

# Notes on Smith normal form and homology

Christophe Vuillot,<sup>1</sup> Alessandro Ciani,<sup>2</sup> and Barbara Terhal<sup>3,4</sup>

<sup>1</sup> *Université de Lorraine, CNRS, Inria, LORIA, F-54000, Nancy, France*

<sup>2</sup> *Institute for Quantum Computing Analytics (PGI-12),  
Forschungszentrum Jülich, 52425 Jülich, Germany*

<sup>3</sup> *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ, Delft, The Netherlands*

<sup>4</sup> *DIAM, EEMCS Faculty, Delft University of Technology,  
Van Mourik Broekmanweg 6, 2628 XE, Delft, The Netherlands*

We show how to compute homology groups using the Smith normal form.

## I. SMITH NORMAL FORM

**Definition 1.** (Smith normal form). Let  $A$  be a  $m \times n$  integer matrix  $A \in \mathbb{Z}^{m \times n}$ . The Smith normal form of  $A$  is a factorization  $A = USV$  where

- $S \in \mathbb{Z}^{m \times n}$  is “diagonal” meaning  $S_{ij} = 0$  for  $i \neq j$ ;
- Each diagonal entry of  $S$  divides the next one that is  $S_{ii} | S_{i+1,i+1}$  and they are called the elementary divisors of  $A$ ;
- $U \in \mathbb{Z}^{m \times m}$ ,  $V \in \mathbb{Z}^{n \times n}$  are invertible over  $\mathbb{Z}$  (unimodular), or equivalently  $\det U, \det V = \pm 1$ .

Every integer matrix has a unique Smith normal form. Also the number of nonzero elementary divisors coincides with the rank of the matrix.

## II. HOMOLOGY FROM THE SMITH NORMAL FORM

We use the same notation introduced in the discussion of homological rotor codes in Ref.[1]. Consider two integer matrices  $H_X \in \mathbb{Z}^{r_x \times n}$  and  $H_Z \in \mathbb{Z}^{r_z \times n}$  such that

$$H_X H_Z^T = 0. \quad (1)$$

This relation defines a chain complex  $\mathcal{C}$  where  $H_X$  and  $H_Z^T$  play the role of the boundary maps. We are interested in understanding the structure of the homology group

$$H_1(\mathcal{C}, \mathbb{Z}) = \ker(H_Z^T) / \text{im}(H_X). \quad (2)$$

Notice that in our convention  $H_X$  and  $H_Z^T$  are matrices that act from the right on  $r_x$ -dimensional and  $n$ -dimensional row vectors, respectively. This means that elements of  $\ker(H_Z^T)$  are  $n$ -dimensional row vectors  $\mathbf{v}$  such that  $\mathbf{v} H_Z^T = 0$ , while elements of  $\text{im}(H_X)$  are  $n$ -dimensional row vectors  $\mathbf{u}$  such that there exists a  $r_x$ -dimensional row vector  $\mathbf{v}$  that gives  $\mathbf{u} = \mathbf{v} H_X$ . Since  $H_Z^T$  is an integer matrix it has a unique Smith normal form

$$H_Z^T = U_Z S_Z V_Z, \quad (3)$$

with  $U_Z \in \mathbb{Z}^{n \times n}$ ,  $S_Z \in \mathbb{Z}^{n \times r_z}$  and  $V_Z \in \mathbb{Z}^{r_z \times r_z}$ . Analogously, we introduce the unique Smith normal form for  $H_X$

$$H_X = U_X S_X V_X, \quad (4)$$

with  $U_X \in \mathbb{Z}^{r_x \times r_x}$ ,  $S_X \in \mathbb{Z}^{r_x \times n}$  and  $V_X \in \mathbb{Z}^{n \times n}$ .

Let us consider  $S_Z$  and its kernel  $\ker(S_Z)$ .  $S_Z$  has the following structure

$$S_Z = \begin{pmatrix} z_1 & & & & \\ & z_2 & & & \\ & & \ddots & & \\ & & & z_{\text{rank}(H_Z)} & \\ & & & 0 & 0 \end{pmatrix} \quad (5)$$

with  $z_k$  the elementary divisors of  $H_Z^T$  and where the 0s denote zero matrices of suitable dimensions. Since  $S_Z$  is diagonal it is immediate to understand that its kernel is generated by the standard  $n$ -dimensional row unit vectors

$$\ker(S_Z) = \text{span}\{e_{\text{rank}(H_Z)+k}\}, \quad k = 1, \dots, n - \text{rank}(H_Z). \quad (6)$$

In fact, notice that the first  $\text{rank}(H_Z)$  of  $e_{\text{rank}(H_Z)+k}$  are all zeros and thus

$$e_{\text{rank}(H_Z)+k} S_Z = 0, \quad \forall k = 1, \dots, n - \text{rank}(H_Z). \quad (7)$$

From this it also follows that

$$e_{\text{rank}(H_Z)+k} U_Z^{-1} H_Z^T = e_{\text{rank}(H_Z)+k} S_Z V_Z = 0, \quad (8)$$

which shows that  $e_{\text{rank}(H_Z)+k} U_Z^{-1} \in \ker(H_Z^T)$ . Moreover, since  $H_Z^T$  and  $S_Z$  have same rank it follows that

$$\ker(H_Z^T) = \text{span}\{e_{\text{rank}(H_Z)+k} U_Z^{-1}, \quad k = 1, \dots, n - \text{rank}(H_Z)\}. \quad (9)$$

We remark that no notion of orthogonality is needed. From Eq. (9) we can interpret  $U_Z^{-1}$  as a map from the  $\ker(S_Z)$  to  $\ker(H_Z^T)$ . More colloquially  $e_{\text{rank}(H_Z)+k} U_Z^{-1}$  are simply the last  $n - \text{rank}(H_Z)$  rows of  $U^{-1}$ .

We proceed similarly for the image of  $H_X$ . Let us consider the image of  $S_X$ .  $S_X$  has the following structure

$$S_X = \begin{pmatrix} x_1 & & & & \\ & x_2 & & & \\ & & \ddots & & 0 \\ & & & x_{\text{rank}(H_X)} & \\ & & 0 & & 0 \end{pmatrix} \quad (10)$$

with  $x_\ell$  the elementary divisors of  $H_X$  and where the 0s denote zero matrices of suitable dimensions. Therefore the image of  $S_X$  are linear combinations of  $x_\ell e_\ell$ , that is

$$\text{im}(S_X) = \text{span}\{x_\ell e_\ell, \quad \ell = 1, \dots, \text{rank}(H_X)\}. \quad (11)$$

Now we want to show that if  $x_\ell e_\ell \in \text{im}(S_X)$ , then  $x_\ell e_\ell V_X \in \text{im}(H_X)$ . In fact,  $x_\ell e_\ell \in \text{im}(S_X)$  implies that  $\exists$  a  $r_x$ -dimensional integer vector  $\mathbf{v}_\ell$  [2] such that

$$\mathbf{v}_\ell S_X = x_\ell e_\ell \implies \mathbf{v}_\ell U_X^{-1} H_X V_X^{-1} = x_\ell e_\ell \implies \underbrace{\mathbf{v}_\ell U_X^{-1}}_{\mathbf{v}'_\ell} H_X = x_\ell e_\ell V_X, \quad (12)$$

which shows that  $\exists \mathbf{v}'_\ell$  such that  $\exists \mathbf{v}'_\ell H_X = x_\ell e_\ell V_X$  and thus  $x_\ell e_\ell V_X \in \text{im}(H_X)$ . Additionally,

$$\text{im}(H_X) = \text{span}\{x_\ell e_\ell V_X, \quad \ell = 1, \dots, \text{rank}(H_X)\}. \quad (13)$$

What this shows is that the image of  $H_X$  is generated by  $x_\ell V_X^{(\ell)}$  with  $V_X^{(\ell)}$  the  $\ell$ -th row of  $V_X$  with  $\ell = 1, \dots, \text{rank}(H_X)$ . In what follows, we will argue that the first  $\text{rank}(H_X)$  rows of  $V_X$  are related to the torsion part of  $H_1(\mathcal{C}, \mathbb{Z})$ . First, it can be shown that

$$H_1(\mathcal{C}, \mathbb{Z}) \cong \bigoplus_{\ell=1}^{\text{rank}(H_X)} \mathbb{Z}/x_\ell \oplus \mathbb{Z}^{r_x - \text{rank}(H_X)}. \quad (14)$$

The parts of  $H_1(\mathcal{C}, \mathbb{Z})$  isomorphic to  $\bigoplus_{\ell=1}^{\text{rank}(H_X)} \mathbb{Z}/x_\ell$  and to  $\mathbb{Z}^{r_x - \text{rank}(H_X)}$  are called the torsion part and free part of  $H_1(\mathcal{C}, \mathbb{Z})$ , respectively. From the previous discussion we conclude that the torsion part is generated by the first

$\text{rank}(H_X)$  rows of  $V_X$ , where we need to exclude the rows associated with the elementary divisors that are trivially 1, since these rows would be in  $\text{im}(H_X)$ . Accordingly, in the homological rotor code construction of Ref. [1] the  $\ell$ -th row of  $V_X$  with  $x_\ell > 1$  identifies a generalized Pauli  $X$  on a  $x_\ell$ -dit. We highlight the fact that the torsion part of  $H_1(\mathcal{C}, \mathbb{Z})$  is completely characterized by  $H_X$ , and if  $\text{rank}(H_X) = r_x$ , we can immediately conclude that  $H_1(\mathcal{C}, \mathbb{Z})$  has no free part.

Finally, we need to characterize the free part of  $H_1(\mathcal{C}, \mathbb{Z})$ . Let us define the  $n$ -dimensional row vectors

$$\mathbf{w}_\ell = \mathbf{e}_\ell V_X U_Z, \quad \ell = 1, \dots, \text{rank}(H_X). \quad (15)$$

We notice that  $\forall \ell = 1, \dots, \text{rank}(H_X)$

$$\mathbf{w}_\ell S_Z = \mathbf{e}_\ell V_X U_Z U_Z^{-1} H_Z^T V_Z^{-1} = \mathbf{e}_\ell V_X H_Z^T V_Z^{-1} = 0, \quad (16)$$

since the first  $\text{rank}(H_X)$  are in  $\ker(H_Z^T)$ . Eq. (16) implies that the first  $\text{rank}(H_Z^T)$  entries of the vectors  $\mathbf{w}_\ell$  are zeros and that  $\mathbf{w}_\ell \in \ker S_Z$ . Let us denote by  $\overline{W}$  the  $\text{rank}(H_X) \times n$  matrix whose rows are the  $\mathbf{w}_\ell$  vectors. The matrix  $\overline{W}$  has the following structure

$$\overline{W} = \begin{pmatrix} 0 & W \end{pmatrix}, \quad (17)$$

where  $W$  is the  $\text{rank}(H_X) \times (n - \text{rank}(H_Z^T))$  matrix with the nonzero elements of the  $\mathbf{w}_\ell$ . Remember that since  $\mathbf{w}_\ell \in \ker(S_Z)$  it follows that  $\mathbf{w}_\ell U_Z^{-1} \in \ker H_Z^T$ . Let us consider the Smith normal form of  $W$

$$W = U_W S_W V_W, \quad (18)$$

with  $U_W \in \mathbb{Z}^{\text{rank}(H_X) \times \text{rank}(H_X)}$ ,  $S_W \in \mathbb{Z}^{\text{rank}(H_X) \times (n - \text{rank}(H_Z^T))}$  and  $V_W \in \mathbb{Z}^{(n - \text{rank}(H_Z^T)) \times (n - \text{rank}(H_Z^T))}$ . Since  $\text{rank}(W) = \text{rank}(H_X)$ ,  $S_W$  has  $\text{rank}(H_X)$  elementary divisors. Let us consider  $V_W$  and in particular its first  $\text{rank}(H_X)$  rows and denote them by  $V_W^{(\ell)}$ . Eq. (18) implies that we can write the nonzero part of  $\mathbf{w}_\ell$  as a linear combination of the rows  $V_W^{(\ell)}$ . Specifically, adding  $\text{rank}(H_Z^T)$  zeros at the beginning of  $V_W^{(\ell)}$  we can write

$$\mathbf{w}_\ell = \sum_{\ell'=1}^{\text{rank}(H_X)} U_W^{(\ell \ell')} s_{\ell'} \begin{pmatrix} 0 & V_W^{(\ell')} \end{pmatrix}, \quad (19)$$

where  $U_W^{(\ell \ell')}$  is the elements of  $U_W$  at position  $(\ell, \ell')$  and  $s_{\ell'}$  the elementary divisors of  $S_W$ . Eq. (19) and Eq (16) imply that

$$\begin{pmatrix} 0 & V_W^{(\ell')} \end{pmatrix} \in \ker(S_Z), \quad (20)$$

but since the  $\mathbf{w}_\ell$  can be written as a linear combination of the  $\begin{pmatrix} 0 & V_W^{(\ell')} \end{pmatrix}$  we conclude that  $\begin{pmatrix} 0 & V_W^{(\ell')} \end{pmatrix} U_Z^{-1}$  is in the torsion part of  $H_1(\mathcal{C}, \mathbb{Z})$  for any  $\ell' = 1, \dots, \text{rank}(H_X)$ . How about the remaining  $n - \text{rank}(H_X) - \text{rank}(H_Z^T)$  rows of  $V_W$ ? Let us define additional  $n$ -dimensional row vectors  $\mathbf{w}_{\text{rank}(H_X)+k}$  as

$$\mathbf{w}_{\text{rank}(H_X)+k} = \begin{pmatrix} 0 & V_W^{(\text{rank}(H_X)+k)} \end{pmatrix}, \quad k = 1, \dots, n - \text{rank}(H_Z^T) - \text{rank}(H_X). \quad (21)$$

Clearly, by construction, these are also in  $\ker(S_Z)$ , but since they are linearly independent of the first  $\text{rank}(H_X)$  rows, we conclude that  $\mathbf{w}_\ell U_Z^{-1}$  is not in the torsion part of  $H_1(\mathcal{C}, \mathbb{Z})$  and so they must be in the free part and indeed generate it.

To summarize, using the definitions of the  $\mathbf{w}_\ell$  for  $\ell = 1, \dots, \text{rank}(H_X)$  in Eq. (15) and of  $\mathbf{w}_{\text{rank}(H_X)+k}$  for  $k = 1, \dots, n - \text{rank}(H_Z^T) - \text{rank}(H_X)$  in Eq. (21),  $H_1(\mathcal{C}, \mathbb{Z})$  is generated by

$$L_X = \begin{pmatrix} L_X^{(\text{tor})} \\ L_X^{(\text{free})} \end{pmatrix} = \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{\text{rank}(H_X)} \\ \mathbf{w}_{\text{rank}(H_X)+1} \\ \vdots \\ \mathbf{w}_{n-\text{rank}(H_Z^T)-\text{rank}(H_X)} \end{pmatrix} U_Z^{-1}. \quad (22)$$


---

- [1] C. Vuillot, A. Ciani, and B. M. Terhal, Homological Quantum Rotor Codes: Logical Qubits from Torsion, [arXiv e-prints](#), [arXiv:2303.13723 \(2023\)](#), [arXiv:2303.13723 \[quant-ph\]](#).
- [2] The vectors  $\mathbf{v}_\ell$  are simply the  $r_x$ -dimensional standard unit vectors.