PRIMES 2015 reading project: Problem set #3

(posted 31 May 2015, to be submitted around 15 June 2015)

Darij Grinberg

The purpose of this problem set is to replace an argument in [BFZ-CA3, proof of Proposition 1.8] with a more elementary argument (which does not use Newton polytopes).[1]

0.1. Some linear algebra basics

Let us start by doing some linear algebra over the ring of integers. You are probably most used to doing linear algebra over fields, since this is the case most suited to doing linear algebra: For example, solving a system of linear equations using Gaussian elimination works over fields but not (say) over $\mathbb{Z}$ or over a polynomial ring.[2] We shall do linear algebra over the ring of integers here, because we will want to use the entries of our vectors as exponents in monomials, and exponents in monomials should be integers (we don't want to work with non-integer powers here). Fortunately, the linear algebra that we will do will be simple enough that it can be made to work over the integers.

If F is a commutative ring[3] and if n and m are two nonnegative integers, then $F^{n\times m}$ denotes the set of all $n \times m$-matrices over F. (These are the matrices whose entries are in F and which have n rows and m columns.) We regard $\mathbb{Z}^{n\times m}$ as a subset of $\mathbb{Q}^{n\times m}$ for all n and m, because a matrix with integer entries can always be regarded as a matrix with rational entries.

If F is a commutative ring and if $n \in \mathbb{N}$, then $\mathrm{GL}_n(F)$ denotes the group of all invertible $n \times n$-matrices $A \in F^{n\times n}$. Here, "invertible" means "invertible in $F^{n\times n}$"; that is, a matrix A is said to be invertible if there exists a matrix $B \in F^{n\times n}$ such that $AB = BA = I_n$ (where I_n is the $n \times n$ identity matrix). The meaning of "invertible" thus depends on F (so we will clarify it by saying "invertible in $F^{n\times n}$" unless F is clear from the context). For example, the five matrices

$$\begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}, \qquad \begin{pmatrix} \frac{1}{2} & \frac{3}{2} \\ 1 & 1 \end{pmatrix}$$

[1] This is not the only place where [BFZ-CA3] uses Newton polytopes; but the other place – in the proof of Lemma 7.3 – is really tangential to what we are doing (it proves the "only if" part of Theorem 1.20, which I would not call particularly interesting).

[2] This is not to say that the situation over $\mathbb{Z}$ and over polynomial rings is hopeless. Some more complicated versions of Gaussian elimination do their job over some of these rings, and lead to certain weaker and more complicated (but also more interesting!) versions of row-reduced matrices.

[3] Recall that a commutative ring is (roughly speaking) a set S whose elements can be added, subtracted and multiplied, and all of these operations give results inside S and satisfy the usual laws (commutativity, associativity, distributivity, existence of 0 and 1).

are invertible in $\mathbb{Q}^{n\times n}$, but only the first two of them are invertible in $\mathbb{Z}^{n\times n}$. (The fifth one, of course, does not lie in $\mathbb{Z}^{n\times n}$ to begin with.)

We shall study $\operatorname{GL}_n(\mathbb{Z})$ in particular. Recall that a matrix $A \in \mathbb{Q}^{n\times n}$ is invertible if and only if its determinant $\det A$ is nonzero. The analogous criterion for $\mathbb{Z}$ is a lot more restrictive: A matrix $A \in \mathbb{Z}^{n\times n}$ is invertible if and only if its determinant $\det A$ has an inverse in $\mathbb{Z}$. (The only integers which have an inverse in $\mathbb{Z}$ are 1 and -1, so this leaves only two possibilities for the determinant.) We will not use this fact, however, but it is important.[4]

We start with some simpler things.

For any $n \in \mathbb{N}$, the sets $\mathbb{Z}^n$ and $\mathbb{Q}^n$ consist of column vectors of length n (at least according to my convention), and we consider $\mathbb{Z}^n$ as a subset of $\mathbb{Q}^n$. I will usually write a column vector $\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ in the form $(v_1, v_2, \ldots, v_n)^T$, because the former (vertical) notation takes too much space. Of course, the notation $(v_1, v_2, \ldots, v_n)^T$ is just a particular case of the general notation A^T for the transpose of a matrix A (at least if we follow the usual convention to think of column vectors as $n \times 1$-matrices and of row vectors as $1 \times n$-matrices).

The column vector of length n whose all entries are 0 will be denoted by 0, or (when n is not clear from the context) by 0_n. It is called the *zero vector*.

For every $n \in \mathbb{N}$ and $i \in \{1, 2, \ldots, n\}$, we let e_i be the column vector

$$(0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)^T \in \mathbb{Z}^n,$$

where the 1 is the i-th entry of the vector. (This vector depends on both i and n; we just leave the n out of the notation e_i because it will always be clear from the context.)

Exercise 1. Let $n \in \mathbb{N}$, and let F be a commutative ring. (Feel free to take $F = \mathbb{Z}$ or $F = \mathbb{Q}$ here.) Show that $\operatorname{GL}_n(F)$ is a group (where the binary operation is multiplication of matrices).

0.2. Gcds of integer vectors

The *greatest common divisor* $\gcd \mathbf{v}$ of a vector $\mathbf{v} \in \mathbb{Z}^n$ is defined as the gcd of all the n entries of $\mathbf{v}$. When $\mathbf{v} = 0$, this is understood to be 0; otherwise, it is a positive integer.

Exercise 2. Let $n \in \mathbb{N}$, let $A \in \mathbb{Z}^{n\times n}$ and $\mathbf{v} \in \mathbb{Z}^n$.

(a) Prove that $\gcd \mathbf{v} \mid \gcd (A\mathbf{v})$.

(b) If $A \in \operatorname{GL}_n(\mathbb{Z})$, then prove that $\gcd (A\mathbf{v}) = \gcd \mathbf{v}$.

[4] We might get to explore it later.

Exercise 3. Let n be a positive integer, and let $\mathbf{v} \in \mathbb{Z}^n$. Let $g = \gcd \mathbf{v}$. Then, there exists a matrix $A \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$\mathbf{v} = gAe_1.$$

This exercise is crucial, so let me comment on it a bit more. First of all, e_1 is the column vector $(1, 0, 0, 0, \ldots) \in \mathbb{Z}^n$ (which has 1 as its first entry and 0's everywhere else). Thus, Ae_1 is the first column of the matrix A (check this if you don't know why it holds), and so gAe_1 is the result of multiplying this first column by $g = \gcd \mathbf{v}$. So Exercise 3 says that if n is a positive integer and if $\mathbf{v} \in \mathbb{Z}^n$, then there exists an invertible matrix $A \in \mathrm{GL}_n(\mathbb{Z})$ whose first column, multiplied by $\gcd \mathbf{v}$, is the vector $\mathbf{v}$. In particular, if $\gcd \mathbf{v} = 1$, then $\mathbf{v}$ itself is the first column of an invertible matrix $A \in \mathrm{GL}_n(\mathbb{Z})$. For instance, the vector $(6, 15, 10)^T \in \mathbb{Z}^3$ is the first column of the invertible matrix $\begin{pmatrix} 6 & 0 & 1 \\ 15 & 1 & 1 \\ 10 & 1 & 0 \end{pmatrix}$ (and, of course, of many other such matrices).

Let me give a few hints for Exercise 3. We want to prove the existence of an invertible matrix $A \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathbf{v} = gAe_1$. This is tantamount to constructing an invertible matrix $B \in \mathrm{GL}_n(\mathbb{Z})$ such that $B\mathbf{v} = ge_1$ (the relation between A and B is that of being mutually inverse). A way to do this is to find a sequence of invertible matrices which, when multiplied onto $\mathbf{v}$ from the left (one after the other), will make the vector $\mathbf{v}$ "simpler" step by step, until $\mathbf{v}$ becomes a vector with only one nonzero entry[5]. Then, the entry will have to be either g or $-g$ (why?). A further invertible matrix (namely, $-I_n$) will get rid of the minus if it is a $-g$; a further multiplication with a permutation matrix (permutation matrices are invertible) will push the nonzero entry into the first spot, and we will have the vector ge_1 in front of us. So the main difficulty is to find that sequence of invertible matrices which "simplify" $\mathbf{v}$. To do so, keep in mind that if $\mathbf{v} \in \mathbb{Z}^n$ is a vector and i and j are two distinct elements of $\{1, 2, \ldots, n\}$, then the matrix $F_{i,j}$ which has 1's on the main diagonal, a -1 in cell (i, j), and 0's everywhere else is invertible (what is its inverse?), and the vector $F_{i,j}\mathbf{v}$ is obtained from $\mathbf{v}$ by subtracting the j-th entry from the i-th entry. How can you "simplify" $\mathbf{v}$ using such subtraction operations?

0.3. Reminders on polynomials

Fix $n \in \mathbb{N}$ from now on. Let $\mathbf{x}$ denote the n-tuple $(x_1, x_2, \ldots, x_n)$ of distinct indeterminates. We can use this n-tuple to define the polynomial ring $\mathbb{Z}[\mathbf{x}] = \mathbb{Z}[x_1, x_2, \ldots, x_n]$, as well as the Laurent polynomial ring $\mathbb{Z}[\mathbf{x}^{\pm 1}] = \mathbb{Z}\left[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}\right]$. The elements of the polynomial ring $\mathbb{Z}[\mathbf{x}]$ are polynomials, i.e., $\mathbb{Z}$-linear combinations of *monomials* (which are expressions of the form $x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$ where

[5] unless $\mathbf{v} = 0$, in which case there is no nonzero entry at all and we are done

$v_1, v_2, \ldots, v_n \in \mathbb{N}$). The elements of the Laurent polynomial ring $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ are Laurent polynomials, i.e., $\mathbb{Z}$-linear combinations of *Laurent monomials* (which are expressions of the form $x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$ where $v_1, v_2, \ldots, v_n \in \mathbb{Z}$). We can view $\mathbb{Z}[\mathbf{x}]$ as a subring of $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$.

Let us recall how the notion of an *irreducible element* of a commutative ring is defined: If R is a commutative ring, then an element $a \in R$ is said to be *irreducible* if and only if

- the element a is not invertible (in R), and
- there are no two elements b and c of R which are not invertible (in R) and satisfy $bc = a$.

For example, the irreducible elements of $\mathbb{Z}$ are the prime numbers and the negatives of the prime numbers. The elements 1 and -1 are not irreducible (they fail the first condition, as they are invertible), and the composite positive integers are not irreducible either (they fail the second condition). On the other hand, $\mathbb{Q}$ has no irreducible elements (indeed, $0 \in \mathbb{Q}$ fails the second condition, while all other elements fail the first one).

The irreducible elements of $\mathbb{Z}[\mathbf{x}]$ are the irreducible polynomials, in the appropriate sense. For example, 2, x_1, $x_2^2 + x_3^2$ and $x_1^2 - 2$ are irreducible, whereas 6, $x_1 x_2$, $x_2^2 - x_3^2$ and $x_1^2 - 4$ are not.

The irreducible elements of $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ are "more or less" the same, but only more or less. The situation is slightly different because all Laurent monomials have become invertible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$. Thus, for example, x_1, although irreducible in $\mathbb{Z}[\mathbf{x}]$, is not irreducible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$, because it is invertible in the latter ring. Exercise 4 **(c)** below shows that "almost-monomials" ($\pm x_1, \pm x_2, \ldots, \pm x_n$) are essentially the only exceptions.

Exercise 4. **(a)** Show that a polynomial $P \in \mathbb{Z}[\mathbf{x}]$ is invertible in $\mathbb{Z}[\mathbf{x}]$ if and only if it equals 1 or -1.

(b) Show that a Laurent polynomial $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ is invertible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ if and only if either P or $-P$ is a (single) Laurent monomial.

(c) Let $P \in \mathbb{Z}[\mathbf{x}]$ be a polynomial such that none of the variables $x_1, x_2, \ldots, x_n$ divides P (in $\mathbb{Z}[\mathbf{x}]$). Then, show that P is irreducible as an element of $\mathbb{Z}[\mathbf{x}]$ if and only if P is irreducible as an element of $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$.

We say that two elements a and b of a commutative ring R are *coprime* if every common divisor of a and b is invertible. When $R = \mathbb{Z}$, this notion of coprimality is exactly the classical notion of coprimality for integers.

0.4. Monomial substitutions

Definition 0.1. Let $A \in \mathbb{Z}^{n\times n}$. If $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ is an n-tuple of invertible elements of a commutative ring R, then we let $A_* \mathbf{u}$ denote the n-tuple defined as follows: Write A in the form $A = \left(a_{i,j}\right)_{1\leq i,j\leq n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$. Then, set

$$A_* \mathbf{u} = \left(u_1^{a_{1,1}} u_2^{a_{1,2}} \cdots u_n^{a_{1,n}}, u_1^{a_{2,1}} u_2^{a_{2,2}} \cdots u_n^{a_{2,n}}, \ldots, u_1^{a_{n,1}} u_2^{a_{n,2}} \cdots u_n^{a_{n,n}}\right).$$

(This is the n-tuple whose j-th entry is $\prod\limits_{i=1}^{n} u_i^{a_{j,i}}$.) Notice that $A_* \mathbf{u}$ is again an n-tuple of invertible elements of R.

For a trivial example, $(I_n)_* \mathbf{u} = \mathbf{u}$ for every n-tuple $\mathbf{u}$. Other examples are

$$\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}_* (u_1, u_2) = \left(u_1^1 u_2^0, u_1^2 u_2^3\right) = \left(u_1, u_1^2 u_2^3\right);$$
$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}_* (u_1, u_2) = \left(u_1^1 u_2^2, u_1^0 u_2^3\right) = \left(u_1 u_2^2, u_2^3\right).$$

Exercise 5. Let $A \in \mathbb{Z}^{n\times n}$ and $B \in \mathbb{Z}^{n\times n}$. Prove that $A_* (B_* \mathbf{u}) = (AB)_* \mathbf{u}$ whenever $\mathbf{u}$ is an n-tuple of invertible elements of a commutative ring R.

A consequence of Exercise 5 is that every $A \in \mathrm{GL}_n(\mathbb{Z})$ and every n-tuple $\mathbf{u}$ of invertible elements of a commutative ring R satisfy

$$\left(A^{-1}\right)_* (A_* \mathbf{u}) = \left(\underbrace{A^{-1}A}_{=I_n}\right)_* \mathbf{u} = (I_n)_* \mathbf{u} = \mathbf{u}. \tag{1}$$

Now, if $\mathbf{u}$ is an n-tuple of invertible elements of a commutative ring R, and if $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ is a Laurent polynomial, then we can substitute the entries of $\mathbf{u}$ for the variables $x_1, x_2, \ldots, x_n$ in P, and obtain an element of R, which we denote by $P[\mathbf{u}]$. (It is more commonly denoted by $P(\mathbf{u})$, but we prefer to write $P[\mathbf{u}]$ due to a lesser chance of confusing it with a product when $\mathbf{u}$ is a 1-tuple.) For instance, if $n = 2$, $R = \mathbb{Q}$, $\mathbf{u} = (1, 3)$ and $P = \dfrac{x_1}{x_2} - \dfrac{x_2}{x_1}$, then $P[\mathbf{u}] = \dfrac{1}{3} - \dfrac{3}{1} = -\dfrac{8}{3}$. Of course, every $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ satisfies $P[\mathbf{x}] = P$, because substituting the variables $x_1, x_2, \ldots, x_n$ for themselves does not change P.

We can combine the notations we have now introduced to describe certain substitutions in Laurent polynomials. Namely, if $A \in \mathbb{Z}^{n\times n}$ is a matrix, then $A_* \mathbf{x}$ is an n-tuple of Laurent monomials (recall that $\mathbf{x} = (x_1, x_2, \ldots, x_n)$), and thus $P[A_* \mathbf{x}]$ is defined for every Laurent polynomial $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$. For instance,

$$P\left[\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}_* \mathbf{x}\right] = P\left[x_1, x_1^2 x_2^3\right].$$

Exercise 6. Let $A \in \mathrm{GL}_n(\mathbb{Z})$.

(a) If $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ is a Laurent polynomial, then show that P is irreducible if and only if $P\left[A_* \mathbf{x}\right]$ is irreducible.

(b) If $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ and $Q \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ are two Laurent polynomials, then show that P and Q are coprime if and only if $P\left[A_* \mathbf{x}\right]$ and $Q\left[A_* \mathbf{x}\right]$ are coprime.

Exercise 6 **(a)** shows that, for example, if $n = 2$, then a Laurent polynomial $P = P\left[x_1, x_2\right] \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ is irreducible if and only if $P\left[x_1, x_1 x_2\right] \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ is irreducible (because $\left(x_1, x_1 x_2\right) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}_* \mathbf{x}$).

If $\mathbf{v} = \left(v_1, v_2, \ldots, v_n\right)^T \in \mathbb{Z}^n$ is any vector, then we define a Laurent monomial $\mathbf{x}^{\mathbf{v}} \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ by $\mathbf{x}^{\mathbf{v}} = x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$. This is a monomial in $\mathbb{Z}[\mathbf{x}]$ when all entries of $\mathbf{v}$ are nonnegative.

Exercise 7. Let n be a positive integer. Let $\mathbf{v} \in \mathbb{Z}^n$ and let $g = \gcd \mathbf{v}$. Prove that there exists an $A \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathbf{x}^{\mathbf{v}} = x_1^g\left[A_* \mathbf{x}\right]$. (To make sense of the notation $x_1^g\left[A_* \mathbf{x}\right]$, recall that x_1^g is a Laurent monomial and thus a Laurent polynomial, and that $A_* \mathbf{x}$ is an n-tuple of Laurent monomials; thus $x_1^g\left[A_* \mathbf{x}\right]$ means the result of substituting $A_* \mathbf{x}$ for $\mathbf{x}$ in x_1^g.

This exercise is useful: It shows that every monomial $\mathbf{x}^{\mathbf{v}}$ can be obtained from the monomial x_1^g (for $g = \gcd \mathbf{v}$) by an invertible substitution of Laurent monomials for its variables. (Why invertible? Because (1) shows that it is undone by a similar substitution using the matrix A^{-1}.) Let us get some mileage out of this:

Exercise 8. Let $\mathbf{v} \in \mathbb{Z}^n$ be such that $\gcd \mathbf{v} = 1$. Prove that the Laurent polynomial $\mathbf{x}^{\mathbf{v}} + 1$ is irreducible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$.

Here are some examples for Exercise 8:

- For $n = 4$ and $\mathbf{v} = (2, 3, 0, -4)^T$, we have $\mathbf{x}^{\mathbf{v}} = x_1^2 x_2^3 x_4^{-4}$, and thus Exercise 8 yields that the Laurent polynomial $x_1^2 x_2^3 x_4^{-4} + 1$ is irreducible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$.

- For $n = 2$ and $\mathbf{v} = (6, 9)^T$, we have $\mathbf{x}^{\mathbf{v}} = x_1^6 x_2^9$, and Exercise 8 cannot be applied (because $\gcd \mathbf{v} = 3 \neq 1$). Nor does its consequent hold: The Laurent polynomial $x_1^6 x_2^9 + 1$ factors as $x_1^6 x_2^9 + 1 = \left(x_1^2 x_2^3 + 1\right)\left(x_1^4 x_2^6 - x_1^2 x_2^3 + 1\right)$, and thus is not irreducible.

- For $n = 2$ and $\mathbf{v} = (2, 4)^T$, we have $\mathbf{x}^{\mathbf{v}} = x_1^2 x_2^4$. Here, Exercise 8 cannot be applied either, but the Laurent polynomial $x_1^2 x_2^4 + 1$ is nevertheless irreducible. So the converse of Exercise 8 does not hold!

The following exercise might help solving Exercise 8:

Exercise 9. Let n be a positive integer. Let h be a positive integer. Let $P \in \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ be a Laurent polynomial which divides $x_1^h + 1$. Show that P has the form $\mathbf{x}^{\mathbf{v}} \cdot Q(x_1)$, where $\mathbf{x}^{\mathbf{v}}$ is a Laurent monomial and $Q \in \mathbb{Z}[t]$ is a polynomial in a single variable t.

Exercise 8 discussed irreducibility. Let us now study coprimality:

Exercise 10. Let $\mathbf{v} \in \mathbb{Z}^n$ and $\mathbf{w} \in \mathbb{Z}^n$. Prove that if the Laurent polynomials $\mathbf{x}^{\mathbf{v}} + 1$ and $\mathbf{x}^{\mathbf{w}} + 1$ are not coprime in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$, then the vectors $\mathbf{v}$ and $\mathbf{w}$ are proportional (i.e., there exists some integers b and c which are not both 0 and which satisfy $b\mathbf{v} = c\mathbf{w}$).

Note that more can be said: Namely, the Laurent polynomials $\mathbf{x}^{\mathbf{v}} + 1$ and $\mathbf{x}^{\mathbf{w}} + 1$ are coprime in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$ if and only if there exist no odd coprime integers b and c such that $b\mathbf{v} = c\mathbf{w}$. This is what Fomin and Zelevinsky need to prove [BFZ-CA3, Lemma 3.1]; but it is not needed for proving [BFZ-CA3, Proposition 1.8], and it is harder to show, so you can just as well ignore it.

0.5. Replacing [BFZ-CA3, Lemma 3.1]

Now, let us show how to use Exercise 10 in place of [BFZ-CA3, Lemma 3.1] in the proof of [BFZ-CA3, Proposition 1.8].

We use the notations of [BFZ-CA3]. Let $\Sigma = \left(\mathbf{x}, \widetilde{B}\right)$ be a seed of geometric type. Assume that the matrix $\widetilde{B}$ has full rank. We need to check that all seeds mutation equivalent to Σ are coprime.

We shall prove that

$$\text{the seed } \Sigma \text{ is coprime.} \tag{2}$$

Why is this sufficient for proving [BFZ-CA3, Proposition 1.8]? Well, assume that we have proven (2). Now, [BFZ-CA3, Lemma 3.2][6] yields that every seed mutation equivalent to Σ has full rank. Then, this seed must be coprime (by (2), applied to this seed instead of Σ) [7]. Therefore, [BFZ-CA3, Proposition 1.8] is proven under the assumption that (2) holds.

So it remains to prove (2). Indeed, recall what it means for the seed Σ to be coprime: It means that the polynomials $P_1, P_2, \ldots, P_n$ appearing in the exchange relations [BFZ-CA3, (1.3)] are coprime in $\mathbb{ZP}[\mathbf{x}]$. [8] Since our seed is of geometric

[6] which, by the way, is a generalization of [Lampe, Exercise 2.4 **(a)**]

[7] Here, we are using the fact that coprimality of a seed is defined in terms of the seed alone. Thus, if $\left(\mathbf{y}, \widetilde{C}\right)$ is a seed in $\mathcal{F}$ obtained by some mutations from an original seed $\left(\mathbf{x}, \widetilde{B}\right)$, then coprimality of the seed $\left(\mathbf{y}, \widetilde{C}\right)$ means that the polynomials appearing in its exchange relations are pairwise coprime in $\mathbb{ZP}[\mathbf{y}]$, not in $\mathbb{ZP}[\mathbf{x}]$.

[8] Recall that $\mathbb{ZP}$ is the Laurent polynomial ring $\mathbb{Z}\left[x_{n+1}^{\pm 1}, x_{n+2}^{\pm 1}, \ldots, x_m^{\pm 1}\right]$ here.

type, we have

$$p_j^+ = \prod_{\substack{n<i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}} \qquad \text{and} \qquad p_j^- = \prod_{\substack{n<i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}$$

for all j. This allows us to simplify the formula [BFZ-CA3, (1.3)] for $P_j(\mathbf{x})$ as follows:

$$\begin{aligned}
P_j(\mathbf{x}) &= \underbrace{p_j^+}_{=\prod\limits_{\substack{n<i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}}} \prod_{\substack{1\leq i\leq n;\\ b_{i,j}>0}} x_i^{b_{i,j}} + \underbrace{p_j^-}_{=\prod\limits_{\substack{n<i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}} \prod_{\substack{1\leq i\leq n;\\ b_{i,j}<0}} x_i^{-b_{i,j}} \\
&= \underbrace{\left(\prod_{\substack{n<i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}}\right)\left(\prod_{\substack{1\leq i\leq n;\\ b_{i,j}>0}} x_i^{b_{i,j}}\right)}_{=\prod\limits_{\substack{1\leq i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}}} + \underbrace{\left(\prod_{\substack{n<i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}\right)\left(\prod_{\substack{1\leq i\leq n;\\ b_{i,j}<0}} x_i^{-b_{i,j}}\right)}_{=\prod\limits_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}} \\
&= \prod_{\substack{1\leq i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}} + \prod_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}. \qquad (3)
\end{aligned}$$

We can further transform the right hand side by noticing that

$$\begin{aligned}
\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}} &= \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}\right)\left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}=0}} \underbrace{x_i^{-b_{i,j}}}_{=x_i^{-0}=x_i^0=1}\right) \\
&= \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}\right)\underbrace{\left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}=0}} 1\right)}_{=1} = \prod_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}.
\end{aligned}$$

Thus, (3) becomes

$$P_j(\mathbf{x}) = \prod_{\substack{1\leq i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}} + \underbrace{\prod_{\substack{1\leq i\leq m;\\ b_{i,j}<0}} x_i^{-b_{i,j}}}_{=\prod\limits_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}} = \prod_{\substack{1\leq i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}} + \prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}. \qquad (4)$$

So far we have been working in $\mathbb{Z}[\mathbf{x}]$. (Indeed, all exponents on the right hand side of (4) are nonnegative.) Let us now work in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$; this allows us to get an even simpler form for $P_j(\mathbf{x})$: Namely,

$$\begin{aligned}
P_j(\mathbf{x}) &= \underbrace{\prod_{\substack{1\leq i\leq m;\\ b_{i,j}>0}} x_i^{b_{i,j}}}_{\substack{=\left(\prod\limits_{1\leq i\leq m} x_i^{b_{i,j}}\right) \Big/ \left(\prod\limits_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{b_{i,j}}\right) \\ \text{(since the } i\text{'s which satisfy } b_{i,j}>0 \text{ are exactly} \\ \text{the } i\text{'s which do not satisfy } b_{i,j}\leq 0\text{)}}} + \prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}} \\
&= \left(\prod_{1\leq i\leq m} x_i^{b_{i,j}}\right) \Big/ \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{b_{i,j}}\right) + \prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}} \\
&= \left(\prod_{1\leq i\leq m} x_i^{b_{i,j}}\right) \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}\right) + \prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}} \\
&= \left(\prod_{1\leq i\leq m} x_i^{b_{i,j}} + 1\right) \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}\right). \qquad (5)
\end{aligned}$$

For every $j \in \{1, 2, \ldots, n\}$, let $\mathbf{b}_j$ be the j-th column of the matrix $\widetilde{B}$. Then, $\mathbf{b}_j = \left(b_{1,j}, b_{2,j}, \ldots, b_{m,j}\right)^T \in \mathbb{Z}^m$, and

$$\mathbf{x}^{\mathbf{b}_j} = \prod_{1\leq i\leq m} x_i^{b_{i,j}}.$$

Hence, (5) simplifies as follows:

$$P_j(\mathbf{x}) = \left(\underbrace{\prod_{1\leq i\leq m} x_i^{b_{i,j}}}_{=\mathbf{x}^{\mathbf{b}_j}} + 1\right) \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}\right) = \left(\mathbf{x}^{\mathbf{b}_j} + 1\right) \left(\prod_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}\right). \qquad (6)$$

Hence,

$$P_j(\mathbf{x}) \mid \mathbf{x}^{\mathbf{b}_j} + 1 \text{ in } \mathbb{Z}\left[\mathbf{x}^{\pm 1}\right] \qquad (7)$$

(because $\prod\limits_{\substack{1\leq i\leq m;\\ b_{i,j}\leq 0}} x_i^{-b_{i,j}}$ is just a Laurent monomial, and thus is invertible in $\mathbb{Z}\left[\mathbf{x}^{\pm 1}\right]$).

Now, let us finally prove that the seed Σ is coprime. To do so, we need to show that the polynomials $P_1, P_2, \ldots, P_n$ are pairwise coprime in $\mathbb{ZP}[\mathbf{x}]$. Indeed, let i and j be two distinct elements of $\{1, 2, \ldots, n\}$. We need to show that P_i and P_j are coprime in $\mathbb{ZP}[\mathbf{x}]$.

Assume the contrary. Then, there exists a non-invertible polynomial $g \in \mathbb{ZP}[\mathbf{x}]$ which divides each of P_i and P_j in $\mathbb{ZP}[\mathbf{x}]$. Consider this g. (We call g a "polynomial", but in truth it is a polynomial over $\mathbb{ZP}$, so it can have inverses of the frozen variables $x_{n+1}, x_{n+2}, \ldots, x_m$ (but not of $x_1, x_2, \ldots, x_n$).)

We have $g \mid P_j = P_j(\mathbf{x}) \mid \mathbf{x}^{\mathbf{b}_j} + 1$ in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$ (because of (7)). Similarly, $g \mid \mathbf{x}^{\mathbf{b}_i} + 1$ in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$.

The matrix $\widetilde{B}$ has full rank. Thus, its columns are linearly independent. In particular, no two of its columns are proportional. Thus, the vectors $\mathbf{b}_i$ and $\mathbf{b}_j$ (being two distinct columns of $\widetilde{B}$) are not proportional. Thus, the Laurent polynomials $\mathbf{x}^{\mathbf{b}_i} + 1$ and $\mathbf{x}^{\mathbf{b}_j} + 1$ must be coprime in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$ (because otherwise, Exercise 10 (applied to m, $\mathbf{b}_i$ and $\mathbf{b}_j$ instead of n, $\mathbf{v}$ and $\mathbf{w}$) would yield that the vectors $\mathbf{b}_i$ and $\mathbf{b}_j$ are proportional). In other words, every Laurent polynomial $h \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ which divides both $\mathbf{x}^{\mathbf{b}_i} + 1$ and $\mathbf{x}^{\mathbf{b}_j} + 1$ must be invertible in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$. Thus, g is invertible in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$ (since g is a Laurent polynomial which divides both $\mathbf{x}^{\mathbf{b}_i} + 1$ and $\mathbf{x}^{\mathbf{b}_j} + 1$).

We are almost done: We know that g is invertible in $\mathbb{Z}[\mathbf{x}^{\pm 1}]$ but non-invertible in $\mathbb{ZP}[\mathbf{x}]$. These two facts almost make a contradiction, but not quite, because $\mathbb{Z}[\mathbf{x}^{\pm 1}] \neq \mathbb{ZP}[\mathbf{x}]$ in general. But Exercise 4 **(b)** (applied to $P = g$) yields that either g or $-g$ is a (single) Laurent monomial. We WLOG assume that g is a Laurent monomial (because otherwise, we can just replace g by $-g$ and get back into this case). In other words, $g = x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}$ for some $k_1, k_2, \ldots, k_m \in \mathbb{Z}$. Consider these $k_1, k_2, \ldots, k_m$.

Since $x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} = g \in \mathbb{ZP}[\mathbf{x}]$, we must have $k_\ell \geq 0$ for all $\ell \leq n$ (because the only indeterminates which are invertible in $\mathbb{ZP}[\mathbf{x}]$ are $x_{n+1}, x_{n+2}, \ldots, x_m$). But if we have $k_\ell = 0$ for all $\ell \leq n$, then the monomial g is invertible in $\mathbb{ZP}[\mathbf{x}]$ (because it is a Laurent monomial in the indeterminates $x_{n+1}, x_{n+2}, \ldots, x_m$ only, and such monomials are already invertible in $\mathbb{ZP}$), which is impossible (because g is non-invertible in $\mathbb{ZP}[\mathbf{x}]$ by definition). Therefore, there exists some $\ell \leq n$ such that $k_\ell > 0$. Consider this ℓ. Clearly, $k_\ell > 0$ shows that $x_\ell \mid g$ in $\mathbb{ZP}[\mathbf{x}]$. Thus,

$$x_\ell \mid g \mid P_j = P_j(\mathbf{x}) = \prod_{\substack{1 \leq i \leq m; \\ b_{i,j} > 0}} x_i^{b_{i,j}} + \prod_{\substack{1 \leq i \leq m; \\ b_{i,j} < 0}} x_i^{-b_{i,j}} \qquad \text{(by (3))}$$

in $\mathbb{ZP}[\mathbf{x}]$. Hence, the term x_ℓ must appear in both monomials $\prod\limits_{\substack{1 \leq i \leq m; \\ b_{i,j} > 0}} x_i^{b_{i,j}}$ and $\prod\limits_{\substack{1 \leq i \leq m; \\ b_{i,j} < 0}} x_i^{-b_{i,j}}$ (because these two monomials surely cannot cancel each other, and because x_ℓ is not invertible in $\mathbb{ZP}[\mathbf{x}]$). Therefore, ℓ must both satisfy $b_{i,\ell} > 0$ (so that it can appear in the first monomial) and satisfy $b_{i,\ell} < 0$ (so that it can appear in the second monomial). But this is clearly absurd. This gives us the contradiction we wanted, and thus (2) is proven. Hence, [BFZ-CA3, Proposition 1.8] is proven.

References

[BFZ-CA3] Arkady Berenstein, Sergey Fomin, Andrei Zelevinsky, *Cluster algebras III: Upper bounds and double Bruhat cells*, arXiv preprint arXiv:math/0305434v3. (This was later published in: Duke Mathematical Journal, Vol. 126, No. 1, 2005.)

[Lampe] Philipp Lampe, *Cluster algebras*, `http://www.math.uni-bielefeld.de/~lampe/teaching/cluster/cluster.pdf` .

A version with my corrections: `https://www.dropbox.com/s/aush67ecrx6twlf/cluster - version 4 dec 2013 EV.pdf?dl=0`