Finding a cycle base of a permutation group in polynomial time

Mikhail Muzychuk, Ilia Ponomarenko

PII: S0021-8693(18)30221-7
DOI: https://doi.org/10.1016/j.jalgebra.2018.03.028
Reference: YJABR 16649

To appear in: *Journal of Algebra*

Received date: 20 March 2018

FINDING A CYCLE BASE OF A PERMUTATION GROUP IN POLYNOMIAL TIME

MIKHAIL MUZYCHUK AND ILIA PONOMARENKO

Abstract. A cycle base of a permutation group is defined to be a maximal set of its pairwise non-conjugate regular cyclic subgroups. It is proved in this paper that a cycle base of a permutation group of degree n can be constructed in polynomial time in n.

1. Introduction

It is well known that the graph isomorphism problem is polynomial-time equivalent to finding the automorphism group of a graph. However, it is not clear whether the automorphism group given as the input can help to test isomorphism. Our main result says that it does help if the input graph (or any other combinatorial object, see the definition below) is circulant. To be more precise, we need the concept of a cycle base explained in the next paragraph.

Any permutation group $K \leq \mathrm{Sym}(n)$ acts by conjugation on the set

$$\mathrm{cyc}(K) = \{G \leq K : \ G \text{ is regular and cyclic}\}.$$

A *cycle base* of K is an arbitrary subset $B \subseteq \mathrm{cyc}(K)$ that intersects each K-orbit of this action by exactly one element. In other words, B is a maximal set of pairwise non-conjugate regular cyclic subgroups of K. Notice that a cycle base is empty if K does not contain a full cycle.

The concept of a cycle base, in a slightly different form, was first used in [15] for efficient recognition and isomorphism testing of circulant tournaments. Ten years later a cycle base technique was successfully applied to construct efficient algorithms for recognition and isomorphism testing of circulant graphs [3, 14]. In particular, an efficient algorithm constructing a cycle base of the automorphism group of a graph had been developed in [3].

Note that elementary counting arguments show that a size of any cycle base of a permutation group $K \leq \mathrm{Sym}(n)$ is bounded from above by $n-1$. Using the classification of finite simple groups, this bound was improved in [13] to $\varphi(n)$, where φ is the Euler function.

In what follows, under a *combinatorial object*, we mean any object X of a concrete category in the sense of [1]; it is called *circulant* if the group $\mathrm{Aut}(X)$ contains a regular cyclic subgroup. The idea to use cycle bases for isomorphism testing of circulant combinatorial objects goes back to Babai's lemma [1, Lemma 3.1] which established a correspondence between Cayley representations of a combinatorial

2010 Mathematics Subject Classification. 20B25, 20B40.

Key words and phrases. Cayley object, cycle base, automorphism group, canonical labeling, polynomial-time algorithm.

The first author was supported by the Israeli Ministry of Absorption.