Isomorphism testing for orthomodular lattices

Tomasz A. Gorazd and Paweł M. Idziak
Wyższa Szkoła Biznesu – National-Louis University
in Nowy Sącz, Poland
{gorazd, idziak}@wsb-nlu edu pl

Abstract

We show that the computational complexity of the isomorphism testing of orthomodular lattices is polynomially equivalent to the graph isomorphism testing.

An isomorphism testing problem for a class $\mathcal{L}$ of structures ($\mathcal{L}$–**Iso**) is to determine the exact computational complexity of the following question:

INSTANCE: Two finite structures from $\mathcal{L}$.

QUESTION: Is there an isomorphism between them ?

Isomorphism testing problem for graphs, $\mathcal{G}$–**Iso**, is one of the most exciting algorithmic problem in the complexity theory. This is because it is one of the few naturally arising problems that are suspected to be of intermediate complexity: It is in the class NP, but neither it is proved to be NP-complete nor a polynomial time algorithm for it is known.

For the discussion on the isomorphism testing problem for algebras we refer the reader to the previous papers of the authors [3, 4]. In particular, in [3], a polynomial time algorithm for isomorphism testing in any directly representable variety was described. A variety is directly representable if it has only finitely many directly indecomposable algebras. In general such a variety splits into a product of two subvarieties – an affine variety over a ring of finite representation type and a semisimple arithmetical variety. A variety is semisimple if each its subdirectly irreducible algebra is simple, i.e.,

has only two congruences. A natural generalization of semisimplicity is congruence linearity, that is the assumption that each subdirectly irreducible algebra has a chain as its congruence lattice. Using a completely different technique, it was shown in [2] that for finitely generated arithmetical varieties the assumption of semisimplicity can be relaxed to congruence linearity and still the isomorphism testing problem in such varieties is solvable in a polynomial time. A natural question to ask is how these assumptions can be further relaxed.

In this paper we show that requiring that the variety is finitely generated is essential. Indeed, we consider the variety generated by the class $\mathcal{K}$ of all orthomodular lattices of height at most 3 i.e., $\mathcal{OML}_3 = HSP(\mathcal{K})$. We prove that this variety is semisimple (and therefore congruence linear) and arithmetical (Lemma 3), but the isomorphism testing for the algebras in $\mathcal{OML}_3$ is as hard as the one for arbitrary graphs (Theorem 5). In view of the result of [2] it suggests that the variety $\mathcal{OML}_3$ is not finitely generated. However, since it may happen that $\mathcal{G}$–**Iso** $\in$ PTIME, we give a direct prove of the fact that $\mathcal{OML}_3$ is not finitely generated (Lemma 4).

An inspiration for considering orthomodular lattices as a realm in which a semisimple arithmetical variety with complex isomorphism testing could be found is taken from the work of M.Sherif [8].

Definition 1 *By an* **ortholattice** *we mean an algebra* $(L, \vee, \wedge, ', 0, 1)$ *of the type* $\langle 2, 2, 1, 0, 0\rangle$ *that satisfy:*

- $(L, \vee, \wedge, 0, 1)$ *is a bounded lattice,*
- $x \wedge x' = 0$ *and* $x \vee x' = 1$,
- $(x \wedge y)' = x' \vee y'$ *and* $(x \vee y)' = x' \wedge y'$
- $(x')' = x$.

If additionally L *satisfies*

- $x \leq y$ *implies* $x \vee (x' \wedge y) = y$

then L *is called an* **orthomodular lattice**.

A system $(L, \leq, ')$ *is an* **orthoposet** *if* $(L, \leq)$ *is a partially ordered set with the least element* 0 *and the largest element* 1, *and the following holds:*

- $x \leq y$ *implies* $y' \leq x'$,
- $(x')' = x$,
- $x \wedge x' = 0$ *and* $x \vee x' = 1$.

Orthomodular lattices generalize Boolean algebras and are commonly used as a natural semantics for quantum logic. We refer to the excellent monograph [5] for basic facts and the arithmetic of orthomodular lattices. In particular we use Greechie diagrams and construction to glue Boolean algebras into orthomodular lattices.

We say that a family $\mathcal{B}$ of finite boolean algebras is **almost disjoint**, if two different Boolean algebras $A, B \in \mathcal{B}$ intersect almost trivially, i.e., either $A \cap B = \{0, 1\}$ where $0_A = 0 = 0_B, 1_A = 1 = 1_B$, or $A \cap B = \{0, 1, x, x'\}$ where x is an atom both in A and in B and $x'^A = x' = x'^B$.

For an almost disjoint family $\mathcal{B}$ of Boolean algebras one can define a partial order on the join $\bigcup \mathcal{B}$ by putting:

$$a \leq b \quad \text{iff} \quad \exists B \in \mathcal{B}\ (a, b \in B\ \&\ a \leq_B b).$$

Moreover one can define a unary operation $'$ on $\bigcup \mathcal{B}$, so that $(\bigcup \mathcal{B}, \leq, ')$ forms an orthoposet.

A family $\mathcal{B}$ of Boolean algebras is said to contain a loop of length n, if there are $B_0, \ldots, B_{n-1}$, in $\mathcal{B}$ such that

$$\begin{aligned} B_i \cap B_{i+1} &= 4 \pmod n, \\ B_i \cap B_j &= \{0, 1\} \text{ for } j \neq i-1, i+1 \pmod n, \\ B_0 \cap B_1 \cap B_2 &= \{0, 1\} \text{ if } n = 3. \end{aligned}$$

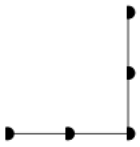
Lemma 2 (Greechie Loop Lemma [5]) *For an almost disjoint family $\mathcal{B}$ of Boolean algebras, the orthoposet $(\bigcup \mathcal{B}, \leq, ')$ is a reduct of an (unique) orthomodular lattice if and only if algebras in $\mathcal{B}$ contain no loops of length 3 or 4.*

Using Loop Lemma one can present orthomodular lattices that are joins of Boolean algebras with the help of so-called Greechie diagrams. Every finite Boolean algebra is determined by the number of its atoms, and therefore in Griechie diagram is drawn as a line containing dots which symbolize the

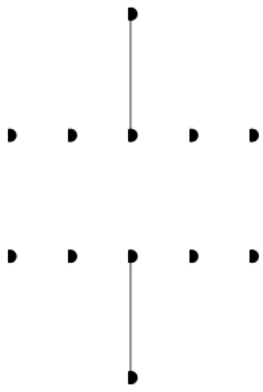
atoms. An orthomodular lattice that is a join of an almost disjoint family $\mathcal{B}$ of Boolean algebras can be then drawn as a set of segments – one for each algebra. By the fact that $\mathcal{B}$ is almost disjoint we know that two segments have at most one point in common.

For example the diagram

represents the Boolean algebra with 3 atoms, i.e., 8 elements, while



is the orthomodular lattice which is a sum of two Boolean algebras with a common atom, that is the lattice



In particular, if all Boolean algebras in $\mathcal{B}$ have 3 atoms then the orthomodular lattice $\bigcup\mathcal{B}$ is of hight 3, i.e., belongs to $\mathcal{OML}_3$.

Now we are ready to prove the following

Lemma 3 *The variety $\mathcal{OML}_3$ is semisimple arithmetical.*

Proof: The variety of orthomodular lattices is congruence distributive because every lattice is congruence distributive [7, Theorem 2.50]. Moreover, one can easily check [5, Exercise 4, page 86] that the term

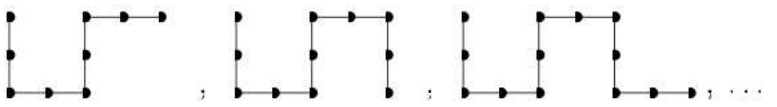
$$p(u, v, w) = (u \vee ((v \vee w) \wedge v')) \wedge (w \vee ((u \vee v) \wedge v'))$$

satisfies the identities $p(x, x, y) = y = p(y, x, x)$, i.e., is a Mal'tsev term for orthomodular lattices so that $\mathcal{OML}_3$ is congruence permutable, and therefore arithmetical.

To show that the variety $\mathcal{OML}_3 = HSP(\mathcal{K})$ is congruence linear, first note that, by Jónsson Lemma all its subdirectly irreducibles are in $HSP_U(\mathcal{K})$. Obviously all lattices in $\mathcal{K}$ are of hight at most 3, and this property can be expressed by a universal first order sentence. Such sentences are obviously preserved by ultraproducts and subalgebras, so that all lattices in $SP_U(\mathcal{K})$ are of hight at most 3. Moreover, homomorphism can only collapse points in a chain. Therefore all algebras in $HSP_U(\mathcal{K})$, and therefore all subdirectly irreducible algebras in $\mathcal{OML}_3$ are of hight at most 3. On the other hand [5, Theorem 9, page 79] tells us that an orthomodular lattice L without infinite chains is subdirectly irreducible if and only if L is simple. Therefore all subdirectly irreducibles of $\mathcal{OML}_3$ are simple and $\mathcal{OML}_3$ is semisimple. ∎

Lemma 4 *The variety $\mathcal{OML}_3$ is not finitely generated.*

Proof: Since the variety $\mathcal{OML}_3$ is congruence distributive it is enough to exhibit infinitely many subdirectly irreducible algebras in it. Obviously all of the algebras from the next picture are in $\mathcal{OML}_3$:



By [5, Theorem 10, page 79] we know that the congruence lattice of an orthomodular lattice L with no infinite chains is isomorphic to the center of L, i.e., the sublattice $C(L) = \{x \in L : x = (x \wedge y) \vee (x \wedge y') \text{ for any } y \in L\}$. Now, let L be one of the orthomodular lattices from the above picture, i.e., L is a union of at least 4 Boolean algebras $B_1, \ldots, B_\ell$ of size 8. Let

$x \in L - \{0,1\}$ belongs to a summand B_i. Since $\ell \geq 4$ then there is j such that $B_j \cap B_i = \{0,1\}$. Taking any $y \in B_j - \{0,1\}$ we have $x \wedge y = 0$ and $x \wedge y' = 0$, a witness for $x \notin C(L)$. Thus $C(L) = \{0,1\}$ and therefore all the lattices with the above Greechie diagrams are simple.

This infinite sequence of subdirectly irreducibles shows that $\mathcal{OML}_3$ is not finitely generated, see [1, Corollary 6.10]. ∎

The next step is to show that the isomorphism problem for $\mathcal{OML}_3$ is isomorphism complete, i.e., polynomial time equivalent to the isomorphism problem for graphs.

Theorem 5 *The isomorphism problem for the variety $\mathcal{OML}_3$ is isomorphism complete.*

Proof: Our proof consists of 3 reductions. First we define two auxiliary classes of finite graphs:

- $\mathcal{G}_3$ – the class of finite graphs with the vertex degree at least 3,
- $\mathcal{C}$ – the class of finite graphs that contain no cycles of size 3 or 4 and in which each vertex has degree at least 2.

The 3 reductions are:

1. $\mathcal{G}$–**Iso** to $\mathcal{G}_3$–**Iso**,
2. $\mathcal{G}_3$–**Iso** to $\mathcal{C}$–**Iso**,
3. $\mathcal{C}$–**Iso** to $\mathcal{OML}_3$–**Iso**.

Let G be a graph with n vertices. Pick 3 pairwise disjoint complete graphs G_1, G_2, G_3 with $n+2$ vertices each and such G has common vertex with neither of them. Then, for each $i = 1,2,3$ pick and fix a vertex $g_i \in G_i$. Define G^* to be the (disjoint) sum of the graphs G, G_1, G_2, G_3 with all additional edges of the form (g, g_i), where $g \in G$ and $i = 1,2,3$.

The vertices of G can be recovered from G^* as the ones that do not belong to any clique of size $n+2$. Now, since G is an induced subgraph of G^*, it is easy to see that for any graphs G_1, G_2 we have $G_1 \cong G_2$ iff $G_1^* \cong G_2^*$.

Obviously the construction of G^* from G is polynomial time, so that the reduction (1) is done.

For our second reduction we start with a graph $G = (V, E)$ in $\mathcal{G}_3$. We treat edges of G as two element subsets of V and assume that $V \cap E = \emptyset$. We form a new graph $G' = (V', E')$ by putting

$$\begin{aligned} V' &= V \cup E, \\ E' &= \{\{x, e\} \ : \ x \in e \in E\}. \end{aligned}$$

Obviously, G' is construable from g in a polynomial time and if $G \in \mathcal{G}_3$ then G' is in $\mathcal{C}$. Moreover, if $G_1, G_2 \in \mathcal{G}_3$ and $G_1 \cong G_2$ then $G_1' \cong G_2'$. To show that also $G_1' \cong G_2'$ implies $G_1 \cong G_2$ it suffices to show that G can be recovered from G' e.g. by first order formulas. Consider the following ones

$$\begin{aligned} VER(x) &\equiv x \text{ has degree at least 3} \\ EDGE(x, y) &\equiv VER(x) \ \& \ VER(y) \ \& \ x \neq y \ \& \ \exists z \ (xE'z \ \& \ yE'z), \end{aligned}$$

and note that the graph $G \in \mathcal{G}_3$ is isomorphic to the graph determined by the pair $(VER, EDGE)$ in G'.

Our final step is a polynomial time reduction from $\mathcal{C}$–**Iso** to $\mathcal{OML}_3$–**Iso**. Our encoding is modelled after the one of [8].

Let $G = (V, E)$ be a graph from $\mathcal{C}$ and let V and E be disjoint. For any element $x \in V \cup E$ define a new element x'. Additionally let 0 and 1 be totally new elements. Now define the family $\mathcal{B}_G = \{B_e \ : \ e \in E\}$ of Boolean algebras where:

$$B_e = \{0, 1, p, p', q, q', e, e'\}$$

for $e = \{p, q\} \in E$.

The Boolean structure of B_e is determined by taking 0 as the least element, p, q, e as the atoms and $'$ for complement. The family $\mathcal{B}_G$ is almost disjoint. Since the graphs from $\mathcal{C}$ do not have 3- or 4-cycles, $\mathcal{B}_G$ has no loops of length 3 or 4. Now using Loop Lemma 2 we get the orthomodular lattice $B(G) = \bigcup \mathcal{B}_G$. Since $B(G) \in O(\ V\ ^2)$ we can obtain $B(G)$ from G in a polynomial time.

Again if $G_1, G_2 \in \mathcal{C}$ are isomprphic then so are $B(G_1)$ and $B(G_2)$ Now let us consider the following formulas in the language of ortholattices:

$$\begin{aligned} AT(x) &\equiv x \text{ is an atom} \\ VER(x) &\equiv AT(x) \ \& \text{ there are at least 5 elements above } x \\ EDGE(x) &\equiv AT(x) \ \& \ \neg VER(x) \\ E(x,y) &\equiv AT(x) \ \& \ AT(y) \ \& \ \exists u \ (EDGE(u) \ \& \ (x \vee y = u')) \end{aligned}$$

One can easily see that the pair (VER, E) determines in $B(G)$ a graph isomorphic to G. Therefore for any $G_1, G_2 \in \mathcal{C}$ with $B(G_1) \cong B(G_2)$ we have $G_1 \cong G_2$, as required by the reduction (3). ∎

As an easy corollary we get

Corollary 6 *The isomorphism problem for the variety of all orthomodular lattices is isomorphism complete.*

References

[1] S.Burris and H.P.Sankappanavar, *A Course in Universal Algebra,* Springer Verlag 1981.

[2] T.A.Gorazd, *Fast isomorphism testing in arithmetical varieties,* International Journal of Algebra and Computation, **13**(2003), 499–506.

[3] T.A.Gorazd, *The isomorphism testing for directly representable varieties,* Reports on Mathematical Logic, **31**(1997), 75–92.

[4] T.A.Gorazd and P.M.Idziak, *The isomorphism problem for varieties generated by a two-element algebra,* Algebra Universalis, **34**(1995), 430–439.

[5] G.Kalmbach, *Orthomodular Lattices,* Academic Press, 1983.

[6] D.Kozen, *Complexity of finitely presented algebras,* Proc. 9^{th} Symposium STOC (1977), 164–177.

[7] R.McKenzie, G.McNulty and W.Taylor, *Algebras, Lattices, and Varieties. Vol. I.* Wadsworth and Brooks/Cole, Mathematics Series, 1987.

[8] M.Sherif, *Decision problem for orthomodular lattices,* Algebra Universalis, **37**(1997), 70–76.