Acta Math. Univ. Comenianae
Vol. LXXXVIII, 3 (2019), pp. 973–975

TESTING ISOMORPHISM OF CIRCULANT OBJECTS IN POLYNOMIAL TIME

M. MUZYCHUK AND I. PONOMARENKO

ABSTRACT. We show that isomorphism testing of two cyclic combinatorial objects may be done in a polynomial time provided that both objects share the same regular cyclic group of automorphisms given in advance.

1. INTRODUCTION

In this note we consider combinatorial objects as the objects of a *concrete category* $\mathfrak{K}$ [**1**]. In such a category, each object $X \in \mathfrak{K}$ is associated with an underlying set $\Omega(X)$, and each isomorphism from X to Y is associated with a bijection $f\colon \Omega(X) \to \Omega(Y)$; the set of all these bijections is denoted by $\mathrm{Iso}_{\mathfrak{K}}(X, Y)$. It is also assumed that for any bijection f from the set $\Omega(X)$ to another set, there exists a unique object $Y = X^f$ for which this set is the underlying one and $f \in \mathrm{Iso}(X, Y)$. Thus,

$$X \cong_{\mathfrak{K}} Y \quad \Leftrightarrow \quad Y = X^f \text{ for some } f \in \mathrm{Iso}(X, Y).$$

Given a set $K \subseteq \mathrm{Sym}(\Omega)$ of permutations and two objects $X, Y \in \mathfrak{K}$ with $\Omega(X) = \Omega(Y)$, we write $\mathrm{Iso}_K(X, Y)$ for the intersection $K \cap \mathrm{Iso}_{\mathfrak{K}}(X, Y)$.

In what follows by a *Cayley object* of $\mathfrak{K}$ over a group G we mean any $X \in \mathfrak{K}$ such that $\Omega(X) = G$ and the group $\mathrm{Aut}_{\mathfrak{K}}(X) := \mathrm{Iso}_{\mathfrak{K}}(X, X)$ contains the subgroup induced by the right regular representation of G.

A particular example of a concrete category is formed by relational structures. A *relational structure* is a pair $X = (\Omega, \mathcal{R})$ consisting of a ground set Ω and a finite set of relations $\mathcal{R}$ over Ω. Isomorphisms and automorphisms of objects in this category are defined in a natural way. In this category a Cayley object over a group G is a relational structure $X = (G, \mathcal{R})$ the automorphism group of which contains the right regular representation of G. In the case of G being cyclic the object will be called *cyclic* or *circulant*.

We present a result which provides a complete solution of the following problem.

Received June 15, 2019.
2010 *Mathematics Subject Classification.* Primary 05E18, 05C60; Secondary 20B25, 68R05.
Key words and phrases. Cyclic Combinatorial Objects; isomorphism problem; polynomial time algorithm.
The first author was supported by the Israeli Ministry of Absorption. The second author was supported by the RFBR grant No. 18-01-00752.

Circulant Objects Isomorphism. *Given a cyclic group C and two Cayley relational structures over C, test whether they are isomorphic and (if so) find an isomorphism between them.*

The first result towards a solution of the above problem was obtained by Pálfy [**9**]. He proved that if the group order $n = |C|$ satisfies $(n, \varphi(n)) = 1$, then $\mathrm{Iso}(X, Y) \neq \emptyset \iff \mathrm{Iso}_{\mathrm{Aut}(C)}(X, Y) \neq \emptyset$ for any pair $X = (C, \mathcal{R}), Y = (C, \mathcal{S})$ of cyclic relational structures. This result provides a simple polynomial-time algorithm for isomorphism testing of circulant combinatorial structures. In order to cover the remaining orders of circulant objects it was proposed in [**2, 3**] to replace $\mathrm{Aut}(C)$ by a bigger set $S \subset \mathrm{Sym}(C)$ with the property $\mathrm{Iso}(X, Y) \neq \emptyset \iff \mathrm{Iso}_S(X, Y) \neq \emptyset$. This idea was further developed in [**6**] where such a set was called a *solving set*. It was shown in [**7, 8, 4**] that various classes of circulant combinatorial objects admit solving sets of polynomial size.

2. Main results

Our first main result shows that there exists a solving set which works for all circulant combinatorial objects.

Theorem 2.1. *Let C be a cyclic group of order n. Then in time* $\mathrm{poly}(n)$, *one can construct a solvable group $K \leq \mathrm{Sym}(C)$ such that for any concrete category $\mathfrak{K}$ and any two Cayley objects $X, Y \in \mathfrak{K}$ over C,*

$$\mathrm{Iso}_{\mathfrak{K}}(X, Y) \neq \varnothing \iff \mathrm{Iso}_K(X, Y) \neq \varnothing. \tag{1}$$

The group K mentioned above is permutation isomorphic to the iterated wreath product

$$K = \mathrm{AGL}(1, p_1) \wr \cdots \wr \mathrm{AGL}(1, p_d),$$

where $p_1 \geq \cdots \geq p_d$ are primes such that $n = p_1 \cdots p_d$. One can replace the group K by a smaller group, e.g., the Hall π- subgroup of K, where $\pi = \{p_1, \ldots, p_d\}$. However, it is doubtful that the order of such a group can be bounded from above by a polynomial in n.

In order to apply the above result to the concrete category of relational structures we represent relational structures by special colored hypergraphs in such a way that the required isomorphisms could be taken inside a solvable group K constructed in Theorem 2.1. Finding an isomorphism $f \in K$ in polynomial time can be done with the help of Miller's algorithm designed for isomorphism testing of hypergraphs [**5**]. This yields us the following result.

Theorem 2.2. *The isomorphism of any two circulant objects can be tested in time polynomial in their sizes.*

As a corollary we obtain the following statement.

Theorem 2.3. *The isomorphism of any two circulant hypergraphs can be tested in time polynomial in their sizes.*

In particular, this result provides a polynomial algorithm for isomorphic testing of circulant Steiner triple systems.

References

1. Babai L., *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Acad. Sci. Hung. **29** (1977), 329–336.

2. Huffman W. G., Job A. and Pless V., *Multipliers and generalized multipliers of cyclic objects and cyclic codes*, J. Combin. Theory Ser. A **62** (1993), 183–215.

3. Huffman W. C., *The equivalence of two cyclic objects on pq elements*, Discrete Math. **154** (1996), 103–127.

4. Koike H., Kovács I., Marušič D. and Muzychuk M., *Cyclic groups are CI-groups for balanced configurations*, Designs, Codes and Cryptography **86** (2019), 1227–1235.

5. Miller M., *Isomorphism of graphs which are pairwise k-separable*, Information and Control **56** (1983), 21–33 .

6. Muzychuk M., *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198** (1999), 589–606.

7. Muzychuk M., *A solution of the isomorphism problem for circulant graphs*, Proc. Lond. Math. Soc. **88** (2004), 1–41.

8. M. Muzychuk, *A solution of an equivalence problem for semisimple cyclic codes*, in: Topics in Finite Fields, Contemp. Math. 632, AMS, 2013, 327–334.

9. Pálfy P. P., *Isomorphism problem for relational structures with a cyclic automorphism*, European J. Combin. **8** (1987), 35–43.

M. Muzychuk, Ben-Gurion University, Beer-Sheva, Israel,
e-mail: `muzychuk@bgu.ac.il`

I. Ponomarenko, Steklov Institute of Mathematics at St. Petersburg, Russia,
e-mail: `inp@pdmi.ras.ru`