On the Smith normal form of dual integer matrices

Baraah Maya

Brno University of Technology - Czech Republic

Graz (10 - 14 July, 2023)

Smith normal form of a matrix

- Let A be a nonzero matrix over a **principal ideal domain PID**. There exist two matrices U and V such that:

$$UAV = \begin{pmatrix} \alpha_0 & 0 & 0 & & & & 0 \\ 0 & \alpha_1 & 0 & & & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ & & & \alpha_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

where U and V are invertible matrices.

Smith normal form of a matrix

- Let A be a nonzero matrix over a **principal ideal domain PID**. There exist two matrices U and V such that:

$$UAV = \begin{pmatrix} \alpha_0 & 0 & 0 & & & & 0 \\ 0 & \alpha_1 & 0 & & & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ & & & \alpha_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

  where U and V are invertible matrices.
- The Smith normal form over a PID is **unique**.

Smith normal form of a matrix

$$UAV = \begin{pmatrix} \alpha_0 & 0 & 0 & & & & 0 \\ 0 & \alpha_1 & 0 & & & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ & & & \alpha_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

- $\alpha_i \mid \alpha_{i+1}$ for all $1 \leq i \leq r$.
- $\alpha_i = \frac{d_i(A)}{d_{i-1}(A)}$.
  $d_i(A)$ is the greatest common divisor of all $i \times i$ minors of A and $d_0(A) := 1$.

The goal

Finding Smith normal form of a matrix over a ring which is not a principal ideal domain.

The ring of dual integers

- Let us consider the ring:

$$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

The ring of dual integers

- Let us consider the ring:

$$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

- Let us consider the polynomial:

$$f(x) = x^2 - 2ax + a^2; \qquad a \in \mathbb{Z}$$

The ring of dual integers

- Let us consider the ring:

$$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

- Let us consider the polynomial:

$$f(x) = x^2 - 2ax + a^2; \qquad a \in \mathbb{Z}$$

- This polynomial has one root in $\mathbb{Z}$:

$$x = a$$

The ring of dual integers

- Let us consider the ring:

$$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

- Let us consider the polynomial:

$$f(x) = x^2 - 2ax + a^2; \qquad a \in \mathbb{Z}$$

- This polynomial has one root in $\mathbb{Z}$:

$$x = a$$

- It has infinitely many roots in $\mathbb{Z}[\varepsilon]$:

$$x = a + b\varepsilon$$

where $b \in \mathbb{Z}$.

- $$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

- $$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$
- The set of zero divisors:
$$Z(\mathbb{Z}[\varepsilon]) = \{b\varepsilon; \quad b \in \mathbb{Z}\} = \varepsilon\mathbb{Z}[\varepsilon]$$

- $$\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \quad a, b \in \mathbb{Z}, \quad \varepsilon^2 = 0\}$$

- The set of units:

$$U(\mathbb{Z}[\varepsilon]) = \{\pm 1 + b\varepsilon; \quad b \in \mathbb{Z}\}$$

The division in $\mathbb{Z}[\varepsilon]$

Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers.

$$\frac{a}{b} = \frac{(a_0 + a_1\varepsilon)(b_0 - b_1\varepsilon)}{(b_0 + b_1\varepsilon)(b_0 - b_1\varepsilon)} = \frac{a_0}{b_0} + \frac{a_1 b_0 - a_0 b_1}{b_0^2}\varepsilon$$

where $b_0 \neq 0$.

- Let $a, b \in \mathbb{Z}$. There exits a unique pair (q, r) such that:

$$a = bq + r$$

where $r = 0$ or $|r| < |b|$.

- Let $a, b \in \mathbb{Z}$. There exits a unique pair (q, r) such that:

$$a = bq + r$$

where $r = 0$ or $|r| < |b|$.

- Let $a, b \in \mathbb{Z}[\varepsilon]$. There exit infinitely many (q, r) such that:

$$a = bq + r$$

- Let $a, b \in \mathbb{Z}$. There exits a unique pair (q, r) such that:

$$a = bq + r$$

where $r = 0$ or $|r| < |b|$.

- Let $a, b \in \mathbb{Z}[\varepsilon]$. There exit infinitely many (q, r) such that:

$$a = bq + r$$

- Let $a = a_0 + a_1\varepsilon$. The pseudo-norm of a is:

$$N(a) = \sqrt{a_0^2 + a_1^2}$$

The division with remainder

To divide $a = a_0 + a_1\varepsilon$ by $b = b_0 + b_1\varepsilon$:

- Find q_0 and r_0 such that $a_0 = b_0 q_0 + r_0$.
- Compute:

$$Q_r = \lfloor \frac{a_1 - b_1 q_0}{b_0} \rfloor, \qquad r_1 = a_1 - b_1 q_0 - b_0 Q_r$$

$$Q_s = \lfloor \frac{a_1 - b_1 q_0}{b_0} \rfloor - 1, \qquad s_1 = a_1 - b_1 q_0 - b_0 Q_s$$

- Put:

$$r = r_0 + r_1\varepsilon, \qquad q_r = q_0 + Q_1\varepsilon$$

$$s = r_0 + s_1\varepsilon, \qquad q_s = q_0 + Q_s\varepsilon$$

Then:

$$a = bq_r + r$$

$$a = bq_s + s$$

The divisors of a dual integer

Let $a = a_0 + a_1\varepsilon$ be a dual integer.

- Find all divisors of a_0 in $\mathbb{Z}$:

$$\{d_0 = 1, d_1, d_2, \dots, d_m\}$$

- For $1 \leq i \leq m$, solve the congruence:

$$\frac{a_0}{d_i} X \equiv a_1 (mod \quad d_i)$$

- If X is a solution in $\{0, 1, 2, \dots, d_i - 1\}$, then there exist infinitely many divisors of the form:

$$d_i + (X + \frac{d_i}{c} k)\varepsilon; \qquad k \in \mathbb{Z}$$

where $c = \gcd(\frac{a_0}{d_i}, a_1, d_i)$.

The primes in $\mathbb{Z}[\varepsilon]$

- Let $p = p_0 + p_1\varepsilon$ be a dual integer. Then p is a prime in $\mathbb{Z}[\varepsilon]$ if:

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \qquad or \qquad p \mid b$$

- **There are no primes in $\mathbb{Z}[\varepsilon]$.**

The irreducible elements in $\mathbb{Z}[\varepsilon]$

- The dual integer $a = a_0 + a_1\varepsilon$ is an irreducible element in $\mathbb{Z}[\varepsilon]$ if:
$$a = bc \quad \Rightarrow \quad b \text{ is a unit or } c \text{ is a unit.}$$

- The irreducible elements in $\mathbb{Z}[\varepsilon]$ are the primes in $\mathbb{Z}$ or:
$$a = p^k + a_1\varepsilon$$
where p is a prime in $\mathbb{Z}$, $k \geq 1$ and $\gcd(p, a_1) = 1$.

The common divisors of two dual integers

Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers.

- Find all common divisors of the integers a_0 and b_0 in $\mathbb{Z}$:

$$\{d_0 = 1, d_1, d_2, \dots, d_m\}$$

- For $1 \leq i \leq m$, solve the system:

$$\frac{a_0}{d_i} X \equiv a_1 (mod \quad d_i)$$

$$\frac{b_0}{d_i} X \equiv b_1 (mod \quad d_i)$$

- If X is a solution in $\{0, 1, 2, \dots, d_i - 1\}$, then there exist infinitely many common divisors of the form:

$$d_i + (X + \frac{d_i}{c} k)\varepsilon; \qquad k \in \mathbb{Z}$$

where $c = \gcd(\frac{a_0}{d_i}, \frac{b_0}{d_i}, a_1, b_1, d_i)$.

The greatest common divisor of two dual integers

Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$, $g = g_0 + g_1\varepsilon$ be dual integers such that:

- $g \mid a$ and $g \mid b$ in $\mathbb{Z}[\varepsilon]$.
- If $d = d_0 + d_1\varepsilon$ is another common divisor of a and b, then $d \mid g$ in $\mathbb{Z}[\varepsilon]$.
- There exist two dual integers x and y such that:

$$ax + by = g$$

The dual integer g is called **good greatest common divisor** of a and b in $\mathbb{Z}[\varepsilon]$.

Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers and $g = g_0 + g_1\varepsilon$ a common divisor of a and b with the greatest real part among all other common divisors. Let $m = m_0 + m_1\varepsilon$ be another common divisor such that:

- $m_0 \mid g_0$ in $\mathbb{Z}$,
- $m \nmid g$ in $\mathbb{Z}[\varepsilon]$.

Then **there does not exist the greatest common divisor** of a and b in $\mathbb{Z}[\varepsilon]$.

The existence of the greatest common divisor of two dual integers

- Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers, and let d be the greatest integer for which the system:

$$\frac{a_0}{d}X \equiv a_1 (mod \quad d)$$

$$\frac{b_0}{d}X \equiv b_1 (mod \quad d)$$

is solvable. The greatest common divisor of a and b in $\mathbb{Z}[\varepsilon]$ exists if and only if the considered system has a **unique solution** X in $\mathbb{Z}_d = \{0, 1, 2, \ldots, d-1\}$. Then:

$$\gcd(a, b) = \{d + (X + dk)\varepsilon; k \in \mathbb{Z}\}$$

The existence of the greatest common divisor of two dual integers

- Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers, and let d be the greatest integer for which the system:

$$\frac{a_0}{d}X \equiv a_1 (mod \quad d)$$

$$\frac{b_0}{d}X \equiv b_1 (mod \quad d)$$

is solvable. The greatest common divisor of a and b in $\mathbb{Z}[\varepsilon]$ exists if and only if the considered system has a **unique solution** X in $\mathbb{Z}_d = \{0, 1, 2, \ldots, d-1\}$. Then:

$$\gcd(a, b) = \{d + (X + dk)\varepsilon; k \in \mathbb{Z}\}$$

- $\gcd(a, b)$ is a good gcd $\quad \Leftrightarrow \quad \gcd(a_0, b_0) = d$

- Let $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$. Then:

$$< a, b >=< d >$$

- Let $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$. Then:

$$< a, b >=< d >$$

- Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers. The ideal $< a, b >$ is a principal ideal in $\mathbb{Z}[\varepsilon]$ if and only if there exists a good greatest common divisor of a and b in $\mathbb{Z}[\varepsilon]$.

- Let $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$. Then:

$$< a, b >=< d >$$

- Let $a = a_0 + a_1\varepsilon$, $b = b_0 + b_1\varepsilon$ be two dual integers. The ideal $< a, b >$ is a principal ideal in $\mathbb{Z}[\varepsilon]$ if and only if there exists a good greatest common divisor of a and b in $\mathbb{Z}[\varepsilon]$.

- **The ring $\mathbb{Z}[\varepsilon]$ is not a principal ideal ring.**

The inverse of a dual matrix

Let $A = A_0 + A_1\varepsilon$ be a dual integer matrix. The matrix A is invertible if and only if its determinant is of the form

$$\det(A) = \pm 1 + k\varepsilon$$

Then:

$$A^{-1} = A_0^{-1} - A_0^{-1} A_1 A_0^{-1} \varepsilon$$

The Smith normal form of a dual integer matrix

Let $A = A_0 + A_1\varepsilon$ be a dual integer matrix. The matrix A can be written in the Smith normal form if there are two invertible matrices $U = U_0 + U_1\varepsilon$ and $V = V_0 + V_1\varepsilon$ and a diagonal matrix $S = S_0 + S_1\varepsilon$ such that:

$$UAV = S$$

The Smith normal form of a dual integer matrix

Let $A = A_0 + A_1\varepsilon$ be a dual integer matrix. The matrix A can be written in the Smith normal form if there are two invertible matrices $U = U_0 + U_1\varepsilon$ and $V = V_0 + V_1\varepsilon$ and a diagonal matrix $S = S_0 + S_1\varepsilon$ such that:

$$UAV = S$$

The matrix S_0 is the Smith normal form of A_0.

The existence of the Smith normal form of a dual matrix

Let $A = A_0 + A_1\varepsilon$ be a dual integer matrix. The necessary and sufficient condition for the existence of the Smith normal form of a dual integer matrix is the existence of a **good greatest common divisor** Δ_i of all $i \times i$ minors of the matrix A, i.e.,

$$\Delta_i = d_i + s_i\varepsilon$$

where d_i is the greatest common divisor of all $i \times i$ minors of the matrix A_0. Then:

$$\alpha_i = \frac{\Delta_i}{\Delta_{i-1}}$$

for $1 \leq i \leq r$ and $\Delta_{i-1} = 1$.

The uniqueness of the Smith normal form

Let $A = A_0 + A_1\varepsilon$ be a dual integer matrix. If the matrix A can be written in the Smith normal form, then its representation in the Smith normal form is unique.

Thank you