Advanced Discrete Mathematics
Lecture 12

Gypsy Alehyar
22nd August 2025

Q: What do you think are topics that are pretty exotic and relatively unknown right now, like the Hecke algebra in your day, that will be super important in the future?

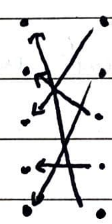
A: (1) Prismatic cohomology
(2) Condensed mathematics
(3) Witt vectors
(4) ∞-categories

Generators and Relations for S_n

Generators A: permutation matrices

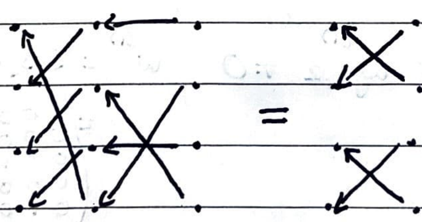
For example:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} =$$



Relations A: matrix multiplication

For example:



Or, as matrices:

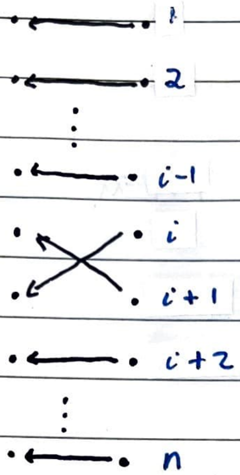
$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Generators B: $s_1, s_2, \ldots, s_{n-1}$

Relations B: (1) $s_j^2 = 1$
(2) $s_j s_k = s_k s_j$ if $k \in \{j-1, j+1\}$
(3) $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$

Step 1 : Generators B in terms of Generators A

$S_i =$

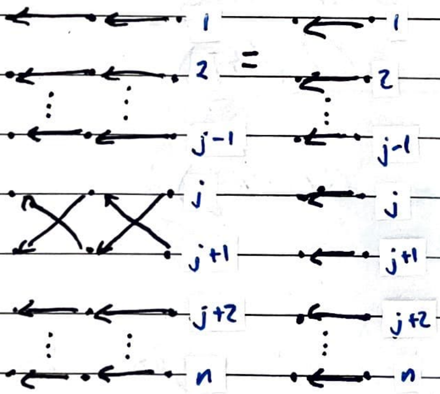


$$= \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

for $i \in \{1, \dots, n-1\}$.

Step 2 : Relations B from Relations A.

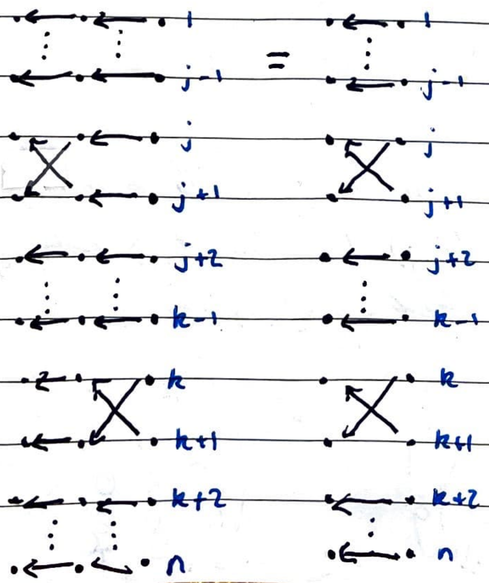
$S_j^2 =$



$= 1$

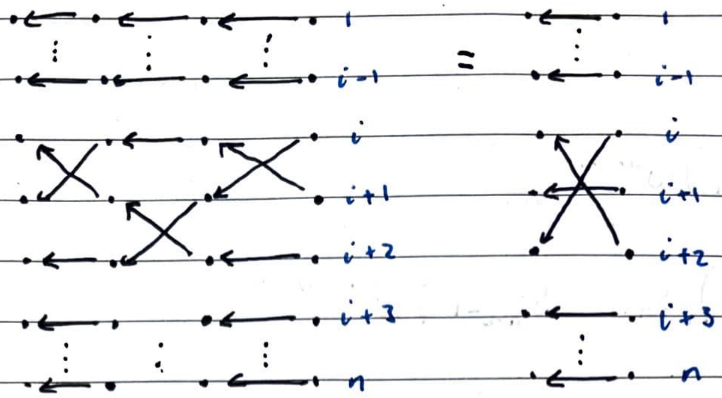
Assume $k \notin \{j-1, j+1\}$

$S_j S_k =$



$= (\cdots) = S_k S_j$

$S_i S_{i+1} S_i =$



$= (\cdots)$

$= S_{i+1} S_i S_{i+1}$

Step 3: Generators A from Generators B
(This is the 'theory of reduced words')

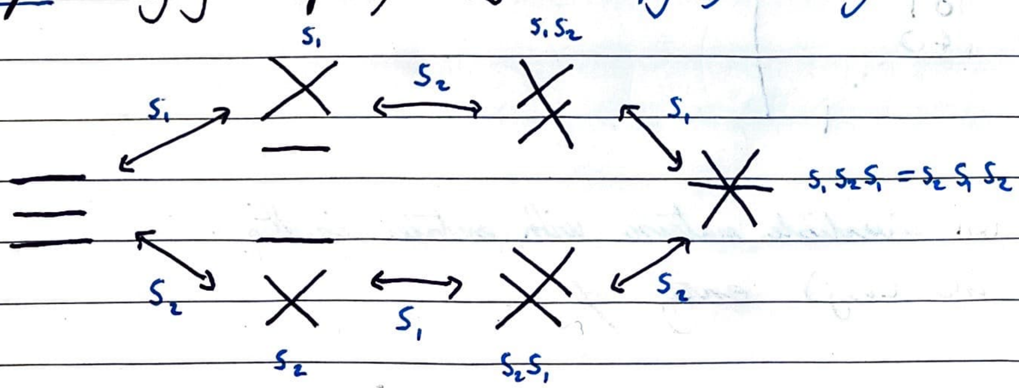
Let $w \in S_n$ be a permutation matrix.
A reduced word for w is an expression

$$w = s_{i_1} \cdots s_{i_l} \quad \text{with} \quad i_1, \dots, i_l \in \{1, \dots, n-1\}$$

and l minimal.

The length of w $l(w)$ is the l in the reduced word for w.

Example: Cayley Graph for S_3 (multiplying on right)



We see here that

(1)  has two reduced words $s_1 s_2 s_1$ and $s_2 s_1 s_2$
so that $\ell(\ast) = 3$

(2)  has a reduced word s_1 so that $\ell(\underline{\times}) = 1$.
In particular, immediately we know $s_1 s_2 s_1 s_1 s_2$
is not a reduced word for $\underline{\times}$.

Q: Given $w \in S_n$, a permutation matrix, how can we construct a reduced word for w?

A: Let w be an $n \times n$ permutation matrix

Let $j_1 > 1$ be maximal such that $w_{j_1,1} \neq 0$
Let

$$w^{(1)} = \begin{cases} w, & \text{if } j_1 \text{ doesn't exist} \\ s_1 \cdots s_{j_1-1}, & \text{if } j_1 \text{ exists} \end{cases}$$

Example:

$$w = \begin{pmatrix} 0&0&0&0&1 \\ 0&0&1&0&0 \\ 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&1&0&0&0 \end{pmatrix}$$

(here, we see $j_1 = 3$)

Let $j_2 > 2$ be maximal such that $w^{(1)}_{j_2,2} \neq 0$
Let

$$w^{(2)} = \begin{cases} w, & \text{if } j_2 \text{ doesn't exist} \\ s_2 \cdots s_{j_2-1}, & \text{if } j_2 \text{ exists} \end{cases}$$

$$w^{(1)} = s_1 s_2 w = \begin{pmatrix} 1&0&0&0&0 \\ 0&0&0&0&1 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&1&0&0&0 \end{pmatrix}$$

(here, we see $j_2 = 5$)

$$w^{(2)} = s_2 s_3 s_4 w^{(1)}$$

$\vdots$

Continue this procedure to obtain

and so on...

$$w^{(1)}, w^{(2)}, \ldots, w^{(n)}.$$

Then $w^{(n)} = 1$.

So, we obtain,

$$w^{(n)} = (s_{n-1} \cdots s_{j_{n-1}-1})\, w^{(n-1)}$$

$$= (s_{n-1} \cdots s_{j_{n-1}-1})(s_{n-2} \cdots s_{j_{n-2}-1})\, w^{(n-2)}$$

$$= (s_{n-1} \cdots s_{j_{n-1}-1})(s_{n-2} \cdots s_{j_{n-2}-1}) \cdots (s_1 \cdots s_{j_1-1})\, w$$

So, since $w^{(n)} = 1$, then

$$w = \left[(s_{n-1} \cdots s_{j_{n-1}-1})(s_{n-2} \cdots s_{j_{n-2}-1}) \cdots (s_1 \cdots s_{j_1-1})\right]^{-1} w^{(n)}$$

$$= (s_{j_1-1} \cdots s_1) \cdots (s_{j_{n-2}} \cdots s_{n-2})(s_{j_{n-1}} \cdots s_{n-1})$$

where we have used $s_j^2 = 1$.

Although we cannot see it just yet, this will be the reduced word for w. One should prove, by induction, that this is the case.

Constructing a reduced word for $GL_n(\mathbb{F}_q)$
(i.e. we want generators and relations for $GL_n(\mathbb{F}_q)$)

Let $y_i(c) = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & c & 1 & \\ & & & 1 & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$ for $i \in \{1, \dots, n-1\}$ and $c \in \mathbb{F}_q$

Let g be an $n \times n$ invertible matrix with entries in $\mathbb{F}_q$.
Let $g(i,j)$ be the (i,j) entry of g.

Let $j_1 > 1$ be maximal such that $g(j_1, 1) \neq 0$.
Let

$$g^{(1)} = \begin{cases} g & \text{, if } j_1 \text{ doesn't exist} \\ y_1\left(\frac{g(1,1)}{g(j_1,1)}\right)^{-1} y_2\left(\frac{g(2,1)}{g(j_1,1)}\right)^{-1} \cdots y_{j_1-1}\left(\frac{g(j_1-1,1)}{g(j_1,1)}\right)^{-1} g & \text{, if } j_1 \text{ exists} \end{cases}$$

In the same way as the S_n case to get

$$g^{(1)}, \dots, g^{(n)}.$$

We have constructed $g^{(n)}$ in a very special way; it has the property that for all $j \in \{1, \dots, n-1\}$ the last nonzero entry in row $j+1$ is to the right of the last nonzero entry in row j.

This, combined with the fact that g is invertible, means that $g^{(n)}$ is invertible and has form

$$g^{(n)} = \begin{pmatrix} b_{11} & & * \\ & b_{22} & \\ 0 & & \ddots \\ & & & b_{nn} \end{pmatrix} \quad \text{with } b_{ii} \neq 0.$$

Write $g^{(n)} = b$.
So, we conclude that

$$g = \left(y_{j_1-1}\left(\frac{g(j_1-1,1)}{g(j_1,1)}\right) \cdots y_1\left(\frac{g(1,1)}{g(j_1,1)}\right)\right) \cdots \left(y_{j_{n-1}-1}\left(\frac{g(j_{n-1}-1,n-1)}{g(j_{n-1},n-1)}\right) \cdots y_{n-1}\left(\frac{g(j_{n-1}-1,n-1)}{g(j_{n-1},n-1)}\right)\right) \times b$$

where b is upper triangular. (Refined Bruhat Decomposition).