On Syzygies for Rings of Invariants of Abelian Groups

M. Domokos

Abstract It is well known that results on zero-sum sequences over a finitely generated abelian group can be translated to statements on generators of rings of invariants of the dual group. Here the direction of the transfer of information between zero-sum theory and invariant theory is reversed. First it is shown how a presentation by generators and relations of the ring of invariants of an abelian group acting linearly on a finite-dimensional vector space can be obtained from a presentation of the ring of invariants for the corresponding multiplicity free representation. This combined with a known degree bound for syzygies of rings of invariants yields bounds on the presentation of a block monoid associated to a finite sequence of elements in an abelian group. The results have an equivalent formulation in terms of binomial ideals, but here the language of monoid congruences and the notion of catenary degree is used.

Keywords Affine monoid · Ring of invariants · Catenary degree · Syzygies · Toric variety

1 Introduction

Let G be an abelian group (written multiplicatively) and $G_0 \subseteq G$ a finite subset. Consider the additive monoid $\mathbb{N}_0^{G_0}$ (maps from G_0 into the set of non-negative integers, with pointwise addition). It contains the submonoid

$$\mathcal{B}(G_0) := \{\alpha \in \mathbb{N}_0^{G_0} \mid \prod_{g \in G_0} g^{\alpha(g)} = 1 \in G\} \tag{1}$$

M. Domokos (✉)
Rényi Institute, Budapest, Hungary
e-mail: domokos.matyas@renyi.hu

called the *block monoid of G_0* or the *monoid of product-one sequences over G_0*, see [14, Definition 3.4.1]. It causes no loss of generality in the construction of $\mathcal{B}(G_0)$ if we assume that the group G is generated by G_0. We note that in most of the related literature the group is written additively, and therefore the terminology of *zero-sum sequences* is used. $\mathcal{B}(G_0)$ is a reduced affine monoid (see for example [14, Theorem 3.4.2.1]), write $\mathcal{A}(\mathcal{B}(G_0))$ for the finite set of its atoms.

Our focus is on a similar but more general construction. Fix an m-tuple $\underline{g} = (g_1, \ldots, g_m) \in G^m$ of elements of the abelian group G, and set

$$\mathcal{B}(\underline{g}) = \{\alpha \in \mathbb{N}_0^m \mid \prod_{i=1}^{m} g_i^{\alpha_i} = 1 \in G\}. \tag{2}$$

This is a finitely generated submonoid of the additive monoid $\mathbb{N}_0^m$. Write $\mathrm{supp}(\underline{g})$ for the subset $\{g_1, \ldots, g_m\}$ of G. In the special case when $g_1, \ldots, g_m$ are distinct, the monoid $\mathcal{B}(\underline{g})$ can be identified with $\mathcal{B}(\mathrm{supp}(\underline{g}))$. In general (i.e., when $g_1, \ldots, g_m$ are not all distinct) the monoid $\mathcal{B}(\underline{g})$ is different from $\mathcal{B}(\mathrm{supp}(\underline{g}))$. So the construction (2) is indeed a generalization of (1) (however, see Remark 6 in Section 4).

Interest in the monoids $\mathcal{B}(G_0)$ and $\mathcal{B}(\underline{g})$ and their semigroup rings comes from several mathematical topics: factorization theory in monoids, multiplicative ideal theory, zero-sum theory, invariant theory, toric varieties, binomial or toric ideals. For example, it has been long known that results on the atoms in monoids of the form $\mathcal{B}(\underline{g})$ can be reformulated in terms of generators or degree bounds for rings of invariants of abelian groups (see, e.g., [9] for some details and references).

In this paper we shall study presentations of reduced affine monoids, with a particular attention on the monoids $\mathcal{B}(\underline{g})$. By a *monoid* we mean a commutative cancellative semigroup with an identity element. A monoid is *affine* if it is a finitely generated submonoid of a finitely generated free abelian group. We say that a monoid is *reduced* if the identity element is its only unit (invertible element). Recall that by Grillet's theorem, reduced affine monoids are exactly the monoids that are isomorphic to a finitely generated submonoid of the additive monoid $\mathbb{N}_0^k$ for some k (see for example [3, Proposition 2.16]).

Let S be a reduced affine monoid (written multiplicatively) and $\mathcal{A}(S)$ the set of atoms in S. Then $\mathcal{A}(S)$ is finite, and it is a minimal generating set of S, see for example Proposition 1.1.7 in [14]. Denote by $\mathbb{N}_0^{\mathcal{A}(S)}$ the additive monoid of functions from $\mathcal{A}(S)$ into the additive monoid $\mathbb{N}_0$ of non-negative integers; this is a free monoid generated by $|\mathcal{A}(S)|$ elements. Take commuting indeterminates $\{x_a \mid a \in \mathcal{A}(S)\}$, and let M denote the free monoid generated by them (written multiplicatively):

$$M = \{x^\alpha = \prod_{a \in \mathcal{A}(S)} x_a^{\alpha(a)} \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(S)}\}$$

with multiplication $x^\alpha x^\gamma = x^{\alpha+\gamma}$. Consider the unique semigroup homomorphism

$$\pi : M \to S \text{ given by } x_a \mapsto a, \quad a \in \mathcal{A}(S)$$

(called *factorization homomorphism* in [1]). Denote by $\sim_S$ the congruence on M defined by

$$x^\alpha \sim_S x^\gamma \iff \pi(x^\alpha) = \pi(x^\gamma) \in S,$$

and call it the *defining congruence of S* (it is called *the monoid of relations of S* in [1]). The semigroup homomorphism π factors through a monoid isomorphism

$$M/\sim_S \xrightarrow{\cong} S.$$

Formally the congruence $\sim_S$ will be viewed as a subset of $M \times M$. The congruence $\sim_S$ is finitely generated by [25]. By a *presentation* of S we mean a finite subset of $M \times M$ generating the conguence $\sim_S$ (see for example [16, Section I.4] for basic notions related to semigroup congruences).

Now let us summarize the content of the present paper. Our Theorem 1 tells in particular how a presentation of $\mathcal{B}(g)$ can be derived from a presentation of $\mathcal{B}(\mathrm{supp}(g))$. It turns out that in most cases the catenary degree (cf. Definition 1) of $\mathcal{B}(g)$ coincides with the catenary degree of $\mathcal{B}(\mathrm{supp}(g))$ (see Corollary 3). Combining Theorem 1 with a degree bound of Derksen [10] for the defining relations of the ring of invariants of a linearly reductive group, we derive in Theorem 4 degree bounds for a presentation of $\mathcal{B}(g)$. In order to formulate this result, we introduce the notion of graded catenary degree of a graded monoid (see Definition 2), which is a refinement of (and an upper bound for) the ordinary catenary degree. These results on presentations of monoids have an equivalent formulation in terms of generators of (binomial) ideals of relations of semigroup rings of monoids, this is pointed out in Section 2. A Gröbner basis version of Theorem 1 is given in Theorem 2. Since the semigroup rings of the form $\mathbb{C}[\mathcal{B}(G)]$ are exactly the rings of invariants of abelian groups, the results have relevance for toric varieties; this is expanded a bit in Section 7, and some examples of toric quiver varieties are reviewed. We point out finally that Theorem 2 provides a source of Koszul algebras.

2 Ring Theoretic Characterization of the Catenary Degree

From now on S will be a reduced affine monoid. The *catenary degree* $c(S)$ of the monoid S is a basic arithmetical invariant studied in factorization theory, let us recall its definition. For $\alpha \in \mathbb{N}_0^{\mathcal{A}(S)}$ we set

$$|\alpha| = \sum_{a \in \mathcal{A}(S)} |\alpha(a)|$$

and

$$a^\alpha := \prod_{a \in \mathcal{A}(S)} a^{\alpha(a)} \in S.$$

For $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ we write $\gcd(\alpha, \gamma)$ for the greatest common divisor of α, γ in the additive monoid $\mathbb{N}_0^{\mathcal{A}(S)}$ (i.e., $\gcd(\alpha, \gamma)(a) = \min\{\alpha(a), \gamma(a)\}$ for each $a \in \mathcal{A}(S)$).

Definition 1. (see [14, Definition 1.6.1]) *For $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ set*

$$d(\alpha, \gamma) := \max\{|\alpha - \gcd(\alpha, \gamma)|, |\gamma - \gcd(\alpha, \gamma)|\}.$$

Given the monoid S as above, we say that α and γ can be connected by a d-chain if there exists a sequence $\alpha^{(0)} = \alpha, \alpha^{(1)}, \ldots, \alpha^{(k)} = \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ such that $a^{\alpha^{(j)}} = a^{\alpha^{(j+1)}}$ and $d(\alpha^{(j)}, \alpha^{(j+1)}) \le d$ for $j = 0, 1, \ldots, k - 1$. The catenary degree $c(S)$ *is the minimal non-negative integer d such that if $a^\alpha = a^\gamma$, then α and γ can be connected by a d-chain.*

Remark 1. Note that $c(S) = 0$ if and only if S is a free (or factorial) monoid (i.e., S is isomorphic to the additive monoid $\mathbb{N}_0^m$ for some m), and $c(S)$ is never equal to 1.

Characterizations of the catenary degree and its variants are given in [22, 23]. In particular, [22, Proposition 16] characterizes the catenary degree in terms of the *monoid* of relations. Now extending an observation from [4] we formulate a characterization of the catenary degree in terms of semigroup congruences. Denote by $c'(S)$ the minimal non-negative integer d such that there exists a generating set $\Lambda \subset M \times M$ of the semigroup congruence $\sim_S$, satisfying that for all $(x^\alpha, x^\gamma) \in \Lambda$ we have $|\alpha| \le d$ and $|\gamma| \le d$. An explicit description of the semigroup congruence generated by a subset of $M \times M$ can be found for example in [18, page 176].

Proposition 1. *We have $c(S) = c'(S)$.*

Proof. Set

$$\Lambda := \{(x^\alpha, x^\gamma) \mid x^\alpha \sim_S x^\gamma \text{ and } |\alpha| \le c(S), \ |\gamma| \le c(S)\}.$$

We claim that Λ generates the semigroup congruence $\sim_S$. Indeed, take a pair $(\alpha, \gamma) \in \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$ such that $x^\alpha \sim_S x^\gamma$. Then α and γ can be connected by a $c(S)$-chain $\alpha^{(0)} = \alpha, \alpha^{(1)}, \ldots, \alpha^{(k)} = \gamma$. For $i = 0, 1, \ldots, k - 1$ the pair $(\alpha^{(i)}, \alpha^{(i+1)})$ is of the form $(\beta^{(i)} + \delta^{(i)}, \rho^{(i)} + \delta^{(i)})$, where $\delta^{(i)}, \beta^{(i)}, \rho^{(i)} \in \mathbb{N}_0^{\mathcal{A}(S)}, |\beta^{(i)}| \le c(S), |\rho^{(i)}| \le c(S)$. Moreover, since S is cancellative, $a^{\alpha^{(i)}} = a^{\alpha^{(i+1)}}$, implies $a^{\beta^{(i)}} = a^{\rho^{(i)}}$, so $x^{\beta^{(i)}} \sim_S x^{\rho^{(i)}}$. Thus $(x^{\beta^{(i)}}, x^{\rho^{(i)}}) \in \Lambda$. It follows that $(x^{\alpha^{(i)}}, x^{\alpha^{(i+1)}}) = (x^{\beta^{(i)}} x^{\delta^{(i)}}, x^{\rho^{(i)}} x^{\delta^{(i)}})$ belongs to the congruence generated by Λ for $i = 0, \ldots, k - 1$, implying in turn that $(x^\alpha, x^\gamma) = (x^{\alpha^{(0)}}, x^{\alpha^{(k)}})$ belongs to the congruence generated by Λ. This proves the inequality $c'(S) \le c(S)$.

The reverse inequality $c(S) \le c'(S)$ is pointed out in [4, Proposition 3.1]. $\square$

Fix a commutative ring R (having an identity element) and consider the semigroup rings $R[M]$ and $R[S]$. Note that $R[M] = R[x_a \mid a \in \mathcal{A}(S)]$ is the polynomial ring over R with indeterminates $\{x_a \mid a \in \mathcal{A}(S)\}$. The monoid homomorphism $\pi : M \to S$ extends uniquely to an R-algebra homomorphism

$$\pi_R : R[M] \to R[S], \quad \pi(x^\alpha) = a^\alpha. \tag{3}$$

The statement below is well known, see [18, Proposition 1.5] or [16, Chapter II.7.]:

Proposition 2. *The following conditions are equivalent for a set of pairs $B \subset \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$:*

(1) The semigroup congruence $\sim_S$ is generated by $\{(x^\alpha, x^\gamma) \mid (\alpha, \gamma) \in B\}$.
(2) The ideal $\ker(\pi_R)$ is generated by the binomials $\{x^\alpha - x^\gamma \mid (\alpha, \gamma) \in B\}$.

Remark 2. Condition (1) of Proposition 2 does not depend on the ring R; therefore, a set of binomials generates the ideal $\ker(\pi_R)$ for some ring R if and only if it generates $\ker(\pi_R)$ for any ring R.

Propositions 1 and 2 imply the following ring theoretic characterization of $c(S)$:

Corollary 1. *The catenary degree $c(S)$ is the minimal positive integer d such that the kernel of $\pi_R : R[M] \to R[S]$ is generated (as an ideal) by binomials of degree at most d for some (hence any) commutative ring R (where $R[M]$ is graded in the standard way, namely, the generators x_a have degree 1 and the non-zero scalars in R have degree 0).*

3 Graded Monoids

Let S be a *graded* monoid; that is, S is partitioned into the disjoint union of subsets $S_d, d \in \mathbb{N}_0$, such that $S_d \cdot S_e \subseteq S_{d+e}$. For $s \in S$ write $|s| = d$ if $s \in S_d$. The identity element of S necessarily belongs to S_0. We call a graded monoid *connected graded* if S_0 consists only of the identity element. It seems natural to modify Definition 1 for graded monoids as follows:

Definition 2. *Given a connected graded reduced affine monoid S, for $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ set*

$$|\alpha|_{\mathrm{gr}} = \sum_{a \in \mathcal{A}(S)} \alpha(a)|a|$$

and

$$d_{\mathrm{gr}}(\alpha, \gamma) := \max\{|\alpha - \gcd(\alpha, \gamma)|_{\mathrm{gr}}, |\gamma - \gcd(\alpha, \gamma)|_{\mathrm{gr}}\}.$$

We say that α and γ can be connected by a chain of weight at most d if there exists a sequence $\alpha^{(0)} = \alpha, \alpha^{(1)}, \dots, \alpha^{(k)} = \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ such that $a^{\alpha^{(j)}} = a^{\alpha^{(j+1)}}$ and $d_{\mathrm{gr}}(\alpha^{(j)}, \alpha^{(j+1)}) \le d$ for $j = 0, 1, \dots, k - 1$. The graded catenary degree $c_{\mathrm{gr}}(S)$ *is the minimal d such that if $a^\alpha = a^\gamma$, then α and γ can be connected by a chain of weight at most d.*

As a straightforward modification of Proposition 1 we get the following.

Proposition 3. *The graded catenary degree $c_{\mathrm{gr}}(S)$ is the minimal non-negative integer d such that there exists a generating set $\Lambda \subset M \times M$ of the semigroup congruence $\sim_S$ satisfying that for all $(x^\alpha, x^\gamma) \in \Lambda$ we have $|\alpha|_{\mathrm{gr}} \leq d$ (note that $x^\alpha \sim_S x^\gamma$ implies $|\alpha|_{\mathrm{gr}} = |\gamma|_{\mathrm{gr}}$).*

The grading of S induces a grading on the semigroup ring $R[S] = \bigoplus_{d=0}^{\infty} R[S]_d$, where $R[S]_d$ is the R-submodule generated by S_d. Lift the grading to M and $R[M]$ by setting the degree of x_a to be equal to the degree $|a|$ of $a \in \mathcal{A}(S)$. Then the map $\pi_R : R[M] \to R[S]$ is a homomorphism of graded algebras, and so $\ker(\pi_R)$ is a homogeneous ideal. Our assumptions on the grading imply that all indeterminates x_a have positive degree. Moreover, $x^\alpha \sim_S x^\gamma$ implies that a^α and a^γ belong to the same homogeneous component of S, and therefore the binomials in $\ker(\pi_R)$ are homogeneous. For an ideal I in $R[M]$ denote by $\mu(I)$ the minimal non-negative integer d such that I is generated by elements of degree at most d; this number is finite for any binomial ideal I.

Corollary 2. *For any connected graded reduced affine monoid we have the equality*

$$c_{\mathrm{gr}}(S) = \mu(\ker(\pi_R)),$$

where $R[M]$ is endowed with the grading that makes π_R a homomorphism of graded algebras.

Proof. Recall that any homogeneous generating system of a homogeneous ideal I contains a minimal (with respect to inclusion) homogeneous generating system, and $\mu(I)$ is the maximal degree of an element in any minimal homogeneous generating system (this follows from the graded Nakayama lemma). The ideal $\ker(\pi_R)$ is generated by homogeneous binomials. Take a minimal set of binomials generating $\ker(\pi_R)$. Then the maximal degree of an element in this set of binomials equals $\mu(\ker(\pi_R))$ on one hand, and it equals $c_{\mathrm{gr}}(S)$ by Propositions 2 and 3, on the other hand.

Remark 3. The notions introduced in this section apply for block monoids. Indeed, $\mathbb{N}_0^m$ is graded by setting the degree of $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ to be $\alpha_1 + \cdots + \alpha_m$, and the submonoid $\mathcal{B}(\underline{g})$ inherits this grading.

4   Repetition of Elements

A surjective monoid homomorphism $\theta : T \to B$ between reduced affine monoids T and B is called a *transfer homomorphism* if for any $t \in T$, $b, c \in B$ with $\theta(t) = bc$, there exist elements $u, v \in T$ such that $t = uv$ and $\theta(u) = b$, $\theta(v) = c$ (see [14, Definition 3.2.1]).

Now let g be an m-tuple of elements in an abelian group G and $\mathcal{B}(g)$, $\mathcal{B}(\mathrm{supp}(g))$ the monoids introduced in Section 1. The map

$$\mathbb{N}_0^m \to \mathbb{N}_0^{\mathrm{supp}(g)}, \quad \alpha \mapsto \left(g \mapsto \sum_{g_i = g} \alpha_i\right) \tag{4}$$

restricts to a *transfer homomorphism* $\mathcal{B}(g) \to \mathcal{B}(\mathrm{supp}(g))$. In factorization theory transfer homomorphisms are used to reduce the computation of arithmetic invariants of monoids to the corresponding invariants of other monoids (frequently of block monoids). In particular, it is known that the catenary degrees of monoids connected by a transfer homomorphism are linked as follows:

Lemma 1. *[14, Theorem 3.2.5.5] Let $\theta : T \to B$ be a transfer homomorphism, where T and B are reduced affine monoids. Then we have the inequalities*

$$c(B) \leq c(T) \leq \max\{c(B), c(T, \theta)\}$$

(see [14, page 171] for the definition of $c(T, \theta)$).

The aim of this section is to refine Lemma 1 for the transfer homomorphism $\mathcal{B}(g) \to \mathcal{B}(\mathrm{supp}(G))$ given by (4). More precisely, it will be shown how one can get a generating system of the defining congruence of $\mathcal{B}(g)$ from a given generating system of the defining congruence of $\mathcal{B}(\mathrm{supp}(g))$. This will be done in a more general setup.

Assume that S is a (not necessarily connected) graded, reduced, affine monoid, and denote by $\tilde{S}$ the monoid

$$\tilde{S} = \{s[i] \mid s \in S, 0 \leq i \leq |s|\} \text{ with multiplication } s[i] \cdot t[j] = (s \cdot t)[i + j]. \tag{5}$$

So $\tilde{S}$ is a submonoid of the direct product of S and the additive monoid $\mathbb{N}_0$. Obviously the map $\tilde{S} \to S$, $s[i] \mapsto s$ is a transfer homomorphism, and

$$\mathcal{A}(\tilde{S}) = \{a[i] \mid a \in \mathcal{A}(S), \ 0 \leq i \leq |a|\}.$$

This transfer homomorphism $\tilde{S} \to S$ induces a monoid homomorphism

$$\kappa : \mathbb{N}_0^{\mathcal{A}(\tilde{S})} \to \mathbb{N}_0^{\mathcal{A}(S)}, \quad \lambda \mapsto \left(a \mapsto \sum_{i=0}^{|a|} \lambda(a[i])\right).$$

Set

$$\delta : \mathbb{N}_0^{\mathcal{A}(\tilde{S})} \to \mathbb{N}_0, \quad \lambda \mapsto \sum_{a[i] \in \mathcal{A}(\tilde{S})} i \lambda(a[i]).$$

Note that for $\lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ we have

$$x^\lambda \sim_{\tilde{S}} x^\mu \iff x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)} \text{ and } \delta(\lambda) = \delta(\mu). \tag{6}$$

Also we have $\delta(\lambda) \le |a^{\kappa(\lambda)}|$.

Lemma 2. *Assume that $\alpha, \beta \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ satisfy*

$$\kappa(\alpha) = \kappa(\beta) \quad and \quad \delta(\alpha) = \delta(\beta).$$

Then $x^\alpha \sim x^\beta$ with respect to the semigroup congruence $\sim$ on the free monoid $\tilde{M} = \{x^\alpha \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}\}$ generated by

$$\{(x_{a[k]}x_{b[l]}, x_{a[k+1]}x_{b[l-1]}) \mid a, b \in \mathcal{A}(S), \ 0 \le k \le |a| - 1, \ 1 \le l \le |b|\}.$$

Proof. Apply induction on $\sum_{a[j] \in \mathcal{A}(\tilde{S})} \alpha(a[j])$. If this number is 1, then clearly $\alpha = \beta$, and so the desired conclusion holds. Assume $\sum_{a[j] \in \mathcal{A}(\tilde{S})} \alpha(a[j]) > 1$.

Case I: x^α and x^β involve a common variable $x_{a[i]}$. Then $x^\alpha = x_{a[i]}x^{\alpha'}$, $x^\beta = x_{a[i]}x^{\beta'}$, and the assumptions on the pair (α, β) in the statement of the lemma hold for the pair (α', β'). By the induction hypothesis we may conclude that $x^{\alpha'} \sim x^{\beta'}$, implying in turn that $x^\alpha \sim x^\beta$.

Case II: x^α and x^β are not divisible by a common variable. Take a variable $x_{a[i]}$ dividing x^α. Then $\kappa(\alpha) = \kappa(\beta)$ implies that x^β is divisible by $x_{a[k]}$ for some $k \ne i$. By symmetry it is sufficient to deal with the case $i > k$. By the assumptions on α, β there must exist an atom $b \in \mathcal{A}(S)$ and integers $j < l$ such that $x_{a[i]}x_{b[j]}$ divides x^α and $x_{a[k]}x_{b[l]}$ divides T^β. We have $x^\alpha = x_{a[i]}x_{b[j]}x^\gamma \sim x_{a[i-1]}x_{b[j+1]}x^\gamma = x^{\alpha'}$. The conditions of the lemma on the pair (α, β) hold also for the pair (α', β). If $i - 1 = k$, then $x^{\alpha'}$ and x^β are divisible by a common variable, and we are back in Case I. Otherwise similarly to the above process we have $x^{\alpha'} \sim x^{\alpha''}$ where $x^{\alpha''}$ is divisible by $x_{a[i-2]}$ and $\kappa(\alpha'') = \kappa(\beta)$ and $\delta(\alpha'') = \delta(\beta)$. After finitely many such steps we get back to Case I.

Remark 4. Lemma 2 says that for the transfer homomorphism $\theta : \tilde{S} \to S, s[i] \mapsto s$ we have $c(\tilde{S}, \theta) \le 2$ in Lemma 1.

Theorem 1. *Suppose that the congruence $\sim_S$ is generated by $\{(x^\lambda, x^\mu) \mid (\lambda, \mu) \in \Lambda\}$ for some $\Lambda \subset \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$. For each $\lambda \in \mathbb{N}_0^{\mathcal{A}(S)}$ such that $(\lambda, \mu) \in \Lambda$ or $(\mu, \lambda) \in \Lambda$ for some μ, and for each $0 \le i \le |a^\lambda|$ choose $\lambda[i] \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ such that $\kappa(\lambda[i]) = \lambda$ and $\delta(\lambda[i]) = i$ (this is clearly possible). Then the congruence $\sim_{\tilde{S}}$ is generated by*

$$\{(x^{\lambda[i]}, x^{\mu[i]}), (x_{a[k]}x_{b[l]}, x_{a[k+1]}x_{b[l-1]}) \mid (\lambda, \mu) \in \Lambda, \ 0 \leq i \leq |a^{\lambda}|,$$
$$a, b \in \mathcal{A}(S), \ 0 \leq k \leq |a| - 1, \ 1 \leq l \leq |b|\}.$$

Proof. The pairs given in the statement do belong to the congruence $\sim_{\tilde{S}}$. Denote by $\sim$ the semigroup congruence on $\tilde{M} = \{x^{\alpha} \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}\}$ generated by them. It is sufficient to show that if $x^{\alpha} \sim_{\tilde{S}} x^{\beta}$ for some $\alpha, \beta \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$, then $x^{\alpha} \sim x^{\beta}$. By (6) we have $x^{\kappa(\alpha)} \sim_S x^{\kappa(\beta)}$ and $\delta(\alpha) = \delta(\beta)$. Therefore there exists a sequence $(\lambda_j, \mu_j) \in \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$ and $\gamma_j \in \mathbb{N}_0^{\mathcal{A}(S)}$ $(j = 1, \ldots, s)$ such that $(\lambda_j, \mu_j) \in \Lambda$ or $(\mu_j, \lambda_j) \in \Lambda$ (implying in particular that $|a^{\lambda_j}| = |a^{\mu_j}|$), $\lambda_1 + \gamma_1 = \kappa(\alpha)$, $\mu_s + \gamma_s = \kappa(\beta)$, and $\mu_j + \gamma_j = \lambda_{j+1} + \gamma_{j+1}$ for $j = 1, \ldots, s-1$. Set $d := \delta(\alpha) = \delta(\beta)$. For each $j = 1, \ldots, s$ choose a non-negative integer k_j with

$$d - |a^{\gamma_j}| \leq k_j \leq |a^{\lambda_j}|.$$

This is possible, because

$$d \leq |a^{\kappa(\alpha)}| = |a^{\lambda_j + \gamma_j}| = |a^{\lambda_j}| + |a^{\gamma_j}|.$$

Taking into account Lemma 2 we get

$$x^{\alpha} \sim x^{\kappa(\alpha)[d]} = x^{(\lambda_1 + \gamma_1)[d]} \sim x^{\lambda_1[k_1]}x^{\gamma_1[d-k_1]} \sim x^{\mu_1[k_1]}x^{\gamma_1[d-k_1]} \sim$$
$$x^{(\mu_1 + \gamma_1)[d]} = x^{(\lambda_2 + \gamma_2)[d]} \sim x^{\lambda_2[k_2]}x^{\gamma_2[d-k_2]} \sim x^{\mu_2[k_2]}x^{\gamma_2[d-k_2]} \sim$$
$$x^{(\mu_2 + \gamma_2)[d]} = x^{(\lambda_3 + \gamma_3)[d]} \sim \cdots \sim x^{(\mu_s + \gamma_s)[d]} = x^{\kappa(\beta)[d]} \sim x^{\beta}.$$

Remark 5. Statements related to Theorem 1 are proved in [21], studying toric ideals associated to nested configurations (see also [26] for some generalization). The construction of $\tilde{S}$ from S (see (5)) can be seen as a special case of the construction of nested configurations. In particular, when S is a submonoid of $\mathbb{N}_0^d$ generated by finitely many elements $\alpha^{(1)}, \ldots, \alpha^{(m)}$ such that there exists a $v \in \mathbb{R}^d$ with $\sum_{j=1}^{d} \alpha_j^{(i)} v_j = 1$ for all $i = 1, \ldots, m$ (this implies that S can be graded in such a way that each generator has degree 1), the results of [21] apply to the binomial ideal associated to the monoid $\tilde{S}$ and yield a system of generators similar to the one given by Theorem 1.

The monoid $\mathcal{B}(\underline{g})$ can be obtained from the monoid $\mathcal{B}(\text{supp}(\underline{g}))$ by a repeated application of the construction (5), and therefore Theorem 1 can be applied to relate the catenary degree of $\mathcal{B}(\underline{g})$ to the catenary degree of $\mathcal{B}(\text{supp}(\underline{g}))$. Indeed, start with an m-tuple $\underline{g} = (g_1, \ldots, g_m) \in G^m$ of not necessarily distinct elements in G, and denote by $\tilde{\underline{g}}$ the $m + 1$-tuple $(g_1, \ldots, g_m, g_m)$ obtained from $\underline{g}$ by repeating the mth component. Consider the grading on the monoid $\mathcal{B}(\underline{g})$ given by

$$\mathcal{B}(\underline{g})_d = \{\alpha \in \mathcal{B}(\underline{g}) \subseteq \mathbb{N}_0^m \mid \alpha_m = d\}.$$

Proposition 4. *We have $\mathcal{B}(\tilde{g}) \cong \tilde{S}$, where $S = \mathcal{B}(\underline{g})$ is endowed with the above grading and $\tilde{S}$ is defined as in (5).*

Proof. A general element of $\tilde{S}$ is of the form $\alpha[i]$ where $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathcal{B}(\underline{g})$ and $0 \le i \le \alpha_m$. The map $\tilde{S} \to \mathcal{B}(\tilde{g})$ sending $\alpha[i] \in \tilde{S}$ to $(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m - i, i)$ is an isomorphism between the monoids $\tilde{S}$ and $\mathcal{B}(\tilde{g})$.

Proposition 1, Theorem 1, and Proposition 4 imply the following:

Corollary 3. *We have $c(\mathcal{B}(\underline{g})) = c(\mathcal{B}(\mathrm{supp}(\underline{g}))$, unless $\mathcal{B}(\mathrm{supp}(\underline{g}))$ is a free monoid and the components $g_1, \ldots, g_m$ of $\underline{g}$ are not all distinct. In the latter case we have $c(\mathcal{B}(\mathrm{supp}(\underline{g}))) = 0$ whereas $c(\mathcal{B}(\underline{g})) = 2$.*

Remark 6. Being a finitely generated reduced Krull monoid, $\mathcal{B}(\underline{g}) \cong \mathcal{B}(H_0)$ for some finite subset H_0 in an abelian group H (different from G in general) by [14, Theorem 2.7.14] also when $g_1, \ldots, g_m$ are not all distinct. However, the representation of our monoid in the form $\mathcal{B}(\underline{g})$ is fundamental for our discussions.

An easy direct proof of the isomorphism $\mathcal{B}(\underline{g}) \cong \mathcal{B}(H_0)$ can be derived from the following observation. Take $\underline{g} \in G^m$, and suppose that $g_{m-1} = g_m$. Consider the group $H := G \times \mathbb{Z}$, and the sequence

$$\underline{h} := ((g_1, 0), \ldots, (g_{m-1}, 0), (g_{m-1}, 1), (0, -1)) \in H^{m+1}.$$

It is easy to see that we have a monoid isomorphism $\mathcal{B}(\underline{g}) \cong \mathcal{B}(\underline{h})$. Now observe that there are less component repetitions in the sequence $\underline{h}$ then the number of component repetitions in $\underline{g}$. Note that the "price" for this manipulation was that we had to extend the group G.

5   Gröbner Bases

In this section we give a Gröbner basis variant of the results of Section 4. As it was explained in Sections 2 and 3, the catenary degree of a monoid can be expressed in terms of generators of a binomial ideal associated to the monoid. Since Gröbner bases are special generating systems of ideals in a polynomial algebra that are at the heart of many algorithms in computational commutative algebra (see for example [7] for Gröbner basis theory), it is worthwhile to translate this notion to the language of semigroup congruences.

Fix an admissible total order $\prec$ on the finitely generated free multiplicative monoid M; that is, $\prec$ is a total order such that for $x, y, z \in M$ with $x \prec y$ we have $xz \prec yz$, and $1 \prec x$ for each $x \in M \setminus \{1\}$. The latter condition ensures that the order $\prec$ is artinian (i.e., there is no infinite strictly descending chain with respect to $\prec$ in M), so any non-empty subset of M contains a unique minimal element. Note also that $\prec$ is a term order of the polynomial ring $\mathbb{F}[M]$ (where $\mathbb{F}$ is a field) in the sense of Gröbner basis theory.

Definition 3. *A finite set $\Lambda \subset M \times M$ is a* Gröbner system of the semigroup congruence $\sim$ on M *if the following conditions hold:*

(i) *$x \sim y$ and $y \prec x$ for each $(x, y) \in \Lambda$;*

(ii) *$z \in M$ is the minimal element in its congruence class with respect to $\sim$ if there is no $(x, y) \in \Lambda$ such that x divides z in M.*

The name *Gröbner system* is justified by the relation to Gröbner bases given in Proposition 5 (iii).

Proposition 5. (i) *If $\Lambda \subset M \times M$ is a Gröbner system of the semigroup congruence $\sim$ then Λ generates $\sim$.*

(ii) *Every semigroup congruence $\sim$ on M has a Gröbner system.*

(iii) *$\Lambda \subset M \times M$ is a Gröbner system of $\sim$ if and only if $\{x - y \mid (x, y) \in \Lambda\}$ is a Gröbner basis (satisfying $y \prec x$ for each of its elements $x - y$) of the ideal $\ker(\pi_{\mathbb{F}})$, where $\mathbb{F}$ is a field and $\pi_{\mathbb{F}} : \mathbb{F}[M] \to \mathbb{F}[M/\sim]$ is induced by the natural surjection $M \to M/\sim$.*

Proof. (i) Denote by $\sim_{\Lambda}$ the congruence generated by Λ. By assumption it is contained in $\sim$, since for each $(x, y) \in \Lambda$ we have $x \sim y$. To see the reverse inclusion it is sufficient to show that for any $z \in M$ we have $z \sim_{\Lambda} u$, where u is the minimal element in the $\sim$-congruence class of z. If $z = u$, we are done. Otherwise $u \prec z$, hence, by assumption there exists a pair $(x, y) \in \Lambda$ and $v \in M$ such that $z = xv$. Set $z_1 = yv$. Then $z_1 = yv \prec xv = z$ and $z \sim_{\Lambda} z_1$. If $z_1 = u$, then we are done. Otherwise repeat the same step for z_1 instead of z (note that $z_1 \sim z \sim u$). We obtain $z_2 \in M$ with $z_2 \prec z_1$ and $z_2 \sim_{\Lambda} z_1$. If $z_2 = u$ we are done, otherwise repeat the above step with z_2 instead of z_1. Since the order $\prec$ is artinian, in finitely many steps we must end up with $z \sim_{\Lambda} z_k = u$.

(ii) It is well known that any binomial ideal has a Gröbner basis consisting of binomials, see for example [28, Lemma 8.2.17]. Therefore the statement follows from (iii).

(iii) Suppose $\{x - y \mid (x, y) \in \Lambda\}$ is a Gröbner basis of the ideal $\ker(\pi_{\mathbb{F}})$ (where $y \prec x$ for each $(x, y) \in \Lambda$). It follows that the initial ideal of $\ker(\pi_{\mathbb{F}})$ is generated by $L := \{x \mid \exists y : (x, y) \in \Lambda\}$. Now take any $z \in M$ which is not minimal in its congruence class with respect to $\sim$. Then there is an $u \prec z$ such that $z \sim u$, so $z - u \in \ker(\pi_{\mathbb{F}})$ has initial term z. Therefore there is an $x \in L$ such that x divides z, so condition (ii) of Definition 3 holds for Λ (it is obvious that condition (i) of Definition 3 holds for Λ).

Conversely, assume that Λ is a Gröbner system of $\sim$, and consider the subset $L := \{x - y \mid (x, y) \in \Lambda\}$ in $\mathbb{F}[M]$. Denote by J the ideal generated by the initial terms in L. Clearly $L \subseteq \ker(\pi_{\mathbb{F}})$, hence, J is contained in the ideal K generated by the initial terms of the ideal $\ker(\pi_{\mathbb{F}})$. By assumption the elements of $M \setminus J$ are all minimal in their congruence class with respect to $\sim$. In particular, they are pairwise incongruent; hence, they are mapped by $\pi_{\mathbb{F}}$ to elements in $\mathbb{F}[M/\sim]$ that are linearly independent over $\mathbb{F}$. On the other hand, $M \setminus J \supseteq M \setminus K$, and the latter is mapped by $\pi_{\mathbb{F}}$ to an $\mathbb{F}$-vector space basis of $\mathbb{F}[M/\sim]$ (see for example [27,

Proposition 1.1]). It follows that $M \setminus J = M \setminus K$, implying in turn that $J = K$. The latter equality means that L is a Gröbner basis of $\ker(\pi_{\mathbb{F}})$.

We keep the notation of Section 4. In particular, S is a reduced, affine, graded monoid, and $\tilde{S}$ is the monoid defined as in (5). Fix an admissible total order $\prec$ on $M = \{x^\alpha \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(S)}\}$. Define an admissible total order (denoted also by $\prec$) on the free monoid $\tilde{M}$ generated by $\{x_a \mid a \in \mathcal{A}(\tilde{S})\}$ as follows. Enumerate the atoms in $\mathcal{A}(S) = \{a_1, \ldots, a_n\}$ such that $x_{a_1} \prec x_{a_2} \prec \cdots \prec x_{a_n}$. Set $d_i = |a_i|$. For $\lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ we set $x^\mu \prec x^\lambda \in \tilde{M}$ if

1. $x^{\kappa(\mu)} \prec x^{\kappa(\lambda)}$ in $(M, \prec)$; or
2. $\kappa(\mu) = \kappa(\lambda)$ and the sequence

$$(\mu(a_1[0]), \mu(a_1[1]), \ldots, \mu(a_1[d_1]), \mu(a_2[0]), \ldots, \mu(a_n[0]), \ldots, \mu(a_n[d_n]))$$

is lexicographically greater than

$$(\lambda(a_1[0]), \lambda(a_1[1]), \ldots, \lambda(a_1[d_1]), \lambda(a_2[0]), \ldots, \lambda(a_n[0]), \ldots, \lambda(a_n[d_n])).$$

Theorem 2. *Suppose that $\{(x^\lambda, x^\mu) \mid (\lambda, \mu) \in \Lambda\}$ is a Gröbner system of the semigroup congruence $\sim_S$. Then $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ is a Gröbner system of the defining congruence $\sim_{\tilde{S}}$ of $\tilde{S}$, where*

$$\Gamma_1 = \{(x^\lambda, x^\mu) \mid \lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}, \quad (\kappa(\lambda), \kappa(\mu)) \in \Lambda, \quad \delta(\lambda) = \delta(\mu)\}$$

$$\Gamma_2 = \{(x_{a[i]}x_{b[j]}, x_{a[i-1]}x_{b[j+1]}) \mid a, b \in \mathcal{A}(S), \ x_a \prec x_b, \ 0 < i \le |a|, \ 0 \le j < |b|\}$$

$$\Gamma_3 = \{(x_{a[i]}x_{a[j]}, x_{a[i-1]}x_{a[j+1]}) \mid a \in \mathcal{A}(S), \ 0 < i \le j < |a|\}.$$

Proof. Take $(x^\lambda, x^\mu) \in \Gamma_1$. Then $(\kappa(\lambda), \kappa(\mu)) \in \Lambda$, hence, $x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)}$ and $x^{\kappa(\mu)} \prec x^{\kappa(\lambda)} \in M$. It follows that $x^\mu \prec x^\lambda \in \tilde{M}$. Moreover, $x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)}$ and $\delta(\lambda) = \delta(\mu)$ imply $x^\lambda \sim_{\tilde{S}} x^\mu$ by (6). Therefore condition (i) of Definition 3 holds for the elements of Γ_1. It obviously holds for the elements of Γ_2 and Γ_3 by definition of the ordering $\prec$ on $\tilde{M}$.

It remains to check that condition (ii) of Definition 3 holds for $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$. In order to do so, take $\lambda \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ such that $x^\lambda \in \tilde{M}$ is not minimal in its congruence class with respect to $\sim_{\tilde{S}}$.

Assume first that $x^{\kappa(\lambda)} \in M$ is not minimal in its congruence class with respect to $\sim_S$. Then by the assumption of the theorem on Λ, there exist $(\alpha, \beta) \in \Lambda$ and $\gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ such that $\kappa(\lambda) = \alpha + \gamma$. Clearly there exist $\tilde{\alpha}, \tilde{\gamma} \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ with $\lambda = \tilde{\alpha} + \tilde{\gamma}$, $\kappa(\tilde{\alpha}) = \alpha$, and $\kappa(\tilde{\gamma}) = \gamma$. Also $x^\alpha \sim_S x^\beta$ implies $\sum_{a \in \mathcal{A}(S)} \alpha(a)|a| = \sum_{a \in \mathcal{A}(S)} \beta(a)|a|$. It is easy to infer from this equality the existence of $\tilde{\beta} \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ with $\kappa(\tilde{\beta}) = \beta$ and $\delta(\tilde{\beta}) = \delta(\tilde{\alpha})$. Moreover, $(\alpha, \beta) \in \Lambda$ implies $x^\beta \prec x^\alpha$, hence, $x^{\tilde{\beta}} \prec x^{\tilde{\alpha}}$.

So $(x^{\tilde{\alpha}}, x^{\tilde{\beta}}) \in \Gamma_1$ by definition of Γ_1. Therefore Γ_1 testifies the non-minimality of x^λ as it is required by (ii) of Definition 3.

Suppose next that $x^{\kappa(\lambda)}$ is minimal in its congruence class in M with respect to $\sim_s$, and $x^\lambda \in \tilde{M}$ is not minimal in its congruence class with respect to $\sim_{\tilde{s}}$. It is easy to deduce from condition 2. of the definition of the ordering $\prec$ on $\tilde{M}$ that there must exist $(y, z) \in \Gamma_2 \cup \Gamma_3$ such that y divides x^λ. Consequently, the non-minimality of x^λ is testified by $\Gamma_2 \cup \Gamma_3$ as it is required by (ii) of Definition 3.

Remark 7. The papers [21, 26] mentioned in Remark 7 also give Gröbner bases of the binomial ideals considered there.

We call a Gröbner system Λ *quadratic* if $|\lambda| \leq 2$, $|\mu| \leq 2$ for all $(\lambda, \mu) \in \Lambda$.

Corollary 4. *If the semigroup congruence $\sim_S$ has a quadratic Gröbner system, then the semigroup congruence $\sim_{\tilde{S}}$ also has a quadratic Gröbner system.*

Koszul algebras form an interesting class of rings well studied in commutative algebra, see for example [5]. In general it is a difficult task to decide whether a quadratic algebra (a factor of the multivariate polynomial algebra modulo an ideal generated by homogeneous quadratic elements) is Koszul or not. The significance of Corollary 4 is that it can be used to produce examples of Koszul algebras. Indeed, note that if S has a quadratic Göbner system, then by Proposition 5 (iii) the ideal of relations among the generators of the semigroup algebra $\mathbb{F}[S]$ has a quadratic Gröbner basis, hence is Koszul (see [24] for background on Koszul algebras). Therefore an iterated use of Corollary 4 yields the following:

Corollary 5. *If $\mathcal{B}(\text{supp}(\underline{g}))$ has a quadratic Gröbner system, then $\mathcal{B}(\underline{g})$ also has a quadratic Gröbner system, and hence, the semigroup algebra $\mathbb{F}[\mathcal{B}(\underline{g})]$ is Koszul.*

Example 1. Consider the additive group $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$, and the monoid $S := \mathcal{B}((1, 2, 3))$. The atoms in this monoid are

$$\mathcal{A}(S) = \{(1, 1, 1), (4, 1, 0), (3, 0, 1), (2, 2, 0), (0, 0, 2), (0, 3, 0), (6, 0, 0)\}.$$

The commuting indeterminates corresponding to the atoms will be denoted by $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, and $\pi : M \to S$ is the monoid homomorphism mapping the generator x_i of the free monoid M to the ith atom in the above list ($i = 1, \ldots, 7$). Denote by $\prec$ the graded reverse lexicographic order on M. That is, $x^\alpha \prec x^\beta$ if $\sum_{i=1}^7 \alpha_i < \sum_{i=1}^7 \beta_i$, or if $\sum_{i=1}^7 \alpha_i = \sum_{i=1}^7 \beta_i$ and for the largest j with $\alpha_j \neq \beta_j$ we have $\alpha_j > \beta_j$ (in particular, $x_7 \prec x_6 \prec \cdots \prec x_1$). We claim that the following is a Gröbner system for S:

$$\Lambda := \{(x_1^2, x_4x_5), (x_2^2, x_4x_7), (x_3^2, x_5x_7), (x_4^2, x_2x_6), (x_1x_2, x_3x_4),$$
$$(x_1x_3, x_2x_5), (x_2x_3, x_1x_7), (x_1x_4, x_3x_6), (x_2x_4, x_6x_7)\}.$$

Indeed, for each pair $(x, y) \in \Lambda$ we have $x \sim_S y$ and $y \prec x$. Moreover, it is easy to see that the elements in M not divisible by any of the first components of the pairs in Λ are the following:

$$\{w x_5^i x_6^j x_7^k \mid i, j, k \in \mathbb{N}_0, \ w \in \{1, x_1, x_2, x_3, x_4, x_3 x_4\}\}.$$

Now the above elements are mapped by π to distinct elements in S. To see this note that the modulo 6 residue of the first component of $\pi(w x_5^i x_6^j x_7^k)$ uniquely determines w, and then i, j, k are determined by $\pi(w x_5^i x_6^j x_7^k)$. Thus S has a quadratic Gröbner system, and consequently by Corollary 5 the algebra $\mathbb{F}[\mathcal{B}(g)]$ is Koszul for any g with $\mathrm{supp}(g) = \{1, 2, 3\} \subset \mathbb{Z}/6\mathbb{Z}$.

6 Relation to Invariant Theory

We need to recall a result from invariant theory (see [11] for an introduction to invariant theory). Let H be a linearly reductive subgroup of the group $GL(V)$ of invertible linear transformations of a finite-dimensional vector space V over an algebraically closed field $\mathbb{F}$. The action of H on V induces an action via graded $\mathbb{F}$-algebra automorphism on the symmetric tensor algebra $S(V)$ of V (graded in the standard way, namely, $V \subset S(V)$ is the degree 1 homogeneous component). Since H is linearly reductive, the algebra $S(V)^H = \{f \in S(V) \mid h \cdot f = f \ \forall h \in H\}$ of polynomial invariants is known to be finitely generated. Let $f_1, \ldots, f_n$ be a minimal homogeneous generating system of $S(V)^H$, enumerated so that $\deg(f_1) \geq \deg(f_2) \geq \cdots \geq \deg(f_n)$. Consider the $\mathbb{F}$-algebra surjection

$$\varphi : \mathbb{F}[x_1, \ldots, x_n] \to S(V)^H \text{ with } x_i \mapsto f_i \quad (i = 1, \ldots, n). \tag{7}$$

Endow $\mathbb{F}[x_1, \ldots, x_n]$ with the grading given by $\deg(x_i) = \deg(f_i)$, so φ is a homomorphism of graded algebras. Recall that the factor of $S(V)$ modulo the ideal generated by $f_1, \ldots, f_n$ is called the *algebra of coinvariants*. It is a finite-dimensional graded vector space when H is finite; in this case write $b(H, V)$ for its top degree (equivalently, all homogeneous elements in $S(V)$ of degree greater than $b(H, V)$ belong to the Hilbert ideal $S(V) f_1 + \cdots + S(V) f_n$, and there is a homogeneous element in $S(V)$ of degree $b(H, V)$ not contained in the Hilbert ideal). Denote by s the Krull dimension of $S(V)^H$. Note that $s \leq n$ with equality only if $\ker(\varphi) = \{0\}$.

Theorem 3. (Derksen [10, Theorems 1 and 2])

(i) *We have the inequality* $\mu(\ker(\varphi)) \leq \sum_{i=1}^{\min\{n, s+1\}} \deg(f_i) - s$,

(ii) *When H is finite, we have the inequality* $\mu(\ker(\varphi)) \leq 2b(G, V) + 2$.

The *Davenport constant of a finite subset G_0* of an abelian group G is defined as

$$\mathsf{D}(G_0) = \max\{|\alpha|\colon \alpha \in \mathcal{A}(\mathcal{B}(G_0))\},$$

where $|\alpha| = \sum_{g \in G_0} \alpha(g)$. When G_0 generates a finite subgroup in G, the *little Davenport constant of G_0* can be defined as

$$\mathsf{d}(G_0) = \max\{|\alpha|\colon \alpha \in \mathbb{N}_0^{G_0}, \ \forall \gamma \in \mathcal{A}(\mathcal{B}(G_0)) \ \exists g \in G_0 \text{ with } \gamma(g) > \alpha(g)\},$$

the maximal length of a sequence over G_0 containing no product-one subsequence (see [14, Proposition 5.1.3.2]).

Now let $\underline{g} = (g_1, \ldots, g_m)$ be a sequence of elements from an arbitrary abelian group G, and use the notation developed in Section 4. Consider the following grading of the block monoid $\mathcal{B}(\underline{g})$: for $\alpha \in \mathcal{B}(\underline{g})$ its degree is $|\alpha| = \sum_{i=1}^{m} \alpha_i$. The graded catenary degree $c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$ is defined in Definition 2 accordingly. Denote by $r(\mathcal{B}(\underline{g}))$ the rank of the free abelian subgroup in $\mathbb{Z}^m$ generated by $\mathcal{B}(\underline{g})$. Obviously $|\mathcal{A}(\mathcal{B}(\underline{g}))| \geq r(\mathcal{B}(\underline{g}))$ with equality if and only if $\mathcal{B}(\underline{g})$ is a free monoid. Set

$$\mathcal{A}(\mathcal{B}(\mathrm{supp}(\underline{g}))) := \{a_1, \ldots, a_n\} \text{ with } |a_1| \geq |a_2| \geq \cdots \geq |a_n|.$$

Theorem 4. *(i) We have the inequalities*

$$c_{\mathrm{gr}}(\mathcal{B}(\underline{g})) \leq \max\{2|a_1|, c_{\mathrm{gr}}(\mathcal{B}(\mathrm{supp}(\underline{g})))\}, \tag{8}$$

and

$$c_{\mathrm{gr}}(\mathcal{B}(\mathrm{supp}(\underline{g}))) \leq \sum_{i=1}^{\min\{n,r+1\}} |a_i| - r, \tag{9}$$

where $r = r(\mathcal{B}(\mathrm{supp}(\underline{g})))$.
(ii) If $g_1, \ldots, g_m$ generate a finite subgroup of G, then

$$c_{\mathrm{gr}}(\mathcal{B}(\underline{g})) \leq 2\mathsf{d}(\mathrm{supp}(\underline{g})) + 2. \tag{10}$$

Proof. We may assume that the components of $\underline{g}$ generate G. So G is a finitely generated abelian group, whence it is isomorphic to $G_1 \times \mathbb{Z}^k$, where G_1 is a finite abelian group, and $\mathbb{Z}^k$ is the free abelian group of rank k. Consider the linear algebraic group $H = G_1 \times T$, where T is the torus $(\mathbb{C}^\times)^k$. For an abelian linear algebraic group A denote by $X(A)$ the group of homomorphisms $A \to \mathbb{C}^\times$ (as algebraic groups). Then $X(G_1) \cong G_1$ and $X(T) \cong \mathbb{Z}^k$, whence $X(H) \cong G_1 \times \mathbb{Z}^k \cong G$. From now on we identify G with $X(H)$. Let V be a $\mathbb{C}$-vector space with basis $x_1, \ldots, x_m$, and define an action of H on V via linear transformations by setting $h \cdot x_i = g_i(h)x_i$ for $i = 1, \ldots, m$. The algebra $S(V)$ is the polynomial algebra $\mathbb{C}[x_1, \ldots, x_m]$. The monomials span 1-dimensional invariant subspaces, and for $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ and $h \in H$ we have that

$$h \cdot x^{\alpha} = \left(\prod_{i=1}^{m} g_i(h)^{\alpha_i} \right) x^{\alpha}.$$

It follows that the map $\mathbb{N}_0^m \to S(V)$, $\alpha \mapsto x^{\alpha}$ induces an isomorphism of the semi-group algebras

$$\mathbb{C}[\mathcal{B}(\underline{g})] \xrightarrow{\cong} \mathbb{C}[x_1, \ldots, x_m]^H. \tag{11}$$

The isomorphism (11) is an isomorphism of graded algebras. We may select as homogeneous generators of $S(V)^H$ the monomials $\{x^{\alpha} \mid \alpha \in \mathcal{A}(\mathcal{B}(\underline{g}))\}$. Then the presentation (7) of $S(V)^H$ is identified via (11) with the presentation (3) of the semigroup algebra $\mathbb{C}[\mathcal{B}(\underline{g})]$. So $\mu(\ker(\varphi)) = \mu(\ker(\pi_{\mathbb{C}}))$ (see (3) in Section 2 for the definition of $\pi_{\mathbb{C}} : \mathbb{C}[M] \to \mathbb{C}[\mathcal{B}(\underline{g})]$). By Corollary 2 we know that $\mu(\ker(\pi_{\mathbb{C}})) = c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$. Thus we have $\mu(\ker(\varphi)) = c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$. On the other hand applying Theorem 3 (i) for $\mu(\ker(\varphi))$ in the special case when $g_1, \ldots, g_m$ are distinct (i.e., when $\mathcal{B}(\underline{g}) = \mathcal{B}(\mathrm{supp}(\underline{g}))$) we obtain the inequality (9) (by (11) the Krull dimension of $\mathbb{C}[x_1, \ldots, x_m]^H$ equals the Krull dimension of $\mathbb{C}[\mathcal{B}(\underline{g})]$, and the latter coincides with the rank of the free abelian subgroup of $\mathbb{Z}^m$ generated by $\mathcal{B}(\underline{g})$). Combining (9) with Theorem 1 and Proposition 4 we get the inequality (8). The explanation of (11) shows also $b(G, V) = \mathsf{d}(\mathrm{supp}(\underline{g}))$, so Theorem 3 (ii) yields (10).

Remark 8. When $G \cong \mathbb{Z}^k$, the group H in the above proof is an algebraic torus, and the results in [29] give various bounds for $|a_1|$ in Theorem 4 (i). Moreover, [30] characterizes the cases when $\mathbb{C}[\mathcal{B}(\underline{g})] \cong S(V)^H$ (for a torus H) is a polynomial ring, i.e., when $c_{\mathrm{gr}}(\mathcal{B}(\underline{g})) = 0$.

Corollary 6. *For any subset G_0 of a finite abelian group G we have the inequalities*

$$c_{\mathrm{gr}}(\mathcal{B}(G_0)) \leq 2\mathsf{d}(G_0) + 2 \leq 2\mathsf{D}(G) \leq 2|G|.$$

Proof. The first inequality is a special case of Theorem 4 (ii). To see the second inequality note the trivial inequality $\mathsf{d}(G_0) \leq \mathsf{d}(G)$, and the well known equality $\mathsf{d}(G) + 1 = \mathsf{D}(G)$ (cf. [14, Proposition 5.1.3.2]).

It follows immediately from Definitions 1 and 2 that

$$c(S) \leq \frac{1}{\min\{|a| : a \in \mathcal{A}(S)\}} c_{\mathrm{gr}}(S). \tag{12}$$

Therefore Theorem 4 implies bounds on the ordinary (not graded) catenary degree. For example, an immediate consequence of Corollary 6 and (12) is the following:

Corollary 7. *Let G_0 be a subset in a finite abelian group G. Then*

$$c(\mathcal{B}(G_0)) \leq \frac{2\mathsf{d}(G_0) + 2}{\min\{|\alpha| : \alpha \in \mathcal{A}(\mathcal{B}(G_0))\}}.$$

As an application we recover the following known bound on $c(\mathcal{B}(G))$:

Corollary 8. [14, Theorem 3.4.10.5] *For any finite abelian group G we have the inequality $c(\mathcal{B}(G)) \leq \mathsf{D}(G)$.*

Proof. The monoid isomorphism $\mathcal{B}(G) \cong \mathcal{B}(G \setminus \{1_G\}) \times \mathcal{B}(\{1_G\}) \cong \mathcal{B}(G \setminus \{1_G\}) \times \mathbb{N}_0$ implies that $c(\mathcal{B}(G)) = c(\mathcal{B}(G \setminus \{1_G\}))$. For a nontrivial group G the minimal degree of an atom in $\mathcal{B}(G \setminus \{1_G\})$ is 2, hence, Corollary 7 gives $c(\mathcal{B}(G \setminus \{1_G\})) \leq \frac{2\mathsf{d}(G)+2}{2} = \mathsf{d}(G) + 1 = \mathsf{D}(G)$.

Example 2. It is known that the bound in Corollary 8 is sharp for G with $|G| \geq 3$ if and only if G is cyclic or G is an elementary 2-group by [14, Theorem 6.4.7] (see also [15], where the finite groups with $c(\mathcal{B}(G)) = \mathsf{D}(G) - 1$ are characterized). The inequality $c_{\mathrm{gr}}(\mathcal{B}(G_0)) \leq 2\mathsf{d}(G_0) + 2$ in Corollary 6, the inequality in Corollary 7, and the inequalities (8) and (10) in Theorem 4 are also sharp for these groups:

(i) Set $G_0 := \{1, -1\} \subset \mathbb{Z}/n\mathbb{Z}$, $S := \mathcal{B}(G_0)$. Then $\mathcal{A}(S) = \{(n, 0), (0, n), (1, 1)\}$. The defining congruence $\sim_S$ of S is generated by $(x_{(1,1)}^n, x_{(n,0)}x_{(0,n)})$ (a single generator). We have $\mathsf{d}(G_0) = n - 1$ and $c_{\mathrm{gr}}(S) = 2n$, whereas $\min\{|\alpha|\colon \alpha \in \mathcal{A}(S)\} = 2$ and $\max\{|\alpha|\colon \alpha \in \mathcal{A}(S)\} = n$.

(ii) Let $e_1, \ldots, e_n$ be a basis of the elementary 2-group of rank $n \geq 2$, and $G_0 := \{e_1 + \cdots + e_n, e_1, \ldots, e_n\}$, $S := \mathcal{B}(G_0)$. Then $\mathcal{A}(S) = \{a_1 := (1, 1, \ldots, 1), a_2 := (2, 0, \ldots, 0), a_3 := (0, 2, 0, \ldots, 0), \ldots, a_{n+2} := (0, \ldots, 0, 2)\}$. The defining congruence of S is generated by $(x_{a_1}^2, x_{a_2} \cdots x_{a_{n+2}})$. We have $\mathsf{d}(G_0) = n$ and $c_{\mathrm{gr}}(S) = 2n + 2$, whereas $\min\{|\alpha|\colon \alpha \in \mathcal{A}(S)\} = 2$ and $\max\{|\alpha|\colon \alpha \in \mathcal{A}(S)\} = n + 1$.

7 Relation to Toric Varieties

The quotient construction of toric varieties (cf. [6]) represents a toric variety as the categorical quotient of a Zariski open subset in a vector space endowed with an action of a diagonalizable group (see [8] for background on toric varieties). Rings of invariants are at the basis of quotient constructions in algebraic geometry. In the proof of Theorem 4, we recalled that the ring of invariants $\mathbb{C}[x_1, \ldots, x_m]^H$ of a diagonalizable group action is isomorphic to a semigroup ring $\mathbb{C}[\mathcal{B}(g)]$ of a block monoid. Therefore the results in Sections 4, 5, 6 have relevance for toric varieties.

In more details, the coordinate rings of affine toric varieties with no torus factors are the semigroup rings (over $\mathbb{C}$) of reduced, affine Krull monoids. This class of rings (up to isomorphism) is the same as the class of rings of invariants $\mathbb{C}[x_1, \ldots, x_m]^H$, where H is an abelian group, and each variable spans an H-invariant subspace (see for example [3, Corollary 5.19]), which is the same as the class of rings of the form $\mathbb{C}[\mathcal{B}(\underline{g})]$.

Projective toric varieties can be constructed as the projective spectrum of semigroup algebras of reduced affine Krull monoids, see for example [20, Chapter

10], [8, Theorem 14.2.13]. Namely, take $\underline{g} = (g_1, \ldots, g_m) \in G^m$ such that $\mathcal{B}(\underline{g}) = \{0\}$, and fix an element $h \in G$. Endow the monoid $\mathcal{B}((\underline{g}, h))$ with the grading given by $\mathcal{B}((\underline{g}, h))_d = \{\alpha \in \mathcal{B}((\underline{g}, h)) \subseteq \mathbb{N}_0^{m+1} \mid \alpha_{m+1} = d\}, d = 0, 1, 2, \ldots$. Then $\mathbb{C}[\mathcal{B}((\underline{g}, h))]$ becomes a graded algebra, whose projective spectrum is a projective toric variety.

Example 3. We reformulate a result on presentations of homogeneous coordinate rings of projective toric quiver varieties from [12] in the terminology of the present paper. Let Γ be an acyclic quiver (i.e., a finite directed graph having no oriented cycles), with vertex set $\{1, \ldots, k\}$ and arrow set $\{e_1, \ldots, e_m\}$. For an arrow e_i denote by $s(e_i)$ the starting vertex of e_i, and denote by $t(e_i)$ the terminating vertex of e_i. In the additive group $\mathbb{Z}^k$ consider the elements $g_i = (g_{i1}, \ldots, g_{ik}), i = 1, \ldots, m$ given by

$$g_{ij} = \begin{cases} -1, & \text{if } j = s(e_i) \\ 1 & \text{if } j = t(e_i) \\ 0 & \text{otherwise.} \end{cases}$$

Pick an element $h \in \mathbb{Z}^k$ whose additive inverse is contained in the subgroup of $\mathbb{Z}^k$ generated by $g_1, \ldots, g_m$. Then [12, Theorem 9.3] asserts that the catenary degree $c(\mathcal{B}((\underline{g}, h)))$ of $\mathcal{B}((\underline{g}, h))$ is at most 3. Moreover, it is shown in [13] that if we assume in addition that if $r(\mathcal{B}((\underline{g}, h))) \leq 5$ (i.e., the corresponding toric variety has dimension at most 4), then $c(\mathcal{B}((\underline{g}, h))) \leq 2$ with essentially one exception. We mention that presentations of the coordinate ring of affine toric quiver varieties are studied in [19].

Well known open conjectures (of increasing strength) in combinatorial commutative algebra are the following (called sometimes Bøgvad's conjecture; see [27, Conjecture 13.19] or [2]): Given a smooth, projectively normal projective toric variety, its

 (i) vanishing ideal is generated by quadratic elements.
 (ii) homogeneous coordinate ring is Koszul.
(iii) vanishing ideal has a quadratic Göbner basis.

For a finite subset G_0 of G with $\mathcal{B}(G_0) = \{0\}$ and an element h whose inverse belongs to the subgroup generated by G_0, the monoid $\mathcal{B}(G_0 \cup \{h\})$ is endowed with the grading such that the degree d component consists of the elements α in $\mathcal{B}(G_0 \cup \{h\})$ with $\alpha(h) = d$. Suppose that $\mathcal{B}(G_0 \cup \{h\})$ has a quadratic Gröbner system. According to the above conjecture this is expected to happen when $\mathcal{B}(G_0 \cup \{h\})$ is generated in degree 1 (so $\mathcal{B}(G_0 \cup \{h\})$ is half-factorial in the sense of factorization theory), and the projective spectrum of $\mathbb{C}[\mathcal{B}(G_0 \cup \{h\})]$ is a smooth projective variety. (For instance, in the setup of Example 3 this holds by [17] for almost all choices of h when Γ is a bipartite directed graph with 3 source and 3 sink vertices.) Then for any $\underline{g}$ with $\text{supp}(\underline{g}) = G_0$ we have by Corollary 5 that $\mathcal{B}((\underline{g}, h))$ has a quadratic Gröbner basis, and hence the algebra $\mathbb{C}[\mathcal{B}((\underline{g}, h))]$ is Koszul (although its projective spectrum typically fails to be a smooth projective variety).

References

1. Blanco, V., García-Sánchez, P.A., Geroldinger, A.: Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids. Illinois J. Math. **55**, 1385–1414 (2011)
2. Bruns, W.: The quest for counterexamples in Toric geometry, Proc. CAAG 2010, Ramanujan Math. Soc. Lect. Notes Series No. 17, 1–17 (2013)
3. Bruns, W., Gubeladze, J.: Polytopes, Rings, and K-theory. Springer, New York (2009)
4. Chapman, S.T., García-Sánchez, P.A., Llena, D., Ponomarenko, V., Rosales, J.C.: The catenary and tame degree in finitely generated commutative cancellative monoids. Manuscripta Math. **120**, 253–264 (2006)
5. Conca, A., De Negri, E., Rossi, M.E.: Koszul algebras and regularity. In: Peeva, I. (ed.) Commutative Algebra: Expository Papers Dedicated to David Eisenbud on the Occasion of His 65th Birthday, pp. 285–315. Springer (2013)
6. Cox, D.: The homogeneous coordinate ring of a toric variety. J. Algebr. Geom. **4**, 15–50 (1995)
7. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, New York, Berlin, Heidelberg (1992)
8. Cox, D., Little, J., Schenck, H.: Toric Varieties. Amer. Math. Soc, Providence, RI (2010)
9. Cziszter, K., Domokos, M., Geroldinger, A.: The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics. In: Chapman, S.T., Fontana, M., Geroldinger, A., Olberding, B. (eds.), Multiplicative Ideal Theory and Factorization Theory, pp. 43–95, Springer (2016)
10. Derksen, H.: Degree bounds for syzygies of invariants. Adv. Math. **185**, 207–214 (2004)
11. Derksen, H., Kemper, G.: Computational Invariant Theory, Encyclopaedia of Mathematical Sciences 130. Springer, Berlin, Heidelberg, New York (2002)
12. Domokos, M., Joó, D.: On the equations and classification of toric quiver varieties. Proc. Royal Soc. Edinburgh: Sect. A Math. **146**, 265–295 (2016)
13. Domokos, M., Joó, D.: Toric quiver cells. arXiv:1609.03618
14. Geroldinger, A., Halter-Koch, F.: Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, Vol. 278, Chapman & Hall/CRC (2006)
15. Geroldinger, A., Zhong, Q.: The catenary degree of Krull monoids II. J. Australian Math. Soc. **98**, 324–354 (2015)
16. Gilmer, R.: Commutative Semigroup Rings. The University of Chicago Press (1984)
17. Haase, C., Paffenholz, A.: Quadratic Gröbner bases for smooth 3×3 transportation polytopes. J. Algebr. Comb. **30**, 477–489 (2009)
18. Herzog, J.: Generators and relations of abelian semigroups and semigroup rings. Manuscripta Math. **3**, 175–193 (1970)
19. Joó, D.: Complete intersection quiver settings with one dimensional vertices. Algebr. Represent. Theory **16**, 1109–1133 (2013)
20. Miller, E., Sturmfels, B.: Combinatorial Commutative Algebra, Graduate Texts in Mathematics, Vol. 227. Springer (2005)
21. Ohsugi, H., Hibi, T.: Toric rings and ideals of nested configurations. J. Commut. Algebra **2**, 187–208 (2010)
22. Philipp, A.: A characterization of arithmetical invariants by the monoid of relations. Semigroup Forum **81**, 424–434 (2010)
23. Philipp, A.: A characterization of arithmetical invariants by the monoid of relations II: the monotone catenary degree and applications to semigroup rings. Semigroup Forum **90**, 220–250 (2015)

24. Polishchuk, A., Positelski, L.: Quadratic Algebras, University Lecture Series 37. AMS, Providence, Rhode Island (2005)
25. Rédei, L.: The theory of Finitely Generated Commutative Semigroups. Pergamon, Oxford-Edinburgh-New York (1965)
26. Shibuta, T.: Gröbner bases of contraction ideals. J. Algebr. Comb. **36**, 1–19 (2012)
27. Sturmfels, B.: Gröbner Bases and Convex Polytopes, University Lecture Series 8. AMS, Providence, Rhode Island (1996)
28. Villareal, R.H.: Monomial Algebras, CRC Press, Chapman and Hall Book, Monographs and Research Notes in Mathematics, Second edition, Boca Raton, Florida (2015)
29. Wehlau, D.: Constructive invariant theory for tori. Ann. Inst. Fourier Grenoble **43**, 1055–1066 (1993)
30. Wehlau, D.: When is a ring of torus invariants a polynomial ring? Manuscripta Math. **82**, 161–170 (1994)