000, 1333[$. Equivalently, let $A \subseteq [0, 333[$ be an arbitrary subset, and let*

$$S \;=\; \langle 1000 + A \rangle_{4000} \;=\; \langle 1000 + A \rangle \cup [4000, \infty[.$$

Then S satisfies Wilf's conjecture.

Indeed, we have $q = 4$, $\rho = 0$, and $P \cap L \subseteq [1000, 1000+333[$ by hypothesis. Hence the above corollary applies.

7.2 The case $|L| \le 6$

Dobbs and Matthews [7] settled Wilf's conjecture for numerical semigroups S satisfying $|L| \le 4$. As briefly commented below, that result easily follows from the now settled case $q \le 3$ of the conjecture. We now informally establish Wilf's conjecture in case $|L| \le 6$, and shall extend that result to the case $|L| \le 10$ in a forthcoming publication.

Proposition 7.4. *Numerical semigroups S with $|L(S)| \le 6$ satisfy Wilf's conjecture.*

Proof. By Corollary 6.5, it suffices to consider the case $q \ge 4$. So, from now on, we assume $|L| \le 6$ and $q \ge 4$. Let $(p_1, \dots, p_{q-1})$ be the profile of S. It follows from Proposition 4.5 and (3) that

$$|L| \;\ge\; 1 + (q-1)p_1 + (q-2)p_2 + \cdots + p_{q-1}. \tag{17}$$

In particular, since $|L| \le 6$, and since $p_1 \ge 1$ always, we must have $q \le 6$. Moreover, we must have $p_1 = 1$, for if $p_1 \ge 2$ then $|L| \ge 7$. Similarly, we must have $p_2 \le 1$, for otherwise $|L| \ge 8$. Therefore, by (17), the only profiles with $4 \le q \le 6$ and compatible with $|L| \le 6$ are

$$(1,1,0),\; (1,0,k),\; (1,0,0,k),\; (1,0,0,0,k)$$

for some small integer $k \geq 0$. We first treat the last three possibilities in one single case.

• Assume S is of profile $(1,0,\dots,0,k) \in \mathbb{N}^{q-1}$ with $q \geq 4$ and $k \in \mathbb{N}$. We then claim

$$W_0(S) = k(k+1) + \rho,$$

and so S satisfies Wilf's conjecture. Indeed, one has

$$(\alpha_0, \alpha_1, \dots, \alpha_{q-1}) = (1,0,\dots,0,k),$$

as easily seen. We have $|P \cap L| = 1+k$, and Proposition 4.5 yields

$$|L| \ = \ q+k, \quad d_q \ = \ 1+k.$$

Therefore $W_0(S) - \rho = (1+k)(q+k) - q(1+k) = k(1+k)$, and we are done.

• Assume now S is of profile $(1,1,0)$, a slightly more delicate case. Here $q = 4$, $|P \cap L| = 2$, and we have

$$\alpha_0 \ = \ 1, \quad \alpha_1 \ = \ 0, \quad \alpha_2 \ = \ 1, \quad \alpha_3 \ \leq \ 1, \quad \alpha_4 \ \leq \ 1,$$

as easily seen. Thus, by Proposition 4.5, we have

$$|L| \ = \ 6 + \alpha_3, \quad d_4 \ = \ 2 + \alpha_3 + \alpha_4.$$

Therefore $W_0(S) - \rho = 2(6+\alpha_3) - 4(2+\alpha_3+\alpha_4) = 4 - 2\alpha_2 - 4\alpha_4$. If either $\alpha_3 = 0$ or $\alpha_4 = 0$, then $W_0(S) - \rho \geq 0$ and we are done. However, if $\alpha_3 = \alpha_4 = 1$, then $W_0(S) - \rho = -2$. But in this case, we must have $X_3 = 2X_2$ and $X_4 \setminus P = 3X_2$. Proposition 3.6 then implies $\rho \geq 2$, whence $W_0(S) \geq 0$, and we are done again.

This settles, albeit informally, Wilf's conjecture for $|L| \leq 6$. □

As mentioned above, we shall extend the verification of Wilf's conjecture to the case $|L| \leq 10$ in a forthcoming publication. More precisely, we shall prove the following result.

Theorem 7.5. *Let S be a numerical semigroup with $|L(S)| \leq 10$. Then $W_0(S) \geq \rho$, except possibly if S is of profile $(1,0,1,0)$. In that special profile, we have $W_0(S) \geq \rho - 1$, and if equality holds, then $\rho \geq 2$. In any case, S satisfies Wilf's conjecture.*

An example where $|L(S)| \leq 10$ and $W_0(S) = \rho - 1$ is given by $S = \langle 5, 13 \rangle_{22}$, for which $|L| = 7$ and $\rho = 3$. Its profile is $(1,0,1,0)$, as expected.

The proof of Theorem 7.5, like that of Proposition 7.4, combines some general reductions, in the spirit of Proposition 6.2, and some ad-hoc arguments for a few specific profiles.

7.3 The case $\gcd(L(S)) \geq 2$

Sammartano proved in [19] that *if the numerical semigroup S satisfies $e \geq m/2$, then it satisfies Wilf's conjecture*. Here is a straightforward consequence.

Proposition 7.6. *Let S be a numerical semigroup such that $\gcd(L(S)) \geq 2$, i.e. such that the left primitives of S have a nontrivial common factor. Then S satisfies Wilf's conjecture.*

Proof. Let $k = \gcd(L(S)) = \gcd(P \cap L)$, and assume $k \geq 2$. Then D_q, the set of right decomposable elements in $S_q = I_q$, is entirely contained in $k\mathbb{N}$. Thus $|D_q| \leq m/k$. Since

$$P_q = S_q \setminus D_q$$

and since $|S_q| = m$, it follows that $e \geq |P_q| \geq m - m/k \geq m/2$. The conclusion now follows from Sammartano's result mentioned above. □

As an application, it follows that all *inductive* numerical semigroups satisfy Wilf's conjecture. These are obtained from $S_0 = \mathbb{N}$ by applying finitely many steps of the form $S \mapsto a \cdot S \cup (ab + \mathbb{N})$, where a, b are varying positive integers and $a \cdot S = \{as \mid s \in S\}$.

The numerical semigroups S satisfying $\gcd(L(S)) \geq 2$ have an interesting geometric interpretation. Let $\mathcal{T}$ denote the tree of all numerical semigroups. Then *a numerical semigroup S satisfies $\gcd(L(S)) \geq 2$ if and only if the subtree $\mathcal{T}_S \subseteq \mathcal{T}$ rooted at S is infinite*.

Here are some explanations; see also [4, Theorem 10 in Section 3]. Recall first that the root of $\mathcal{T}$ is $\mathbb{N} = \langle 1 \rangle$, that the father in $\mathcal{T}$ of the numerical semigroup $S \neq \mathbb{N}$ is the numerical semigroup $\widehat{S} = S \,\dot{\cup}\, \{F(S)\}$, and that for all $g \in \mathbb{N}$, the vertices at level g in $\mathcal{T}$ are all numerical semigroups of genus g. As mentioned earlier, the down degree of S in $\mathcal{T}$ is the number p_q of right primitives in S. For instance, S is a leaf in $\mathcal{T}_S$ if and only if $p_q = 0$. Finally, let us denote by $\mathcal{T}_S$ the subtree of $\mathcal{T}$ rooted at S. For instance, we have $\mathcal{T}_S = \{S\}$ if and only if S is a leaf in $\mathcal{T}$.

Let us now prove the above characterization. Let $A = L(S)$ and $k = \gcd(A)$. Note first that if T is any descendant of S, then $A \subseteq T \subseteq S$ by construction.

• If $k \geq 2$, then S has infinitely many descendants S' in $\mathcal{T}$, e.g. all $S' = \langle A \rangle_d$ with $d > \max(A) + 2$. This is indeed an infinite collection, since if $d_1 < d_2$, the equality $\langle A \rangle_{d_1} = \langle A \rangle_{d_2}$ can only occur if $d_1 \equiv 0 \bmod k$ and $d_2 = d_1 + 1$.

• Conversely, if $k = 1$, let $S_0 = \langle A \rangle$. Then S_0 is a numerical subsemigroup of S, and any descendant T of S satisfies $S_0 \subseteq T \subseteq S$. Therefore $\mathcal{T}_S$ is finite in this case, as desired.

Acknowledgment. It is a pleasure to thank several people for helpful discussions and/or bibliographical references related to this work, including Maria Bras-Amorós, Manuel Delgado, Ralph Fröberg, Ornella Greco, Jorge Ramírez Alfonsín, Giuseppe Valla and Santiago Zarzuela. Special thanks are due to Pedro A. García-Sánchez and Alessio Sammartano for comments on an earlier version of this paper and, last but not least, to Jean Fromentin for several lively discussions and computer experiments.

References

[1] B. BOLLOBÁS, Combinatorics. Set systems, hypergraphs, families of vectors and combinatorial probability. Cambridge University Press, Cambridge, 1986.

[2] M. BRAS-AMORÓS, Fibonacci-like behavior of the number of numerical semigroups of a given genus, Semigroup Forum 76 (2008) 379–384.

[3] M. BRAS-AMORÓS, Bounds on the number of numerical semigroups of a given genus, J. Pure and Applied Algebra 213 (2009) 997–1001.

[4] M. BRAS-AMORÓS AND S. BULYGIN, Towards a better understanding of the semigroup tree, Semigroup Forum 79 (2009) 561–574.

[5] W. BRUNS AND J. HERZOG, Cohen-Macaulay rings. Cambridge Studies in Advanced Mathematics, 39. Cambridge University Press, Cambridge, 1993.

[6] M. DELGADO, P.A. GARCÍA-SÁNCHEZ AND J. MORAIS, "Numericalsgps": a GAP package on numerical semigroups. (`http://www.gap-system.org/Packages/numericalsgps.html`)

[7] D. DOBBS AND G. MATTHEWS, On a question of Wilf concerning numerical semigroups, in: Focus on Commutative Rings Research, Nova Sci. Publ., New York, 2006, pp. 193–202.

[8] R. FRÖBERG, C. GOTTLIEB AND R. HÄGGKVIST, On numerical semigroups, Semigroup Forum 35 (1987) 63–83.

[9] J. FROMENTIN, personal communication (September 2014).

[10] J. FROMENTIN AND F. HIVERT, Exploring the tree of numerical semigroups, Math.Comp. (2015), to appear.

[11] N. KAPLAN, Counting numerical semigroups by genus and some cases of a question of Wilf, J. Pure Appl. Algebra 216 (2012) 1016–1032.

[12] L. LOVÁSZ, Combinatorial problems and exercises. North-Holland, Amsterdam, 1979.

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

[14] A. MOSCARIELLO AND A. SAMMARTANO, On a conjecture by Wilf about the Frobenius number, Math. Z. 280 (2015) 47–53.

[15] J. MERMIN AND I. PEEVA, Hilbert functions and lex ideals, J. Algebra 313 (2007) 642–656.

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

[17] J.L. RAMÍREZ ALFONSÍN, The Diophantine Frobenius problem. Oxford Lecture Series in Mathematics and its Applications 30, Oxford University Press, Oxford, 2005.

[18] J.C. ROSALES AND P.A. GARCÍA-SÁNCHEZ, Numerical semigroups. Developments in Mathematics, 20. Springer, New York, 2009.

[19] A. SAMMARTANO, Numerical semigroups with large embedding dimension satisfy Wilf's conjecture, Semigroup Forum 85 (2012) 439–447.

[20] A. SAMMARTANO, personal communication (May 2015).

[21] E.S. SELMER, On a linear Diophantine problem of Frobenius, J. Reine Angew. Math. 293/294 (1977) 1–17.

[22] J.J. SYLVESTER, Mathematical questions with their solutions, Educational Times 41 (1884) 21.

[23] H. WILF, A circle-of-lights algorithm for the money-changing problem, Amer. Math. Monthly 85 (1978) 562–565.

[24] A. ZHAI, Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum 86 (2013) 634–662.

Author's address:
• Shalom Eliahou[a,b],
[a]Univ. Littoral Côte d'Opale, EA 2597 - LMPA - Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62228 Calais, France
[b]CNRS, FR 2956, France
e-mail: eliahou@lmpa.univ-littoral.fr