

Smith Normal Form and Combinatorics

Richard P. Stanley

December 31, 2017

Smith normal form

A : $n \times n$ matrix over commutative ring **R** (with 1)

Suppose there exist **P, Q** $\in \text{GL}(n, R)$ such that Smith normal form (SNF) of A .

Smith normal form

A: $n \times n$ matrix over commutative ring **R** (with 1)

Suppose there exist **P**, **Q** $\in \text{GL}(n, R)$ such that Smith normal form (SNF) of **A**.

Note. (1) Can extend to $m \times n$.

$$(2) \text{ unit} \cdot \det(A) = \det(B) = d_1^n d_2^{n-1} \cdots d_n.$$

Thus SNF is a refinement of det.

Who is Smith?

Henry John Stephen Smith

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career
- twice president of London Mathematical Society

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career
- twice president of London Mathematical Society
- 1861: SNF paper in *Phil. Trans. R. Soc. London*

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career
- twice president of London Mathematical Society
- 1861: SNF paper in *Phil. Trans. R. Soc. London*
- 1868: Steiner Prize of Royal Academy of Sciences of Berlin

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career
- twice president of London Mathematical Society
- 1861: SNF paper in *Phil. Trans. R. Soc. London*
- 1868: Steiner Prize of Royal Academy of Sciences of Berlin
- died 9 February 1883 (age 56)

Who is Smith?

Henry John Stephen Smith

- born 2 November 1826 in Dublin, Ireland
- educated at Oxford University (England)
- remained at Oxford throughout his career
- twice president of London Mathematical Society
- 1861: SNF paper in *Phil. Trans. R. Soc. London*
- 1868: Steiner Prize of Royal Academy of Sciences of Berlin
- died 9 February 1883 (age 56)
- April 1883: shared *Grand prix des sciences mathématiques* with Minkowski



Row and column operations

From now on, assume $R = \mathbb{Z}$.

Can put a matrix into SNF by the following operations.

- Add a multiple of a row to another row.
- Add a multiple of a column to another column.
- Multiply a row or column by a **unit** in R .

Row and column operations

From now on, assume $R = \mathbb{Z}$.

Can put a matrix into SNF by the following operations.

- Add a multiple of a row to another row.
- Add a multiple of a column to another column.
- Multiply a row or column by a **unit** in R .

Over a field, SNF is **row reduced echelon form** (with all unit entries equal to 1).

Existence of SNF

Theorem (Smith). A has a unique SNF up to units.

Algebraic interpretation of SNF

A: an $n \times n$ matrix over \mathbb{Z} with rows
 $v_1, \dots, v_n \in R^n$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

Algebraic interpretation of SNF

A: an $n \times n$ matrix over \mathbb{Z} with rows
 $v_1, \dots, v_n \in R^n$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

Theorem.

$$\mathbb{Z}^n / (v_1, \dots, v_n) \cong (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_n\mathbb{Z}).$$

Algebraic interpretation of SNF

A: an $n \times n$ matrix over \mathbb{Z} with rows
 $v_1, \dots, v_n \in R^n$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

Theorem.

$$\mathbb{Z}^n / (v_1, \dots, v_n) \cong (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_n\mathbb{Z}).$$

$\mathbb{Z}^n / (v_1, \dots, v_n)$: **(Kasteleyn) cokernel** of A

An explicit formula for SNF

A: an $n \times n$ matrix over \mathbb{Z} with $\det(A) \neq 0$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

An explicit formula for SNF

A: an $n \times n$ matrix over \mathbb{Z} with $\det(A) \neq 0$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

Theorem. $e_1 e_2 \cdots e_i$ is the gcd of all $i \times i$ minors of A .

minor: determinant of a square submatrix

An explicit formula for SNF

A: an $n \times n$ matrix over \mathbb{Z} with $\det(A) \neq 0$

$\text{diag}(e_1, e_2, \dots, e_n)$: SNF of A

Theorem. $e_1 e_2 \cdots e_i$ is the gcd of all $i \times i$ minors of A .

minor: determinant of a square submatrix

Special case: e_1 is the gcd of all entries of A .

Laplacian matrices

$L(G)$: Laplacian matrix of the graph G

rows and columns indexed by vertices of G

$$L(G)_{uv} = \begin{cases} -\#(\text{edges } uv), & u \neq v \\ \text{deg}(u), & u = v. \end{cases}$$

Laplacian matrices

$L(G)$: Laplacian matrix of the graph G

rows and columns indexed by vertices of G

$$L(G)_{uv} = \begin{cases} -\#(\text{edges } uv), & u \neq v \\ \text{deg}(u), & u = v. \end{cases}$$

reduced Laplacian matrix $L_0(G)$: for some vertex v , remove from $L(G)$ the row and column indexed by v

Matrix-tree theorem

Matrix-tree theorem. $\det \mathbf{L}_0(G) = \kappa(G)$, the number of spanning trees of G .

Matrix-tree theorem

Matrix-tree theorem. $\det \mathbf{L}_0(G) = \kappa(G)$, the number of spanning trees of G .

In general, SNF of $\mathbf{L}_0(G)$ not understood.

Matrix-tree theorem

Matrix-tree theorem. $\det \mathbf{L}_0(G) = \kappa(G)$, the number of spanning trees of G .

In general, SNF of $\mathbf{L}_0(G)$ not understood.

$$\mathbf{L}_0(G) \xrightarrow{\text{snf}} \text{diag}(e_1, \dots, e_{n-1}) \Rightarrow \mathbf{L}(G) \xrightarrow{\text{snf}} \text{diag}(e_1, \dots, e_{n-1}, 0)$$

Matrix-tree theorem

Matrix-tree theorem. $\det \mathbf{L}_0(G) = \kappa(G)$, the number of spanning trees of G .

In general, SNF of $\mathbf{L}_0(G)$ not understood.

$$\mathbf{L}_0(G) \xrightarrow{\text{snf}} \text{diag}(e_1, \dots, e_{n-1}) \Rightarrow \mathbf{L}(G) \xrightarrow{\text{snf}} \text{diag}(e_1, \dots, e_{n-1}, 0)$$

Applications to sandpile models, chip firing, etc.

An example

Reduced Laplacian matrix of K_4 :

$$A = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

An example

Reduced Laplacian matrix of K_4 :

$$A = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

Matrix-tree theorem $\implies \det(A) = 16$, the number of spanning trees of K_4 .

An example

Reduced Laplacian matrix of K_4 :

$$A = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

Matrix-tree theorem $\implies \det(A) = 16$, the number of spanning trees of K_4 .

What about SNF?

An example (continued)

$$\begin{aligned} \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} &\rightarrow \begin{bmatrix} 0 & 0 & -1 \\ -4 & 4 & -1 \\ 8 & -4 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & -1 \\ -4 & 4 & 0 \\ 8 & -4 & 0 \end{bmatrix} \\ &\rightarrow \begin{bmatrix} 0 & 0 & -1 \\ 0 & 4 & 0 \\ 4 & -4 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & -1 \\ 0 & 4 & 0 \\ 4 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} \end{aligned}$$

Reduced Laplacian matrix of K_n

$$L_0(K_n) = nI_{n-1} - J_{n-1}$$
$$\det L_0(K_n) = n^{n-2}$$

Reduced Laplacian matrix of K_n

$$\mathbf{L}_0(K_n) = nI_{n-1} - J_{n-1}$$

$$\det L_0(K_n) = n^{n-2}$$

Theorem. $\mathbf{L}_0(K_n) \xrightarrow{\text{SNF}} \text{diag}(1, n, n, \dots, n)$, a refinement of Cayley's theorem that $\kappa(K_n) = n^{n-2}$.

Proof that $L_0(K_n) \xrightarrow{\text{SNF}} \text{diag}(1, n, n, \dots, n)$

Trick: 2×2 submatrices (up to row and column permutations):

$$\begin{bmatrix} n-1 & -1 \\ -1 & n-1 \end{bmatrix}, \quad \begin{bmatrix} n-1 & -1 \\ -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix},$$

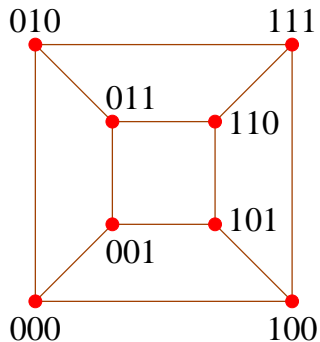
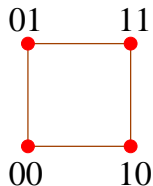
with determinants $n(n-2)$, $-n$, and 0 . Hence $e_1 e_2 = n$. Since $\prod e_j = n^{n-2}$ and $e_j | e_{j+1}$, we get the SNF $\text{diag}(1, n, n, \dots, n)$.

The n -cube

C_n : graph of the n -cube

The n -cube

C_n : graph of the n -cube



An open problem

$$\kappa(C_n) = 2^{2^n - n - 1} \prod_{i=1}^n i \binom{n}{i}$$

An open problem

$$\kappa(C_n) = 2^{2^n - n - 1} \prod_{i=1}^n i \binom{n}{i}$$

Easy to prove by linear algebra; combinatorial (but not bijective) proof by **O. Bernardi**, 2012.

An open problem

$$\kappa(C_n) = 2^{2^n - n - 1} \prod_{i=1}^n i \binom{n}{i}$$

Easy to prove by linear algebra; combinatorial (but not bijective) proof by **O. Bernardi**, 2012.

SNF of $L(K(C_n))$ known for all odd primes p (**Hua Bai**, 2003)

An open problem

$$\kappa(C_n) = 2^{2^n - n - 1} \prod_{i=1}^n i \binom{n}{i}$$

Easy to prove by linear algebra; combinatorial (but not bijective) proof by **O. Bernardi**, 2012.

SNF of $L(K(C_n))$ known for all odd primes p (**Hua Bai**, 2003)

2-adic behavior is **unknown**.

SNF of random matrices

with **Yinghui Wang**

SNF of random matrices

with **Yinghui Wang** (王颖慧)

SNF of random matrices

with **Yinghui Wang** (王颖慧)

Huge literature on random matrices, mostly connected with eigenvalues.

Not much work on SNF of random matrices over \mathbb{Z} .

Is the question interesting?

$\text{Mat}_k(n)$: all $n \times n$ \mathbb{Z} -matrices with entries in $[-k, k]$ (uniform distribution)

$p_k(n, d)$: probability that if $M \in \text{Mat}_k(n)$ and $\text{SNF}(M) = (e_1, \dots, e_n)$, then $e_1 = d$.

Is the question interesting?

$\text{Mat}_k(n)$: all $n \times n$ \mathbb{Z} -matrices with entries in $[-k, k]$ (uniform distribution)

$p_k(n, d)$: probability that if $M \in \text{Mat}_k(n)$ and $\text{SNF}(M) = (e_1, \dots, e_n)$, then $e_1 = d$.

Recall: $e_1 = \text{gcd}$ of 1×1 minors (entries) of M

Is the question interesting?

$\text{Mat}_k(n)$: all $n \times n$ \mathbb{Z} -matrices with entries in $[-k, k]$ (uniform distribution)

$p_k(n, d)$: probability that if $M \in \text{Mat}_k(n)$ and $\text{SNF}(M) = (e_1, \dots, e_n)$, then $e_1 = d$.

Recall: $e_1 = \text{gcd}$ of 1×1 minors (entries) of M

Theorem. $\lim_{k \rightarrow \infty} p_k(n, d) = \frac{1}{d^{n^2} \zeta(n^2)}$

Sample result

$\mu_k(n)$: probability that the SNF of a random $A \in \text{Mat}_k(n)$ satisfies $e_1 = 2$, $e_2 = 6$.

$$\mu(n) = \lim_{k \rightarrow \infty} \mu_k(n).$$

Conclusion

$$\begin{aligned}\mu(n) &= 2^{-n^2} \left(1 - \sum_{i=(n-1)^2}^{n(n-1)} 2^{-i} + \sum_{i=n(n-1)+1}^{n^2-1} 2^{-i} \right) \\ &\quad \cdot \frac{3}{2} \cdot 3^{-(n-1)^2} (1 - 3^{(n-1)^2}) (1 - 3^{-n})^2 \\ &\quad \cdot \prod_{p>3} \left(1 - \sum_{i=(n-1)^2}^{n(n-1)} p^{-i} + \sum_{i=n(n-1)+1}^{n^2-1} p^{-i} \right).\end{aligned}$$

Cyclic cokernel

$\kappa(n)$: probability that an $n \times n$ \mathbb{Z} -matrix has SNF $\text{diag}(e_1, e_2, \dots, e_n)$ with $e_1 = e_2 = \dots = e_{n-1} = 1$

Cyclic cokernel

$\kappa(n)$: probability that an $n \times n$ \mathbb{Z} -matrix has SNF $\text{diag}(e_1, e_2, \dots, e_n)$ with $e_1 = e_2 = \dots = e_{n-1} = 1$

Theorem.
$$\kappa(n) = \frac{\prod \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \dots + \frac{1}{p^n} \right)}{\zeta(2)\zeta(3)\dots}$$

Cyclic cokernel

$\kappa(n)$: probability that an $n \times n$ \mathbb{Z} -matrix has SNF $\text{diag}(e_1, e_2, \dots, e_n)$ with $e_1 = e_2 = \dots = e_{n-1} = 1$

Theorem.
$$\kappa(n) = \frac{\prod \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \dots + \frac{1}{p^n} \right)}{\zeta(2)\zeta(3)\dots}$$

Corollary (T. Ekedahl, 1991)

$$\begin{aligned} \lim_{n \rightarrow \infty} \kappa(n) &= \frac{1}{\zeta(6) \prod_{j \geq 4} \zeta(j)} \\ &\approx 0.846936 \dots \end{aligned}$$

Small number of generators

g : number of generators of cokernel (number of entries of SNF $\neq 1$) as $n \rightarrow \infty$

previous slide: $\text{Prob}(g = 1) = 0.846936 \dots$

Small number of generators

g : number of generators of cokernel (number of entries of SNF $\neq 1$) as $n \rightarrow \infty$

previous slide: $\text{Prob}(g = 1) = 0.846936\dots$

$$\text{Prob}(g \leq 2) = 0.99462688\dots$$

Small number of generators

g : number of generators of cokernel (number of entries of SNF $\neq 1$) as $n \rightarrow \infty$

previous slide: $\text{Prob}(g = 1) = 0.846936\dots$

$$\text{Prob}(g \leq 2) = 0.99462688\dots$$

$$\text{Prob}(g \leq 3) = 0.99995329\dots$$

Small number of generators

g : number of generators of cokernel (number of entries of SNF $\neq 1$) as $n \rightarrow \infty$

previous slide: $\text{Prob}(g = 1) = 0.846936\dots$

$$\text{Prob}(g \leq 2) = 0.99462688\dots$$

$$\text{Prob}(g \leq 3) = 0.99995329\dots$$

Theorem. $\text{Prob}(g \leq \ell) =$

$$1 - (3.46275\dots)2^{-(\ell+1)^2}(1 + O(2^{-\ell}))$$

Small number of generators

g : number of generators of cokernel (number of entries of SNF $\neq 1$) as $n \rightarrow \infty$

previous slide: $\text{Prob}(g = 1) = 0.846936 \dots$

$$\text{Prob}(g \leq 2) = 0.99462688 \dots$$

$$\text{Prob}(g \leq 3) = 0.99995329 \dots$$

Theorem. $\text{Prob}(g \leq \ell) =$

$$1 - (3.46275 \dots) 2^{-(\ell+1)^2} (1 + O(2^{-\ell}))$$

3.46275...

$$3.46275\dots = \frac{1}{\prod_{j \geq 1} \left(1 - \frac{1}{2^j}\right)}$$

Two Catalan determinants

Theorem. *There is a unique sequence a_0, a_1, \dots of integers satisfying*

$$\begin{vmatrix} a_0 & a_1 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_{n+1} \\ a_2 & a_3 & \cdots & a_{n+2} \\ \vdots & \vdots & & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & \cdots & a_{n+1} \\ a_2 & a_3 & \cdots & a_{n+2} \\ a_3 & a_4 & \cdots & a_{n+3} \\ \vdots & \vdots & & \vdots \\ a_{n+1} & a_{n+2} & \cdots & a_{2n+1} \end{vmatrix} = 1.$$

Two Catalan determinants

Theorem. *There is a unique sequence a_0, a_1, \dots of integers satisfying*

$$\begin{vmatrix} a_0 & a_1 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_{n+1} \\ a_2 & a_3 & \cdots & a_{n+2} \\ \vdots & \vdots & & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & \cdots & a_{n+1} \\ a_2 & a_3 & \cdots & a_{n+2} \\ a_3 & a_4 & \cdots & a_{n+3} \\ \vdots & \vdots & & \vdots \\ a_{n+1} & a_{n+2} & \cdots & a_{2n+1} \end{vmatrix} = 1.$$

Namely, $a_n = \frac{1}{n+1} \binom{2n}{n}$ (**Catalan number**).

A q -analogue

Let

$$\mathcal{A}_n = \{(i_1, \dots, i_n) : 0 \leq i_1 \leq \dots \leq i_n, \quad i_k \leq k - 1\},$$

so $\#\mathcal{A}_n = C_n$. Define the **q -Catalan polynomial**

$$\tilde{C}_n(q) = \sum_{(i_1, \dots, i_n) \in \mathcal{A}_n} q^{\binom{n}{2} - (i_1 + \dots + i_n)}.$$

A q -analogue

Let

$$\mathcal{A}_n = \{(i_1, \dots, i_n) : 0 \leq i_1 \leq \dots \leq i_n, \quad i_k \leq k - 1\},$$

so $\#\mathcal{A}_n = C_n$. Define the **q -Catalan polynomial**

$$\tilde{C}_n(q) = \sum_{(i_1, \dots, i_n) \in \mathcal{A}_n} q^{\binom{n}{2} - (i_1 + \dots + i_n)}.$$

Example. $\mathcal{A}_3 = \{000, 001, 011, 002, 012\}$, so

$$\tilde{C}_3(q) = q^3 + q^2 + 2q + 1.$$

Ramanujan

$$C_n(q) = q^{\binom{n}{2}} \tilde{C}_n(1/q)$$

$$\begin{aligned} F(q, x) &:= \sum_{n \geq 0} C_n(q) x^n \\ &= \frac{1}{1 - \frac{x}{1 - \frac{qx}{1 - \frac{q^2x}{1 - \dots}}}}} \end{aligned}$$

Ramanujan

$$C_n(q) = q^{\binom{n}{2}} \tilde{C}_n(1/q)$$

$$\begin{aligned} F(q, x) &:= \sum_{n \geq 0} C_n(q) x^n \\ &= \frac{1}{1 - \frac{x}{1 - \frac{qx}{1 - \frac{q^2x}{1 - \dots}}}}} \end{aligned}$$

$$e^{-2\pi/5} F(e^{-2\pi}, -e^{-2\pi}) = \frac{1}{\sqrt{\frac{5+\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}}}.$$

Determinant and SNF

$$U_n = [\tilde{C}_{i+j}(q)]_{i,j=0}^n, \quad V_n = [\tilde{C}_{i+j+1}(q)]_{i,j=0}^n$$

Theorem (Fürlinger-Hofbauer 1985, Cigler 1999).

$$\det U_n = q^{n(n+1)(4n-1)/6}$$

$$\det V_n = q^{n(n+1)(4n+5)/6}$$

Determinant and SNF

$$U_n = [\tilde{C}_{i+j}(q)]_{i,j=0}^n, \quad V_n = [\tilde{C}_{i+j+1}(q)]_{i,j=0}^n$$

Theorem (Fürlinger-Hofbauer 1985, Cigler 1999).

$$\det U_n = q^{n(n+1)(4n-1)/6}$$

$$\det V_n = q^{n(n+1)(4n+5)/6}$$

Theorem (Bessenrodt-RS 2015). Over the ring $\mathbb{Z}[q]$ we have

$$U_n \xrightarrow{\text{snf}} \text{diag}(1, q, q^6, q^{15}, \dots, q^{\binom{2n}{2}})$$

$$V_n \xrightarrow{\text{snf}} \text{diag}(1, q^3, q^{10}, q^{21}, \dots, q^{\binom{2n+1}{2}}).$$

Determinant and SNF

$$U_n = [\tilde{C}_{i+j}(q)]_{i,j=0}^n, \quad V_n = [\tilde{C}_{i+j+1}(q)]_{i,j=0}^n$$

Theorem (Fürlinger-Hofbauer 1985, Cigler 1999).

$$\det U_n = q^{n(n+1)(4n-1)/6}$$

$$\det V_n = q^{n(n+1)(4n+5)/6}$$

Theorem (Bessenrodt-RS 2015). Over the ring $\mathbb{Z}[q]$ we have

$$U_n \xrightarrow{\text{snf}} \text{diag}(1, q, q^6, q^{15}, \dots, q^{\binom{2n}{2}})$$

$$V_n \xrightarrow{\text{snf}} \text{diag}(1, q^3, q^{10}, q^{21}, \dots, q^{\binom{2n+1}{2}}).$$

Special case of a much more general multivariate result.

The last slide

The last slide



The last slide

