MONOMIAL SUBRINGS AND SYSTEMS OF SUBINTEGRALITY

LES REID AND LESLIE G. ROBERTS

ABSTRACT. We compute the seminormalization and weak normalization of subrings of $\mathbb{Z}[t]$ generated by monomials, and show how such rings arise in the study of systems of subintegrality.

1. INTRODUCTION.

By a monomial subring of $\mathbb{Z}[t]$ we mean a subring A of $B = \mathbb{Z}[t]$ generated as an abelian group by "monomials" at^i ($a \in \mathbb{Z}$, $i \geq 1$). Such rings arise naturally from our study of weakly subintegral ring extensions (for example from the "elementary weakly subintegral" extensions in [RR, Section 3] or the systems of subintegrality of [RRS]). For each i we can take b_i to be the smallest positive integer such that $b_i t^i \in A$ (or $b_i = 0$ if there is no such positive integer). Then A has $\mathbb{Z}$-basis consisting of all the $b_i t^i$ such that $b_i \neq 0$. We will refer to the sequence $\{b_i\}_{i \geq 0}$ as the coefficient sequence of A. We will eventually assume that $b_i = 1$ for some $i > 0$ and that $b_i \neq 0$ for i sufficiently large. (The first assumption covers the cases arising from [RR], [RRS] and seems more tractable than the general case. The second assumption is harmless as we will see.) The seminormalization ${}^+_B A$ and weak normalization ${}^*_B A$ of A in B are both monomial subrings of B. We describe in Theorem 3.3 and Theorem 4.2 the coefficient sequences of ${}^+_B A$ and ${}^*_B A$ in terms of the stabilization sequence (Definition 2.5) of A, and characterize (Theorems 3.5 and 4.2) those coefficient sequences that arise from seminormal and weakly normal monomial subrings of B.

In Section 5 we discuss how monomial subrings arise from systems of subintegrality [RS],[RRS] and determine in Corollary 5.5 the stabilization sequence for one of the monomial subrings of greatest interest to us. In doing this we prove in Lemma 5.4 a result about the greatest common divisor of binomial coefficients where the "numerator" is in a certain arithmetic progression. This appears to be not well known, and of independent interest.

A reference for weak subintegrality is [Y], and seminormality is discussed in [S]. We also will make use of systems of subintegrality, which were introduced in [RS], [RRS]. These concepts will be reviewed briefly when needed.

Throughout, $\mathbb{Z}^+$ denotes the non-negative integers, and $\mathbb{N}$ the positive integers.

2. MONOMIAL SUBRINGS OF $\mathbb{Z}[t]$.

Let A be a monomial subring of $\mathbb{Z}[t]$ with coefficient sequence $\{b_i\}_{i \geq 0}$. Clearly $b_0 = 1$ and b_i divides $\mathrm{GCD}(b_j b_{i-j} \mid 0 < j < i)$. In general A need not be a finitely

1991 *Mathematics Subject Classification.* Primary: 13B22; Secondary: 19A49.

This work was supported by the NSERC grant of the second author. The first author thanks Queen's University for its hospitality. The authors also thank Keith Pardue for helpful suggestions.

generated $\mathbb{Z}$-algebra. For example if $b_i = 2$ for $i \geq 1$ then A requires all the algebra generators $\{2t^i\}_{i\geq 1}$.

Note that if $b_i \neq 0$ and $b_j \neq 0$ then $b_{i+j} \neq 0$ (as can be seen by multiplying $b_i t^i$ by $b_j t^j$), i.e. $\{i | b_i \neq 0\}$ is a submonoid of $\mathbb{N}$. From this it follows there is a smallest positive integer ϵ such that, for all i, $b_i \neq 0$ only if i is a multiple of ϵ and, if i is sufficiently large, then $b_i \neq 0$ if and only if i is a multiple of ϵ (of course we are not interested in the trivial case $A = \mathbb{Z}$). We have $A \subseteq \mathbb{Z}[t^\epsilon]$ and since ${}^{+}_{\mathbb{Z}[t]}\mathbb{Z}[t^\epsilon] = {}^{*}_{\mathbb{Z}[t]}\mathbb{Z}[t^\epsilon] = \mathbb{Z}[t^\epsilon]$ we have ${}^{+}_{\mathbb{Z}[t]}A = {}^{+}_{\mathbb{Z}[t^\epsilon]}A$ and ${}^{*}_{\mathbb{Z}[t]}A = {}^{*}_{\mathbb{Z}[t^\epsilon]}A$. Furthermore if we define A' as the monomial subring of $\mathbb{Z}[u]$ with coefficient sequence $\{1, b_\epsilon, b_{2\epsilon}, \ldots, \}$ then the map $u \to t^\epsilon$ defines an isomorphism $A' \cong A$. Thus there is no loss of generality if we assume

$$b_i \neq 0 \text{ for all sufficiently large } i. \tag{2.1}$$

In general for any integers $c_i \geq 0$ $(i \geq 1)$ the condition that $\mathbb{Z} \oplus (\oplus_{i\geq 1} \mathbb{Z} c_i t^i)$ be a ring is that the product of two basis elements be in the abelian group, i.e. that

$$c_{i+j} \mid c_i c_j. \tag{2.2}$$

(In such considerations all integers divide zero.)

Usually we will assume that

$$b_i = 1 \text{ for some } i > 0. \tag{2.3}$$

It follows easily from the discussion below that A is then a finitely generated $\mathbb{Z}$-algebra. However, for a given integer i such that $b_i = 1$, the number of generators can be arbitrarily large. For example (with $i = 2$) the monomial subring A with coefficient sequence $\{1, 2^a, 1, 2^{a-1}, 1, 2^{a-2}, \ldots, 1, 2, 1, 1 \ldots\}$ requires algebra generators $\{2^a t, t^2, 2^{a-1}t^3, 2^{a-2}t^5, \ldots, 2t^{2a-1}, t^{2a+1}\}$.

Now note that $\{i | b_i = 1\}$ is a submonoid of $\mathbb{N}$. Thus if δ=GCD$(i \mid b_i = 1)$ then $b_{n\delta} = 1$ for all sufficiently large n (say for $n \geq N$) and (for any j) $b_j = 1$ implies $\delta \mid j$. Furthermore if GCD$(b_i, b_j) = 1$ then GCD$(b_i^j, b_j^i) = 1$ from which it follows that $b_{ij} = 1$. Then we have

Theorem 2.4. *Let A be a monomial subring of $\mathbb{Z}[t]$, with coefficient sequence $\{b_i\}$ satisfying* (2.1) *and* (2.3). *As above let δ=*GCD$(i \mid b_i = 1)$. *Then the sequence $\{b_i\}$ $(i >> 0)$ is periodic with period δ. (That is, there exists an integer N so that if $i \geq N$ then $b_{i+\delta} = b_i$. Furthermore δ is the smallest integer with this property).*

Proof. We are not assuming that $t^\delta \in A$. However we will have $t^{m\delta} \in A$ for sufficiently large m. Pick such an m. Then for $i \geq 0$, $k \geq 0$, we have $b_{i+(k+1)m\delta} \mid b_{i+km\delta}$ $(k \geq 0)$. The sequence $\{b_{i+km\delta}\}_{k\geq 0}$ must then stabilize as k increases, at some integer a_i (depending only on the congruence class of i mod $m\delta$) . Note that $a_0 = 1$. Suppose i and j are congruent mod δ (but not necessarily congruent mod $m\delta$). Let α be large enough that $a_i t^{i+\alpha m\delta} \in A$. For sufficiently large M, $t^{M\delta} \in A$. Further take M so that $M \equiv (j-i)/\delta$ mod m. Then $M\delta \equiv (j-i)$ mod $m\delta$ and $i + \alpha m\delta + M\delta \equiv j$ mod $m\delta$. Multiplying $a_i t^{i+\alpha m\delta}$ by $t^{M\delta}$ we conclude that $a_i t^{i+\alpha m\delta+M\delta} \in A$ and hence $a_j \mid a_i$. Similarly we obtain that $a_i \mid a_j$ proving periodicity mod δ. That δ is the smallest period follows from the definition of δ. □

Definition 2.5. Let δ be as discussed in (2.4). Then δ will be referred to as the period of A (or of $\{b_i\}$). The sequence $\{a_i\}$ obtained from $\{b_i\}$ in the proof of (2.4) will be referred to as the stabilization sequence of A (or of $\{b_i\}$).

We have that a_i depends only on the congruence class of i mod δ. Each sequence $\{b_{i+k\delta}\}_{k\geq 0}$ $(0 \leq i < \delta)$ must stabilize at value a_i . However we need not have $b_{i+(k+1)\delta} \mid b_{i+k\delta}$ (see (2.7b) below). We must of course have $a_{n\delta} = 1$ for $n \geq 0$. We claim:

Theorem 2.6. *Let $\{a_i\}_{i\geq 0}$ be the stabilization sequence of a monomial subring $A \subseteq \mathbb{Z}[t]$. Then $A' := \mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}a_i t^i)$ is a ring, which we will call the stabilization of A. (A' is thus obtained from A by extending the periodicity right back to a_0.)*

Proof. It suffices to prove that if $i + j \equiv k$ mod δ then $a_k \mid a_i a_j$ $(i, j, k \geq 0)$. Pick integers i', j' so that $i \equiv i', j \equiv j'$ mod δ and $b_r = a_r$ for all $r \geq \min(i', j')$. Let $k' = i' + j'$. The generator of the degree k' part of A is $a_k t^{k'}$. Also $a_i t^{i'} \in A, a_j t^{j'} \in A$, hence $a_i a_j t^{i'+j'} \in A$. From this it follows that $a_k \mid a_i a_j$ as we wished to show. $\square$

Note that A' is the subgroup of A generated by all monomials $M = bt^n$ such that $Mt^{i\delta} \in A$ for all sufficiently large i, (so A' can be thought of as a sort of saturation). This observation easily gives an alternate proof of (2.6). Furthermore note that the stabilization ring A' is generated as a $\mathbb{Z}$-algebra by $\{a_i t^i | 1 \leq i \leq \delta\}$.

Let $\{a_i\}_{0\leq i\leq \delta-1}$ be any set of δ integers with $a_0 = 1$ and $a_i > 1$ for $i \neq 0$, satisfying $a_k \mid a_i a_j$ whenever $i+j \equiv k$ mod δ. Extend to $\{a_i\}$ $(i \in \mathbb{N})$ by periodicity. Then $\mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}a_i t^i)$ is a ring and $\{a_i\}_{i\geq 0}$ is its own stabilization sequence. The condition $a_k \mid a_i a_j$ whenever $i + j \equiv k$ mod δ is readily satisfied, so there are lots of stabilization sequences.

Examples 2.7. (a) Let $A = \mathbb{Z}[t^3, 3t^4, 6t^5]$, with coefficient sequence 1 0 0 1 3 6 1 3 3 1 .... The stabilization of A is $\mathbb{Z}[3t, 3t^2, t^3]$ with coefficient sequence 1 3 3 1 ....

(b) $A = \mathbb{Z}[2t^4, 4t^5, 8t^6, 16t^7, t^8, 2t^9, 4t^{10}, 8t^{11}, t^{12}]$. Here $\delta = 4$ but $t^4 \notin A$. The sequence of coefficients is 1 0 0 0 2 4 8 16 1 2 4 8 1 4 8 16 1 2 4 8 1 (now repeating with periodic part 1 2 4 8). Part of the sequence of coefficients of degree congruent to 3 mod 4 is 16 8 16 8 ... illustrating the claim made in the paragraph before (2.6) that each term need not be divisible by the next in its congruence class.

Example (2.7a) is part of a more general set up that we will develop in section 5, whereas (2.7b) is just a brute force calculation.

3. The seminormalization of a monomial subring of $\mathbb{Z}[t]$.

We will first briefly recall a few facts about seminormalization. An extension $A \subseteq B$ of commutative rings is defined to be subintegral [S] if B is integral over A, the induced map Spec(B) $\rightarrow$Spec(A) is a bijection, and the induced maps on residue field extensions are isomorphisms. An element $b \in B$ is defined to be subintegral over A if the extension $A \subseteq A[b]$ is subintegral. An extension $A \subset A[b]$ with $b^2, b^3 \in A$ is subintegral. Given $A \subseteq B$ there is a largest subring ${}^+_B A$ of B such that $A \subseteq {}^+_B A$ is subintegral. The ring ${}^+_B A$ is called the seminormalization of A in B and A is defined to be seminormal in B if $A = {}^+_B A$. Furthermore A is seminormal in B if $b \in B, b^2 \in A, b^3 \in A$ implies $b \in A$.

Definition 3.1. Let a be any positive integer. Then the radical $\bar{a}$ of a is the product of the prime divisors of a ($\bar{1} = 1$).

Lemma 3.2. *Let $\{a_i\}_{i\geq 0}$ be the stabilization sequence of a monomial subring of $\mathbb{Z}[t]$ whose coefficient sequence satisfies* (2.1) *and* (2.3), *with period δ. Then $\bar{A} = \mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}\bar{a}_i t^i)$ is a ring which is seminormal in $\mathbb{Z}[t]$.*

Proof. If $a_k \mid a_i a_j$ whenever $i + j \equiv k \pmod{\delta}$ then $(\bar{a}_k) \mid \bar{a}_i \bar{a}_j$ so $\mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}\bar{a}_i t^i)$ is a ring. To show seminormality it suffices to show that if $(at^i)^2, (at^i)^3 \in \bar{A}$ then $at^i \in \bar{A}$ [LV, 2.4]. This is equivalent to showing that if $\bar{a}_{2i} \mid a^2$ and $\bar{a}_{3i} \mid a^3$ then $\bar{a}_i \mid a$. For $n \geq 1$ there exist α and $\beta \geq 0$ so that $1 + n\delta = 2\alpha + 3\beta$. Then $\bar{a}_i = \bar{a}_{i+ni\delta} \mid (\bar{a}_{2i})^{\alpha}(\bar{a}_{3i})^{\beta} \mid a^{1+n\delta}$, and since $\bar{a}_i$ has no repeated prime factors, $\bar{a}_i \mid a$ as we wished to show. □

Theorem 3.3. *Let $A = \mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}b_i t^i)$ be a monomial subring of $\mathbb{Z}[t]$ with coefficient sequence satisfying* (2.1), (2.3), *with period δ and stabilization $A' = \mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}a_i t^i)$. Then the seminormalization of A in $\mathbb{Z}[t]$ is the ring $\bar{A} = \oplus_{i\geq 0}\mathbb{Z}(\bar{a}_i)t^i$.*

Proof. By (3.2), $\bar{A}$ is a ring which is seminormal in $\mathbb{Z}[t]$. It suffices to show that $\bar{A}$ is subintegral over A, and to do this it suffices to show that for all $i, (\bar{a}_i t^i)^n \in A$ for n sufficiently large (a priori n could depend on i). If n is sufficiently large then $b_{ni} = a_{ni}$ so any prime dividing b_{ni} has to divide a_i^n and hence also $\bar{a}_i$. Because the sequence a_j is periodic there are only finitely many distinct a_{ni}. Let N be the highest power to which any prime divides the a_{ni}. Then $b_{ni} \mid (\bar{a}_i)^n$ hence $(\bar{a}_i t^i)^n \in A$ if $n \geq N$ and n is large enough so that $b_{ni} = a_{ni}$. □

Example 3.4. Let A be as in (2.7b). Then the seminormalization of A has coefficient sequence 1 2 2 2 1 2 2 2 1 ... with period 4.

The condition (2.2) can be checked at each prime q. From this we easily obtain

Theorem 3.5. *The coefficient sequences of monomial seminormal subrings of $\mathbb{Z}[t]$ whose coefficient sequence satisfies* (2.1), (2.3) *are exactly the sequences that are the co-ordinatewise product of sequences of the form $1\ q\ q\ q\ \ldots\ q\ 1 \ldots$ of period a divisor δ_q of δ, q ranging over a finite set of distinct primes, with the* LCM *of the periods being δ.*

We will refer to δ_q as the period of q in the coefficient sequence.

Examples 3.6. (a) Consider the coefficient sequence 1 6 3 2 3 6 1 .... Then this is the co-ordinatewise product of the sequences 1 2 1 2 1 2 1 ... of period 2 and the sequence 1 3 3 1 3 3 1 ... of period 3.

(b) Consider the coefficient sequence 1 6 2 3 2 6 1 ... (repeating with period 6). This is the product of the sequences 1 2 2 1 2 2 1 ... (of period 3) and the sequence 1 3 1 3 1 3 1 ... (of period 2).

4. The weak normalization of a monomial subring of $\mathbb{Z}[t]$.

In this section we determine the weak normalization of a monomial subring of $\mathbb{Z}[t]$. First let us recall a few basic facts about weak normalization. An extension $A \subseteq B$ of commutative rings is defined to be weakly subintegral [Y] if B is integral over A, the induced map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a bijection, and the induced maps on residue field extensions are purely inseparable. An element $b \in B$ is defined to be weakly subintegral over A if the extension $A \subseteq A[b]$ is weakly subintegral [RRS 1.1.2]. A subintegral extension is weakly subintegral, and the extension $A \subseteq A[b]$ is weakly subintegral if $b^q \in A$ and $qb \in A$ (q a prime integer). Given $A \subseteq B$ there is a largest subring ${}^*_BA$ of B such that $A \subseteq {}^*_BA$ is weakly subintegral. The ring ${}^*_BA$ is called the weak normalization of A in B and A is defined to be weakly normal in B if $A = {}^*_BA$.

We can first take the seminormalization of A in $\mathbb{Z}[t]$ as in (3.3). Hence assume that $A = \mathbb{Z} \oplus (\oplus_{i\geq 1}\mathbb{Z}a_it^i)$ where the sequence $\{a_i\}_{i\geq 0}$ is periodic of period δ and the a_i are square free, satisfying (3.5).

Before tackling the weak normalization of A in $\mathbb{Z}[t]$ we need the following result:

Lemma 4.1. *Let $A \subseteq B$ be an extension of graded rings (graded by any totally ordered monoid). Then the weak normalization ${}^*_BA$ of A in B can be obtained as the filtered union of all subrings of B that can be obtained by a finite sequence of elementary subintegral and elementary weakly subintegral extensions by homogeneous elements.*

Proof. Recall from [S] that an elementary subintegral extension $R \subseteq S$ of commutative rings is an extension of the form $S = R[s]$ with $s^2, s^3 \in R$, and from [Y] that an elementary weakly subintegral extension is one of the form $S = R[s]$ where $s^q \in R$ and $qs \in R$ for some prime q.

Let A' be the union of all extensions of A in B that can be obtained by a finite sequence of extensions of the form $R \subseteq R[x]$ with x homogeneous and either $x^2, x^3 \in R$ or $x^q, qx \in R$ (q a prime). By [LV] A' is seminormal in B, and clearly A' is a graded subring of B. If A' is not equal to ${}^*_BA$ then there exists an element $s \in B$ and a prime q such that $s^q, qs \in A', s \notin A'$. We can write $s = s_1 + s_2 + \ldots + s_l$ where the s_i are non-zero homogeneous and $\deg(s_1) < \deg(s_2) < \ldots < \deg(s_l)$. Choose such an s with $l = l(s)$ as small as possible (but of course $l \geq 2$, otherwise $s \in A'$). The homogeneous pieces of s^q and qs lie in A' since A' is graded. We conclude from this that $s_1^q \in A'$ and $qs_1 \in A'$ since these are homogeneous components of s^q and qs respectively. Hence $s_1 \in A'$. Furthermore if $1 \leq i \leq q-1$ and $n \geq q-1$ then $(qs^i)^n \in A'$. Since A' is seminormal in B we have that $qs^i \in A'$ $(1 \leq i \leq q-1)$. Now let $t = s - s_1$. Then $t^q = (s-s_1)^q = s^q + \Sigma_{i=1}^{q-1}(-1)^i\binom{q}{i}s^{q-i}s_1^i + s_1^q$. We have $s^q \in A'$ by assumption and $s_1 \in A'$ by the above discussion. All the binomial coefficients $\binom{q}{i}$ are divisible by q so all factors $\binom{q}{i}s^{q-i}$ $(1 \leq i \leq q-1)$ are in A', again by the above discussion. Altogether we get $t^q \in A'$. And clearly $qt = qs - qs_1 \in A'$ also. But $l(s - s_1) = l(s) - 1$ so we must have $t \in A'$, hence $s \in A'$, contradiction. □

Theorem 4.2. *Let $\{a_i\}_{i\geq 0}$ be the coefficient sequence of a seminormal monomial subring A of $\mathbb{Z}[t]$ (whose coefficient sequence satisfies (2.1), (2.3)), decomposed as in (3.5). Then the weak normalization ${}^*_BA$ of A in $B := \mathbb{Z}[t]$ is obtained as follows: if a prime q occurs as the sequence $1\ q\ q\ q \ldots\ q\ 1 \ldots$ of period δ_q, then q occurs in the coefficient sequence of ${}^*_BA$ with period the maximal factor of δ_q relatively prime to q .*

Proof. First note that ${}^*_BA$ is a graded subring of $\mathbb{Z}[t]$ by (4.1), hence is a monomial subring of $\mathbb{Z}[t]$. Let A' be the subring of $\mathbb{Z}[t]$ constructed as in the statement of the Theorem. We first show that A' can be obtained from A by elementary weakly subintegral extensions (hence that $A' \subseteq {}^*_BA$). Let q be a prime that divides some a_i and suppose that q has period δ_q in the decomposition of (3.5). If q does not divide δ_q there is nothing to show. Hence suppose that $\delta_q = q^b c$ where q does not divide c and $b > 0$ (c could be 1). Then $a_{q^{b-1}c} = qr$ where q does not divide r. Consider $x = rt^{q^{b-1}c}$. We have $x^q \in A$ and $qx \in A$. Hence $A \subseteq A[x]$ is an elementary weakly subintegral extension. Repeating the process we conclude that $st^c \in A'$ where $a_c = sq$. The prime q now has period c, as claimed. Now let A be a monomial subring of $\mathbb{Z}[t]$ as in (3.5), with each δ_q relatively prime to q. In order to complete the proof it suffices to show that A is weakly normal in $\mathbb{Z}[t]$. Suppose not. Then since A is seminormal, by (4.1) there must be some prime q and monomial at^b such that $at^b \notin A$ but $(at^b)^q \in A$ and $qat^b \in A$. Since $at^b \notin A$ but $qat^b \in A$ we must have that b is not a multiple of δ_q and q does not divide a. But then bq is not a multiple of δ_q either since δ_q is relatively prime to q. Since $(at^b)^q \in A$ we must then we have $q \mid a^q$ which is a contradiction. $\square$

Examples 4.3. (a) In (3.6a) the coefficient sequence 1 2 1 2 1 ... has period 2 and the maximal factor of 2 relatively prime to 2 is 1, so by (4.2) the corresponding component of the weak normalization has coefficient sequence 1 1 1 1 .... Similarly the sequence 1 3 3 1 ... has weak normalization with coefficient sequence 1 1 1 1 .... Therefore the weak normalization of $\mathbb{Z}[6t, 3t^2, 2t^3, 3t^4, 6t^5, t^6]$ in $\mathbb{Z}[t]$ is $\mathbb{Z}[t]$. Note that this is also immediate from [RR, 2.2] (taking $N = 1$ in the remark in the first sentence of the proof).

(b) In (3.6b) the coefficient sequence 1 2 2 1 2 2 1 ... has period 3 and the maximal factor of 3 relatively prime to 2 is 3, so by (4.2) the corresponding component of the weak normalization has coefficient sequence 1 2 2 1 2 2 1 .... Combining this with a similar argument for the sequence 1 3 1 3 ... shows that $\mathbb{Z}[6t, 2t^2, 3t^3, 2t^4, 6t^5, t^6]$ is weakly normal in $\mathbb{Z}[t]$.

5. Systems of subintegrality.

In [RRS] we gave the following elementwise characterization of weak subintegrality: Let $A \subseteq B$ be an extension of commutative rings. Then $b \in B$ is weakly subintegral over A if and only if the following condition holds:

(5.1) There exist $p \in \mathbb{Z}^+$, elements $c_1, \dots, c_p \in B$, and $N \in \mathbb{N}$ such that $b^k + \sum_{i=1}^{p} \binom{k}{i} c_i b^{k-i} \in A$ for $k \in \mathbb{N}, k \geq N$.

In [RS(section 4), RR] we called the tuple $(p, N, c_0, \dots, c_p)$ (with $c_0 = 1$) such that (5.1) is satisfied a system of subintegrality for b over A, SOSI for short. (Note that p, the c_i and N are all part of the data. For example replacing N by a larger integer changes the SOSI. [RS] had another parameter s which we take to be 0 here). An element $x \in B$ such that $x^k + \sum_{i=1}^{p} \binom{k}{i} c_i x^{k-i} \in A$ for $k \in \mathbb{N}$, $k \geq N$ will be said to satisfy the SOSI $(p, N, c_0, \dots, c_p)$. It was also proved in [RRS] that if b has a SOSI for some N, then b has a SOSI with $N = 1$ (but usually with larger p). If $N = 1$ we have the following description of a SOSI: on $B[[T]]$ define a "multiplication" * by setting $T^r * T^s = \binom{r+s}{s} T^{r+s}$, and then extending by bilinearity and completion to $f * g$ for all $f, g \in B[[T]]$ and let $\mathrm{Exp}(b) \in B[[T]]$ be defined by $\mathrm{Exp}(b) = \sum_{i \geq 0} b^i T^i$. By multiplying and comparing the coefficients of T^i we have that $\mathrm{Exp}(b) * (1 + c_1 T + c_2 T^2 + \dots c_p T^p) \in A[[T]]$ if and only if $(p, 1, c_0, \dots, c_p)$ is a SOSI satisfied by b [RRS,(3.3)]. If $N > 1$ we do not have such a conceptual alternative description of a SOSI.

We now examine the passage to $N = 1$ for one of the simplest SOSI's. Suppose that $b^i \in A$ for $i \geq n$, i.e. b satisfies the SOSI $(0, n, 1)$. We have $\mathrm{Exp}(-b) * \mathrm{Exp}(b) = 1$.

If we take only the terms up to b^{n-1} in $\mathrm{Exp}(-b)$, that is, take $g(T) = \sum_{i=0}^{n-1}(-b)^i T^i \in B[T]$, then $g(T)*\mathrm{Exp}(b)$ has all coefficients in A since only powers b^i for $i \geq n$ remain. More explicitly:

(5.2) The coefficient of T^d in $g(T)*\mathrm{Exp}(b)$ is equal to 0 for $1 \leq d \leq n-1$ and to $(-1)^{n-1}\binom{d-1}{n-1}b^d$ for $d \geq n$.

This follows from the identity $\Sigma_{i=0}^{n-1}\binom{d}{i}(-1)^i = (-1)^{n-1}\binom{d-1}{n-1}$, which is easily proved by induction on n. As in [RRS, section 3] we now have $(n-1, 1, \{(-b)^i \mid 1 \leq i \leq n-1\})$ (i.e. $c_i = (-b)^i, 1 \leq i \leq n-1$) is a SOSI for b over A if and only if $\binom{d-1}{n-1}b^d \in A$ for $d \geq n$. (Note that $n-1$ here plays the role of p in (5.1)). If $\mathbb{Q} \subseteq A$ satisfying the SOSI $(n-1, 1, \{(-b)^i\}_{1 \leq i \leq n-1})$ is equivalent to $b^d \in A$ for $d \geq n$, but if we do not assume that $\mathbb{Q} \subseteq A$ the situation is more interesting. First of all by [RRS 2.2], in order for b to satisfy the SOSI $(n-1, 1, \{(-b)^i\}_{1 \leq i \leq n-1})$ it suffices to have $\binom{d-1}{n-1}b^d \in A$ for $n \leq d \leq 2n-1$. More elements might satisfy the condition $\binom{d-1}{n-1}b^d \in A$ for $n \leq d \leq 2n-1$ than satisfy $b^d \in A$ for $n \leq d \leq 2n-1$. Thus we have lost information in passing from $N = n$ to $N = 1$ in our SOSI. However we could have used $n + i$ $(1 \leq i \leq n-1)$ instead of n. This will give us $n-1$ more SOSI's which respectively imply that $b^d \in A,\ n+1 \leq d \leq 2n-1$. All together these n SOSI's imply that $b^d \in A,\ n \leq d \leq 2n-1$, (and hence $b^d \in A$ for $d \geq n$) so n SOSI's with $N = 1$ are equivalent to the original SOSI $b^d \in A$ for $d \geq n$.

The above discussion leads us to consider the monomial subring $R = \mathbb{Z}[\{\binom{d-1}{n-1}t^d\}_{n \leq d \leq 2n-1}]$ of $\mathbb{Z}[t]$, which can be thought of as a universal example. It is clear that $\binom{d-1}{n-1}t^d \in R$ for $n \leq d \leq 2n-1$ but $t^d \notin R,\ n < d \leq 2n-1$. We do not know the coefficient sequence for R in general, but we are able to find the stabilization of R.

To help us get oriented let us consider a few examples:

Examples 5.3. (a) $(n = 3)$. Then $R = \mathbb{Z}[t^3, 3t^4, 6t^5, 10t^6, 15t^7, 21t^8, \ldots]$ which has coefficient sequence 1 0 0 1 3 6 1 3 3 1 .... Thus $R = \mathbb{Z}[t^3, 3t^4, 6t^5]$, so we have the example of (2.7a). The last equality is predicted by [RRS, 2.2]. By construction, t is weakly subintegral over R. The weak subintegrality of t over R also follows from [RR, (2.2)] with $a = 3, r_1 = 4, r_2 = 8$.

(b) $(n = 4)$. Then $R = \mathbb{Z}[t^4, 4t^5, 10t^6, 20t^7]$. Here R has coefficient sequence 1 0 0 0 1 4 10 20 1 4 2 20 1 4 2 4 1 ... with the pattern now repeating (the last 1 corresponding to t^{16}). Here the weak subintegrality of t over R also follows from [RR, (2.2)] with $a = 4, r_1 = 9, r_2 = 10, r_3 = 15$.

Now we claim the following:

Lemma 5.4. *Let $N \geq n$. Then* $\mathrm{GCD}(\binom{d-1}{n-1} \mid d \equiv i \bmod n, d \geq N) = \frac{n}{\mathrm{GCD}(n,i)}$.

Before proving (5.4) we will examine its consequences for the structure of the ring $R = \mathbb{Z}[\{\binom{d-1}{n-1}t^d\}_{n \leq d \leq 2n-1}]$ described above. Setting $d = n$ we obtain that $t^n \in R$, so R contains the products $\binom{d-1}{n-1}t^d, t^n \cdot \binom{d-1-n}{n-1}t^{d-n}, t^{2n} \cdot \binom{d-1-2n}{n-1}t^{d-2n}, \ldots,$ $t^{in} \cdot \binom{d-1-in}{n-1}t^{d-in} \ldots$ (continuing so long as $d - in \geq n$). From (5.4) we conclude that if d is sufficiently large in the congruence class of i mod n, then $e_d \mid \frac{n}{\mathrm{GCD}(n,d)}$ where as above e_d is the smallest positive integer such that $e_d t^d \in R$ $(d \geq n)$.

Sublemma 5.4.1. *If $\ell + m = d$ then* $\frac{n}{\mathrm{GCD}(n,d)} \mid \frac{n}{\mathrm{GCD}(n,\ell)} \cdot \frac{n}{\mathrm{GCD}(n,m)}$.

Proof of (5.4.1). The assertion of (5.4.1) is equivalent to $\frac{n}{\mathrm{GCD}(n,\ell)} \cdot \frac{\mathrm{GCD}(n,d)}{\mathrm{GCD}(n,m)} \in \mathbb{Z}$. We show this as follows: Let $v_q(d)$ be the $q-$adic valuation of d, i.e. the highest power to which the prime q divides an integer d in $\mathbb{Z}$ (then extend to $\mathbb{Q}$ in the obvious way). Suppose that $v_q(\ell) = a,\ v_q(m) = b,\ v_q(n) = c$. Without loss of generality it suffices to consider three cases: (i) $a \leq b \leq c$. Then $v_q(\mathrm{GCD}(n,\ell)) = a,\ v_q(\mathrm{GCD}(n,m)) = b,\ v_q(\mathrm{GCD}(n,d)) \geq a$, and $v_q(n) = c \geq b$, so $v_q(\frac{n}{\mathrm{GCD}(n,\ell)} \cdot \frac{\mathrm{GCD}(n,d)}{\mathrm{GCD}(n,m)}) \geq 0$. (ii) $a \leq c < b$. Then $v_q(\mathrm{GCD}(n,\ell)) = a, v_q(\mathrm{GCD}(n,m)) = c, v_q(n) = c$ and $v_q(\mathrm{GCD}(n,d)) \geq a$ so again $v_q(\frac{n}{\mathrm{GCD}(n,\ell)} \cdot \frac{\mathrm{GCD}(n,d)}{\mathrm{GCD}(n,m)}) \geq 0$. (iii) $c < a \leq b$. Then $v_q(\mathrm{GCD}(n,\ell)) = v_q(\mathrm{GCD}(n,m)) = v_q(\mathrm{GCD}(n,d)) = c$ so again $v_q(\frac{n}{\mathrm{GCD}(n,\ell)} \cdot \frac{\mathrm{GCD}(n,d)}{\mathrm{GCD}(n,m)}) \geq 0$ (in fact the last case is an equality). $\square$.

Now let $a_j := \frac{n}{\mathrm{GCD}(n,j)},\ j \geq 1$. By (5.4.1), $G := \mathbb{Z} \oplus (\oplus_{j\geq 1} a_j \mathbb{Z} t^j)$ is a ring. By (5.4), $a_j \mid \binom{j-1}{n-1}$ $(j \geq n)$ so G contains the algebra generators of R, which implies that $R_d \subseteq G_d$ for all d. But by the argument before (5.4.1) we saw that (5.4) implies that $G_d \subseteq R_d$ in sufficiently high degree d. Thus we have:

Corollary 5.5. *Let $R = \mathbb{Z}[\{\binom{j-1}{n-1} t^j\}_{n \leq j \leq 2n-1}]$. If d is sufficiently large then the smallest non-zero positive integer e_d such that $e_d t^d \in R$ is $\frac{n}{\mathrm{GCD}(n,d)}$. That is, the stabilization sequence of R is $\{\frac{n}{\mathrm{GCD}(n,d)}\}_{d \geq 1}$. In all cases $\frac{n}{\mathrm{GCD}(n,d)}$ divides e_d.*

Now we prove (5.4). (There is no loss of generality if we assume that $1 \leq i \leq n$):

Let q be any prime, and $v_q(i) = r,\ v_q(n) = s$ and $d \equiv i \bmod n$. We have $\binom{d-1}{n-1} = \binom{d}{n}\frac{n}{d}$ so $v_q\binom{d-1}{n-1} \geq v_q(\frac{n}{d}) = s - v_q(d)$ and of course $v_q\binom{d-1}{n-1} \geq 0$ so $v_q\binom{d-1}{n-1} \geq \max(0, s - v_q(d)) = v_q(\frac{n}{\mathrm{GCD}(n,d)}) = v_q(\frac{n}{\mathrm{GCD}(n,i)})$. It now follows that $\frac{n}{\mathrm{GCD}(n,i)} \mid \binom{d-1}{n-1}$. The proof will be complete if we show (a) if $s > r$ (in which case $v_q(d) = v_q(i)$ and $v_q(\frac{n}{\mathrm{GCD}(n,i)}) = s - r$) there is a $d \equiv i \bmod n$ (say $d = i + \lambda n$) such that $q \nmid \binom{d}{n}$ (so that $v_q\binom{d-1}{n-1} = v_q(\frac{n}{d}) = s - r = v_q(\frac{n}{\mathrm{GCD}(n,i)})$) and (b) if $s \leq r$ (in which case $v_q(\frac{n}{\mathrm{GCD}(n,i)}) = 0$) then there is a $d \equiv i \bmod n$ (again write $d = i + \lambda n$) such that $q \nmid \binom{d-1}{n-1}$. We prove (a) and (b) as follows:

(a) The case $s > r$: Let the base q expansions of i and n be $i = a_r q^r + \ldots + a_{r'} q^{r'}$ and $n = b_s q^s + \ldots + b_{s'} q^{s'}$, $r < \ldots < r'$, $s < \ldots < s'$, a_r and $b_s \neq 0$. By Gauss' Lemma (Proposition 15.21 of [E]) it suffices to choose λ so that all the coefficients in the base q expansion of $i + \lambda n$ are greater than or equal to the corresponding coefficients in $b_s q^s + \ldots + b_{s'} q^{s'}$. If $s > r'$ we can take $\lambda = 1$. Otherwise write $i = a_r q^r + \ldots a_{s-1} q^{s-1} + q^s v$ $(v \in \mathbb{N})$. We have that $n = q^s u$ where u is a unit mod q^e for any $e \in \mathbb{N}$. Thus we can choose λ so that $v + \lambda u \equiv u \bmod q^{s'-s+1}$. Then the base q expansion of $d = i + \lambda n$ agrees with that of n in the range $q^s, \ldots, q^{s'}$ so by Gauss' Lemma we have that $q \nmid \binom{d}{n}$ as desired.

(b) The case $r \geq s$: Again let the base q expansions of i and n be $i = a_r q^r + \ldots a_{r'} q^{r'}$ and $n = b_s q^s + \ldots + b_{s'} q^{s'}$, a_r and $b_s \neq 0, s \leq r$. We require the base q expansions of $d - 1 = -1 + i + \lambda n$ and $n - 1 = -1 + b_s q^s + \ldots + b_{s'} q^{s'}$. Since the $q-$adic expansion of -1 starts out $(q-1) + (q-1)q + (q-1)q^2 + \ldots$, the base q expansions of $d-1$ and $n-1$ both start out $S = (q-1) + (q-1)q + (q-1)q^2 + \ldots + (q-1)q^{s-1}$ $(S = 0$ if $s = 0)$. Then $n - 1 = S + q^s(u-1)$ and $d - 1 = S + q^s(\lambda u + v - 1)$ where u is as in part (a) and we write $i = q^s v, v \in \mathbb{N}$. Since u is a unit mod any power of q we can choose $\lambda \in \mathbb{N}$ so that $\lambda u + v - 1 \equiv u - 1 \bmod q^{s'-s+1}$, so that again by Gauss' Lemma $q \nmid \binom{d-1}{n-1}$.

Noting that λ can be chosen arbitrarily large in the proofs of (a) and (b), this completes the proof of (5.4). □

Now suppose we begin the argument of (5.2) with a general SOSI having $p > 0$. That is, suppose that $a_k := b^k + \sum_{i=1}^{p} \binom{k}{i} c_i b^{k-i} \in A$ for $k \in \mathbb{N}, k \geq n$. The intuitive argument in the paragraph before (5.2) of multiplying $\mathrm{Exp}(b)$ by its inverse $\mathrm{Exp}(-b)$ does not seem to generalize easily to the case $p > 0$. Instead we can use the general technique of [RRS, section 2].

Switch to the universal extension $R \subseteq S$ where $R = \mathbb{Z}[\{\gamma_k\}_{k \geq n}] \subseteq S = \mathbb{Z}[x_1, \ldots, x_p, t]$ and $\gamma_k := t^k + \Sigma_{j=1}^{p} \binom{k}{j} x_j t^{k-j}$. If we map S to B by sending t to b and x_i to c_i then γ_k maps to $a_k \in A$ so we recover our system of subintegrality for b over A. Let $F(U,t) = 1 + \Sigma_{j=1}^{p} \binom{U}{j} x_j t^{-j}$, so that $\gamma_k = t^k F(k,t)$. In order to form a SOSI with $N = 1$ we can multiply F by an integer valued polynomial $h(U)$ such that $h(0) = 1, h(i) = 0$ $(1 \leq i \leq n-1)$. The simplest such h is $h(U) = (-1)^{n-1}\binom{U-1}{n-1}$ (which as noted after (5.2) is also equal to $\Sigma_{i=0}^{n-1}(-1)^i\binom{U}{i}$). Now let $G(U,t) = h(U)F(U,t)$ and define a SOSI by taking $\gamma'_k = t^k G(k,t)$ (which is possible by the discussion of [RRS section 2]). By the definition we see that $\gamma'_k = (-1)^{n-1}\binom{k-1}{n-1}\gamma_k$. In particular $\gamma'_n = (-1)^{n-1}\gamma_n$ and $\gamma'_k = 0$ for $1 \leq k \leq n-1$. But if $k > n$ then γ'_k is a multiple of γ_k by an integer greater than 1 in absolute value. Thus again we have that (potentially) more elements of B satisfy the system of subintegrality given by the γ'_k than by the γ_k. If $p = 0$ we recover the system of subintegrality discussed after (5.2), as is seen by writing $h(U) = F(U,t)$ in the form $\Sigma_{i=0}^{n-1}(-1)^i t^i \binom{U}{i} t^{-i}$.

By [RRS 1.2.*] we need only have $a_k \in A$ for $n \leq k \leq 2n + 2p - 1$ so if we consider the $n + 2p$ systems of subintegrality obtained as above by taking polynomials $h_i(U) = (-1)^{n-2+i}\binom{U-1}{n-2+i}$, $1 \leq i \leq n + 2p$ ($i = 1$ being the h considered above) then (because $h_i(n-1+i) = (-1)^{n-2+i}$) we have that the elements of B that satisfy the original system of subintegrality are the same as those that satisfy the $n + 2p$ systems of subintegrality in which N has become 1.

The above three paragraphs and the discussion after (5.2) suggest that if b is subintegral over A then there might be a finite collection of polynomials $g_i \in B[T]$ such that $g_i(0) = 1$ and $\mathrm{Exp}(b) * g_i \in A[[T]]$ for all i, such that any element $b' \in B$, with $\mathrm{Exp}(b') * g_i \in A[[T]]$ for all i is also subintegral over A. However we do not know any examples of such collections except those arising from the discussion after (5.2).

6. A more complicated example.

In this section we strengthen the result in (5.5):

Theorem 6.1. *Let $N \geq n$. Then $R_N := \mathbb{Z}[\{\binom{d-1}{n-1}t^d\}_{d \geq N}]$ has the same stabilization sequence $\{n/\mathrm{GCD}(n,d)\}_{d \geq 0}$ as was obtained in* (5.5) *for $N = n$.*

Proof. Observe that if $N = n$ then the coefficient $\binom{n-1}{n-1}$ of t^n is one. Thus the period of $\mathbb{Z}[\{\binom{d-1}{n-1}t^d\}_{d \geq n}]$ is a divisor of n, and in fact is exactly n by (5.5). Since $R_N \subseteq R_n$ the period for R_N must be a multiple of n (provided that $t^i \in R_N$ for some i, so that R_N in fact does have a period). First we show that $t^{in} \in \mathbb{Z}[\{\binom{d-1}{n-1}t^d\}_{d \geq N}]$ for all sufficiently large i. Recall the following property of integer-valued polynomials [CC, Chapter 1, Exercise 3 (page 19)].

(6.2) Let $f(X) \in \mathbb{Q}[X]$ be an integer valued polynomial of degree p and $a \in \mathbb{Z}$. Then $\mathrm{GCD}(f(k) \mid k \in \mathbb{Z}) = \mathrm{GCD}(f(k) \mid a \leq k \leq a+p)$.

We apply this to the polynomials $g_\lambda(k) = \binom{n-1+\lambda k}{n-1}$ (for various values of $\lambda > 0$). Here $p = n-1$ and $g_\lambda(0) = 1$, so we have by (6.2) that $\mathrm{GCD}(\binom{n-1+\lambda k}{n-1} \mid 1 \leq k \leq n) = 1$. Now we consider only values of λ so that $n-1+\lambda \geq N$. Then $\binom{n-1+\lambda k}{n-1} t^{n+\lambda k} \in R_N$, $1 \leq k \leq n$, and since $\mathrm{GCD}(\binom{n-1+\lambda k}{n-1} \mid a \leq k \leq a+n-1) = 1$ we have $t^{M_\lambda} \in R_N$ for M_λ=LCM$(\{n+\lambda k\}_{a \leq k \leq a+n-1})$. It now suffices to show that the GCD of the M_λ obtained for various values of λ is n. We know that $n \mid M_\lambda$ for all λ since the period of R_N must be a multiple of n. Furthermore any one M_λ contains only a finite number of prime divisors. Thus it suffices to show that for any prime q there exists sufficiently large λ so that $v_q(n) = v_q(M_\lambda)$. Simply take $\lambda = q^i$ for $i > v_q(n)$, i sufficiently large so that $n-1+\lambda \geq N$. We now have that $t^{jn} \in R_N$ for all sufficiently large j, say $j \geq S$. By multiplying $\binom{i-1}{n-1}t^i$, $\binom{i+n-1}{n-1}t^{i+n}, \ldots, \binom{i+(n-1)n-1}{n-1}t^{i+(n-1)n}$ $(i \geq N)$ by suitable powers t^{jn} we obtain that $\binom{i-1}{n-1}t^d, \binom{i+n-1}{n-1}t^d, \ldots, \binom{i+(n-1)n-1}{n-1}t^d \in R_N$, d any sufficiently large integer congruent to i mod n. By (6.2) and (5.4) we conclude that R_N has the desired stabilization sequence. $\square$

As a consequence of (6.1) R_n and R_N have the same seminormalization in $\mathbb{Z}[t]$ (hence they have the same weak normalization, which is $\mathbb{Z}[t]$ by (4.2)). This does not hold in general for systems of subintegrality. For example consider the generic example $A_N = \mathbb{Z}[\{\gamma_n\}_{n \geq N}]$ with $p = 1, \gamma_n = t^n + nx_1t^{n-1}$. We have $x_1^2 \in A_1$ but x_1 is not even integral over A_2, so A_1 and A_2 do not have the same seminormalization in $\mathbb{Z}[x_1, t]$ (although both have the same quotient field as $\mathbb{Z}[x_1, t]$).

References

[CC] P.-J.Cahen and J.-L.Chabert, Integer-Valued Polynomials, American Math. Society, Providence, 1997.

[E] D.Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995.

[LV] J.Leahy and M.Vitulli, Seminormal graded rings and weakly normal projective varieties, Internat.J. Math. Math.Sci. 8(1985)231-240.

[RR] L.Reid and L.G.Roberts, A new criterion for weak subintegrality, Comm.Alg.24(10)3335-3342(1996).

[RS] L.G.Roberts and B.Singh, Subintegrality, invertible modules and the Picard Group, Compositio Math.85 (1993)249-279.

[RRS] L.Reid, L.G.Roberts, and B.Singh, On weak subintegrality. J.P.A.A. 114(1996)93-109.

[S] R.G.Swan, On seminormality, J.Alg.67(1980)210-229.

[Y] H.Yanagihara, On an intrinsic definition of weakly normal rings, Kobe J.Math. 2(1985)89-98.

Department of Mathematics, Southwest Missouri State University, Springfield, Missouri, 65804

E-mail address: `les@math.smsu.edu`

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada, K7L 3N6

E-mail address: `robertsl@mast.queensu.ca`