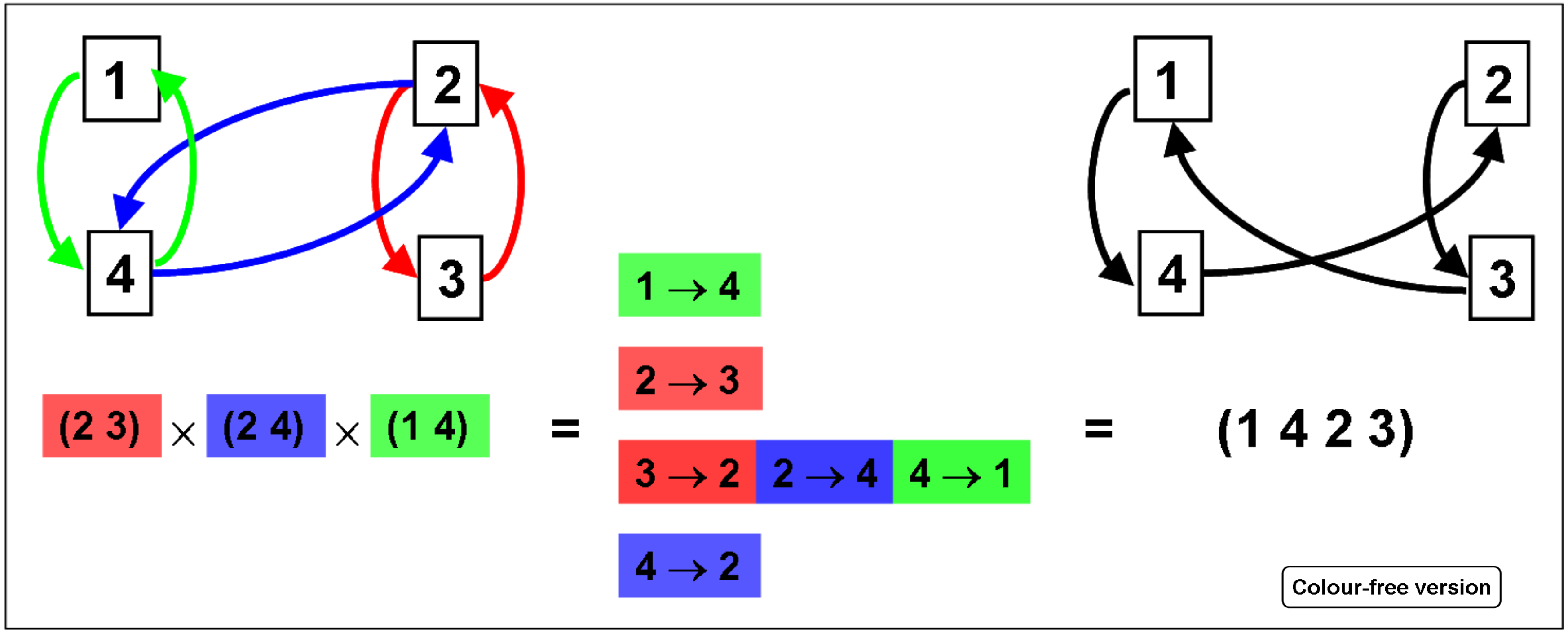
THEOREM OF THE DAY

Netto's Conjecture (Dixon's Theorem) *The proportion of pairs of permutations of n elements which generate the whole symmetric group tends to $\frac{3}{4}$ as $n \to \infty$.*



Multiplying permutations is order-dependent. A diagrammatic depiction is given, on the left, of the product of three *transpositions* (permutations of two elements): (2 3), (2 4) and (1 4). When colour-coded, as in the example on the left, the product permutes an element along the longest path *keeping to the order of the colours*. So, 1 only gets permuted as far as 4, because this uses a green arrow which is the final one available in the red-blue-green ordering which reflects the multiplication order. But 3 can get all the way to 1.

Any permutation may be written as a product of either an even or an odd number of transpositions but not both. Here, (1 4 2 3) is produced as the product of 3 transpositions and is consequently called an *odd* permutation.

Suppose we take *two* permutations of n elements, p and q, at random and build all products by combining p and q as often as we like and in any order we like. How many of the n! permutations constituting the *symmetric group* will we produce altogether? If p and q are both even then we will only ever get even permutations. But 3/4 of the time at least one will be odd. Netto conjectured that, when n becomes large, almost all such pairs will generate the whole symmetric group.

Eugen Netto's 1882 conjecture waited nearly a century for a proof. In 1969 Dixon proved that, when n is sufficiently large, the proportion of pairs of permutations of n elements that either generates the symmetric group or generates all possible even permutations (the *alternating group*) exceeds $1 - 2/(\log\log n)^2$. (This number approaches 1 very slowly, requiring $n \approx 10^{10^6}$ to give 0.99.) Dixon conjectured that the actual proportion would be $1 - 1/n + O(1/n^2)$, with the $1/n$ term arising from the probability of the two permutations having a common fixed point (no points are fixed in the above example). Dixon's conjecture was proved in 1989 by L. Babai, assuming the classification of the finite simple groups.

Web link: mathstat.carleton.ca/~jdixon/Prgrpth.pdf. See www.renyi.hu/~maroti/wiegold.pdf for recent developments regarding probability bounds for the theorem.

Further reading: *Introduction to Algebra, 2nd Edition* by Peter J. Cameron, Oxford University Press, 2007, chapter 3.