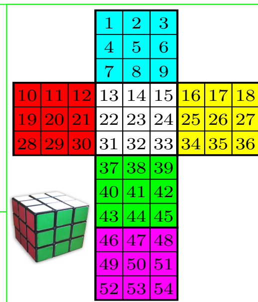
Non-Commutative Gaussian Elimination and Rubik's Cube

The Problem. Let $G=\langle g_1,\dots,g_\alpha\rangle$ be a subgroup of S_n, with $n=O(100)$. Before you die, understand G:

1. Compute $|G|$.
2. Given $\sigma\in S_n$, decide if $\sigma\in G$.
3. Write a $\sigma\in G$ in terms of $g_1,\dots,g_\alpha$.
4. Produce *random* elements of G.



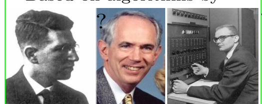
The Commutative Analog. Let $V=\operatorname{span}(v_1,\dots,v_\alpha)$ be a subspace of $\mathbb{R}^n$. Before you die, understand V.

Solution: Gaussian Elimination. Prepare an empty table,

1	2	3	4	⋯	$n-1$	n

Space for a vector $u_4\in V$, of the form $u_4=(0,0,0,1,*,\dots,*)$; $1 :=$"the pivot".

Based on algorithms by



O. Schreier C. Sims D. Knuth

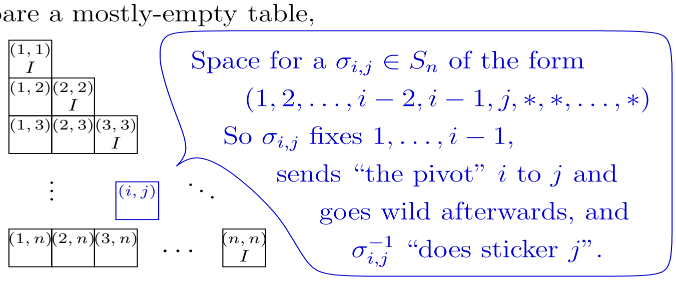
See also *Permutation Group Algorithms* by Á. Seress, *Efficient Representation of Perm Groups* by D. Knuth.

Feed $v_1,\dots,v_\alpha$ in order. To feed a non-zero v, find its pivotal position i.

1. If box i is empty, put v there.
2. If box i is occupied, find a combination v' of v and u_i that eliminates the pivot, and feed v'.

Non-Commutative Gaussian Elimination

Prepare a mostly-empty table,



Feed $g_1,\dots,g_\alpha$ in order. To feed a non-identity σ, find its pivotal position i and let $j:=\sigma(i)$.

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

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

Claim 1. The process stops in our lifetimes, after at most $O(n^6)$ operations. Call the resulting table T.

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

Claim 3. Anything fed in T is now a monotone product in T:
f was fed $\Rightarrow f\in M_1:=\{\sigma_{1,j_1}\sigma_{2,j_2}\cdots\sigma_{n,j_n}:\forall i,\ j_i\geq i\ \&\ \sigma_{i,j_i}\in T\}$

The Generators

```
n = 54;
g1 = Cycles[{{1, 18, 45, 28}, {2, 27, 44, 19}, {3, 36, 43, 10}, {46, 52, 54, 48},
    {47, 49, 53, 51}}];
g2 = Cycles[{{7, 16, 39, 30}, {8, 25, 38, 21}, {9, 34, 37, 12}, {13, 15, 33, 31},
    {14, 24, 32, 22}}];
g3 = Cycles[{{28, 31, 34, 48}, {29, 32, 35, 47}, {30, 33, 36, 46}, {37, 39, 45, 43},
    {38, 42, 44, 40}}];
g4 = Cycles[{{1, 3, 9, 7}, {2, 6, 8, 4}, {10, 54, 16, 13}, {11, 53, 17, 14},
    {12, 52, 18, 15}}];
g5 = Cycles[{{1, 13, 37, 46}, {4, 22, 40, 49}, {7, 31, 43, 52}, {10, 12, 30, 28},
    {11, 21, 29, 19}}];
g6 = Cycles[{{3, 48, 39, 15}, {6, 51, 42, 24}, {9, 54, 45, 33}, {16, 18, 36, 34},
    {17, 27, 35, 25}}];
```
Enter

Claim 4. If two monotone products are equal,

$$\sigma_{1,j_1}\cdots\sigma_{n,j_n}=\sigma_{1,j'_1}\cdots\sigma_{n,j'_n},$$

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

Claim 5. Let M_k denote the set of monotone products in T starting in column k:

$$M_k:=\{\sigma_{k,j_k}\cdots\sigma_{n,j_n}:\forall i\geq k, j_i\geq i \text{ and } \sigma_{i,j_i}\in T\}.$$

then for every k, $M_kM_k\subset M_k$ (and so each M_k is a subgroup of G).

Proof. By backwards induction. Clearly $M_nM_n\subset M_n$. Now assume that $M_5M_5\subset M_5$ and show that $M_4M_4\subset M_4$. Start with $\sigma_{8,j}M_4\subset M_4$:

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

$$\overset{3}{=}\cup_j\sigma_{4,j}(M_5M_5)\overset{4}{\subset}\cup_j\sigma_{4,j}M_5\subset M_4$$

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

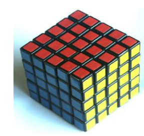
$$(\sigma_{4,j'_4}\sigma_{5,j'_5}\cdots)(\sigma_{4,j_4}\sigma_{5,j_5}\cdots)$$

falls like a chain of dominos.

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

A Demo Program

```
σ_ ∘ τ_ := PermutationProduct[τ, σ];
Feed[Cycles[{}]] := Null;
Feed[τ_] := Module[{i, j, k, l},
   i = Min[PermutationSupport[τ]];
   j = PermutationReplace[i, τ];
   If[Head[σi,j] === Cycles,
    Feed[InversePermutation[σi,j] ∘ τ],
    (*Else*) σi,j = τ;
    For[k = 1, k < n, ++k,
     For[l = k + 1, l ≤ n, ++l,
      If[Head[σk,l] === Cycles,
       Feed[σi,j ∘ σk,l]; Feed[σk,l ∘ σi,j]]
     ]]
   ]];
$RecursionLimit = ∞;
```
Enter



www.geocities.com/jaapsch/puzzles/

www.powerstrike.net/puzzles/

http://lodelnic.free.fr/

Homework Problem 1.
Can you do cosets?

www.powerstrike.net/puzzles/

The Results

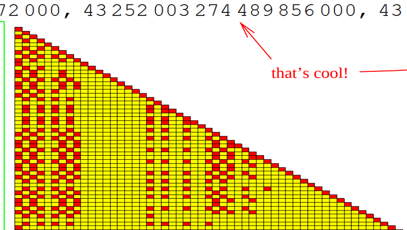
```
Table[Feed[gα]; ∏_{i=1}^{n} (1 + Count[Range[n], j_ /; Head[σi,j] == Cycles]), {α, 6}]
```
Enter

{4, 16, 159 993 501 696 000, 21 119 142 223 872 000, 43 252 003 274 489 856 000, 43 252 003 274 489 856 000}

Homework Problem 2.
Can you do categories (groupoids)?

7	9	2	5
1	4	8	3
6	10	11	12
13	14	15	

Rubik's magic



that's cool!

43, 252, 003, 274, 489, 856, 000

$$=\frac{8!\,3^8\,12!\,2^{12}}{12}$$

In Inuit:

Video and more at http://www.math.toronto.edu/~drorbn/Talks/Cambridge-1301/, see also http://www.math.toronto.edu/~drorbn/Talks/Mathcamp-0907/