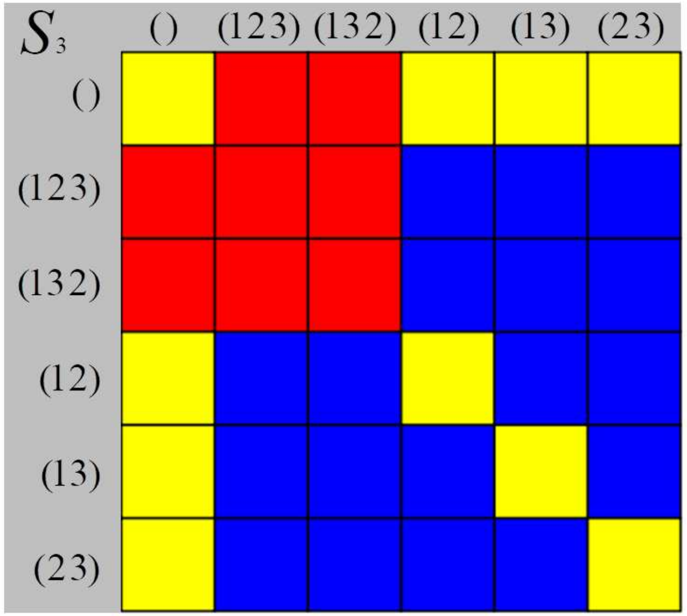
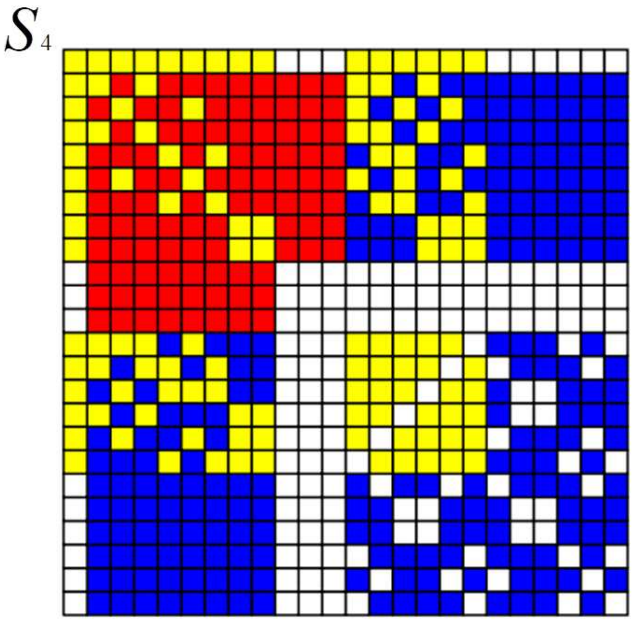
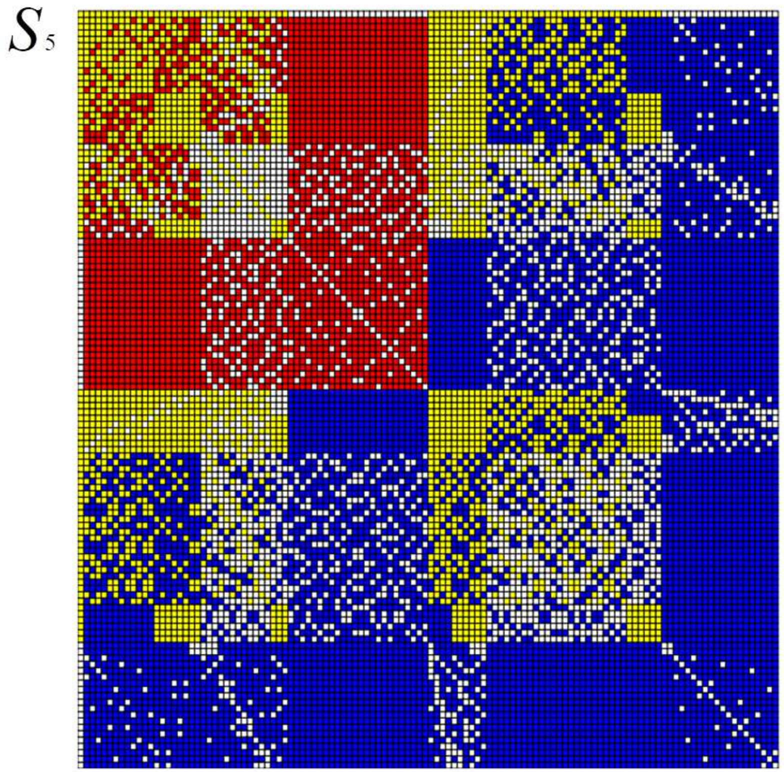
THEOREM OF THE DAY

Netto's Conjecture (Dixon's Theorem) *Two random permutations of* $\{1, \ldots, n\}$ *generate either the symmetric group* S_n *or the alternating group* A_n *with probability tending to 1 as n tends to infinity.*







Indexed by even permutation pair generating all of A_n

Indexed by permutation pair generating all of S_n

Indexed by permutation pair fixing a point in common

The symmetric group S_n consists of all $n!$ permutations of $\{1, \ldots, n\}$. For example, each S_n, for $n \geq 5$, contains the permutation (13)(254) (written in so-called 'disjoint cycle notation'): it permutes two numbers, 1 and 3 (this called is a transposition) and cycles through 2, 5 and 4. Each permutation has a parity, even or odd, which may be computed as the parity of the number of gaps between numbers: (13)(254) has three gaps (i.e. 1-3, 2-5 and 5-4) and is an odd permutation, whereas (13254) has four gaps and is even. The alternating group A_n is the subgroup of all $n!/2$ even permutations. The tables above record those pairs of permutations which generate (via combining permutations by multiplication) all of A_n or S_n. This is immediately impossible for pairs which fix a common point: such pairs are also recorded, in yellow. In the limit the white and yellow cells become a vanishingly small proportion.

Eugen Netto's 1882 conjecture waited nearly a century for a proof. In 1969 John D. Dixon proved that, when n is sufficiently large, the proportion of pairs of permutations of n elements that generate either S_n or A_n exceeds $1 - 2/(\log\log n)^2$. This number approaches 1 very slowly (e.g. staying below 0.99 until $n \approx 10^{10^6}$); Dixon conjectured that the actual proportion would be $1 - 1/n + O(1/n^2)$, with the $1/n$ term being the contribution of pairs of permutations having a common fixed point (the yellow squares in our illustration). Dixon's conjecture was proved in 1989 by László Babai, assuming the classification of the finite simple groups.

Web link: cameroncounts.wordpress.com/2011/04/09

Further reading: Permutation Groups by John D. Dixon and Brian Mortimer, Springer, 1996.