The regularity of cycles in permutation groups

1 Content

Since the end of previous century there has been a growing interest in application of probability in finite groups. Probability can be applied to the theory of finite groups in a number of cases like probabilistic statements about groups, construction of randomized algorithms in computational group theory or application of probabilistic methods to prove deterministic theorems in group theory. When we talk about probabilistic statements about groups, we talk about the statistical group theory.

We are interested in the number of regular cycles in a given permutation group of degree n. In more detail, let G be a subgroup of S_n. Then we have a conjecture, that $\frac{|C(G)|}{|G|} \leq \frac{\varphi(n)}{n}$, where $|C(G)|$ is the number of all cycles of length n in the group G and $\varphi(n)$ is Euler's totient function.

The expression $\frac{|C(G)|}{|G|}$ can also be interpreted as the probability, that a randomly selected element from permutation group is a cycle of length n (generates a transitive group). Another interpretation of this problem is related to the notion of the cycle index. See the book *Graphical enumeration* Frank Harary, Edgar M. Palmer for further details.

Moreover it should be mentioned that Gareth A. Jones referred in his article *Primitive permutation groups containing a cycle* on similarly questions, which have been raised by Zvonkin.

The statistics of random permutations, such as the cycle structure are of fundamental importance in the analysis of algorithms, especially of sorting algorithms, which operate on random permutations.

2 Methods of the investigation

The methods used are combinatorial and probabilistic methods in the theory finite groups.

We also used the computer algebra system GAP. We developed an algorithm to successfully verify the conjecture for groups of degree $16-30$. GAP was chosen, because it has a classification of all transitive subgroups of the symmetrical group up to conjugacy of order less than 31.

3 Results

In this work the above conjecture was proved for primitive and imprimitive groups separately.

A partition of the set $1,\ldots,n$ is $1,\ldots,n = \bigcup\limits_{i=1}^{m} B_i$, where $\{B_i\}_{i=1}^{m}$ are mutually disjoint sets. A permutation group G is called primitive, if it does not preserve any nontrivial partition; otherwise it called imprimitive.

The case of primitive groups based on the Jones's classification, which was published in 2004. He listed all primitive groups that contain at least one cycle of length n. But nothing about the number of such cycles was known.

We proved the conjecture for solvable primitive groups. For unsolvable primitive groups we umproved the estimate.

Theorem 1. *Let G be an unsolvable primitive permitation group of degree n. Then $\frac{|C(G)|}{|G|} \leq \frac{2}{n}$. Moreover, the equality holds if and only if G is A_n for odd $n \geq 3$, $P\Gamma L_2(8) \subset S_9$, $PSL_2(11) \subset S_{11}$, $M_{11} \subset S_{11}$, $M_{23} \subset S_{23}$.*

The case of imprimitive groups was reduced to studying such interesting structures as the wreath products of groups.

The wreath product of groups G and $H (G\,wr\,H)$ can be constructed in the next way. Take m copies of group G and let group H acts on these m copies. Other words, the wreath product of groups G and H is a semidirect product of a direct product of m groups G with group H.

Theorem 2. *Suppose the conjecture holds for subgroups $G \subset S_n$ and $H \subset S_m$. Then it also holds for the wreath product $G\,wr\,H \subset S_{nm}$.*

Theorem 3. *The conjecture holds for arbitrary subgroups of the wreath product of two cyclic groups $C_n\,wr\,C_m \subset S_{nm}$.*

In addition, we explicitly described all cases from *Theorem 3*, when the equality holds. This involves various techniques from number theory.

4 Conclusion

Summing up, we obtained the following new results. The frequency of the cycles of the length n in permutations groups of degree n was estimated. For unsolvable primitive groups we obtained an exacted upper bound of $\frac{2}{n}$ and described all cases, when this bound is achieved. For imprimitive the estimate was known only for trivial cases like the wreath product of two cyclic groups. This paper presents the results for the wreath product of arbitrary groups and for all subgroups of wreath product of cyclic groups.

In the latter case we found call such subgroups, when equality holds.