

# THEOREM OF THE DAY

**The McIver–Neumann Half- $n$  Bound** Let  $\Omega$  be a set of order  $n$ ,  $n \neq 3$ , and let  $G$  be a permutation group acting on  $\Omega$ . Then  $G$  can be generated by  $\lfloor n/2 \rfloor$  elements.

$$S = \{(1\ 2)(3\ 4), (1\ 2\ 3\ 5)\}$$



**Sift( $\sigma$ )**  
**while**  $\sigma \neq 1$  and not done **do**  
 $i :=$  smallest row no. moved by  $\sigma$   
 $j := \sigma(i)$   
**if**  $M_{ij}$  not empty **then**  $\sigma := \sigma \times M_{ij}^{-1}$   
**else**  $M_{ij} = \sigma$  and done := true

**Schreier-Sims( $S$ )**

Queue :=  $S$

**while** Queue not empty

$\sigma :=$  first permutation in Queue (thereupon removed)

**if** Sift( $\sigma$ ) updates  $M$  with  $\sigma'$  **then**

add  $\{M_{ij} \times \sigma', \sigma' \times M_{ij} \mid 1 \leq i < j \leq n\}$  to Queue

1	(1 2)(3 4)			
	1			
		1		
			1	
				1



1	(1 2)(3 4)			
	1		(2 4 3 5)	
		1		
			1	
				1



1	(1 2)(3 4)		(1 4 5 2)	
	1		(2 4 3 5)	
		1		
			1	
				1



(about 40 steps, with maximum Queue size about 30)



1	(1 2)(3 4)	(1 3 4 5)	(1 4 5 2)	(1 5)(2 4)
	1	(2 3)(4 5)	(2 4 3 5)	(2 5 3 4)
		1	–	–
			1	–
				1

The generation of a permutation group from a set of permutations is illuminated by the wonderful algorithm which Charles Sims derived from a 1927 lemma of Otto Schreier. In the illustration above, the algorithm is applied to a set of two permutations. The main work is done by the Sift routine, which first places  $(1\ 2)(3\ 4)$  into row 1 column 2 cell in the  $5 \times 5$  table  $M$ . The next permutation  $\sigma = (1\ 2\ 3\ 5)$  is a candidate for the same cell since  $\sigma(1) = 2$ ; since the cell is occupied by  $(1\ 2)(3\ 4)$  we calculate  $\sigma := \sigma \times M_{12}^{-1} = (1\ 2\ 3\ 5) \times (1\ 2)(3\ 4) = (2\ 4\ 3\ 5)$ . The new cell  $M_{24}$  is now indicated for  $\sigma$  because now  $\sigma(2) = 4$ . Subsequently, the queue is augmented in the main algorithm by pre- and post-multiplying  $(2\ 4\ 3\ 5)$  with each non-identity entry of  $M$ . The queue now begins with  $(1\ 2)(3\ 4) \times (2\ 4\ 3\ 5) = (1\ 4\ 5\ 2)$  which Sift places directly into position  $M_{1,4}$ . Although the queue tends to grow rapidly it must eventually become empty; in the current example the algorithm terminates with table shown above, bottom-right. This table describes the generated group in the following way: the order of the group is the product of the numbers of permutations in each row, in this case  $5 \times 4 \times 1 \times 1 \times 1 = 20$  (the group happens to be the Frobenius group of order 20, aka the Galois group of the polynomial  $x^5 - 2$ ); membership of the group is tested by running Sift on a candidate permutation  $\sigma$  which will be allocated to an empty table location if and only if it does not belong to the group. **Exercise:** try the algorithm with  $\Omega = \{1, \dots, 8\}$  and  $S = \{(1\ 2), (3\ 4), (5\ 6), (7\ 8)\}$ .

It is easy to generate large groups from a very few permutations;  $n/2$  permutations may sometimes be necessary as the Exercise above easily shows. But Annabelle McIver and Peter M. Neumann's 1987 theorem seems to be deep and mysterious: it rests on the Classification of the Finite Simple Groups and suggests no obvious way of finding a generating set meeting its bound.

**Web link:** [www.maths.qmul.ac.uk/~pjc/slides/pggt.pdf](http://www.maths.qmul.ac.uk/~pjc/slides/pggt.pdf). Read about Frobenius 20 here: [manu.amiot.free.fr/pdf/Articles/chords.pdf](http://manu.amiot.free.fr/pdf/Articles/chords.pdf).

**Further reading:** *Permutation Groups* by P.J. Cameron, Cambridge University Press, 1999, sections 1.13 and 1.14.

