

Strong isomorphism reductions in complexity theory*

Sam Buss[†], Yijia Chen[‡], Jörg Flum[§], S.-D. Friedman[¶], Moritz Müller[¶]

[†]Department of Mathematics, University of California, San Diego, La Jolla, California 92093-0112, USA
sbuss@math.ucsd.edu

[‡]Basic Studies in Computing Science (BASICS), Department of Computer Science, Shanghai Jiaotong University, Shanghai 200030, China
yijia.chen@cs.sjtu.edu.cn

[§]Mathematisches Institut, Albert-Ludwigs Universität Freiburg, 79104 Freiburg, Germany
joerg.flum@math.uni-freiburg.de

[¶]Kurt Gödel Research Center, Währinger Straße 25, A-1090 Wien, Austria
sdf@logic.univie.ac.at, moritz.mueller@univie.ac.at

Abstract. We give the first systematic study of strong isomorphism reductions, a notion of reduction more appropriate than polynomial time reduction when, for example, comparing the computational complexity of the isomorphism problem for different classes of structures. We show that the partial ordering of its degrees is quite rich. We analyze its relationship to a further type of reduction between classes of structures based on purely comparing for every n the number of nonisomorphic structures of cardinality at most n in both classes. Furthermore, in a more general setting we address the question of the existence of a maximal element in the partial ordering of the degrees.

Introduction

In many areas of computational complexity, polynomial time reduction is the appropriate notion for comparing the complexity of problems. However, suppose that we face, for example, the problem of comparing the complexity of the isomorphism problem for two classes C and D of graphs. Here

$$\text{Iso}(C) := \{(\mathcal{A}, \mathcal{B}) \mid \mathcal{A}, \mathcal{B} \in C \text{ and } \mathcal{A} \cong \mathcal{B}\}$$

is the isomorphism problem for C (more precisely, the set of positive instances of this problem) and $\text{Iso}(D)$ is defined analogously. Probably we would not accept a polynomial time computable function $f : C \times C \rightarrow D \times D$ with

$$(\mathcal{A}, \mathcal{B}) \in \text{Iso}(C) \iff f(\mathcal{A}, \mathcal{B}) \in \text{Iso}(D)$$

as the right notion of reduction in this context but we would seek a *strong isomorphism reduction*, that is, a polynomial time computable function $f : C \rightarrow D$ with

$$(1) \quad \mathcal{A} \cong \mathcal{B} \iff f(\mathcal{A}) \cong f(\mathcal{B}).$$

This paper is devoted to the study of this type of reduction. For us the motivation for this study came from various areas:

* Published in *Journal of Symbolic Logic* 76(4): 1381-1402, 2011. The authors thank the John Templeton Foundation for its support through Grant #13152, *The Myriad Aspects of Infinity*

[†] The first author has been supported in part by NSF grant DMS-0700533.

Computational complexity: The isomorphism relation (on a class C) is an equivalence relation. In the context of arbitrary equivalence relations a notion of reduction defined analogously as in (1) (and that for the isomorphism relation coincides with our notion) has been introduced in [7]. However that paper is mainly devoted to other problems (see the end of Section 6 for some more details); concerning the notion of reduction only some open problems are stated in [7], problems we address in our paper.

Descriptive set theory: For the isomorphism relation our notion of reduction was first considered by the fourth author (see [8]) inspired by the analogous notion from descriptive set theory (see [9]). In descriptive set theory, C and D denote classes of structures with universe \mathbb{N} and the function f satisfying (1) is required to be Borel (in the topology generated by the first-order definable classes).

Descriptive complexity: The existence of a logic capturing polynomial time remains the central open problem of descriptive complexity theory. For many classes C of graphs (or of other types of structures), one shows that a logic L captures polynomial time on C by defining in L an invariantization for C . From the definition of invariantization (given in Section 3), one immediately gets that if C is strongly isomorphism reducible to D , then C has an invariantization if D has one.

This paper contains the first systematic study of strong isomorphism reductions. In Section 2 and Section 3 we introduce our framework, derive some basic properties of strong isomorphism reductions, and explain via invariantizations and canonizations the relationship to logics capturing polynomial time mentioned above. At various places of our analysis, invariantizations and canonizations will be valuable tools. Their relationship and the computational complexity of problems related to these notions have been studied in [2, 3, 7, 11, 15, 16].

We denote by \leq_{iso} the partial ordering on the set of degrees induced by strong isomorphism reductions. In Section 2 we observe that (the degree of) the class of graphs is the \leq_{iso} maximum element. Furthermore, by Theorem 3.7 we see that some “basic algebraic classes of structures” all have the same strong isomorphism degree. In Section 4 we show that the structure of \leq_{iso} is rich already when restricting to classes with an invariantization.

Assume that C is strongly isomorphism reducible to D . Since such reductions are computable in polynomial time we know that for some polynomial $p \in \mathbb{N}[X]$ and all $n \in \mathbb{N}$ the number of isomorphism types of structures in C with at most n elements is at most the number of isomorphism types of structures in D with at most $p(n)$ elements. If this condition is satisfied, then following [8] we say that C is potentially reducible to D . Already in Section 4 this concept is the main tool to demonstrate the richness of the partial ordering \leq_{iso} . We believe that the notions of strong isomorphism reducibility and that of potential reducibility are distinct but can only show this under the hypothesis $\text{U2EXP} \cap \text{co-U2EXP} \neq \text{2EXP}$ (see Section 5). It turns out in Section 6 that we would get $\text{P} \neq \#\text{P}$ if we could separate the two notions without any complexity-theoretic assumption.

The isomorphism relation is an equivalence relation in NP. In Section 7 we study reductions (defined in analogy to (1)) between arbitrary equivalence relations in NP. In particular, we show that there is a maximum element in the corresponding partial ordering if and only if there is an effective enumeration of these equivalence relations by means of clocked Turing machines. Even if we restrict to equivalence relations in P (=

PTIME), we cannot show that a maximum element exists; we can guarantee its existence if a p-optimal propositional proof system exists. The existence of a maximum element for equivalence relations in P was addressed in [7, Open Question 4.14].

The authors wish to acknowledge the generous support of the John Templeton Foundation and the Centre de Recerca Matemàtica through the CRM Infinity Project. Sam Buss' work was supported in part by NSF grant DMS-0700533. This article will appear in the December 2011 issue of the Journal of Symbolic Logic.

1 Some preliminaries

Throughout the paper Σ denotes the alphabet $\{0, 1\}$, and Σ^* is the set of strings over this alphabet. For $n \in \mathbb{N}$ we denote by 1^n the string $11 \dots 1$ of length n . An ordered pair (x, y) of strings $x = x_1 \dots x_k$, $y = y_1 \dots y_\ell$ with $x_1, \dots, y_\ell \in \Sigma$ is coded (identified) with the string $x_1 x_1 \dots x_k x_k 0 1 y_1 y_1 \dots y_\ell y_\ell$. We do similarly for tuples of arbitrary length. Sometimes statements containing a formulation like “there is a $d \in \mathbb{N}$ such that for all $x \in \Sigma^*$: $\dots \leq |x|^d$ ” can be wrong for $x \in \Sigma^*$ with $|x| \leq 1$ (here $|x|$ denotes the length of the string x). We trust the reader's common sense to interpret such statements reasonably.

1.1 Structures and classes of structures

A *vocabulary* τ is a finite set of relation symbols, function symbols, and constant symbols. The universe of a τ -structure \mathcal{A} will be denoted by the corresponding Latin letter A and the interpretation of a symbol $s \in \tau$ in \mathcal{A} by $s^{\mathcal{A}}$.

All structures in this paper are assumed to be finite and to have $[n] := \{1, 2, \dots, n\}$ as universe for some $n \in \mathbb{N}$.

Therefore, in a canonical way we can identify structures with nonempty strings over Σ . In particular, $|\mathcal{A}|$ for a structure \mathcal{A} is the length of the string \mathcal{A} . Furthermore, we may assume that for every vocabulary τ there is a polynomial $q_\tau \in \mathbb{N}[X]$ such that $|\mathcal{A}| \leq |\mathcal{A}| \leq q_\tau(|\mathcal{A}|)$ for every τ -structure \mathcal{A} , where for a set M we denote by $|M|$ its cardinality.

A class C of τ -structures is *closed under isomorphism* if for all structures \mathcal{A} and \mathcal{B}

$$\mathcal{A} \in C \text{ and } \mathcal{A} \cong \mathcal{B} \text{ imply } \mathcal{B} \in C$$

(recall that we restrict to structures with universe $[n]$ for some $n \in \mathbb{N}$).

In the rest of the paper C (and D) will always denote a class of structures which is in P, is closed under isomorphism, and contains arbitrarily large (finite) structures. Moreover, all structures in a fixed class will have the same vocabulary.

Examples of such classes are:

- The classes SET, BOOLE, FIELD, GROUP, ABELIAN, and CYCLIC of sets (structures of empty vocabulary), Boolean algebras, fields, groups, abelian groups, and cyclic groups, respectively.
- The class GRAPH of (undirected and simple) graphs. We view graphs as τ_{GRAPH} -structures, where $\tau_{\text{GRAPH}} := \{E\}$ for a binary relation symbol E .
- The class ORD of linear orderings. Here we use the vocabulary $\tau_{\text{ORD}} := \{<\}$ with a binary relation symbol $<$.

- The class LOP of *Linear Orderings* with a distinguished *Point* and the class LOU of *Linear Orderings* with a *Unary* relation. Let $\tau_{\text{LOP}} := \tau_{\text{ORD}} \cup \{c\}$ with a constant symbol c and $\tau_{\text{LOU}} := \tau_{\text{ORD}} \cup \{P\}$ with a unary relation symbol P . Then LOP (LOU) is the class of all τ_{LOP} -structures (τ_{LOU} -structures) \mathcal{A} such that $(A, <^{\mathcal{A}}) \in \text{ORD}$.

There is a natural one-to-one correspondence between strings in Σ^* and structures in LOU, namely the function which assigns to a string $x = x_1 \dots x_n \in \Sigma^*$ the structure $\mathcal{A} \in \text{LOU}$ with universe $[n]$, where $<^{\mathcal{A}}$ is the natural ordering on $[n]$ and $P^{\mathcal{A}} := \{i \in [n] \mid x_i = 1\}$.

2 Strong isomorphism reductions

We define the notion of strong isomorphism reduction already indicated in the Introduction and present first examples.

Definition 2.1 Let C and D be classes. We say that C is *strongly isomorphism reducible* to D and write $C \leq_{\text{iso}} D$, if there is a function $f : C \rightarrow D$ computable in polynomial time such that for all $\mathcal{A}, \mathcal{B} \in C$

$$\mathcal{A} \cong \mathcal{B} \iff f(\mathcal{A}) \cong f(\mathcal{B}).$$

We then say that f is a *strong isomorphism reduction* from C to D and write $f : C \leq_{\text{iso}} D$. If $C \leq_{\text{iso}} D$ and $D \leq_{\text{iso}} C$, denoted by $C \equiv_{\text{iso}} D$, then C and D have the same strong isomorphism degree.

Examples 2.2

- The map sending a field to its multiplicative group shows that $\text{FIELD} \leq_{\text{iso}} \text{CYCLIC}$.
- $\text{CYCLIC} \leq_{\text{iso}} \text{ABELIAN} \leq_{\text{iso}} \text{GROUP}$; more generally, if $C \subseteq D$, then $\text{id}_C : C \leq_{\text{iso}} D$ for the identity function id_C on C .
- $\text{SET} \equiv_{\text{iso}} \text{ORD} \equiv_{\text{iso}} \text{CYCLIC}$.

Remark 2.3 We can reduce the notion of strong isomorphism reduction to the notion of polynomial time reduction. For this, we introduce the problem

$\text{ISO}(C)$ <i>Instance:</i> $\mathcal{A}, \mathcal{B} \in C$. <i>Problem:</i> Is $\mathcal{A} \cong \mathcal{B}$?
--

A function $f : C \rightarrow D$ induces the function $\hat{f} : C \times C \rightarrow D \times D$ with $\hat{f}(\mathcal{A}, \mathcal{B}) := (f(\mathcal{A}), f(\mathcal{B}))$. Then

$$f : C \leq_{\text{iso}} D \iff \hat{f} : \text{ISO}(C) \leq_p \text{ISO}(D),$$

where $\hat{f} : \text{ISO}(C) \leq_p \text{ISO}(D)$ means that \hat{f} is a polynomial time reduction from $\text{ISO}(C)$ to $\text{ISO}(D)$.

Of course, it is easy to construct polynomial time reductions from $\text{ISO}(C)$ to $\text{ISO}(D)$ that are not of the form \hat{f} for some $f : C \leq_{\text{iso}} D$. Moreover, in Remark 4.2 we shall present classes C and D such that

$$\text{ISO}(C) \leq_p \text{ISO}(D) \text{ but not } C \leq_{\text{iso}} D.$$

This answers [7, Open Question 4.13].

As already mentioned in the Introduction one of our goals is to study the relation \leq_{iso} . First we see that this relation has a maximum element:

Proposition 2.4 $C \leq_{\text{iso}} \text{GRAPH}$ for all classes C .

Proof. Let τ be a vocabulary and S be the class of all τ -structures. It is well-known that there is a strong isomorphism reduction from S to GRAPH (even a first-order interpretation, e.g. see [6, Proposition 11.2.5 (i)]). In particular, its restriction to a class C of τ -structures shows that $C \leq_{\text{iso}} \text{GRAPH}$. \square

3 Invariantizations and canonizations

One of the central aims of algebra and of model theory is to describe the isomorphism type of a structure by means of an invariant. The underlying notion of invariantization is also relevant in our context. We use it (and the related notion of canonization) to show that most classes of structures mentioned in Section 1.1 have the same strong isomorphism degree (cf. Corollary 3.8).

Definition 3.1 An *invariantization* for C is a polynomial time computable function $\text{Inv} : C \rightarrow \Sigma^*$ such that for all $\mathcal{A}, \mathcal{B} \in C$

$$\mathcal{A} \cong \mathcal{B} \iff \text{Inv}(\mathcal{A}) = \text{Inv}(\mathcal{B}).$$

Lemma 3.2 If $C \leq_{\text{iso}} D$ and D has an invariantization, then also C has an invariantization.

Proof. If Inv is an invariantization for D and $f : C \leq_{\text{iso}} D$, then $\text{Inv} \circ f$ is an invariantization for C . \square

LOU is a maximum class among those with an invariantization:

Proposition 3.3 For a class C the following are equivalent.

- (1) C has an invariantization.
- (2) $C \leq_{\text{iso}} \text{LOU}$.
- (3) There is a class D of ordered structures such that $C \leq_{\text{iso}} D$.

Here, a class D is a class of ordered structures if its vocabulary contains a binary relation symbol which in all structures of D is interpreted as a linear ordering of the universe.

Proof. (1) implies (2) by the natural correspondence between strings in Σ^* and structures in LOU . That (2) implies (3) is trivial. To see that (3) implies (1) assume that there is a class D of ordered structures such that $C \leq_{\text{iso}} D$. As ordered structures have no nontrivial automorphisms, every ordered structure \mathcal{A} is isomorphic to a unique structure \mathcal{A}' whose ordering $<^{\mathcal{A}'}$ is the natural linear ordering on its universe $\{1, \dots, |\mathcal{A}'|\}$. Thus the mapping on D defined by $\mathcal{A} \mapsto \mathcal{A}'$ is an invariantization of D . Now we apply Lemma 3.2. \square

It is open whether the class GRAPH has an invariantization or equivalently (by Proposition 2.4 and Proposition 3.3) whether LOU is a maximum element of \leq_{iso} . Moreover, it is known [11, 15] that an invariantization for GRAPH yields a canonization.

Definition 3.4 A function $\text{Can} : C \rightarrow C$ computable in polynomial time is a *canonization* for C if

- (1) for all $\mathcal{A}, \mathcal{B} \in C$: $(\mathcal{A} \cong \mathcal{B} \iff \text{Can}(\mathcal{A}) = \text{Can}(\mathcal{B}))$;
- (2) for all $\mathcal{A} \in C$: $\mathcal{A} \cong \text{Can}(\mathcal{A})$.

Every class C of ordered structures, in particular LOU, has a canonization. In fact, the mapping $\mathcal{A} \mapsto \mathcal{A}'$ defined for all ordered structures in the previous proof is a canonization for C .

We do not define the notion of a *logic capturing P on a class C* (e.g. see [6]). However we mention that canonizations and invariantizations are important in descriptive complexity theory as:

Proposition 3.5

- (1) *If C has a canonization, then there is a logic capturing P on C .*
- (2) *If GRAPH has an invariantization, then there is a logic capturing P (on all finite structures).*

Clearly, every canonization is an invariantization. Often the invariantizations we encounter in mathematics yield canonizations. For example, consider the class FIELD of fields. Then an invariant for a field \mathcal{K} is the pair $(p_{\mathcal{K}}, n_{\mathcal{K}})$, where $p_{\mathcal{K}}$ is its characteristic and $n_{\mathcal{K}}$ its dimension over the prime field. As for every invariant (p, n) one can explicitly construct a canonical field \mathcal{F}_{p^n} of this invariant, we see that the mapping $\mathcal{K} \mapsto \mathcal{F}_{p_{\mathcal{K}}^{n_{\mathcal{K}}}}$ is a canonization. This canonization has a further property, it is a canonization that has a polynomial time enumeration:

Definition 3.6 Let Can be a canonization for the class C . The *enumeration induced by Can* is the enumeration

$$\mathcal{A}_1, \mathcal{A}_2, \dots$$

of the image $\text{Can}(C)$ of C such that $\mathcal{A}_i <_{\text{lex}} \mathcal{A}_j$ ¹ for $i < j$. If the mappings $\mathcal{A}_n \mapsto 1^n$ and $1^n \mapsto \mathcal{A}_n$ are computable in polynomial time, then Can has a polynomial time enumeration.

Note that the mapping $\mathcal{A}_n \mapsto 1^n$ is computable in polynomial time if and only if we get an invariantization Inv of C by setting

$$\text{Inv}(\mathcal{A}) := 1^n \iff \text{Can}(\mathcal{A}) = \mathcal{A}_n.$$

The classes SET, FIELD, ABELIAN, CYCLIC, ORD, and LOP have canonizations with polynomial time enumerations (for ABELIAN see [13], for example). The classes BOOLE and LOU have canonizations but none with a polynomial time enumeration: For BOOLE the function $1^n \mapsto \mathcal{A}_n$ will not be computable in polynomial time, as there are, up to equivalence, “too few” Boolean algebras of cardinality $\leq n$, namely $\lfloor \log n \rfloor$; for LOU the function $\mathcal{A}_n \mapsto 1^n$ won’t be computable in polynomial time, as there are “too many” structures in LOU of cardinality $\leq n$, namely $2^{n+1} - 1$.

Theorem 3.7 *Assume that the classes C and D have canonizations with polynomial time enumerations. Then $C \equiv_{\text{iso}} D$.*

Corollary 3.8 *The classes SET, FIELD, ABELIAN, CYCLIC, ORD, and LOP all have the same strong isomorphism degree.*

Proof of Theorem 3.7. Let C and D be classes with canonizations Can_C and Can_D which have polynomial time enumerations $\mathcal{A}_1, \mathcal{A}_2, \dots$ and $\mathcal{B}_1, \mathcal{B}_2, \dots$ respectively. We define a strong isomorphism reduction f from C to D by:

$$f(\mathcal{A}) = \mathcal{B}_n \iff \text{Can}_C(\mathcal{A}) = \mathcal{A}_n.$$

¹By $<_{\text{lex}}$ we denote the standard (length-)lexicographic ordering on Σ^* .

Hence, $C \leq_{\text{iso}} D$; by symmetry we get $D \leq_{\text{iso}} C$. \square

An analysis of the previous proof shows that we already obtain $C \leq_{\text{iso}} D$ if the mappings $\mathcal{A}_n \mapsto 1^n$ and $1^n \mapsto \mathcal{B}_n$ are computable in polynomial time. By this, we get, for example, $\text{BOOLE} \leq_{\text{iso}} \text{CYCLIC}$.

4 On \leq_{iso} below Lop

As we have seen that the structure of \leq_{iso} between LOU and GRAPH is linked with central open problems of descriptive complexity, we turn our attention to the structure below LOU. In this section we show that there, in fact even below LOP, the structure is quite rich. In fact, this section is devoted to a proof of the following result: ²

Theorem 4.1 *The partial ordering of the countable atomless Boolean algebra is embeddable into the partial ordering induced by \leq_{iso} on the degrees of strong isomorphism reducibility below LOP. More precisely, let \mathcal{B} be a countable atomless Boolean algebra. Then there is a one-to-one function $b \mapsto C_b$ defined on B such that for all $b, b' \in B$*

- C_b is a subclass of LOP;
- $b \leq b' \iff C_b \leq_{\text{iso}} C_{b'}$.

Recall that the partial ordering of an atomless Boolean algebra has infinite antichains and infinite chains, even chains of ordertype the rationals.

Remark 4.2 By the preceding result, for example we see that there exist an infinite \leq_{iso} -antichain of classes C below LOP, whose problems $\text{ISO}(C)$ are pairwise equivalent under usual polynomial time reductions. Indeed, even $\text{ISO}(C) \in \text{P}$ for all $C \subseteq \text{LOP}$.

The reader not interested in the details of the proof of Theorem 4.1 should read until Lemma 4.5 and can then skip the rest of this section. We obtain Theorem 4.1 by comparing the number of isomorphism types of structures with universe of bounded cardinality in different classes. First we introduce the relevant notations and concepts.

For a class C we let $C(n)$ be the subclass consisting of all structures in C with universe of cardinality $\leq n$ and we let $\#C(n)$ be the number of isomorphism types of structures in $C(n)$, more formally

$$C(n) := \{\mathcal{A} \in C \mid |\mathcal{A}| \leq n\} \quad \text{and} \quad \#C(n) := |C(n)/\cong|$$

Here, for a class of structures S we denote by S/\cong the set of isomorphism classes in S .

Examples 4.3

- (1) $\#\text{BOOLE}(n) = \lfloor \log n \rfloor$, $\#\text{CYCLIC}(n) = n$ and $\#\text{SET}(n) = \#\text{ORD}(n) = n + 1$.
- (2) $\#\text{LOP}(n) = \sum_{i=1}^n i = (n+1) \cdot n/2$ and $\#\text{LOU}(n) = \sum_{i=0}^n 2^i = 2^{n+1} - 1$.
- (3) For every vocabulary τ there is a polynomial $p_\tau \in \mathbb{N}[X]$ such that $\#C(n) \leq 2^{p_\tau(n)}$ for all $n \in \mathbb{N}$ (see Subsection 1.1).
- (4) (E.g. see [1]) $\#\text{GROUP}(n)$ is superpolynomial but subexponential (more precisely, $\#\text{GROUP}(n) \leq n^{O(\log^2 n)}$).

Definition 4.4 A class C is *potentially reducible* to a class D , written $C \leq_{\text{pot}} D$, if there is some polynomial $p \in \mathbb{N}[X]$ such that $\#C(n) \leq \#D(p(n))$ for all $n \in \mathbb{N}$. Of course, by $C \equiv_{\text{pot}} D$ we mean $C \leq_{\text{pot}} D$ and $D \leq_{\text{pot}} C$.

²Recall that up to isomorphism there is a unique countable atomless Boolean algebra (e.g. see [10]).

The following lemma explains the term potentially reducible.

Lemma 4.5 *If $C \leq_{\text{iso}} D$, then $C \leq_{\text{pot}} D$.*

Proof. Let $f : C \leq_{\text{iso}} D$. As f is computable in polynomial time, there is a polynomial p such that for all $\mathcal{A} \in C$ we have $|f(\mathcal{A})| \leq p(|\mathcal{A}|)$, where $f(\mathcal{A})$ denotes the universe of $f(\mathcal{A})$. As f strongly preserves isomorphisms, it therefore induces a one-to-one map from $\{\mathcal{A} \in C \mid |\mathcal{A}| \leq n\} / \cong$ to $\{\mathcal{B} \in D \mid |\mathcal{B}| \leq p(n)\} / \cong$. \square

We state some consequences of this simple observation:

Proposition 4.6

- (1) $\text{CYCLIC} \not\leq_{\text{iso}} \text{BOOLE}$ and $\text{LOU} \not\leq_{\text{iso}} \text{LOP}$.
- (2) $C \leq_{\text{pot}} \text{LOU}$ for all classes C and $\text{LOU} \equiv_{\text{pot}} \text{GRAPH}$.
- (3) The strong isomorphism degree of GROUP is strictly between that of LOP and GRAPH , that is, $\text{LOP} \leq_{\text{iso}} \text{GROUP} \leq_{\text{iso}} \text{GRAPH}$, but $\text{LOP} \not\equiv_{\text{iso}} \text{GROUP}$ and $\text{GROUP} \not\equiv_{\text{iso}} \text{GRAPH}$.
- (4) The potential reducibility degree of GROUP is strictly between that of LOP and LOU , that is, $\text{LOP} \leq_{\text{pot}} \text{GROUP} \leq_{\text{pot}} \text{LOU}$, but $\text{LOP} \not\equiv_{\text{pot}} \text{GROUP}$ and $\text{GROUP} \not\equiv_{\text{pot}} \text{LOU}$.

Proof. Using the previous lemma we see that

- (1) follows by Examples 4.3 (1), (2);
- (2) from Examples 4.3 (2), (3) and Proposition 2.4;
- $\text{GROUP} \leq_{\text{iso}} \text{GRAPH}$ holds by Proposition 2.4 and

$$\text{LOP} \leq_{\text{iso}} \text{CYCLIC} \leq_{\text{iso}} \text{GROUP}$$

by Corollary 3.8 and Example 2.2 (b); the remaining claims in (3) follow from (4) as $\text{LOU} \equiv_{\text{pot}} \text{GRAPH}$;

- the first claim follows from the first claim in (3) as $\text{LOU} \equiv_{\text{pot}} \text{GRAPH}$; the remaining claims follow from Examples 4.3 (2), (4). \square

The following concepts and tools will be used in the proof of Theorem 4.1. We call a function $f : \mathbb{N} \rightarrow \mathbb{N}$ *value-polynomial* if it is increasing and $f(n)$ can be computed in time $f(n)^{O(1)}$. Let VP be the class of all value-polynomial functions.

For $f \in \text{VP}$ the set

$$C_f := \{\mathcal{A} \in \text{LOP} \mid |\mathcal{A}| \in \text{im}(f)\}$$

is in P and is closed under isomorphism. As there are exactly $f(k)$ pairwise nonisomorphic structures of cardinality $f(k)$ in LOP , we get

$$\#C_f(n) = \sum_{k \in \mathbb{N} \text{ with } f(k) \leq n} f(k).$$

The following proposition contains an essential idea underlying the proof of Theorem 4.1, even though it is not used explicitly. Loosely speaking, if the gaps between consecutive values of $f \in \text{VP}$ “kill” every polynomial, then there are classes C and D with $C \not\leq_{\text{pot}} D$.

Proposition 4.7 *Let $f \in \text{VP}$ and assume that for every polynomial $p \in \mathbb{N}[X]$ there is an $n \in \mathbb{N}$ such that*

$$(2) \quad \sum_{k \in \mathbb{N} \text{ with } f(2k) \leq n} f(2k) > \sum_{k \in \mathbb{N} \text{ with } f(2k+1) \leq p(n)} f(2k+1).$$

Then C_{g_0} is not potentially reducible to C_{g_1} , where $g_0, g_1 : \mathbb{N} \rightarrow \mathbb{N}$ are defined by $g_0(n) := f(2n)$ and $g_1(n) := f(2n + 1)$.

Proof. By contradiction, assume that there is some polynomial $p \in \mathbb{N}[X]$ such that $\#C_{g_0}(n) \leq \#C_{g_1}(p(n))$ for all $n \in \mathbb{N}$. Choose n such that (2) holds. Then

$$\#C_{g_0}(n) = \sum_{f(2k) \leq n} f(2k) > \sum_{f(2k+1) \leq p(n)} f(2k+1) = \#C_{g_1}(p(n)),$$

a contradiction. \square

Lemma 4.8 *The images of the functions in VP together with the finite subsets of \mathbb{N} are the elements of a countable Boolean algebra \mathcal{V} (under the usual set-theoretic operations). The factor algebra \mathcal{V}/\equiv , where for $b, b' \in \mathcal{V}$*

$$b \equiv b' \iff (b \setminus b') \cup (b' \setminus b) \text{ is finite,}$$

is a countable atomless Boolean algebra.

Proof. For a function $f : \mathbb{N} \rightarrow \mathbb{N}$ we denote by $\text{im}(f)$ the image of f . Using the definition of value-polynomial function we verify that for $f, g \in \text{VP}$ the sets

$$\mathbb{N} \setminus \text{im}(f), \quad \text{im}(f) \cap \text{im}(g), \quad \text{and} \quad \text{im}(f) \cup \text{im}(g)$$

are images of value-polynomial functions provided they are infinite. For example, assume that $\mathbb{N} \setminus \text{im}(f)$ is infinite. We choose an algorithm \mathbb{A} and a polynomial $p \in \mathbb{N}[X]$ such that for every $n \in \mathbb{N}$ the algorithm \mathbb{A} computes $f(n)$ in time $p(f(n))$. Let h be the function enumerating $\mathbb{N} \setminus \text{im}(f)$ in increasing order, that is, $h : \mathbb{N} \rightarrow (\mathbb{N} \setminus \text{im}(f))$ is increasing and surjective. We show that h is value-polynomial too.

A corresponding algorithm inductively computes pairs $(h(0), m_0), (h(1), m_1), \dots$ with

$$f(m_n) < h(n) < f(m_n + 1)$$

for all $n \in \mathbb{N}$; if $f(0) > 0$ and hence $h(0) = 0$, we set $(h(0), m_0) = (0, -1)$. For $n \geq 1$ the algorithm gets $(h(n), m_n)$ from $(h(n-1), m_{n-1})$ by the following steps:

1. Let $k := h(n-1) + 1$ and $\ell := m_{n-1}$.
2. Simulate \mathbb{A} on $\ell + 1$ for at most $p(k)$ steps.
3. If \mathbb{A} does not halt or if it outputs $f(\ell + 1)$ and $f(\ell + 1) > k$, then $(h(n), m_n) = (k, \ell)$.
4. Otherwise (i.e., if $f(\ell + 1) = k$), let $k := k + 1$ and $\ell := \ell + 1$, and goto 2.

It should be clear that the algorithm yields $(h(n), m_n)$ (more precisely, $(h(0), m_0), (h(1), m_1), \dots, (h(n), m_n)$) in time polynomial in $h(n)$.

We leave the proof of the remaining claims to the reader. \square

The lemma just proved shows that the set of images of functions in VP has a rich structure. We compose the functions in VP with a “stretching” function h , which guarantees that the gaps between consecutive values “kill” every polynomial. Then we can apply the idea of the proof of Proposition 4.7 to show that the set of the \leq_{pot} -degrees has a rich structure too.

We define $h : \mathbb{N} \rightarrow \mathbb{N}$ by recursion: $h(0) := 0$ and

$$h(n+1) = (h(0) + \dots + h(n))^n.$$

One easily verifies that h is value-polynomial.

For $f, g \in \text{VP}$ set

$$f \subseteq^* g \iff \text{im}(f) \setminus \text{im}(g) \text{ is finite.}$$

By the homogeneity properties of atomless countable Boolean algebras, to prove Theorem 4.1 it suffices to find a corresponding embedding defined only on the nonzero elements of \mathcal{V}/\equiv . In general $f \subseteq^* g$ and $g \subseteq^* f$ do not imply $C_{hof} = C_{hog}$. However, by the following lemma we get an embedding of \mathcal{V}/\equiv into the partial ordering of the \leq_{iso} -degrees as required by Theorem 4.1 by defining the mapping on a set of representatives, more precisely on a set $R \subseteq \text{VP}$ such that

- for every $f \in \text{VP}$ there is exactly one $g \in R$ with $f \subseteq^* g$ and $g \subseteq^* f$.

Lemma 4.9 *The mapping $f \mapsto C_{hof}$ from VP to $\{C \subseteq \text{LOU} \mid C \text{ a class}\}$ is one-to-one, and for all $f, g \in \text{VP}$:*

- (1) *if $C_{hof} \leq_{\text{iso}} C_{hog}$, then $f \subseteq^* g$;*
- (2) *if $f \subseteq^* g$ and $g \not\subseteq^* f$, then $C_{hof} \leq_{\text{iso}} C_{hog}$.*

For the proof of Lemma 4.9 we need an appropriate way to invert increasing functions $f : \mathbb{N} \rightarrow \mathbb{N}$. We define $f^{-1} : \mathbb{N} \rightarrow \mathbb{N}$ by

$$f^{-1}(n) := \max\{i \mid f(i) \leq n\},$$

where we set $\max \emptyset := 0$. We collect some properties of this inverse in the following lemma, whose simple proof we omit. We denote by $\text{id}_{\mathbb{N}}$ the identity function on \mathbb{N} .

Lemma 4.10 (1) *If $f : \mathbb{N} \rightarrow \mathbb{N}$ is increasing, then f^{-1} is nondecreasing, $f^{-1} \leq \text{id}_{\mathbb{N}}$, $f^{-1} \circ f = \text{id}_{\mathbb{N}}$ and $f(f^{-1}(n)) \leq n$ for all $n \geq f(0)$.*
 (2) *If $f, g : \mathbb{N} \rightarrow \mathbb{N}$ are increasing, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.*
 (3) *If $f \in \text{VP}$, then f^{-1} is computable in polynomial time.*

A further notation is useful: For $f : \mathbb{N} \rightarrow \mathbb{N}$ let $f^{\Sigma} : \mathbb{N} \rightarrow \mathbb{N}$ be defined by

$$f^{\Sigma}(n) := \sum_{i \leq n} f(i).$$

Lemma 4.11 *Let $f, g : \mathbb{N} \rightarrow \mathbb{N}$ be functions and assume g is increasing. Then $(f \circ g)^{\Sigma} \leq f^{\Sigma} \circ g$.*

Proof. This is seen by direct calculation:

$$(f \circ g)^{\Sigma}(n) = \sum_{i \leq n} f(g(i)) = \sum_{\substack{i \leq g(n) \\ i \in \text{im}(g)}} f(i) \leq \sum_{i \leq g(n)} f(i) = f^{\Sigma} \circ g(n);$$

here the second equality uses that g is increasing. □

Furthermore observe that:

Lemma 4.12 *If $f \in \text{VP}$, then for all $n \in \mathbb{N}$ we have $\#C_f(n) = (f^{\Sigma} \circ f^{-1})(n)$.*

Proof of Lemma 4.9. The mapping $f \mapsto C_{hof}$ is one-to-one: Assume $C_{hof} = C_{hog}$. Then $\text{im}(h \circ f) = \text{im}(h \circ g)$ and thus, $\text{im}(f) = \text{im}(g)$ as h is one-to-one. Since f and g are both increasing, this yields $f = g$. We prove the remaining statements of Lemma 4.9 by the following two claims.

Claim 1: Let $f, g \in \text{VP}$ and $f \subseteq^* g$ and $g \not\subseteq^* f$. Then $C_{hof} \leq_{\text{iso}} C_{hog}$.

Proof of Claim 1: By our assumptions, the set $\text{im}(h \circ f) \setminus \text{im}(h \circ g)$ is finite (as $f \subseteq^* g$ implies $h \circ f \subseteq^* h \circ g$) and (by injectivity of h) the set $\text{im}(h \circ g) \setminus \text{im}(h \circ f)$ is infinite. Then $C_{hof} \leq_{\text{iso}} C_{hog}$ is witnessed by a function sending the (up to \cong) finitely many structures in $C_{hof} \setminus C_{hog}$ to $C_{hog} \setminus C_{hof}$ and which is the identity on all other structures in C_{hof} .

Claim 2: Let $f, g \in \text{VP}$ and $f \not\leq^* g$. Then $C_{h \circ f} \not\leq_{\text{iso}} C_{h \circ g}$.

Proof of Claim 2: By contradiction assume $C_{h \circ f} \leq_{\text{iso}} C_{h \circ g}$. Then $C_{h \circ f}$ is potentially reducible to $C_{h \circ g}$ by Lemma 4.5. Hence there is $p \in \mathbb{N}[X]$ such that $\#C_{h \circ f}(n) \leq \#C_{h \circ g}(p(n))$ for all $n \in \mathbb{N}$. We show that this is wrong for some n . For this purpose we choose k such that

$$(3) \quad g(0) < f(k), \quad p(h(f(k))) < h(f(k) + 1), \quad \text{and} \quad f(k) \in \text{im}(f) \setminus \text{im}(g)$$

(by the definition of h and the assumption $f \not\leq^* g$ such a k exists). Then we get

$$\begin{aligned} & \#C_{h \circ g}(p(h(f(k)))) \\ &= (h \circ g)^\Sigma \circ (h \circ g)^{-1}(p(h(f(k)))) \quad (\text{by Lemma 4.12}) \\ &= (h \circ g)^\Sigma \circ (g^{-1} \circ h^{-1})(p(h(f(k)))) \quad (\text{by Lemma 4.10(2)}) \\ &\leq (h \circ g)^\Sigma \circ g^{-1}(f(k)) \quad (\text{by } p(h(f(k))) < h(f(k) + 1) \text{ (see (3))}) \\ & \quad \text{and by definition of } h^{-1}) \\ &= (h \circ g)^\Sigma \circ g^{-1}(f(k) - 1) \quad (\text{as } f(k) \notin \text{im}(g)) \\ &\leq h^\Sigma \circ g \circ g^{-1}(f(k) - 1) \quad (\text{by Lemma 4.11}) \\ &\leq h^\Sigma(f(k) - 1) \quad (\text{by Lemma 4.10(1) as } g(0) < f(k)) \\ &< h(f(k)) \quad (\text{by definition of } h) \\ &\leq \#C_{h \circ f}(h(f(k))) \quad (\text{by definition of } \#C_{h \circ f}). \end{aligned}$$

□

5 Strong isomorphism reducibility and potential reducibility

We know that $\text{GRAPH} \leq_{\text{pot}} \text{LOU}$ while $\text{GRAPH} \leq_{\text{iso}} \text{LOU}$ is equivalent to GRAPH having an invariantization (cf. Propositions 4.6 (2) and 3.3). However, so far in all concrete examples of classes C and D , for which we know the status of $C \leq_{\text{iso}} D$ and of $C \leq_{\text{pot}} D$, we had that

$$C \leq_{\text{iso}} D \iff C \leq_{\text{pot}} D.$$

So the question arises whether the relations of strong isomorphism reducibility and potential reducibility coincide. Recall that we require the classes C and D to be closed under isomorphism and decidable in polynomial time. Generalizing the proof idea of Theorem 3.7, we shall see in the next section that indeed the relations \leq_{iso} and \leq_{pot} coincide if $\text{P} = \#\text{P}$. We believe that they are distinct but could only show:

Theorem 5.1 *If $\text{U2EXP} \cap \text{co-U2EXP} \neq \text{2EXP}$, then the relations of strong isomorphism reducibility and that of potential reducibility are distinct.*

Recall that

$$\text{2EXP} := \text{DTIME} \left(2^{2^{n^{O(1)}}} \right) \quad \text{and} \quad \text{N2EXP} := \text{NTIME} \left(2^{2^{n^{O(1)}}} \right)$$

The complexity class U2EXP consists of those $Q \in \text{N2EXP}$ for which there is a nondeterministic Turing machine of type N2EXP that for every $x \in Q$ has exactly one accepting run. Finally, $\text{co-U2EXP} := \{\Sigma^* \setminus Q \mid Q \in \text{U2EXP}\}$.

The rest of this section is devoted to a proof of this result. We explain the underlying idea: Assume $Q \in \text{U2EXP} \cap \text{co-U2EXP}$. We construct classes C and D which contain structures in the same cardinalities and which contain exactly two nonisomorphic structures in these cardinalities. Therefore they are potentially reducible to each other. While it is trivial to exhibit two nonisomorphic structures in C of the same cardinality, from any two concrete nonisomorphic structures in D we obtain information on membership in Q for all strings of a certain length. If $C \leq_{\text{iso}} D$, we get concrete nonisomorphic structures in D (in time allowed by 2EXP) by applying the strong isomorphism reduction to two nonisomorphic structures in C and therefore obtain $Q \in \text{2EXP}$.

Proof of Theorem 5.1. Let $Q \in \text{U2EXP} \cap \text{co-U2EXP}$. Then there exists a nondeterministic Turing machine \mathbb{M} and a constant $d \geq 2$ such that (M1)–(M5) hold:

- (M1) The machine \mathbb{M} has three terminal states ‘yes,’ ‘no,’ and ‘maybe.’
- (M2) For $x \in \Sigma^*$, every run of \mathbb{M} on input x stops after *exactly* $2^{2^{|x|^d}}$ many steps.
- (M3) For $x \in Q$ exactly one run of \mathbb{M} on x stops in ‘yes’ and none in ‘no.’
- (M4) For $x \notin Q$ exactly one run of \mathbb{M} on x stops in ‘no’ and none in ‘yes.’
- (M5) The machine \mathbb{M} has exactly two different choices for the next step in every nonterminal state.

We say that a run of \mathbb{M} *takes a decision* if it ends in ‘yes’ or in ‘no.’

For $n \in \mathbb{N}$ we set $\ell(n) := 2^{2^{n^d}}$. For $x \in \Sigma^n$, by (M2) and (M5), every run of \mathbb{M} on input x can be identified with a binary string $r \in \{0, 1\}^{\ell(n)}$. Conversely, from such a string r we can determine a run of \mathbb{M} on x .

Let $m(n) := 2^n$ and $x_1, x_2, \dots, x_{m(n)}$ be the enumeration of all strings of Σ^n in the lexicographic ordering. We call a binary string s of length $m(n) \cdot \ell(n) = 2^n \cdot 2^{2^{n^d}}$ a *decision string* if for every $i \in [m(n)]$ the i th substring of s of length $\ell(n)$ corresponds to a run of \mathbb{M} on x_i taking a decision; more precisely, if we have $s = s_1 \hat{s}_2 \cdots \hat{s}_{m(n)}$ with $|s_i| = \ell(n)$ for $i \in [m(n)]$, then s_i corresponds to a run of \mathbb{M} on x_i taking a decision. By our assumptions (M3) and (M4) we get:

- (4) for every $n \in \mathbb{N}$ there is exactly one decision string of length $m(n) \cdot \ell(n)$.

We turn every string s of length $m(n) \cdot \ell(n)$ into a structure $\mathcal{A}(s)$ over the vocabulary $\tau = \{\text{One}, \text{Zero}, R\}$, where *One* and *Zero* are unary relation symbols and *R* is a binary relation symbol. Let

$$\begin{aligned} A(s) &:= [m(n) \cdot \ell(n)], \\ R^{\mathcal{A}(s)} &:= \{(j, j+1) \mid j \in [m(n) \cdot \ell(n) - 1]\}. \end{aligned}$$

For s a decision string, let

$$\begin{aligned} \text{One}^{\mathcal{A}(s)} &:= \{j \mid j \in [m(n) \cdot \ell(n)] \text{ and the } j\text{th bit of } s \text{ is one}\}, \\ \text{Zero}^{\mathcal{A}(s)} &:= \{j \mid j \in [m(n) \cdot \ell(n)] \text{ and the } j\text{th bit of } s \text{ is zero}\}, \end{aligned}$$

and let $\text{One}^{\mathcal{A}(s)} = \text{Zero}^{\mathcal{A}(s)} = \emptyset$ otherwise. By (4) for every $s, s' \in \{0, 1\}^{m(n) \cdot \ell(n)}$

- (5) $\mathcal{A}(s) \cong \mathcal{A}(s') \iff$ exactly one of s and s' is a decision string.

Let D_n be the class containing, up to isomorphism, the structures $\mathcal{A}(s)$ with $s \in \{0, 1\}^{m(n) \cdot \ell(n)}$. The following is straightforward.

- (D1) The universe of every structure in D_n has cardinality $m(n) \cdot \ell(n)$.
(D2) $|D_n/\cong| = 2$.

We set

$$D := \bigcup_{n \in \mathbb{N}} D_n.$$

Finally, we let

$$C := \bigcup_{n \in \mathbb{N}} C_n,$$

where for $n \in \mathbb{N}$ every structure in the class C_n is isomorphic to the complete graph $K_{m(n) \cdot \ell(n)}$ on $m(n) \cdot \ell(n)$ vertices or to its complement $\bar{K}_{m(n) \cdot \ell(n)}$. Then:

- (C1) The universe of every structure in C_n has cardinality $m(n) \cdot \ell(n)$.
(C2) $|C_n/\cong| = 2$.

Hence, $C \leq_{\text{pot}} D$.

Claim: If $f : C \leq_{\text{iso}} D$, then there is $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$

$$(6) \quad f(C_n/\cong) = D_n/\cong.$$

By this equality we mean:

- $f(\mathcal{A}) \in D_n$ for every $\mathcal{A} \in C_n$;
- for every $\mathcal{B} \in D_n$ there exists an $\mathcal{A} \in C_n$ such that $f(\mathcal{A}) \cong \mathcal{B}$.

Proof of the Claim: First observe that by (C2) and (D2) it suffices to show that $f(C_n) \subseteq D_n$ for all sufficiently large $n \in \mathbb{N}$. As f is computable in polynomial time there is $c \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ and $\mathcal{A} \in C_n$

the universe of $f(\mathcal{A})$ has $\leq (2^n \cdot 2^{2^{n^d}})^c$ elements.

We choose $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$

$$\left(2^n \cdot 2^{2^{n^d}}\right)^c < 2^{n+1} \cdot 2^{2^{(n+1)^d}}.$$

Hence, for $n \geq n_0$

$$f\left(\bigcup_{q \leq n} C_q\right) \subseteq \bigcup_{q \leq n} D_q.$$

As $\bigcup_{q \leq n} C_q$ and $\bigcup_{q \leq n} D_q$ contain, up to isomorphism, the same number of structures, the Claim follows.

Now assume that $f : C \leq_{\text{iso}} D$. Then the following algorithm \mathbb{A} witnesses that $Q \in 2\text{EXP}$. Let n_0 be as in the Claim. For $x \in \Sigma^n$ with $n \geq n_0$ the algorithm \mathbb{A} computes the structures

$$f(K_{m(n) \cdot \ell(n)}) \quad \text{and} \quad f(\bar{K}_{m(n) \cdot \ell(n)});$$

they are nonisomorphic and in D_n by the Claim. In particular, by (5) we get a run of \mathbb{M} on input x taking a decision; the algorithm \mathbb{A} answers accordingly. \square

6 If strong isomorphism reducibility and potential reducibility are distinct then $P \neq \#P$

In the previous section we have seen that under some complexity-theoretic assumption the two notions of reduction (strong isomorphism reducibility and potential reducibility) are distinct. One might wonder whether we can separate them without any such complexity-theoretic assumption. We show in this section that this would settle some open problem in complexity theory; more precisely, we show the statement of the title of this section.³ In particular, by Proposition 4.6 (2), if LOU is not a maximum element of \leq_{iso} , then $P \neq \#P$. We prove the main result in a more general setting.

For a class C consider the equivalence relation $E(C)$ on Σ^* induced by the isomorphism relation, that is,

$$(7) \quad E(C) := \{(\mathcal{A}, \mathcal{B}) \mid \mathcal{A}, \mathcal{B} \in C \text{ and } \mathcal{A} \cong \mathcal{B}\} \\ \cup \{(x, y) \mid x, y \in \Sigma^*, x \notin C \text{ and } y \notin C\}.$$

Of course, $E(C)$ is in NP. In this section we consider arbitrary such equivalence relations on Σ^* and show that the corresponding two notions of reduction coincide if $P = \#P$. We start by introducing all relevant concepts; we do not restrict ourselves to equivalence relations in NP, but consider equivalence relations in an arbitrary complexity class (for an equivalence relation E on Σ^* we also write xEy for $(x, y) \in E$).

Definition 6.1

- (1) Let CC be an arbitrary complexity class. Then we denote by CC(eq) the set of equivalence relations E on Σ^* with $E \in \text{CC}$.
- (2) Let E and E' be equivalence relations on Σ^* . We say that E is *strongly equivalence reducible to E'* and write $E \leq_{\text{eq}} E'$, if there is a function $f : \Sigma^* \rightarrow \Sigma^*$ computable in polynomial time such that for all $x, y \in \Sigma^*$

$$xEy \iff f(x)E'f(y).$$

We then say that f is a *strong equivalence reduction* from E to E' and write $f : E \leq_{\text{eq}} E'$.

Clearly, $E(C) \in \text{NP}(\text{eq})$ for every class C of structures; furthermore, $E(\text{LOU}) \in \text{P}(\text{eq})$. Let PROP and TAUT denote the set of all formulas of propositional logic and the set of tautologies, respectively. Note that $E_{\text{equiv}} \in \text{co-NP}(\text{eq})$, where

$$E_{\text{equiv}} := \{(\alpha, \beta) \mid \alpha, \beta \in \text{PROP} \text{ and } (\alpha \leftrightarrow \beta) \in \text{TAUT}\} \\ \cup \{(x, y) \mid x, y \notin \text{PROP}\}.$$

Clearly, if C and D are classes of structures as in the previous sections, then

$$C \leq_{\text{iso}} D \iff E(C) \leq_{\text{eq}} E(D).$$

We generalize the notion of potential reducibility to equivalence relations.

³Recall that $P = \#P$ means that for every polynomial time nondeterministic Turing machine \mathbb{M} the function $f_{\mathbb{M}}$ such that $f_{\mathbb{M}}(x)$ is the number of accepting runs of \mathbb{M} on $x \in \Sigma^*$ is computable in polynomial time. The class $\#P$ consists of all the functions $f_{\mathbb{M}}$.

Definition 6.2 Let E and E' be equivalence relations on Σ^* . We say that E is *potentially reducible* to E' and write $E \leq_{\text{pot}} E'$ if there is a $p \in \mathbb{N}[X]$ such that for all $n \in \mathbb{N}$ the number $|\Sigma^{\leq n}/E|$ of E -equivalence classes containing a string in

$$\Sigma^{\leq n} := \{x \in \Sigma^* \mid |x| \leq n\}$$

is at most $|\Sigma^{\leq p(n)}/E'|$.

Due to our definition (7) of $E(C)$, the new notion coincides with the old one for equivalence relations of the form $E(C)$:

Proposition 6.3 *Let C and C' be classes. Then*

$$C \leq_{\text{pot}} C' \iff E(C) \leq_{\text{pot}} E(C').$$

Proof. Recall that the empty string is not (the encoding of) a structure. Let C be a class of τ -structures and C' a class of τ' -structures. By the assumptions made in Subsection 1.1, there are polynomials $p_\tau, p_{\tau'} \in \mathbb{N}[X]$ such that for every τ -structure \mathcal{A}

$$(8) \quad |A| \leq |\mathcal{A}| \leq p_\tau(|A|)$$

and for every τ' -structure \mathcal{B}

$$(9) \quad |B| \leq |\mathcal{B}| \leq p_{\tau'}(|B|).$$

Assume first that $C \leq_{\text{pot}} C'$, say $\#C(n) \leq \#C'(p(n))$ for some polynomial p . Then

$$|\Sigma^{\leq n}/E(C)| \leq \#C(n) + 1 \leq \#C'(p(n)) + 1 \leq |\Sigma^{\leq p_\tau(p(n))}/E(C')|$$

(the first inequality holds by (7) and (8), the last one by (7) and (9)). Conversely, assume that $E(C) \leq_{\text{pot}} E(C')$, say $|\Sigma^{\leq n}/E(C)| \leq |\Sigma^{\leq p(n)}/E(C')|$ with $p \in \mathbb{N}[X]$. Then

$$\#C(n) + 1 \leq |\Sigma^{\leq p_\tau(n)}/E(C)| \leq \left| \Sigma^{\leq p(p_\tau(n))}/E(C') \right| \leq \#C'(p(p_\tau(n))) + 1.$$

□

Along the lines of the proof of Lemma 4.5, one shows that $E \leq_{\text{eq}} E'$ implies $E \leq_{\text{pot}} E'$. For equivalence relations we can show that \leq_{eq} is finer than \leq_{pot} under weaker assumptions than that of Theorem 5.1:

Proposition 6.4 *If $\text{NP} \neq \text{P}$, then the relations of strong equivalence reduction and that of potential reducibility do not coincide on $\text{NP}(\text{eq})$.*

Proof. Assume $Q \in \text{NP} \setminus \text{P}$. We define E_Q by

$$xE_Qy \iff \left(x = y \text{ or } (x = b^{\wedge}z \text{ and } y = (1-b)^{\wedge}z \text{ for some } z \in Q \text{ and } b \in \Sigma) \right).$$

By our assumptions on Q , we have $E_Q \in \text{NP}(\text{eq})$. We let E be the identity on Σ^* . Clearly, $E_Q \leq_{\text{pot}} E$. As $Q \notin \text{P}$, we get $E_Q \not\leq_{\text{eq}} E$, as any $f : E_Q \leq_{\text{eq}} E$ would yield a polynomial time decision procedure for Q . □

Generalizing the proof idea of Theorem 3.7 we show:

Theorem 6.5 *If the relations of strong equivalence reduction and that of potential reducibility do not coincide on $\text{NP}(\text{eq})$, then $\text{P} \neq \#\text{P}$.*

To prove this theorem we first generalize the notions of canonization and of enumeration induced by a canonization.

Definition 6.6 Let $E \in \text{CC}(\text{eq})$. A function $\text{Can} : \Sigma^* \rightarrow \Sigma^*$ is a *canonization for E* if it is polynomial time computable and

- (1) for all $x, y \in \Sigma^*$: $(xEy \iff \text{Can}(x) = \text{Can}(y))$;
- (2) for all $x \in \Sigma^*$: $xE \text{Can}(x)$.

Let Can be a canonization of E . The *enumeration induced by Can* is the enumeration

$$x_1, x_2 \dots$$

of $\text{Can}(\Sigma^*)$ such that $x_i <_{\text{lex}} x_j$ for $i < j$.

If E has a canonization, then $E \in \text{P}$: to decide whether xEy we compute $\text{Can}(x)$ and $\text{Can}(y)$ and check whether $\text{Can}(x) = \text{Can}(y)$.

Now it is easy to explain the idea underlying the proof of Theorem 6.5. First we show that (under the assumption $\text{P} = \text{NP}$) every $E \in \text{P}(\text{eq})$ has a canonization Can_E . Then, given $E, E' \in \text{P}(\text{eq})$, we define a strong equivalence reduction $f : \Sigma^* \rightarrow \Sigma^*$ from E to E' as follows: Let $x \in \Sigma^*$. If $\text{Can}_E(x)$ is the i th element in the enumeration induced by Can_E , then we let $f(x)$ be the i th element in the enumeration induced by $\text{Can}_{E'}$. By the properties of canonizations it should be clear that

$$xEy \iff f(x)E'f(y)$$

(we can even replace $f(x)E'f(y)$ by $f(x) = f(y)$). So it remains to show (under suitable assumptions) that f is computable in polynomial time and to show that every equivalence relation has a canonization.

The following lemma was already proven in [2].

Lemma 6.7 *If $\text{P} = \text{NP}$, then every $E \in \text{P}(\text{eq})$ has a canonization; in fact, then the mapping sending each $x \in \Sigma^*$ to the \leq_{lex} -first member of the E -equivalence class of x is a canonization.*

Proof. Let $E \in \text{P}(\text{eq})$ and assume $\text{P} = \text{NP}$. Then we know that the polynomial hierarchy collapses, $\text{P} = \text{PH}$. So it suffices to show that the mapping defined in the statement of this lemma can be computed by an alternating polynomial time algorithm \mathbb{A} with a constant number of alternations. This is easy: on input $x \in \Sigma^*$ the algorithm \mathbb{A} guesses existentially $y \in \Sigma^*$ with $|y| \leq |x|$ and xEy ; then \mathbb{A} guesses universally a further $z \in \Sigma^*$ with $|z| \leq |x|$ and xEz ; if $y \leq_{\text{lex}} z$, then \mathbb{A} outputs y otherwise it rejects. \square

Lemma 6.8 *Let $E \in \text{P}(\text{eq})$ be an equivalence relation with a canonization Can . Then the following problem is in $\#\text{P}$:*

Instance: $x \in \Sigma^*$.
Problem: Compute i (in binary) such that $\text{Can}(x)$ is the i th element in the enumeration induced by Can .

Proof. Consider a nondeterministic polynomial time algorithm \mathbb{A} which on input $x \in \Sigma^*$ runs as follows: It first computes the string $y := \text{Can}(x)$. Then \mathbb{A} guesses a string $z \in \Sigma^*$ with $|z| \leq |y|$. Finally it accepts if $\text{Can}(z) = z$ and $z \leq_{\text{lex}} y$. It should be clear that the number of accepting runs of \mathbb{A} on x is

$$|\{z \mid z \leq_{\text{lex}} \text{Can}(x) \text{ and } \text{Can}(z) = z\}|.$$

\square

Proof of Theorem 6.5. Assume that $P = \#P$. Let $E, E' \in \text{NP}(\text{eq})$ be equivalence relations and assume that $E \leq_{\text{pot}} E'$, that is, $|\Sigma^{\leq n}/E| \leq |\Sigma^{\leq p(n)}/E'|$ for some polynomial p and all $n \in \mathbb{N}$. We show $E \leq_{\text{eq}} E'$.

As $P = \#P$, we have $P = \text{NP}$. Hence $E, E' \in \text{P}(\text{eq})$. Therefore, by Lemma 6.7 there are canonizations Can_E of E and $\text{Can}_{E'}$ of E' and there are polynomial time algorithms \mathbb{A} and \mathbb{A}' that solve the problem of the preceding lemma for E and E' , respectively. The following nondeterministic polynomial time algorithm computes an $f : E \leq_{\text{eq}} E'$. On input $x \in \Sigma^*$, it computes $\text{Can}_E(x)$ and $n := |\text{Can}_E(x)|$ and guesses a string $x' \in \Sigma^{\leq p(n)}$ with $\text{Can}_{E'}(x') = x'$. Simulating \mathbb{A} and \mathbb{A}' , it checks whether $\text{Can}_E(x)$ and x' are at the same position in the enumeration induced by Can_E and in the enumeration induced by $\text{Can}_{E'}$, respectively; in the positive case it outputs x' , otherwise it rejects. As $|\Sigma^{\leq n}/E| \leq |\Sigma^{\leq p(n)}/E'|$ such an $x' \in \Sigma^{\leq p(n)}$ with $\text{Can}_{E'}(x') = x'$ at the same position as $\text{Can}_E(x)$ exists. As $P = \text{NP}$, the function f is computable in polynomial time. \square

We briefly point to the papers [2, 3, 7] that deal with related problems. Let $\text{Inv}(\text{eq})$ be the class of equivalence relations having an invariantization (defined in analogy to Definition 3.1), $\text{Can}(\text{eq})$ the class of equivalence relations having a canonization and finally, $\text{Lexfirst}(\text{eq})$ the class of equivalence relations having a canonization that maps every string to the \leq_{lex} -first element of its equivalence class. Clearly

$$(10) \quad \text{Lexfirst}(\text{eq}) \subseteq \text{Can}(\text{eq}) \subseteq \text{Inv}(\text{eq}) \subseteq \text{P}(\text{eq}).$$

Lemma 6.7 shows that $\text{Lexfirst}(\text{eq}) = \text{Can}(\text{eq}) = \text{Inv}(\text{eq}) = \text{P}(\text{eq})$ if $P = \#P$. Blass and Gurevich [2], for example, prove that $\text{Lexfirst}(\text{eq}) \neq \text{Can}(\text{eq})$ unless the polynomial hierarchy collapses, and Fortnow and Grochow [7] show that $\text{Can}(\text{eq}) = \text{Inv}(\text{eq})$ would imply that integers can be factored in probabilistic polynomial time. Blass and Gurevich [2, 3] compare the complexity of the “problems underlying the definition of the sets in (10).” Finally, the book [16], among other things, deals with the question whether two propositional formulas are logically equivalent up to a permutation of their variables. It is not hard to see that the isomorphism problem for a class C can be rephrased in these terms; however no analogue of \leq_{iso} is considered in [16].

7 On maximum elements in $\text{P}(\text{eq})$ and $\text{NP}(\text{eq})$

In this section we study whether there is a maximum element with respect to strong equivalence reductions in the classes $\text{P}(\text{eq})$ and $\text{NP}(\text{eq})$, that is, in the classes of deterministic and nondeterministic polynomial time equivalence relations. We already mentioned that the existence of a maximum element in $\text{P}(\text{eq})$ is mentioned as [7, Open Question 4.14]; the notion of strong equivalence reduction was already introduced in that paper and called kernel reduction there.

Let SAT be the set of satisfiable propositional formulas. Consider the NP-equivalence relation

$$E_{\text{sat}} := \{(\alpha, \beta) \mid \alpha, \beta \in \text{PROP and } (\alpha = \beta \text{ or } \alpha, \beta \in \text{SAT})\};$$

more precisely, to get an equivalence relation on Σ^* , we define E_{sat} to be

$$\{(\alpha, \beta) \mid \alpha, \beta \in \text{PROP and } (\alpha = \beta \text{ or } \alpha, \beta \in \text{SAT})\} \cup \{(x, y) \mid x, y \notin \text{PROP}\}.$$

However, henceforth if we speak of an equivalence relation E whose field $\text{Fld}(E) := \{x \mid (x, x) \in E\}$ is a proper subset of Σ^* , we identify it with the equivalence relation $E \cup \{(x, y) \mid x, y \in \Sigma^* \setminus \text{Fld}(E)\}$. We use E_{sat} to show:

Proposition 7.1 *If the polynomial hierarchy PH does not collapse, then $E(\text{GRAPH})$ is not a maximum element in $(\text{NP}(\text{eq}), \leq_{\text{eq}})$; in fact, then $E_{\text{sat}} \not\leq_{\text{eq}} E(\text{GRAPH})$.*

Proof. For $\alpha \in \text{PROP}$ and a propositional variable X we have the equivalence $(\alpha \in \text{SAT} \iff \alpha E_{\text{sat}} X)$. By contradiction, assume that $f : E_{\text{sat}} \leq_{\text{eq}} E(\text{GRAPH})$. We have $f(X) \in \text{GRAPH}$; otherwise, $\text{SAT} \in \text{P}$, which contradicts our assumption that the polynomial hierarchy does not collapse. Then for every $\alpha \in \text{PROP}$

$$\alpha \in \text{SAT} \iff f(\alpha) \cong f(X).$$

Thus $E(\text{GRAPH})$ would be NP-complete. It is well-known [4] that this implies $\Sigma_2^P = \text{PH}$. \square

We show that the existence of a maximum element in $(\text{NP}(\text{eq}), \leq_{\text{eq}})$ is equivalent to the existence of an effective enumeration of $\text{NP}(\text{eq})$. This result is also true for $\text{P}(\text{eq})$ and $\text{co-NP}(\text{eq})$. Effective enumerations of problems have been used to characterize promise classes possessing complete languages, that is, maximum elements under polynomial time reductions (e.g., see [12, 14]). Even though we are dealing with a different type of reduction, our method is similar. To state our precise result we introduce some notions. A deterministic or nondeterministic Turing machine \mathbb{M} is *clocked* (more precisely, *polynomially time-clocked*), if (the code of) \mathbb{M} contains a natural number $\text{time}(\mathbb{M})$ such that $n^{\text{time}(\mathbb{M})}$ is a bound for the running time of \mathbb{M} on inputs of length n . So, by this definition, all runs of a clocked machine are of polynomial length. Of course, the function $\mathbb{M} \mapsto \text{time}(\mathbb{M})$, defined on the set of clocked machines, is computable in polynomial time.

Definition 7.2 Let $\text{CC} \in \{\text{P}, \text{NP}, \text{co-NP}\}$. Let L be a set of languages L with $L \subseteq \Sigma^*$. We say that

$$L_0, L_1, \dots$$

is a *CC-enumeration of L by clocked Turing machines*, if $L = \{L_0, L_1, \dots\}$ and there is a computable function \mathbb{M} defined on \mathbb{N} such that $\mathbb{M}(i)$ for $i \in \mathbb{N}$ is (the code of) a clocked Turing machine of type CC accepting L_i .

Proposition 7.3 *Let $\text{CC} \in \{\text{P}, \text{NP}, \text{co-NP}\}$. Then the following are equivalent:*

- (1) $(\text{CC}(\text{eq}), \leq_{\text{eq}})$ has a maximum element.
- (2) There is a CC -enumeration E_0, E_1, \dots of $\text{CC}(\text{eq})$ by clocked Turing machines.

Proof. (1) \Rightarrow (2): Assume that E is a maximum in $(\text{CC}(\text{eq}), \leq_{\text{eq}})$ and let \mathbb{M}_{max} be a Turing machine of type CC accepting E . Of course, there is a computable function \mathbb{M}' such that $\mathbb{M}'(i)$ for $i \in \mathbb{N}$ is a deterministic clocked Turing machine computing a function $f_i : \Sigma^* \rightarrow \Sigma^*$ such that f_0, f_1, \dots is an enumeration of all polynomial time computable functions from Σ^* to Σ^* . We define the machine $\mathbb{M}_{\text{max}} \circ \mathbb{M}'(i)$ in a straightforward manner such that it decides

$$E_i := \{(x, y) \mid (f_i(x), f_i(y)) \in E\}.$$

We let \mathbb{M} be the function defined on \mathbb{N} with $\mathbb{M}(i) := \mathbb{M}_{\text{max}} \circ \mathbb{M}'(i)$. As from a polynomial bounding \mathbb{M}_{max} and $\text{time}(\mathbb{M}'(i))$ we get a time bound for $\mathbb{M}(i)$, we can assume that $\mathbb{M}(i)$ is clocked. It should be clear that E_0, E_1, \dots has the desired properties.

(2) \Rightarrow (1): Let E_0, E_1, \dots be as in (2) and let \mathbb{M} be a corresponding computable function. By padding if necessary, we may assume that the graph $\{(1^i, 1^{|\mathbb{M}(i)|}) \mid i \in \mathbb{N}\}$ is decidable in polynomial time and that $i \leq |\mathbb{M}(i)|$ for all $i \in \mathbb{N}$. We define the relation E as follows (for better reading we denote here, and in the proof of Lemma 7.6, the string 1^ℓ , that is the string $11\dots 1$ of length ℓ , by $\langle \ell \rangle$):

$$E := \left\{ \left((\mathbb{M}(i), x, \langle (2 + 2|x|)^{\text{time}(\mathbb{M}(i))} \rangle), (\mathbb{M}(i), y, \langle (2 + 2|y|)^{\text{time}(\mathbb{M}(i))} \rangle) \right) \mid i \in \mathbb{N} \text{ and } (x, y) \in E_i \right\}.$$

By the effectivity properties of \mathbb{M} , we have $E \in \text{CC}(\text{eq})$ (more precisely $E \cup \{(x, y) \mid x, y \in \Sigma^* \setminus \text{Fld}(E)\} \in \text{CC}(\text{eq})$). Clearly, for $i \in \mathbb{N}$ the mapping $x \mapsto (\mathbb{M}(i), x, \langle (2 + 2|x|)^{\text{time}(\mathbb{M}(i))} \rangle)$ is a strong equivalence reduction from E_i to E , hence E is a maximum element. \square

Below we will show that $(\text{NP}(\text{eq}), \leq_{\text{eq}})$ has a maximum element if $\text{NP} = \text{co-NP}$. Note that we do not even know whether $(\text{P}(\text{eq}), \leq_{\text{eq}})$ has a maximum element. The main result concerning this problem that we have reads as follows (later we recall the definition of p-optimal proof system):

Theorem 7.4 *If TAUT has a p-optimal proof system, then $(\text{P}(\text{eq}), \leq_{\text{eq}})$ has a maximum element.*

The following observations will lead to a proof of this result.

Definition 7.5 Let \mathbb{M} be a deterministic or nondeterministic Turing machine and $n \in \mathbb{N}$. The machine \mathbb{M} defines an equivalence relation on $\Sigma^{\leq n}$ if the set

$$\{(x, y) \mid x, y \in \Sigma^{\leq n} \text{ and } \mathbb{M} \text{ accepts } (x, y)\}$$

is an equivalence relation on $\Sigma^{\leq n}$.

An analysis of the complexity of the first of the following problems will be crucial for our purposes.

EQUIV(P)

Instance: A deterministic clocked Turing machine \mathbb{M} and $n \in \mathbb{N}$.

Problem: Does \mathbb{M} define an equivalence relation on $\Sigma^{\leq n}$?

EQUIV(NP)

Instance: A nondeterministic clocked Turing machine \mathbb{M} and $n \in \mathbb{N}$.

Problem: Does \mathbb{M} define an equivalence relation on $\Sigma^{\leq n}$?

Lemma 7.6

- (1) *If $(\mathbb{M}, n) \in \text{EQUIV(P)}$ is solvable by a deterministic algorithm in time $n^{f(\|\mathbb{M}\|)}$ for some function $f : \mathbb{N} \rightarrow \mathbb{N}$, then $\text{P}(\text{eq})$ has a maximum element.⁴*
- (2) *If $(\mathbb{M}, n) \in \text{EQUIV(NP)}$ is solvable by a nondeterministic algorithm in time $n^{f(\|\mathbb{M}\|)}$ for some function $f : \mathbb{N} \rightarrow \mathbb{N}$, then $\text{NP}(\text{eq})$ has a maximum element.*

⁴By $\|\mathbb{M}\|$ we denote the length of a reasonable encoding of \mathbb{M} by a string of Σ^* .

Proof. Let \mathbb{A} be an algorithm, deterministic for (1) and nondeterministic for (2), witnessing that $(\mathbb{M}, n) \in \text{EQUIV}(\text{P})$ in (1) and $(\mathbb{M}, n) \in \text{EQUIV}(\text{NP})$ in (2) is solvable in time $n^{f(\|\mathbb{M}\|)}$ for some $f : \mathbb{N} \rightarrow \mathbb{N}$. An equivalence relation E_0 on Σ^* is defined by letting uE_0v hold if and only if

$$u = v \text{ or } \left(u = (\mathbb{M}, x, (2 + 2 \cdot |x|)^{\text{time}(\mathbb{M})}, 1^t) \text{ and } \right. \\ \left. v = (\mathbb{M}, x', (2 + 2 \cdot |x'|)^{\text{time}(\mathbb{M})}, 1^{t'}) \text{ and (i) - (iii) are fulfilled} \right),$$

where

- (i) \mathbb{M} is a clocked Turing machine of type CC , where $\text{CC} = \text{P}$ for (1) and $\text{CC} = \text{NP}$ for (2);
- (ii) \mathbb{A} accepts $(\mathbb{M}, |x|)$ in at most t steps and $(\mathbb{M}, |x'|)$ in at most t' steps;
- (iii) \mathbb{M} accepts (x, x') .

Clearly, $E_0 \in \text{CC}(\text{eq})$. We show that E_0 is a maximum element. Let $E \in \text{CC}(\text{eq})$ be arbitrary and let \mathbb{M} be a clocked Turing machine deciding E . Then

$$x \mapsto (\mathbb{M}, x, (2 + 2 \cdot |x|)^{\text{time}(\mathbb{M})}, \langle |x|^{f(\|\mathbb{M}\|)} \rangle)$$

is computable in polynomial time and hence a strong equivalence reduction from E to E_0 . \square

Theorem 7.7 *The following hold:*

- (1) *If $\text{E} = \text{NE}$, then $\text{P}(\text{eq})$ has a maximum element.*
- (2) *If $\text{NP} = \text{co-NP}$, then $\text{NP}(\text{eq})$ has a maximum element.*

Proof. (1) We may assume that n is written in binary in the instances (\mathbb{M}, n) of $\text{EQUIV}(\text{P})$ (and that a string of length $\|\mathbb{M}\| \cdot \log n$ is given as an additional input). We consider the following nondeterministic algorithm \mathbb{A} accepting the complement of $\text{EQUIV}(\text{P})$. On input (\mathbb{M}, n) , it guesses one of the three axioms of an equivalence relation, say, the transitivity axiom; then \mathbb{A} guesses $x, y, z \in \Sigma^{\leq n}$, it simulates \mathbb{M} on input (x, y) , on input (y, z) , and on input (x, z) and accepts if \mathbb{M} accepts the first two inputs but not the third one. As we may assume that $\|\mathbb{M}\| \geq \text{time}(\mathbb{M})$, the algorithm \mathbb{A} runs in time $\|\mathbb{M}\| \cdot n^{O(\text{time}(\mathbb{M}))} = 2^{O(\|\mathbb{M}\| \cdot \log n)}$. By the assumption $\text{E} = \text{NE}$, there is a deterministic algorithm deciding the complement of $\text{EQUIV}(\text{P})$ and hence $\text{EQUIV}(\text{P})$ itself in time $2^{O(\|\mathbb{M}\| \cdot \log n)}$. Now our claim follows from the preceding lemma.

(2) The following alternating algorithm \mathbb{A} decides the complement of $\text{EQUIV}(\text{NP})$: On input (\mathbb{M}, n) (again we may assume that $\|\mathbb{M}\| \geq \text{time}(\mathbb{M})$), it existentially guesses one of the three axioms of an equivalence relation, say, the transitivity axiom; then \mathbb{A} existentially guesses $x, y, z \in \Sigma^{\leq n}$ and runs of \mathbb{M} accepting (x, y) and (y, z) ; furthermore it yields the string $\langle n^{\|\mathbb{M}\|} \rangle$. Finally \mathbb{A} universally simulates \mathbb{M} on input (x, z) and accepts if \mathbb{M} rejects. The algorithm \mathbb{A} has one alternation. By our assumption $\text{NP} = \text{co-NP}$, its universal part (an algorithm of type co-NP with inputs \mathbb{M} , (x, z) , and $\langle n^{\|\mathbb{M}\|} \rangle$) can be simulated by a nondeterministic algorithm running in time $n^{O(\|\mathbb{M}\|)}$. Altogether we get a nondeterministic algorithm accepting (the complement of) $\text{EQUIV}(\text{NP})$ in time $n^{O(\|\mathbb{M}\|)}$. Now our claim follows from the preceding lemma. \square

We consider the *acceptance problem for nondeterministic Turing machines*:

$$\text{ACC}_{\leq}$$

Instance: A nondeterministic Turing machine \mathbb{M} and $n \in \mathbb{N}$.

Problem: Does \mathbb{M} accept the empty input tape in $\leq n$ steps?

Lemma 7.8 *The following are equivalent:*

- (1) $(\mathbb{M}, n) \in \text{ACC}_{\leq}$ is solvable deterministically in time $n^{f(\|\mathbb{M}\|)}$ for some $f : \mathbb{N} \rightarrow \mathbb{N}$.
- (2) $(\mathbb{M}, n) \in \text{EQUIV}(\text{P})$ is solvable deterministically in time $n^{f(\|\mathbb{M}\|)}$ for some $f : \mathbb{N} \rightarrow \mathbb{N}$.

Proof. (1) \Rightarrow (2): Assume that $(\mathbb{M}, n) \in \text{ACC}_{\leq}$ (where \mathbb{M} is a nondeterministic machine and $n \in \mathbb{N}$) can be solved by an algorithm \mathbb{A} in time $n^{f(\|\mathbb{M}\|)}$ for some $f : \mathbb{N} \rightarrow \mathbb{N}$. Then the following algorithm \mathbb{B} will witness that $\text{EQUIV}(\text{P})$ is decidable in the time claimed in (2). Let (\mathbb{M}, n) be an instance of $\text{EQUIV}(\text{P})$, in particular \mathbb{M} is a deterministic clocked Turing machine. We may assume that \mathbb{M} on input (x, y) runs for exactly $|(x, y)|^{\text{time}(\mathbb{M})}$ steps. Let $\tilde{\mathbb{M}}$ be the nondeterministic Turing machine that on empty input tape, in the first phase guesses one of the three axioms of an equivalence relation, say, the transitivity axiom; then in the second phase $\tilde{\mathbb{M}}$ guesses $x, y, z \in \Sigma^*$; finally in the third phase it simulates \mathbb{M} on input (x, y) , on input (y, z) , and on input (x, z) and accepts if \mathbb{M} accepts the first two inputs but not the third one. We can assume that $\tilde{\mathbb{M}}$ does this simulation in such a way that it runs for exactly $(2 + 2 \cdot \max\{|x|, |y|, |z|\})^{\text{time}(\mathbb{M})}$ steps on each of the tuples (x, y) , (y, z) , and (x, z) .

Let k_1 , $k_2(x, y, z)$, and $k_3(x, y, z)$ be the exact time $\tilde{\mathbb{M}}$ uses for the first phase, the second phase and the third phase, respectively. As indicated for the third phase we may arrange things in such a way that there are (nonconstant) polynomials k'_2, k'_3 such that

$$\begin{aligned} k_2(x, y, z) &= k'_2(\max\{|x|, |y|, |z|\}) \text{ and} \\ k_3(x, y, z) &= k'_3(\max\{|x|, |y|, |z|\}) \end{aligned}$$

and such that if for example $\tilde{\mathbb{M}}$ has chosen the symmetry axiom and $x, y \in \Sigma^*$, then $k'_2(\max\{|x|, |y|\})$ is also the exact number of steps $\tilde{\mathbb{M}}$ uses for the second phase. As k'_2 and k'_3 are increasing functions, we get

$$(\mathbb{M}, n) \notin \text{EQUIV} \iff (\tilde{\mathbb{M}}, k + k'_2(n) + k'_3(n)) \in \text{ACC}_{\leq},$$

which gives the desired bound.

(2) \Rightarrow (1): For a nondeterministic Turing machine \mathbb{M} let $\hat{\mathbb{M}}$ be the deterministic Turing machine that on input (x, y) with $x, y \in \Sigma^*$ first checks whether $x \neq y$; if so, it accepts; if $x = y$, it simulates the $|x|$ steps of a run of \mathbb{M} on empty input tape, namely the steps corresponding to (the bits in) x and rejects if in these $|x|$ steps \mathbb{M} accepts; otherwise $\hat{\mathbb{M}}$ accepts. Thus for every $n \in \mathbb{N}$

$$(\mathbb{M}, n) \in \text{ACC}_{\leq} \iff$$

$\hat{\mathbb{M}}$ does not define an equivalence relation on $\Sigma^{\leq n}$.

As from the definition of $\hat{\mathbb{M}}$ we immediately get a polynomial time bound, we can assume that $\hat{\mathbb{M}}$ is clocked, so that the preceding equivalence immediately gives the claim. \square

A *proof system* for TAUT is a surjective function $S : \Sigma^* \rightarrow \text{TAUT}$ computable in polynomial time. The proof system S for TAUT is *p-optimal* if for every proof system S'

for TAUT there is a polynomial time computable $T : \Sigma^* \rightarrow \Sigma^*$ such that for all $w \in \Sigma^*$

$$S(T(w)) = S'(w).$$

It is not known whether there is a p-optimal proof system for TAUT, even though it is conjectured there is no such p-optimal proof system. In [5] it has been shown that:

Proposition 7.9 *The following are equivalent:*

- (1) *There is a p-optimal proof system for TAUT.*
- (2) *$(\mathbb{M}, n) \in \text{ACC}_{\leq}$ is solvable in time $n^{f(\|\mathbb{M}\|)}$ for some function $f : \mathbb{N} \rightarrow \mathbb{N}$.*

Proof of Theorem 7.4. If there is a p-optimal proof system for TAUT, by the previous proposition and Lemma 7.8 we see that $(\mathbb{M}, n) \in \text{EQUIV}(\text{P})$ is solvable in time $n^{f(\|\mathbb{M}\|)}$ for some function $f : \mathbb{N} \rightarrow \mathbb{N}$. Now the claim follows from Lemma 7.6. \square

References

- [1] H.U. Besche, B. Eick and E.A. O'Brien. The groups of order at most 2000, *Electronic Research announcements of the American Mathematical Society* 7:1–4, 2001.
- [2] A. Blass and Y. Gurevich. Equivalence relations, invariants, and normal forms. *SIAM Journal of Computing*, 13:682–689, 1984.
- [3] A. Blass and Y. Gurevich. Equivalence relations, invariants, and normal forms, II. Lecture Notes in Computer Science, 171:24–42, 1984.
- [4] R. B. Boppana, J. Hastad and S. Zachos. Does co-NP have short interactive proofs? *Information Processing Letters*, 25(2):127–132, 1987.
- [5] Y. Chen and J. Flum. On p-optimal proof systems and logics for PTIME. In *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10)*, Lecture Notes in Computer Science 6199, pp. 321–332, Springer, 2010.
- [6] H.-D. Ebbinghaus and J. Flum. *Finite Model Theory*, Second Edition. Perspectives in Mathematical Logic, Springer 1999.
- [7] L. Fortnow and J. Grochow. Complexity classes of equivalence problems revisited, [arXiv:0907.4775v1](https://arxiv.org/abs/0907.4775v1) [cs.CC], 2009.
- [8] S. Friedman. Descriptive set theory for finite structures, Lecture at the Kurt Gödel Research Center, 2009, Available at <http://www.logic.univie.ac.at/~sdf/papers/wien-spb.pdf>
- [9] H. Friedman and L. Stanley. A Borel reducibility theory for classes of countable structures, *Journal Symbolic Logic* 54, (1989), 894–914.
- [10] S. Givant and P. Halmos. *Introduction to Boolean algebras*, Springer, 2008.
- [11] Y. Gurevich. From invariants to canonization. *Bulletin of the European Association for Theoretical Computer Science* 63, pp. 115–119, 1997.
- [12] J. Hartmanis and L. Hemachandra. Complexity classes without machines: On complete languages for UP. *Theoretical Computer Science* 58, 129–142, 1988.
- [13] T. Kavitha. Efficient algorithms for abelian group isomorphism and related problems. In *Proceedings of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'02)*, Lecture Notes in Computer Science 2914, pp. 277–288, Springer, 2003.
- [14] W. Kowalczyk. Some connections between presentability of complexity classes and the power of formal systems of reasoning. In *Proceedings of Mathematical Foundations of Computer Science, (MFCS'84)*, Lecture Notes in Computer Science 176, Springer, pp. 364–369, 1984.
- [15] G. Miller. Isomorphism testing for graphs of bounded genus. In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC'80)*, 225–235, 1980.
- [16] T. Thierauf. *The computational complexity of equivalence and isomorphism problems*. Lecture Notes in Computer Science, 1852, Springer, 2000.