

This is Dror Bar-Natan's 2025 MAT 347 personal notebook. It is publically available but it comes with no guarantees whatsoever. Its content may or may not be correlated with the actual class content.

**Non-Commutative Gaussian Elimination and Rubik's Cube**

The Problem. Let  $G = \langle \sigma_1, \dots, \sigma_n \rangle$  be a subgroup of  $S_n$  with  $n \leq 1000$ . Before you die, understand  $G$ .

- Compute  $|G|$ .
- Given  $\sigma \in S_n$ , find  $\sigma \in G$ .
- Write  $\sigma \in G$  as a product of  $\sigma_1, \dots, \sigma_n$ .

Produce random elements of  $G$ .

**Analysis.** Let  $V$  be a subspace of  $\mathbb{R}^n$ . Do you die, understand  $V$ .

**Solution: Gaussian Elimination.** Prepare an empty table.

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|
| 1   | 2   | 3   | 4   | ... | n   |
| ... | ... | ... | ... | ... | ... |

Space for a vector  $v_i \in V$  of the form  $v_i = (0, 0, 0, 1, \dots, \dots)$ . 1 := "the pivot".

**Find  $v_1, \dots, v_n$  in order.** To find a non-zero  $v_i$ , find its pivot position  $i$ .

- If box  $i$  is empty, put  $v_i$  there.
- If box  $i$  is occupied, find a combination  $v'$  of  $v$  and  $v_i$  that eliminates the pivot, and find  $v'$ .

**Non-Commutative Gaussian Elimination**

Prepare a neatly-empty table.

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|
| 1   | 2   | 3   | 4   | ... | n   |
| ... | ... | ... | ... | ... | ... |

Space for a  $\sigma_{i,j} \in S_n$  of the form  $(1, 2, \dots, i-1, i, j, i+1, \dots, n)$ . No  $\sigma_{i,j}$  from  $1, \dots, i-1$ .

No  $\sigma_{i,j}$  from  $1, \dots, i-1$ .

Send "the pivot"  $i$  to  $j$  and give wild elsewhere, and  $\sigma_{i,j}$  "does stider  $j$ ".

**Find  $\sigma_1, \dots, \sigma_n$  in order.** To find a non-identity  $\sigma$ , find its pivot position  $i$  and let  $j := \sigma(i)$ .

- If box  $(i, j)$  is empty, put  $\sigma$  there.
- If box  $(i, j)$  contains  $\sigma_{i,j}$ , find  $\sigma' := \sigma_{i,j}^{-1}\sigma$ .

**The Test.** When done, for every occupied  $(i, j)$  and  $(k, l)$ , find  $\sigma_{i,j}\sigma_{k,l}$ . Repeat until the table stops changing.

**Chain 1.** The process stops in our lifetime, after at most  $O(n^2)$  operations. Call the resulting table  $T$ .

**Chain 2.** Every  $\sigma_{i,j}$  in  $T$  is in  $G$ .

**Chain 3.** Anything left in  $T$  is now a monotone product in  $T$ .

**Chain 4.** If  $\sigma \in G$ ,  $\sigma = \sigma_{i_1, j_1} \sigma_{i_2, j_2} \dots \sigma_{i_k, j_k}$  for  $k \leq n$ .

**Homework Problem 1.** The Rubik's Cube

Can you do counts?

**Homework Problem 2.** Can you do categories (groups)?

Rubik's Cube

Dear Ben Natan: Academic Perspective: 2013-01: NCGE

**The Back Side**

A homomorphism from  $S_4$  to  $S_3$ :

A homomorphism from  $A_5$  to the symmetry group of a dodecahedron, to  $A_5$ :

<http://shorin.net/Academic/Perspective/2013-01/NCGE/> images from <http://shorin.net/Academic/Perspective/2011-12/>

+ Def of a group  
 uniqueness of  $e$   
 Uniqueness of  $y^{-1}$   
 Cancellation  
 $(ab)^{-1} = b^{-1}a^{-1}$

Examples  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, 2\mathbb{Z}, V$   
 $\mathbb{Q}^x, \mathbb{R}^x, \mathbb{C}^x, F^x$   
 The Rubik's cube  
 $S_7, [ ]$  notation  
 $S(\otimes)$   
 $O(3)$

It's a tough class!

$$\sigma \cdot \tau = \sigma \circ \tau$$

Goal: within your lifetime, understand

$$G = \langle g_1, \dots, g_\alpha \rangle \subseteq S_n :$$

$$1. |G| = ? \quad 2. \sigma \in G?$$

3. write  $\sigma \in G$  in terms of  $g_1, \dots, g_\alpha$

4. Random  $\sigma$ .

on board!

Classical row reduction as in handout.

Describe the NCGE algorithm as in handout.

Claim 0. The process ends after at most  $n^6$  steps. Call the resulting table  $T$ .

Claim 1 Every  $\sigma_{ij}$  in  $T$  is in  $G$ .

Claim 2 Anything fed to  $T$  is now a monotone product  $\sigma_{1j_1} \sigma_{2j_2} \sigma_{3j_3} \dots$   $j_i \geq i$

Claim 3 IF two monotone products are equal,

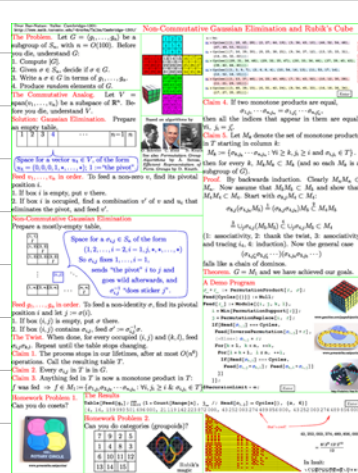
$$\sigma_{1j_1} \dots \sigma_{nj_n} = \sigma_{1j'_1} \dots \sigma_{nj'_n}$$

then all the indices are equal,  $\forall i \ j_i = j'_i$ .

Claim 4 Let  $M_k = \{ \text{monotone products beginning with } k \} = \{ \sigma_{k j_k} \dots \sigma_{nj_n} \}$ ,

then for every  $k$ ,  $M_k \cdot M_k \subseteq M_k$  (and so each

$M_k$  is a subgroup of  $S_n$ ).



**Proof.** By backwards induction. Clearly  $M_n M_n \subset M_n$ . Now assume that  $M_5 M_5 \subset M_5$  and show that  $M_4 M_4 \subset M_4$ . Start with  $\sigma_{8,j} M_4 \subset M_4$ :

$$\sigma_{8,j}(\sigma_{4,j_4}M_5) \stackrel{1}{=} (\sigma_{8,j}\sigma_{4,j_4})M_5 \stackrel{2}{\subset} M_4M_5$$

$$\stackrel{3}{=} \cup_j \sigma_{4,j}(M_5 M_5) \stackrel{4}{\subset} \cup_j \sigma_{4,j} M_5 \subset M_4$$

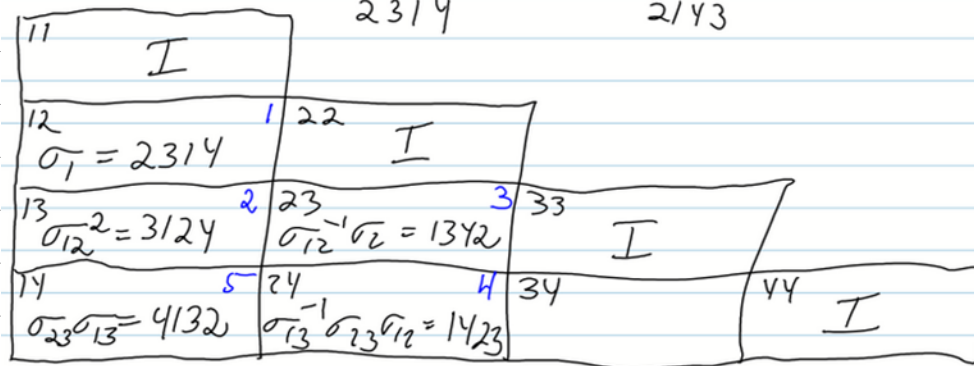
(1: associativity, 2: thank the twist, 3: associativity and tracing  $i_4$ , 4: induction). Now the general case

$$(\sigma_{4,j'_4} \sigma_{5,j'_5} \cdots)(\sigma_{4,j_4} \sigma_{5,j_5} \cdots)$$

falls like a chain of dominos.

**Theorem.**  $G = M_1$  and we have achieved our goals.

Example  $\sigma_1 = (123)$   $\sigma_2 = (12)(34)$ , in  $S_4$



on  
board  
(minus  
fills)

Feed  $\sigma_1 = 2314 \dots$  Feed @  $\sigma_{12}$

Feed  $\sigma_{12}^2 = 3124 \therefore$  Feed @  $\sigma_{13}$

Feed  $\sigma_2 = 2143 \dots$  Feed  $\sigma_{12}^{-1}\sigma_2 = 1342 \dots$  Feed @  $\sigma_{23}$

Feed  $\sigma_{12}\sigma_{23} = 2143 \dots$  feed  $\sigma_{12}^{-1}\sigma_{12}\sigma_{23} = \sigma_{23} \dots$

No point feeding  $\sigma_{ij} \sigma_{kl}$  if  $k \neq j$

Field  $\sigma_{23}\sigma_{12} = 3^4 | 2 \dots$  Field  $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1423 \dots$  to  $\sigma_{24}$

Feed  $\sigma_{23}\sigma_{13} = 4132 \dots$  to  $\sigma_{14}$

Feed  $\sigma_{24}\sigma_{12} = 4213 \dots$  Feed  $\sigma_{14}^{-1}\sigma_{24}\sigma_{12} = 1423 \dots$  drop.

$$\Rightarrow |G| = 4 \cdot 3 \cdot 1 \cdot 1 = 12. \quad \nexists s \quad 4|23 \in G \stackrel{?}{\circ}$$

write 2431 in terms of  $\sigma_{1,2}$ .