Elementary Column Matrices and the Smith Normal Form

Ethan Kalika and Chloe Borentain

December 2024

Linear Algebra Review

- Given an $m \times n$ matrix A there are three types of **elementary row operations**.
  - **Adding a multiple of a row**, that is adding c times row i to row j.
  - **Swapping 2 rows**, that is putting row i in the position of row j and j in the position of i.
  - **Scaling a row**, that is multiplying each entry in a row by some scalar c.

Unimodular Elementary Row Operations

- The 3 unimodular elementary row operations are almost exactly the same as the same as the elementary row operations except we can only add integral multiples or rows and for the third operation we are only allowed to scale by -1.
- The **unimodular elementary row operations** defined are as follows.
  - **Adding a multiple of a row**, that is adding c times row i to row j where $c \in \mathbb{Z}$.
  - **Swapping 2 rows**, that is putting row i in the position of row j and j in the position of i.
  - **Scaling a row**, that is multiplying each entry in a row by some scalar -1.

Matrix Representation

- We can express the unimodular elementary row operations as left multiplication by elementary matrices.
- Given an $m \times n$ matrix A and an integer t we make the following notations.
  - We will denote the elementary matrix corresponding to adding t times row j to row i by $\rho_1(m, i, j, t)$.
  - We will denote the elementary matrix corresponding to swapping rows i and j by $\rho_2(m, i, j)$.
  - We will denote the elementary matrix corresponding to multiplying row i by -1 as $\rho_3(m, i)$.

Matrix Representation Continued

- We define $\rho_1(m,i,j,t)$, $\rho_2(m,i,j)$, and $\rho_3(m,i)$ as follows.
  - $\rho_1(m,i,j,t)_{ij} = t$.
  - $\rho_2(m,i,j)_{ij} = \rho_2(m,i,j)_{ji} = 1$ and $\rho_2(m,i,j)_{ii} = \rho_2(m,i,j)_{jj} = 0$.
  - $\rho_3(m,i)_{ii} =$ -1.
  - All entries not explicitly defined are as they would be in I_m
- Multiplying an $m \times n$ matrix A on the left by one these matrices will perform the corresponding unimodular elementary row operation on A

$$\rho_1(4,3,1,7) = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 7&0&1&0 \\ 0&0&0&1 \end{pmatrix},\ \rho_2(3,1,3) = \begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix},\ \rho_3(3,2) = \begin{pmatrix} 1&0&0 \\ 0&-1&0 \\ 0&0&1 \end{pmatrix}$$

Figure: Here are some examples of what such matrices may look like. [HEO05]

Unimodular Elementary Column Operations

- The **unimodular elementary column operations** are defined in an analogous way to the unimodular elementary row operations.
  - **Adding a multiple of a column**, that is adding c times row i to row j where $c \in \mathbb{Z}$.
  - **Swapping 2 columns**, that is putting row i in the position of row j and j in the position of i.
  - **Scaling a column**, that is multiplying each entry in a row by some scalar -1.

Matrix Representation

- We can express the unimodular elementary column operations as right multiplication by elementary matrices.
- Given an $m \times n$ matrix A and an integer t we make the following notations.
  - We will denote the elementary matrix corresponding to adding a t times row j to row i by $\gamma_1(n, i, j, t)$.
  - We will denote the elementary matrix corresponding to swapping rows i and j by $\gamma_2(n, i, j)$.
  - We will denote the elementary matrix corresponding to multiplying row i by -1 as $\gamma_3(n, i)$.

Matrix Representation Continued

- We define $\gamma_1(n, i, j, t)$, $\gamma_2(n, i, j)$, and $\gamma_3(n, i)$ as follows.
  - $\gamma_1(n, i, j, t)_{ij} = t$.
  - $\gamma_2(n, i, j)_{ij} = \gamma_2(n, i, j)_{ji} = 1$ and $\gamma_2(n, i, j)_{ii} = \gamma_2(n, i, j)_{jj} = 0$.
  - $\gamma_3(n, i)_{ii} =$ -1.
  - All entries not explicitly defined are as they would be in I_n
- Multiplying an $m \times n$ matrix A on the right by one these matrices will perform the corresponding unimodular elementary column operation on A

What is $GL(n, \mathbb{Z})$?

- In the coming slides we will often refer to $GL(n, \mathbb{Z})$.
- It is important to note here that we typically define matrices in a ring on fields like $\mathbb{R}$ or $\mathbb{Z}_p$.
- $\mathbb{Z}$ is not a field, so we take $GL(n, \mathbb{Z})$ to mean the group generated by invertible $n \times n$ integral matrices whose inverses are also integral.

Smith Normal From

- The integral $m \times n$ matrix M is said to be in **Smith normal form (SNF)** if the following conditions hold.
  - $M_{ij} = 0$ whenever $i \neq j$
  - $M_{ii} \geq 0$ for $1 \leq i \leq \min(m, n)$
  - For $1 \leq i \leq \min(m, n)$ we have $M_{ii} | M_{i+1,i+1}$

Existence and Uniqueness of SNF

Theorem

Let M be any $n \times n$ matrix over $\mathbb{Z}$. Then we can put M into SNF by applying a sequence of elementary unimodular row and column operations to M. Hence, there exists an $A \in GL(m, \mathbb{Z})$ and $B \in GL(n, \mathbb{Z})$ such that AMB is in SNF.

Theorem

Let M be an $m \times n$ matrix over $\mathbb{Z}$. If AMB and CMD are both in SMF, with $A, C \in GL(m, \mathbb{Z})$ and $B, D \in GL(n, \mathbb{Z})$, then $AMB = CMD$.

SNF Example

- [HEO05] provides and algorithm for finding the SNF of a given matrix
  - This algorithm also serves as an algorithmic proof of the existence theorem for the SNF.
- The following illustrates a matrix and its corresponding SNF.

$$M = \begin{pmatrix} 1 & -2 & -1 & 1 & 1 & -3 \\ -1 & 2 & -3 & 1 & -3 & -9 \\ 1 & -2 & -5 & 3 & -1 & -3 \\ 1 & -2 & 1 & 0 & 3 & 8 \\ 4 & -8 & -4 & 4 & 6 & 2 \end{pmatrix}$$

SNF Example Continued

- In the image below, M is the SNF of the matrix on the previous slide and AMB is equal to the matrix on the previous slide.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ -3 & 0 & 1 & 2 & 0 \\ 4 & 1 & 1 & 4 & -2 \\ 7 & 2 & 1 & 6 & -3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & -3 & 25 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & -11 & 2 & 0 \\ 0 & 0 & 1 & -11 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- M is in SNF because the only nonzero entries are on the diagonal and the divisibility condition for entries on the diagonal is also met.

How are Matrices Related to Group Theory

- Any abelian group can be expressed as a direct sum of cycles.
- For example if we have $K := 2\mathbb{Z} \oplus 6\mathbb{Z} \oplus 12\mathbb{Z}$ and $G := \mathbb{Z}^3/K \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ then the elements of K all lie in the row space of the matrix

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{bmatrix}.$$

- K however, is isomorphic to $\mathbb{Z}^3$ regardless of the coefficients of the cyclic groups, so while we can represent its elements as elements of a row space, it makes more sense to associate the matrix A with G because G will vary depending on the coefficients in K.
- In fact performing modular elementary row operations on K does not change its row space, so G can be represented by any matrix derivable from A by elementary row operations.

How is SNF related to Group Theory

- Let the $m \times n$ matrix M represent some cyclic group K.
  - Note that the matrix representation can be rectangular if any coefficients in K are 0. All such summands are moved to the end of the sum by convention.
- Now let $A \in GL(m, \mathbb{Z})$ and $B \in GL(n, \mathbb{Z})$
- Notice that AM is also an $m \times n$ matrix the rows of which are linearly independent linear combinations of rows of M. This means that AM and M have the same row space and hance both represent $\mathbb{Z}^n/K$.

How is SNF related to Group Theory Continued

- Multiplying on the right by B is the equivalent of performing column operations on M, which does change the row space. However, multiplication of vector representations of elements of K by B serves as an isomorphism of K into some other group because multiplication by B is an invertible linear transformation and so follows the homomorphism property.
- Because of this the abelian groups $\mathbb{Z}^n/K$ and $\mathbb{Z}^n/K'$, where K and K' represented by M and AMB respectively, are isomorphic.
- This is true in particular when $M = ANB$ where N is the SMF of M.

The Divisibility Condition

- An abelian group G has type $(d_1, \ldots, d_n)$, for $d_i \in \mathbb{N}_0$ if it is isomorphic to the direct sum of cyclic groups $\mathbb{Z}/d_i\mathbb{Z}$. We say that $(d_1, \ldots, d_n)$ satisfies the **divisibility condition** if $d_i \neq 1$ for $1 \leq i \leq n$, and $d_i | d_{i+1}$ for $1 \leq i \leq n$.

Theorem

A finitely generated abelian group has type $(d_1, \ldots, d_n)$ for some $d_i \in \mathbb{N}_0$ that satisfy the divisibility criterion.

Uniqueness of Type

Theorem

Suppose that the abelian group G has type $(d_1, \ldots, d_n)$ and also has type $(c_1, \ldots, c_m)$, where $(d_1, \ldots, d_n)$ and $(c_1, \ldots, c_m)$ both satisfy the divisibility condition. Then $m = n$ and $d_i = c_i$ for $1 \leq i \leq n$.

- Note that the divisibility condition is necessary here because for example, the abelian groups of the types (4, 3, 5), (12, 5), (4, 15), (3, 20), and (60) are all isomorphic to each other, but have different number of factors.

Finding Abelian Invariants of $G/[G,G]$

- The following example is from [HEO05].
- The principal use of SNF in CTG is for finding invariants of $G/[G,G]$ in a finitely presented group G.
- We are given the following group presentation. (Relations without an "=" sign are called relators are equal to 1 by convention).

$$G := \langle x, y, z \mid (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2 \rangle.$$

- If we take $G/[G,G]$, then x, y, and z become representatives of cosets that commute, so we can write the following.

$$G/[G,G] = \mathrm{Ab}\langle x, y, z \mid 2x+2y-2z, -2x+4y+2z, 2x-4y-2z \rangle$$

Finding Abelian Invariants of $G/[G,G]$ Continued

- We can represent $G/[G,G]$ by

$$M = \begin{bmatrix} 2 & 2 & -2 \\ -2 & 4 & 2 \\ 2 & -4 & -2 \end{bmatrix}$$

because $2x + 2y - 2z$, $-2x + 4y + 2z$, and $2x - 4y - 2z$ can all be treated as generators for cyclic subgroups of $\mathbb{Z}^3$ which can be added to create a subgroup, K of $\mathbb{Z}^3$ and $G/[G,G] \cong \mathbb{Z}^n/K$.

- M however, does not tell us much about K and $G/[G,G]$ so we can bring it into SNF as shown below.

$$N = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Finding Abelian Invariants of $G/[G,G]$ Continued

- From the SNF of M we see that $G/[G,G] \cong H := \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$.
- The matrix B also shows us the epimorphism, μ from $G/[G,G]$ to H.
- More specifically, it shows us that if a, b, and c are taken to be the generators of H, then $\mu(x) = a - b + c$, $\mu(y) = b$, and $\mu(z) = c$.

References


D.F. Holt, B. Eick, and E.A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and Its Applications, CRC Press, 2005.