ALGEBRAIC COMBINATORICS

Syed Waqar Ali Shah

Smith normal form of matrices associated with differential posets

Volume 7, issue 6 (2024), p. 1887-1899.

https://doi.org/10.5802/alco.393

© The author(s), 2024.

This article is licensed under the
CREATIVE COMMONS ATTRIBUTION (CC-BY) 4.0 LICENSE.
http://creativecommons.org/licenses/by/4.0/

Algebraic Combinatorics is published by The Combinatorics Consortium
and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 7, issue 6 (2024), p. 1887–1899
https://doi.org/10.5802/alco.393

Smith normal form of matrices associated with differential posets

Syed Waqar Ali Shah

Abstract We prove a conjecture of Miller and Reiner on the existence of Smith normal form for the DU-operators for a certain class of r-differential posets.

1. Introduction

Let r be a positive integer. We say that a partially ordered set (poset) P is r-*differential*, if it satisfies the following three conditions:

(D1) P is graded, locally finite, has all ranks finite and possesses a unique minimal element.
(D2) If two distinct elements of P have exactly k elements that are covered by both of them, then there are exactly k elements that cover them both.
(D3) If an element of P covers exactly k elements, then it is covered by exactly $k + r$ elements.

Associated to every r-differential poset are two families of maps, known as *up* and *down* maps. Let P_n be the n-th rank of P, which we take to be the empty set if $n < 0$, and set $p_n := |P_n|$. For any commutative ring R with identity and characteristic 0, let $RP_n \cong R^{p_n}$ be the free module over R with basis P_n. We define

$$U_n : RP_n \to RP_{n+1}$$
$$D_n : RP_n \to RP_{n-1}$$

for all $n \geqslant 0$ on basis elements as follows: U_n sends $x \in P_n$ to the sum (with coefficients 1) of all elements in P_{n+1} that cover x and D_n sends x to the sum of all the elements in P_{n-1} that are covered by x. We then define

$$UD_n := U_{n-1} \circ D_n$$
$$DU_n := D_{n+1} \circ U_n$$

The two conditions (D2) and (D3) can then be recast as

$$DU_n - UD_n = r \cdot \mathbb{1}.$$

The most well-known examples of 1-differential posets are the Young's lattice $\mathbf{Y}$ and Young-Fibonacci lattice $\mathbf{Y}F$. Their r-fold cartesian products are examples of r-differential posets. Another important example of an r-differential poset is the r-Fibonacci poset $Z(r)$ where $Z(1) = \mathbf{Y}F$.

Manuscript received 3rd June 2024, revised 15th July 2024, accepted 22nd July 2024.

Keywords. differential poset, Smith normal form, canonical forms, invariant factor decomposition.

Differential posets were first defined by Stanley in [5] with up and down maps defined over fields. Later, Miller and Reiner defined them over arbitrary rings in [3] and conjectured a remarkable property of the DU_n-operators over the ring of integers which we now describe. Recall that an $m\times n$ matrix $A=(a_{ij})$ over an integral domain R is said to have *Smith normal form* (SNF) over R if there exist invertible matrices $P\in R^{m\times m}$, $Q\in R^{n\times n}$ such that $B=PAQ$ is a diagonal matrix in the sense that $b_{ij}=0$ if $i\neq j$, and $s_i:=b_{ii}$ for $1\leqslant i\leqslant k=\min\{m,n\}$ satisfy the divisibilities

$$s_1|s_2|\dots|s_k.$$

It is known that if R is a PID, any matrix A always has SNF which is unique in the sense that the diagonal entries s_i are unique up to units of R. If R is not a PID, such a form does not necessarily exist. If it does exist however, it is still unique.

Assume now that $R=\mathbb{Z}$. Let $[DU_n]$ be the matrix of DU_n with respect to the standard basis of $\mathbb{Z}P_n$ and I_{p_n} be the $p_n\times p_n$ identity matrix.

Conjecture 1.1. [3, Miller-Reiner] *For all n, the matrix $[DU_n]+xI_{p_n}$ has SNF over $\mathbb{Z}[x]$.*

Miller and Reiner verified this conjecture for the r-Fibonacci poset $Z(r)$ in [3]. The problem was later investigated by Cai and Stanley in [1] for the case $\mathbf{Y}^r$ and the case $r=1$ was settled in the affirmative. As noted in the survey [6], the case $r>1$ was later handled by Zipei Nie, though a written proof has not yet appeared.

In this paper, we prove this conjecture for any r-differential poset that satisfies certain conditions which are stated in Theorem 5.3. These conditions are closely related to two additional conjectures (Conjectures 2.3 and 2.4 of [3]) made by Miller and Reiner. Our strategy is to study the $\mathbb{Z}[x]$-module structure of $\mathbb{Z}P_n$ where the action of x is induced by the operator DU_n. The statement on the Smith normal form of $[DU_n]+xI_{p_n}$ is then easily translated into a statement on the existence of *integral canonical form* for DU_n which is an integral analogue of the rational canonical form. This allows us to relate the structure of DU_n and DU_{n+1} which paves the way for an induction argument.

2. Recollections

We start with a theorem of Stanley.

Theorem 2.1. [5, §4] *Let P be an r-differential poset and R a field of characteristic 0. Then*

$$\mathrm{Ch}(DU_n)=\prod_{j=0}^{n}(x-rj-r)^{\Delta p_{n-j}}$$

$$\mathrm{Ch}(UD_n)=\prod_{j=0}^{n}(x-rj)^{\Delta p_{n-j}}$$

where $\mathrm{Ch}(A)=\mathrm{Ch}(A,x)$ denotes the characteristic polynomial of the operator A, and $\Delta p_n:=p_n-p_{n-1}$ denotes the rank difference. Furthermore, the operators DU_n and UD_n are diagonalizable.

We make some immediate conclusions. First, the rank function is non-decreasing as Δp_n must be non-negative in the expressions above. Second, DU_n is invertible as all its eigenvalues are non-zero. Thus U_n is injective and D_{n+1} is surjective for all $n\geqslant 0$. Third, the sequence of invariant factors of the torsion $R[x]$-module RP_n where x acts via DU_n is uniquely determined by $\mathrm{Ch}(DU_n)$ for each n. More precisely, there exists a decomposition

$$RP_n=M_1\oplus M_2\oplus\dots\oplus M_k$$

where $k := \max\{\Delta p_0, \dots, \Delta p_n\}$ and each M_i is a monogenic torsion $R[x]$-module with annihilator

$$a_i(x) = \prod_{\substack{j \in \{0,\dots,n\} \\ \Delta p_{n-j} \geqslant k-i+1}} (x - rj - r). \tag{1}$$

Note that $a_1(x)|a_2(x)|\dots|a_k(x)$. That $a_i(x)$ must be given by (1) follows from diagonalizability of DU_n which forces $a_i(x)$ to have no repeated factors. Since the non-constant polynomials in the Smith normal form of $xI_{p_n} - [DU_n]$ are the invariant factors of RP_n as an $R[x]$-module, the SNF of $xI_{p_n} - [DU_n]$ over $R[x]$ is

$$\mathrm{diag}(1, \dots, 1, a_1(x), a_2(x), \dots, a_k(x)).$$

See [3, §8.2] for details.

Many of these conclusions fail when one replaces the field R by a PID of characteristic zero. For instance, DU_n and UD_n are not necessarily diagonalizable over R. An explicit counterexample is given by DU_2 for $P = \mathbf{Y}$. In the standard basis, the matrix is $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Diagonalizability of A is equivalent to requiring that $R^2 = \ker(DU_2 - I_2) \oplus \ker(DU_2 - 3I_2)$ or that

$$R = R\left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) \oplus R\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$$

This is however absurd if $2 \notin R^\times$. Invertibility of DU_n is also no longer guaranteed as the determinant of its matrix may not land in $R^\times$. For instance, $\det(A) = 3$ in the example above. In particular, DU_n is not necessarily surjective and one cannot deduce the surjectivity of down maps. Finally since $R[x]$ is not a PID, one in general does not expect a similar decomposition to exist for RP_n as an $R[x]$-module. However the existence of such a decomposition is equivalent to the conjecture of Miller and Reiner. We explain this in the next section.

3. Integral canonical forms

Throughout this section, R denotes an integral domain and F its field of fractions. For an $R[x]$-module M, we let $\mathrm{Ann}(M)$ denote the annihilator of M. For a monic polynomial $a(x) \in R[x]$, we denote its Frobenius companion matrix by $\mathcal{C}_{a(x)}$. For m, n positive integers, we let $\mathrm{Mat}_{m\times n}(R)$ denote the set of all $m \times n$-matrices with entries in R. Two matrices $A, B \in \mathrm{Mat}_{m\times n}(R[x])$ are said to be congruent if there exist $P \in \mathrm{GL}_m(R[x])$, $Q \in \mathrm{GL}_n(R[x])$ such that $B = PAQ$.

Definition 3.1. *An $R[x]$-module is said to have an invariant factor decomposition if there exist monogenic $R[x]$-submodules $M_1, M_2, \dots, M_k$ of M such that $\mathrm{Ann}(M_i)$ is generated by a monic, non-constant polynomial $a_i = a_i(x)$ that satisfy the chain of divisibilities*

$$a_1|a_2|\cdots|a_k$$

and $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

If M is an $R[x]$-module admitting such a decomposition, it is necessarily free of finite rank over R. Tensoring both sides of $M = M_1 \oplus \cdots . \oplus M_k$ with F yields the usual invariant factor decomposition of the $F[x]$-module $M \otimes_R F$. The uniqueness of invariant factor decomposition over fields implies that the sequence of polynomials a_i is uniquely determined by M. We will therefore refer to $a_1, \dots, a_k$ as the *invariant factor sequence* for M.

Let us denote $d_i := \deg a_i(x)$, $v_i \in M_i$ an $R[x]$-generator and $\varphi : M \to M$ the R-linear endomorphism given by multiplication by x. Then

$$\alpha := (v_1, \dots, x^{d_1-1}v_1, v_2, \dots, x^{d_2-1}v_2, \dots, v_k, \dots, x^{d_k-1}v_k)$$

is an R-basis for M with respect to which the matrix of φ is block-diagonal with k block matrices, the i-th block being the companion matrix of $a_i(x)$. In other words,

$$[\varphi]_\alpha = \begin{pmatrix} \mathcal{C}_{a_1}(x) & & & \\ & \mathcal{C}_{a_2(x)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_k(x)} \end{pmatrix} \tag{2}$$

Theorem 3.2. *Let M be an $R[x]$-module that is free of finite rank m over R and β be an R-basis for M. Then M admits an invariant factor decomposition if and only if the matrix $B(x) = xI_m - [\varphi]_\beta$ has Smith normal form over $R[x]$.*

Proof. ($\Longrightarrow$) By the discussion above, we can find an R-basis α for M such that $[\varphi]_\alpha$ is as in (2). Let $A(x) = xI_m - [\varphi]_\alpha$. It suffices to show that $A(x)$ has SNF over $R[x]$. Indeed, if $S \in \mathrm{GL}_n(R)$ denotes the change of basis matrix from β to α and if $P(x), Q(x) \in \mathrm{GL}_m(R[x])$ are such that $P(x) \cdot A(x) \cdot Q(x)$ is in SNF, then $P(x)S \cdot B(x) \cdot S^{-1}Q(x)$ returns the same SNF. Now

$$A(x) = \begin{pmatrix} xI_{d_1} - \mathcal{C}_{a_1}(x) & & & \\ & xI_{d_2} - \mathcal{C}_{a_2(x)} & & \\ & & \ddots & \\ & & & xI_{d_k} - \mathcal{C}_{a_k(x)} \end{pmatrix}.$$

It is easily seen by elementary row and column operations that $\mathrm{SNF}\big(xI_{d_i} - \mathcal{C}_{a_i}(x)\big) = \mathrm{diag}(1, \dots, 1, a_i(x))$. Thus the matrix above is congruent over $R[x]$ to

$$\mathrm{diag}(1, \dots, 1, a_1(x), 1, \dots, 1, a_2(x), \dots, 1, \dots, 1, a_k(x)).$$

Applying a few elementary row and column operations of switching, one obtains the desired SNF.

($\Longleftarrow$) Say $\beta = (b_1, \dots, b_m)$. Let $\mathcal{M} := R[x]^m$ and $e_1, \dots, e_m$ be the standard $R[x]$-basis for $\mathcal{M}$. Let $\psi : \mathcal{M} \to M$ be the surjective homomorphism that sends e_i to b_i. It induces an isomorphism $\mathcal{M}/\ker\psi \cong M$. Suppose that $[\varphi]_\beta = (a_{i,j})$. For each $j \in \{1, \dots, m\}$, set

$$u_j = xe_j - \sum_{i=1}^{m} a_{i,j} e_i \in \mathcal{M}.$$

Then $u_j \in \ker\psi$. Since $xe_j - u_j$ lies in the R-span of $e_1, \dots, e_m$, we see that

$$\begin{aligned} \mathcal{M} &= R[x]e_1 + \cdots + R[x]e_m \\ &= R[x]u_1 + \cdots + R[x]u_m + Re_1 + \cdots + Re_m. \end{aligned}$$

In other words, every element of $\mathcal{M}$ can be written as a sum of an element in the $R[x]$-submodule U generated by $u_1, u_2, \dots, u_m$, and an element of the R-submodule V generated by $e_1, e_2, \dots, e_m$ inside $\mathcal{M}$. We wish to show that $\ker\psi = U$. Pick $a \in \ker\psi$. Then, $a = u + v$ for some $u \in U$, $v \in V$. Then $\psi(v) = \psi(u+v) = \psi(a) = 0$. But $\psi(v)$ is 0 if and only if $v = 0$, since β is a basis for M. So $a = u \in U$.

Consider now the matrix $B(x)$. Its j-th column is the coordinate vector of u_j computed w.r.t. the standard basis $(e_i)_i$ of $\mathcal{M}$. Therefore right multiplication of $B(x)$ by elements of $\mathrm{GL}_m(R[x])$ amounts to changing the set of generators of $\ker\psi$ and left multiplication amounts to changing the standard basis of $\mathcal{M}$. Thus saying that $B(x)$ has SNF over $R[x]$ is equivalent to saying that there is an $R[x]$-basis of $\mathcal{M}$, say $f_1, f_2, \dots, f_m$ and polynomials $a_i \in R[x]$ satisfying $a_1|a_2|\dots|a_m$ such that

$a_1 f_1, \dots, a_m f_m$ forms a set of generators of $\ker\psi$. This immediately implies that $\ker\psi$ is a free $R[x]$-module and

$$\begin{aligned} M &\cong \mathcal{M}/\ker\psi \\ &\cong \left(\bigoplus_{j=1}^{m} R[x]f_i\right)\Big/\left(\bigoplus_{i=1}^{m} R[x]a_i f_i\right) \\ &\cong \bigoplus_{i=1}^{m} R[x]/(a_i) \end{aligned}$$

All of the a_i can be taken to be monic, since the product of a_i equals $\det(A(x))$ which is monic. If some a_i is 1, we can discard the corresponding summand in the direct sum decomposition above since $R[x]/(a_i) = 0$ in that case. ☐

Remark 3.3. The proof of the the backward direction is inspired by exercises 22-25 of [2, §2].

Definition 3.4. *We say that $A \in \mathrm{Mat}_{m\times m}(R)$ has* canonical form *over R if its rational canonical form (when A is seen over F) lies in $\mathrm{Mat}_{m\times m}(R)$ and is a $\mathrm{GL}_m(R)$-conjugate of A. In the case $R = \mathbb{Z}$, such a form is also referred to as an* integral canonical form*. We similarly define this notions for endomorphisms of a free R-module of finite rank.*

It is easy to see that an $R[x]$-module M that is free of finite rank over R admits an invariant factor decomposition if and only if the map φ induced by x has canonical form over R. By replacing x with $-x$ in the theorem above, we obtain the following.

Corollary 3.5. *For an r-differential poset, Conjecture 1.1 is true for some integer n if and only if $DU_n : \mathbb{Z}P_n \to \mathbb{Z}P_n$ has integral canonical form.*

4. Lifting canonical forms

For all of this section, R denotes a principal ideal domain. For any homomorphism ψ between two free R-modules of finite rank, the rank of ψ equals the number of non-zero entries in a Smith normal form for ψ. By analogy, we refer to the number of unit entries as the *unital rank* of ψ. It describes the size of any maximal subset of $\mathrm{im}(\psi)$ that can be extended to a basis of the target of ψ. The nullity of ψ is denoted by $\mathrm{null}(\psi)$. If A is a free R-module of finite rank, an element $x \in A$ is said to be *primitive* if $x \notin IA$ for any proper ideal $I \triangleleft R$. Then primitive elements are precisely those that can be extended to an R-basis for A.

4.1. Tweaking decompositions.

Fix now an $R[x]$-module M that admits an invariant factor decomposition and let $a_1, \dots, a_k$ denote its invariant factor sequence.

Lemma 4.1. *Suppose $k \geqslant 2$, $M = M_1 \oplus \cdots \oplus M_k$ is an invariant factor decomposition and $v_i \in M_i$ is an $R[x]$-module generator of M_i for each i. Let $j, \ell \in \{1, \dots, k\}$ be two distinct indices and $c \in R[x]$ be arbitrary. Set*

$$v'_\ell := \begin{cases} v_\ell + c v_j & \text{if } j < \ell \\ v_\ell + \dfrac{c a_j}{a_\ell} v_j & \text{if } j > \ell \end{cases}$$

and let M'_ℓ be the $R[x]$-submodule of M generated by v'_ℓ. Then $M_1 \oplus \cdots \oplus M'_\ell \oplus \cdots \oplus M_k$ is also an invariant factor decomposition for M.

Proof. Since v'_ℓ is an $R[x]$-linear combination of v_ℓ and v_j with the coefficient of v_ℓ being 1 and $S = \{v_1, \ldots, v_k\}$ generates M as an $R[x]$-module, the set $\{v'_\ell\} \cup (S \smallsetminus \{v_\ell\})$ generates M as well. Say $p_1, \ldots, p_k \in R[x]$ are such that

$$p_\ell v'_\ell + \sum_{i \neq \ell} p_i v_i = 0 \tag{3}$$

We divide into two cases.

Case 1: $j < \ell$.

We can rewrite (3) as $(p_j + cp_\ell)v_j + \sum_{i \neq j} p_i v_i = 0$. As $M_1, \ldots, M_k$ form a direct sum, $p_i v_i = 0$ for all $i \neq j$ and $(p_j + cp_\ell)v_j = 0$. Since a_i generates $\mathrm{Ann}(M_i)$ for all i, we see that

$$a_j \mid (p_j + cp_\ell) \quad \text{and} \quad a_\ell | p_\ell.$$

Since $a_j | a_\ell$ and $a_\ell | p_\ell$, p_ℓ annihilates both v_j and v_ℓ. Hence, it annihilates $v'_\ell = v_\ell + cv_j$. Similarly since a_j divides both $p_j + cp_\ell$ and p_ℓ, it divides p_j and therefore p_j annihilates v_j. Thus all summands in (3) vanish, and so the modules M_i for $i \neq \ell$ form a direct sum with M'_ℓ. Clearly a_ℓ annihilates M'_ℓ. Moreover any $f \in \mathrm{Ann}(M'_\ell)$ satisfies $fv_\ell + fcv_j = 0$ which by the direct sum property implies that $fv_\ell = fcv_j = 0$. So $f \in (a_\ell)$ and thus $(a_\ell) = \mathrm{Ann}(M'_\ell)$.

Case 2: $j > \ell$.

In this case, (3) can be rewritten as $(p_j + cp_\ell a_j/a_\ell)v_j + \sum_{i \neq j} p_i v_i = 0$. As before, this implies that $p_i v_i = 0$ for all $i \neq j$ and $(p_j + cp_\ell a_j/a_\ell)v_\ell = 0$. Thus

$$a_j | (p_j + cp_\ell a_j/a_\ell) \quad \text{and} \quad a_\ell | p_\ell.$$

So $p_\ell v'_\ell = p_\ell v_\ell + c\,(p_\ell/a_\ell)\,a_j v_j = 0$ and $p_j v_j = (p_j + cp_\ell a_j/a_\ell)v_j - c(p_\ell/a_\ell)a_j v_j = 0$. This establishes the direct sum property. One similarly verifies that a_ℓ generates $\mathrm{Ann}(M'_\ell)$. □

4.2. Ascensions. Let M be as in §4.1 and N be an arbitrary $R[x]$-module that is free of finite rank over R. Suppose that

$$U : M \to N \qquad\qquad D : N \to M$$

are $R[x]$-module homomorphisms such that $DU : M \to M$, $UD : N \to N$ coincide with multiplication by x, D is surjective, DU is injective and $\mathrm{coker}(U)$ is free over R.

Definition 4.2. *An* ascension *for an invariant factor decomposition $M_1 \oplus \cdots \oplus M_k$ of M is a sequence $W_1, \ldots, W_k$ of monogenic $R[x]$-submodules of N such that $D(W_i) = M_i$. We say that the ascension is* split *if $W_1, \ldots, W_k$ form a direct sum. An* ascension for *M is an ascension for some invariant factor decomposition of M.*

Let $W_1, \ldots, W_k$ be an ascension for M. If w_i is a generator for W_i, the image $v_i = D(w_i)$ is a generator for $D(W_i)$. So an ascension for $M = M_1 \oplus \cdots \oplus M_k$ can equivalently be described as a choice of generators $v_i \in M_i$ for each i and a choice of $w_i \in D^{-1}(v_i)$, though different choices may yield the same ascension.

Lemma 4.3. *The annihilator of the i-th member in an ascension for M is either (a_i) or (xa_i).*

Proof. Let $W_1, \ldots, W_k$ be an ascension, $M_i := D(W_i)$, $w_i \in W_i$ be generators and $v_i = D(w_i)$. First note that $xW_i = U(D(W_i)) = U(M_i)$. Since DU is injective, so is U. Hence $U(M_i)$ is isomorphic to M_i which means that $\mathrm{Ann}(U(M_i)) = (a_i)$. Therefore

xa_i annihilates W_i. Now either xa_i generates $\mathrm{Ann}(W_i)$ or it does not. If latter, pick any $p \in R[x] \setminus (xa_i)$ such that $pW_i = 0$. Then $0 = D(pW_i) = pM_i$ forces $p \in (a_i)$. So $p = ca_i$ for some $c \in R[x]$. Since xa_i annihilates W_i, we may assume wlog that c is a non-zero element of R. But since N is free over R, $ca_iW_i = 0$ implies $a_iW_i = 0$. So $\mathrm{Ann}(W_i) = (a_i)$ in this case. □

Proposition 4.4. *If $a_1(0) \in R$ is non-invertible, any ascension for M is split and the annihilator of the i-th ascended member equals (xa_i).*

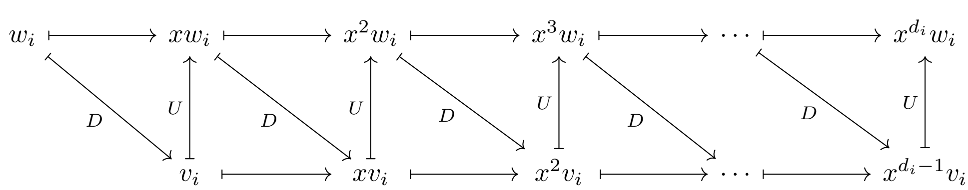
Proof. Let $W_1, \dots, W_k$ be an ascension, $M_i := D(W_i)$, $w_i \in W_i$ be generators and $v_i = D(w_i)$. Suppose that $p_1, \dots, p_k \in R[x]$ are such that

$$p_1w_1 + \cdots + p_kw_k = 0 \tag{4}$$

Applying D gives $p_1v_1 + \cdots + p_kv_k = 0$. Therefore $p_i \in (a_i)$ for all $i = 1, \dots, k$. Let $c_i \in R[x]$ be such that $p_i = c_ia_i$. Since xa_i annihilates w_i by Lemma 4.3, we may assume wlog that $c_i \in R$. Let $I = (c_1, \dots, c_k) \subset R$ be the ideal generated by these. If $I = (0)$, all of the p_i vanish, so assume otherwise. By replacing p_i with $\gamma^{-1}p_i$ for a generator $\gamma \in I$, we may also assume wlog that $I = R$. Now (4) can be rewritten as

$$\sum_{i=1}^{k} c_i\big(a_i(x) - a_i(0)\big)w_i = -\sum_{i=1}^{k} c_ia_i(0)w_i \tag{5}$$

Let $\omega := \bigcup_{i=1}^{k} \left\{x^jw_i \,|\, 0 \leqslant j \leqslant d_i - 1\right\} \subset N$ and $\omega_1 := x\omega$. Since DU acts as x and U is injective, we see that ω_1 is an R-basis for the image of U (see the diagram below).



Since $\mathrm{coker}(U)$ is free over R, the image $\mathrm{im}(U) = R\omega_1$ is a direct summand of N, i.e. ω_1 can be extended to an R-basis for N. Now the LHS of (5) is an R-linear combination over ω_1 and the monicity of the a_i implies that the ideal generated by the coefficients of this linear combination equals R. Thus the LHS of (5) is a primitive element of N. The RHS however is an element of $a_1(0)N$ since $a_i(0) \in (a_1(0))$ for all i. As $a_1(0) \notin R^\times$, this contradicts the primitivity of the LHS. Thus I must vanish and so must p_i. Therefore $W_1 + \cdots + W_k$ is a direct sum. The same argument reveals that $p \in R[x]$ annihilates w_i if and only if $p \in (xa_i)$ which establishes the second claim. □

Corollary 4.5. *If $a_1(0)$ is non-invertible,* $\mathrm{null}(D) \geqslant k$.

Proof. This follows by noting that $a_iw_i \in W_i \cap \ker(D)$ and $\{a_1w_1, \dots, a_kw_k\}$ is an R-linearly independent subset of $\ker(D)$ of cardinality k. □

Given an ascension $W_1, \dots, W_k$, one can construct new ones by replacing the generators $w_i \in W_i$ using one of the following operations:

(A) replace w_ℓ with $w_\ell + t$ for any index ℓ and $t \in \ker(D)$,
(B) replace w_ℓ with $w_\ell + cw_j$ for any $j < \ell$ and $c \in R$
(C) replace w_ℓ with $w_\ell + c(a_j/a_\ell)w_j$ for any $j > \ell$ and $c \in R$.

Operation (A) is justified since $w_\ell + t \in D^{-1}(v_\ell)$. Operations (B), (C) are justified by Lemma 4.1 and amount to changing the underlying invariant factor decomposition for M.

Theorem 4.6. *If* $a_1(0)$ *is non-invertible and* $\mathrm{null}(D) \geqslant k+1$*,* N *has an invariant factor decomposition.*

Proof. Fix an ascension $W_1, \dots, W_k$ for M and let M_i, w_i, v_i be as above. Let $\kappa_0 := \{a_1 w_1, \dots, a_k w_k\} \subset \ker(D)$ and $p := \mathrm{null}(D)$. Since R is a PID, the inclusion $R\kappa_0 \hookrightarrow \ker D$ admits a Hermite normal form (cf. [4, §3.2]). More precisely, there is an R-basis $t_1, \dots, t_p$ of $\ker(D)$ such that for all j,

$$a_j w_j = \sum_{i=1}^{j} c_{i,j} t_i \tag{6}$$

where $c_{i,j} \in R$. In other words, the matrix of the inclusion $R\kappa_0 \hookrightarrow \ker(D)$ is

$$E = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k} \\ & c_{2,2} & \cdots & c_{2,k} \\ & & \ddots & \vdots \\ & & & c_{k,k} \\ & & & \end{pmatrix} \in \mathrm{Mat}_{p\times k}(R).$$

Let E_i denote the i-th column of E. Let us record how E changes when we modify the generators w_i with respect to operations (A), (B), (C):

(A) replace E_ℓ with $E_\ell + a_\ell(0)F$ for any ℓ and $F \in \mathrm{Mat}_{p\times 1}(R)$,
(B) replace E_ℓ with $E_\ell + c\big((a_\ell/a_j)(0)\big)E_j$ for any $j < \ell$ and $c \in R$,
(C) replace E_ℓ with $E_\ell + cE_j$ for any $j > \ell$ and $c \in R$.

We say that E is *connected* to $E' \in \mathrm{Mat}_{p\times k}(R)$ if there exists $P \in \mathrm{GL}_p(R)$ such that E' can be obtained from PE by applying operations (A), (B), (C) a finite number of times.

Claim: E is connected to the matrix that has 1_R on its diagonal and zero elsewhere. Begin by placing $a_1(0)$ in $(2,1)$-position of E via operation (A) and call this matrix E' for the moment. We claim that ideal J generated by $a_1(0)$ and $c_{1,1}$ equals R. Suppose not. Then (6) implies that

$$(a_1(x) - a_1(0))\, w_1 = c_{1,1}t_1 - a_1(0)w_1 \in JN.$$

This is however a contradiction, since the LHS is a primitive element of N (see the proof of Proposition 4.4). So the first column of E describes a primitive vector in $R^2 \subset R^p$ where (R^2 is embedded in the first two components). There is thus an element $P \in \mathrm{GL}_p(R)$ which is a block diagonal sum of a 2×2 invertible matrix with the $(k-2)\times(k-2)$ identity matrix such that the first column of PE' is $(1,0,\dots,0)^t$. Operation (C) then allows us to replace PE' with a matrix E'' whose first row is $(1,0,\dots,0)$. Relabeling everything, we can assume that

$$E = \begin{pmatrix} 1 & & & \\ & c_{2,2} & \cdots & c_{2,k} \\ & & \ddots & \vdots \\ & & & c_{k,k} \\ & & & \end{pmatrix}.$$

Since $a_1(0)|\cdots|a_k(0)$, we can continue inductively: place $a_i(0)$ in the $(i+1,i)$-entry, use primitivity of elements to establish $(a_i(0), c_{i,i}) = R$, transform by multiplying on the left by an element of $\mathrm{GL}_2(R)$ to make (i,i)-entry 1 and then use this entry to make all entries to its right 0. Note that $p > k$ is necessary to execute this procedure in the k-th column. The claim is established.

Thus we may assume that the ascension $W_1, \dots, W_k$ is such that $R\kappa_0 = \bigoplus_{i=1}^k Ra_iw_i$ is a direct summand of $\ker(D)$. Let $\omega := \bigcup_{i=1}^k \left\{x^jw_i \,|\, 0 \leqslant j \leqslant d_i - 1\right\}$. Since D maps ω bijectively onto the R-basis $\bigcup_{i=1}^k \left\{x^jv_i \,|\, 0 \leqslant j \leqslant d_i - 1\right\}$ of M, we have

$$N = R\omega \oplus \ker(D).$$

Choose κ a basis of $\ker(D)$ that extends κ_0, so that $\omega \cup \kappa$ is an R-basis for N. Then the set ν obtained by replacing each $a_iw_i \in \omega \cup \kappa$ with $a_iw_i + (x^{d_i} - a_i)w_i = x^{d_i}w_i$ is also an R-basis since $(x^{d_i} - a_i)w_i \in R\omega$. We can write ν as the union of $\bigcup_{i=1}^k \left\{x^jw_i \,|\, 0 \leqslant j \leqslant d_i\right\}$ with $\kappa \setminus \kappa_0 \subset \ker(D)$. Then if $s_1, \dots, s_{p-k}$ denote the $p-k$ elements of $\kappa \setminus \kappa_0$,

$$N = R\nu = Rs_1 \oplus \cdots \oplus Rs_{p-k} \oplus W_1 \oplus \cdots \oplus W_k.$$

is the desired invariant factor decomposition for N. □

Remark 4.7. Note that the proof above goes through without ever invoking operation (B). However we chose to include it for the sake of completeness, as this operation seemed natural in the formulation of Lemma 4.1.

4.3. Invertible constants. It will be necessary to generalize Theorem 4.6 to some cases where $a_1(0) \in R^\times$. We record such a generalization below.

We continue to assume the notation and terminology introduced so far. Observe that the injectivity of DU implies that the intersection $\ker(D) \cap \operatorname{im}(U)$ is trivial. Let ι denote the inclusion $\ker(D) \oplus \operatorname{im}(U) \hookrightarrow N$. Note that this is a full rank inclusion. Let k_0 denote the number of non-invertible terms in the sequence $(a_1(0), \dots, a_k(0))$.

Lemma 4.8. *A Smith normal form for ι is given by* $\operatorname{diag}(1, \dots, 1, a_1(0), \dots, a_k(0))$. *In particular,* $\operatorname{null}(D) \geqslant k_0$.

Proof. Let $L := \ker(D) \oplus \operatorname{im}(U)$. Then L is the kernel of the composition $N \xrightarrow{D} M \xrightarrow{\pi} M/xM$ where π denotes the canonical quotient map. So we have an isomorphism

$$N/L \simeq M/xM \simeq \bigoplus_{i=k_0}^{k} R/(a_i(0)).$$

of R-modules and the first claim easily follows from this. Since $\operatorname{im}(U)$ is a direct summand of N, the unital rank of ι is at least $\operatorname{rank}_R(M)$. Since this unital rank is exactly $\operatorname{rank}_R(N) - k_0$ in light of the first claim, the second claim also follows. □

Theorem 4.9. *Suppose that there is a positive integer $\delta \leqslant k$ such that $a_1 = \cdots = a_\delta = x - 1$, $a_i(0)$ is non-invertible for $i > \delta$ and* $\operatorname{null}(D) \geqslant k - \delta + 1$. *Then N admits an invariant factor decomposition.*

Proof. Note that $k_0 = k - \delta$ by definition of δ. Fix an ascension $W_1, \dots, W_k$ for M and let M_i, w_i, v_i be as usual. By replacing w_i with $xw_i = w_i + (x-1)w_i$, we may assume that $xw_i = w_i$ for $i = 1, \dots, \delta$. Then $\operatorname{Ann}(W_i) = (x-1)$ for $1 \leqslant i \leqslant \delta$ and the argument of Proposition 4.4 still goes through to show that any such ascension splits and that $\operatorname{Ann}(W_i) = (xa_i)$ for $i > \delta$. Similarly the argument of Theorem 4.6 can be executed to show that there is a modification of the $k - \delta = k_0$ generators $w_{\delta+1}, \dots, w_k$ by elements of $\ker(D)$ so that $\kappa_0 = \{a_iw_i \,|\, \delta < i \leqslant k\}$ extends to an R-basis of $\ker(D)$. Let $\omega = \bigcup_{i=1}^k \left\{x^jw_i \,|\, 0 \leqslant j \leqslant d_i - 1\right\}$ as before and let κ be a basis of $\ker(D)$ that extends κ_0. Then $\omega \cup \kappa$ is an R-basis for N and therefore so is

$$\nu' := \omega \cup (\kappa \setminus \kappa_0) \cup \left\{x^{d_i}w_i \,|\, \delta < i \leqslant k\right\}.$$

Let $p = \operatorname{null}(D)$ and $s_1, \dots, s_{p-k_0}$ denote the $p - k_0$ elements of $\kappa \setminus \kappa_0$. Note that $p - k_0 = p - k + \delta \geqslant 1$.

Case 1: $p - k_0 \geqslant \delta$.

Construct the R-basis $\nu := \{s_i + w_i \,|\, 1 \leqslant i \leqslant \delta\} \cup (\nu' \smallsetminus \{s_1, \dots, s_\delta\})$ for N. If W_i° denotes the $R[x]$-submodule generated by $w_i + s_i$ for $i = 1, \dots, \delta$, then $\mathrm{Ann}(W_i^\circ) = x(x-1)$. Therefore

$$N = R\nu = (Rs_{\delta+1} \oplus \cdots \oplus Rs_{p-k_0}) \oplus (W_1^\circ \oplus \ldots \oplus W_\delta^\circ) \oplus (W_{\delta+1} \oplus \ldots \oplus W_k)$$

is an invariant factor decomposition for N.

Case 2: $p - k_0 < \delta$

Construct the R-basis $\nu := \{s_i + w_{\delta-i+1} \,|\, 1 \leqslant i \leqslant p - k_0\} \cup (\nu' \smallsetminus \{s_1, \dots, s_{p-k_0}\})$. Let $W_{\delta-i+1}^\circ$ denote the $R[x]$-submodule generated by $s_i + w_{\delta-i+1}$ for $i = 1, \dots, p - k_0$. Then again,

$$N = R\nu = (W_1 \oplus \ldots \oplus W_{\delta+k_0-p}) \oplus \left(W_{\delta+k_0-p+1}^\circ \oplus \ldots \oplus W_\delta^\circ\right) \oplus (W_{\delta+1} \oplus \ldots \oplus W_k)$$

is an invariant factor decomposition. ☐

5. The main theorem

We now apply the results of the previous section to differential posets. Let P denote an r-differential poset, P_n its n-th rank (which is empty if the integer n is negative), p_n the cardinality of P_n and Δp_n the difference $p_n - p_{n-1}$. Define U_n, D_n, etc. as in the introduction for $R = \mathbb{Z}$. Let $\delta_{i,j}$ denote the Kronecker delta.

Lemma 5.1. *For an r-differential poset, the map D_{n+1} is surjective if and only if U_n has free cokernel.*

Proof. That U_n has free cokernel is equivalent to saying that the Smith normal form of U_n consists of only ones and zeros. The same applies to D_{n+1}. But since D_{n+1} is of full rank, freeness of cokernel is equivalent to surjectivity. Now note that the matrices of D_{n+1}, U_n in the standard basis are transposes of each other and thus the same is true for their Smith normal forms. ☐

Proposition 5.2. *Suppose that D_{n+1} is surjective and DU_n has integral canonical form for some n. Then $\Delta p_{n+1} \geqslant \Delta p_{n-i-\delta_{r,1}}$ for all $i \geqslant 0$.*

Proof. We proceed via induction. The case $n = 0$ is trivial. Say the claim is true for some $n \geqslant 0$. Set

$$M := \mathbb{Z}P_n, \qquad N := \mathbb{Z}P_{n+1}$$

and view these are $\mathbb{Z}[x]$-modules via DU_n, UD_{n+1} respectively. Let $D : N \to N$, $U : M \to N$ be the up and down maps respectively. Note that both of these respect the $\mathbb{Z}[x]$-module structures. Moreover, our induction hypothesis implies that M has an invariant factor decomposition. Thus we are in the setup of §4.2. By the discussion in §2, the integer k for the invariant factor decomposition for M equals $\max\{\Delta p_0, \dots, \Delta p_n\}$. If $r > 1$, Corollary 4.5 and the expression (1) for $a_1(x)$ implies that $\Delta p_{n+1} = \mathrm{null}(D) \geqslant k$. If $r = 1$, the integer $k_0 = \max\{\Delta p_0, \dots, \Delta p_{n-1}\}$ computes the number of invariant factors of M whose constant term is non-invertible in $\mathbb{Z}$. In this case, Lemma 4.8 implies the claim. ☐

Theorem 5.3. *Suppose that for the r-differential poset P,*

- *all the down maps are surjective,*
- *there exists a non-negative integer m such that $\Delta p_n > \Delta p_{n-1-\delta_{r,1}}$ for every $n > m$,*
- *$DU_0, \dots, DU_m$ have integral canonical forms.*

Then DU_n has integral canonical form for every n.

Proof. We proceed via strong induction on n. Base case verification is included in the third bullet. Say all of $DU_0, \dots, DU_n$ have integral canonical forms for some $n \geqslant m$. Denote as in Proposition 5.2 $M = \mathbb{Z}P_n$, $N = \mathbb{Z}P_{n+1}$ and write D, U for up and down maps between M, N. Then M has invariant factor decomposition with $k = \max\{\Delta p_0, \dots, \Delta p_n\}$ factors. Proposition 5.2 implies that

$$k = \begin{cases} \Delta p_n & \text{if } r > 2 \\ \max\{\Delta p_n, \Delta p_{n-1}\} & \text{if } r = 1. \end{cases}$$

If either $r = 2$ or if $r = 1$ and $k = \Delta p_{n-1}$, we see from (1) that $a_1(0)$ is non-invertible in $\mathbb{Z}$. So Theorem 4.6 implies that N has an invariant factor decomposition. If on the other hand $r = 1$ and $k = \Delta p_n > \Delta p_{n-1}$, the integer $\delta = \Delta p_n - \Delta p_{n-1} \geqslant 1$ is such that $a_1 = \ldots = a_\delta = x - 1$ and $a_i(0)$ is non-invertible for $i > \delta$. In this case, Theorem 4.9 implies that N has an invariant factor decomposition. In either case, we see that UD_{n+1} has integral canonical form. Equivalently, $xI_{p_{n+1}} - [UD_{n+1}]$ has Smith normal form over $\mathbb{Z}[x]$ (see Theorem 3.2). Since

$$DU_{n+1} = UD_{n+1} + r \cdot \mathbb{1},$$

$xI_{p_{n+1}} - [DU_{n+1}]$ also has Smith normal form over $\mathbb{Z}[x]$ which is given by replacing x with $x - r$ in the Smith normal form of UD_{n+1}. Then again, this implies that DU_{n+1} has integral canonical form. This completes the induction step. ☐

Remark 5.4. Combining Proposition 5.2 with [3, Proposition 2.5], we see that Conjecture 2.3 and 2.4 of *loc.cit.* are equivalent whenever Conjecture 1.1 holds. Then Theorem 5.3 may be seen as a converse of sorts. It would be interesting to relax the second condition of Theorem 5.3 to the bound given in Proposition 5.2.

6. Applications

In this section, we record some applications.

Theorem 6.1. *Let P and Q be differential posets of rank sizes p_n, q_n respectively. Suppose that $\Delta q_n \geqslant \Delta q_{n-1}$ for all $n \geqslant 2$, and that all the down maps of at least one of the posets are surjective. Then Conjecture 1.1 holds for $P \times Q$.*

Proof. By Corollary 3.5, it is enough to show that the DU_n maps of $P \times Q$ have integral canonical form. Notice that $P \times Q$ is an r-differential poset for some $r \geqslant 2$. It was proved in [3, Proposition 4.5] that the up maps of a cartesian product have free cokernel if one of the posets in the product has this property. So Lemma 5.1 implies that the down maps of $P \times Q$ are surjective. Denote the rank sizes of $P \times Q$ by ρ_n. Then $\rho_n = \sum_{i=0}^{n} q_{n-i} p_i$, so

$$\Delta\rho_n - \Delta\rho_{n-1} = q_0(\Delta p_n) + \Delta q_1 p_{n-1} + \sum_{i=0}^{n-2} (\Delta q_{n-i} - \Delta q_{n-i-1}) p_i. \tag{7}$$

Suppose that $n \geqslant 2$. If Q is 1-differential, then $\Delta q_2 - \Delta q_1 = 1$. So the last summand of the sum in (7) contributes a non-zero term. If Q is s-differential for some $s > 1$, then $\Delta q_1 = s - 1$ which means that $\Delta q_1 p_{n-1} \geqslant 1$. Since all the terms in the sum (7) are non-negative, we see that

$$\Delta\rho_n > \Delta\rho_{n-1}$$

for all $n \geqslant 2$. Additionally if PQ is r-differential for $r \geqslant 3$, then $\Delta\rho_1 - \Delta\rho_0 = r - 2$ is at least 1. Now DU_0 trivially has integral canonical form, so Theorem 5.3 with $m = 0$ gives the result. If $r = 2$, the matrix for DU_1 is always $\left(\begin{smallmatrix} 3 & 1 \\ 1 & 3 \end{smallmatrix}\right)$, and one can easily verify that it has an integral canonical form. So in this case, Theorem 5.3 applies with $m = 1$. □

Corollary 6.2. *The Conjecture* 1.1 *is true for* $\mathbf{Y}^r$ *for every* $r \geqslant 1$.

Proof. Suppose first that $r = 1$. It was proved in [3, §6.1] that the up maps of $\mathbf{Y}$ have free cokernel and hence, the down maps are surjective. We claim that

$$\Delta p_n > \Delta p_{n-2}$$

holds for all $n > 2$. Since $\Delta p_1 = 0$ and $\Delta p_3 = 1$, the condition holds for $n = 3$. So assume $n \geqslant 4$. Notice that $\Delta p_n = p_n - p_{n-1}$ counts the number of partitions of n with no part equal to 1. Let S_n be the set of all such partitions of n. For each partition in S_{n-2}, we can add a 2 to the largest part, and obtain a partition of n in S_n. This injects S_{n-2} in S_n and so $|S_n| \geqslant |S_{n-2}|$. If n is even, the partition $2, 2, 2, \ldots, 2$ with $n/2$ number of 2s cannot be obtained from the said injection of S_{n-2} into S_n. Similarly if n is odd, the partition $3, 2, 2, \ldots, 2$ with $\lfloor n/2 \rfloor - 1$ number of 2s does not arise from a partition in S_{n-2}. So we have

$$|S_n| > |S_{n-2}|$$

for $n \geqslant 4$, and we obtain the desired inequality. Now one can easily verify that DU_0, DU_1 and DU_2 for $\mathbf{Y}$ all have integral canonical form. Invoking Theorem 5.3 (with $m = 2$) and Corollary 3.5, we get the result in this case.

For the case $r > 1$, note that there is an injection S_{n-1} in S_n given by adding 1 to the largest part in a partition from S_{n-1}. This implies that $|S_n| \geqslant |S_{n-1}|$ for all $n \geqslant 2$. The claim then follows by Theorem 6.1 with $P = \mathbf{Y}^{r-1}$ and $Q = \mathbf{Y}$. □

Corollary 6.3. *The Conjecture* 1.1 *holds for* $Z(r)$ *for all* $r \geqslant 1$.

Proof. The surjectivity of down maps for $Z(r)$ was proved in [3, §5]. Recall that the rank sizes of $Z(r)$ satisfy the recursion given by $p_0 = 1$, $p_1 = r$ and $p_n = rp_{n-1} + p_{n-2}$ for $n \geqslant 2$. Therefore the rank differences satisfy $\Delta p_0 = 1$, $\Delta p_1 = r - 1$ and

$$\Delta p_n = (r-1)(\Delta p_{n-1}) + rp_{n-2}, \qquad n \geqslant 2.$$

So if $r > 2$, $\Delta p_n > \Delta p_{n-1}$ holds for all $n > 0$ and Theorem 5.3 applies with $m = 0$ (the base case is trivial). If $r = 2$, $\Delta p_n > \Delta p_{n-1}$ for $n > 1$ and Theorem 5.3 applies with $m = 1$ (base case for DU_1 is the same as in Theorem 6.1). Finally if $r = 1$, $\Delta p_n > \Delta p_{n-2}$ holds $n > 3$. It is easily verified that DU_0, DU_1, DU_2 and DU_3 all have integral canonical forms. Therefore Theorem 5.3 applies with $m = 3$. □

Remark 6.4. This result was also proved in [3, §5].

Acknowledgements. I would like to specially thank my mentor, Dr. Shaheen Nazir, for introducing me to this topic and providing help and guidance throughout my research journey and Ivan Sadofschi Costa, for providing help with various computations in Sage, helpful edits and for being a constant source of support. I would also like to thank Brian Conrad for his valuable feedback and insightful conversations. In addition, I thank Victor Reiner for his comments on an earlier version, Alexander Miller for sharing the data on rank sizes and Richard Stanley for useful communication. Finally, I wish to thank the anonymous referees for pointing out an error and for their valuable comments and suggestions.

References

[1] T. W. Cai and R. P. Stanley, *The Smith normal form of a matrix associated with Young's lattice*, Proc. Amer. Math. Soc. **143** (2015), no. 11, 4695–4703.

[2] D. S. Dummit and R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[3] A. R. Miller and V. Reiner, *Differential posets and Smith normal forms*, Order **26** (2009), no. 3, 197–228.

[4] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1997.

[5] R. P. Stanley, *Differential posets*, J. Amer. Math. Soc. **1** (1988), no. 4, 919–961.

[6] Richard P. Stanley, *Smith normal form in combinatorics*, J. Combin. Theory Ser. A **144** (2016), 476–495.

Syed Waqar Ali Shah, Lahore University of Management Sciences, Department of Mathematics, Lahore, 54792 (Pakistan)
Department of Mathematics, University of California, Santa Barbara, CA 93106 (USA)
E-mail : swaqar.66080@gmail.com
E-mail : swshah@ucsb.edu
Url : https://sites.google.com/view/swshah/home