Lemma 1: Let $U, V \in \mathbb{K}^{D\times M}$ be matrices with random entries and $s = (U^{tr}T_1^iV)_{i\geq 0}$. If $Z = \sum_{i=0}^{\infty} s^{(i)}/t^{i+1}$, then each entry of Z is in the form n_*/P, where P is the minimum scalar generator for s.

Proof: Rewrite U, V as $U = [u_1, u_2, \cdots, u_M], V = [v_1, v_2, \cdots, v_M]$, then

$$s^{(i)} = \begin{bmatrix} u_1^{tr}T_1^iv_1 & u_1^{tr}T_1^iv_2 & \cdots & u_1^{tr}T_1^iv_M \\ u_2^{tr}T_1^iv_1 & \cdots & \cdots & u_2^{tr}T_1^iv_M \\ \vdots & \ddots & \ddots & \vdots \\ u_M^{tr}T_1^iv_1 & \cdots & \cdots & u_M^{tr}T_1^iv_M \end{bmatrix}$$

Thus,

$$Z = \begin{bmatrix} \sum u_1^{tr}T_1^iv_1/t^{i+1} & \cdots & \cdots & \sum u_1^{tr}T_1^iv_M/t^{i+1} \\ \vdots & \ddots & \ddots & \vdots \\ \sum u_M^{tr}T_1^iv_1/t^{i+1} & \cdots & \cdots & \sum u_M^{tr}T_1^iv_M/t^{i+1} \end{bmatrix}$$

So each entry separately is what would be computed in the scalar case. Therefore, we can rewrite each entry as n_*/P for some numerator n_*.

Lemma 2: Let S be the minimum generating polynomial matrix for s and $D = ASB$ be the Smith normal form of S. Furthermore, let $s_1, \cdots s_M$ be invariant factors of S such that $s_1|s_2|\cdots|s_M$. Then, there exists a vector $\tilde{u}$ such that $\tilde{u}S = [0, \cdots, 0, s_M]$

Proof: Let $[b_1, \cdots, b_M]$ be the last row of B and $w = [\frac{s_Mb_1}{s1}, \frac{s_Mb_2}{s2}, \cdots, \frac{s_Mb_{M-1}}{s_{M-1}}, b_M]$ (since $s_i|s_M$), then

$$\begin{aligned}(wA)A^{-1}D &= [\frac{s_Mb_1}{s1}, \frac{s_Mb_2}{s2}, \cdots, \frac{s_Mb_{M-1}}{s_{M-1}}, b_M] \begin{bmatrix} s_1 & & \\ & \ddots & \\ & & s_M \end{bmatrix} \\ &= [s_Mb_1, s_Mb_2, \cdots, s_Mb_M] \\ &= [0, \cdots, 0, s_M]B\end{aligned}$$

Therefore, if we choose $\tilde{u} = wA$, we get $\tilde{u}S = (wA)A^{-1}DB^{-1} = [0, \cdots, 0, s_M]$ as needed.

Lemma 2 (bis): Let S be the minimum generating polynomial matrix for s. Then, there exists a vector $\tilde{u}$ such that $\tilde{u}S = [0, \ldots, 0, s_M]$, where s_M is the largest invariant factor of S.

Proof: By definition, s_M is the monic polynomial of least degree such that s_MS^{-1} has polynomial entries (indeed, s_M is a multiple of all the entries of the Smith form of S). Taking $\tilde{u}$ has the last row of s_MS^{-1}, we obtain $\tilde{u}S = [0 \ \cdots \ 0 \ s_M]$.

Alternative proof: The $(M+1) \times M$ matrix $\begin{bmatrix} S \\ 0 \ \cdots \ 0 \ 1 \end{bmatrix}$ has rank M. Writing $D = \deg(\det(S))$, the $(0, \ldots, 0, D)$-Popov left kernel basis for this matrix is a row vector $[\tilde{v} \ \ \lambda] \in$

$\mathbb{K}^{1\times(M+1)}$ such that $\tilde{v}S = [0, \ldots, 0, \lambda]$, where the polynomial λ is the GCD of the entries in the last column of S. By definition, s_D is divisible by λ, so that $\tilde{u} = \frac{s_D}{\lambda}\tilde{v}$ has the wanted property.

Remark: One may alternatively:

- compute the Smith form of S, along with the unimodular transformations, and use the formulas in the proof of Lemma 2 (first version);
- compute s_D via the inversion algorithm of Zhou-Labahn-Storjohann (Sec. 5.1, 2015), and then solve the system to find $\tilde{u}$.

The first solution is significantly more expensive if the full transformations are needed. Here we might be happy with only the transformations with entries reduced modulo the corresponding invariant factors, in which case both solutions have the same theoretic speed. Yet, note that computing the Smith form efficiently is randomized (Storjohann, 2003) and uses high-order lifting (not in LinBox), while the second solution is deterministic and uses tools close to approximant basis computation (already partially implemented in LinBox). In the second solution, the system solving can be done via minimal kernel basis (and also via lifting since the matrix S is reduced, but no issue with large degrees?).

Lemma 3: If $\sum_{i=0}^{\infty} s^{(i)}t^i = S^{-1}N$, then $deg(N)$ is less than or equal to $deg(S)$. TODO

Theorem 1: If $S^{-1}N = \sum_{i=0}^{\infty} s^{(i)}/t^{i+1}$, the first entry of the last row of $\tilde{u}N$ is the numerator of the generating function for $(u_M^{tr}T_1^i v_1)_{i\geq 0}$.

Proof: Let $S^{-1}N = \sum_{i=0}^{\infty} s^{(i)}/t^{i+1}$, then by lemma 1

$$N = S\sum_{i=0}^{\infty} s^{(i)}/t^{i+1} = S\begin{bmatrix} n_{1,1}/P & \cdots & n_{1,M}/P \\ \vdots & \ddots & \vdots \\ n_{M,1}/P & \cdots & n_{M,M}/P \end{bmatrix}$$

From theorem 1 of (randomXY-proof), we know that the i^{th} invariant factor of $XI - A$ is equal to the i^{th} invariant factor of S for generic choice of U, V. Thus, $s_D = P$ and by lemma 2

$$\begin{aligned} \tilde{u}N &= \tilde{u}S\begin{bmatrix} n_{1,1}/P & \cdots & n_{1,M}/P \\ \vdots & \ddots & \vdots \\ n_{M,1}/P & \cdots & n_{M,M}/P \end{bmatrix} \\ &= [0, \cdots, 0, P]\begin{bmatrix} n_{1,1}/P & \cdots & n_{1,M}/P \\ \vdots & \ddots & \vdots \\ n_{M,1}/P & \cdots & n_{M,M}/P \end{bmatrix} \\ &= [n_{M,1}, \cdots, n_{M,M}] \end{aligned}$$