Electronic Colloquium on Computational Complexity, Report No. 69 (2006)

The Complexity of Unions of Disjoint Sets

Christian Glaßer[*], Alan L. Selman[†],
Stephen Travers[‡], and Klaus W. Wagner[*]

Abstract

This paper is motivated by the open question whether the union of two disjoint NP-complete sets always is NP-complete. We discover that such unions retain much of the complexity of their single components. More precisely, they are complete with respect to more general reducibilities.

Moreover, we approach the main question in a more general way: We analyze the scope of the complexity of unions of m-equivalent disjoint sets. Under the hypothesis that NE $\neq$ coNE, we construct degrees in NP where our main question has a positive answer, i.e., these degrees are closed under unions of disjoint sets.

1 Introduction

We report progress on the open question [Sel88] of whether the union of two disjoint NP-complete sets is NP-complete. We prove that the union of two disjoint NP-complete sets belongs to the class High_1, the first level of Schöning's high hierarchy [Sch83]. Specifically, for every $k \geq 1$, if $A \in \mathrm{High}_k$ and $B \in \mathrm{NP}$ such that $A \cap B = \emptyset$, then $A \cup B \in \mathrm{High}_k$. As a consequence [KS97], if A and B are disjoint NP-complete sets, then $A \cup B$ is a strongly-nondeterministic complete set for NP [Lon78].

In order to give further evidence that unions of disjoint NP-complete sets are not far from being NP-complete, we show that the union of an NP-complete set with a disjoint set in NP is nonuniformly NP-complete, under the following assumption: There exists a set $A \in \mathrm{NP}$ such that A is not infinitely-often in coNP. Non-uniform reductions are of interest in cryptography, where they model an adversary who is capable of long preprocessing [BV97]. They also have applications in structural complexity theory. Agrawal [Agr02] and Hitchcock and Pavan [HP06] investigate non-uniform reductions and show under reasonable hypotheses that every many-one complete set for NP is also hard for length-increasing, non-uniform reductions.

[*] Theoretische Informatik, Universität Würzburg, {glasser,wagner}@informatik.uni-wuerzburg.de.

[†] Research supported in part by NSF grant CCR-0307077 and by the Alexander von Humboldt-Stiftung, selman@cse.buffalo.edu.

[‡] Supported by the Konrad-Adenauer-Stiftung, travers@informatik.uni-wuerzburg.de.

ISSN 1433-8092

Then we raise the more general question, given two many-one-equivalent, disjoint, sets A and B in NP, what can we say about the complexity of the union $A \cup B$. Define a set A to be *m-idempotent* if for all sets B and C,

$$(A \equiv_{\mathrm{m}}^{\mathrm{p}} B \equiv_{\mathrm{m}}^{\mathrm{p}} C) \wedge (B \cap C = \emptyset) \Longrightarrow A \equiv_{\mathrm{m}}^{\mathrm{p}} B \cup C.$$

The set SAT is m-idempotent if and only if the union of two disjoint NP-complete sets always is NP-complete. We prove that every p-selective set is m-idempotent. It follows readily that if NE $\neq$ coNE, then there exists $A \in$ NP$-$coNP such that A is m-idempotent, and it follows that the class EXP contains m-idempotent sets.

Finally, we show that it is possible for the union of two disjoint sets to be harder than either of its components. We prove that if the polynomial hierarchy is infinite, then there exist sets A and B in NP(2) such that $A \equiv_{\mathrm{m}}^{\mathrm{p}} B$, $A \leq_{\mathrm{m}}^{\mathrm{p}} A \cup B$, and $A \cup B$ does not m-reduce to A. More precisely, we show this under the weaker assumption that the Boolean hierarchy over NP does not collapse to the second level.

To explore this possibility within NP, we show under an hypothesis that asserts strong immunity conditions that there exist disjoint sets $E, F \in$ NP $-$ coNP such that $E \equiv_{\mathrm{m}}^{\mathrm{p}} F$, but $E \cup F \not\leq_{\mathrm{m}}^{\mathrm{p}} E$.

Glasser et al. [GPSZ05] recently showed that all NP-complete sets are m-mitotic. This means that any NP-complete set A can be partitioned into disjoint NP-complete sets A_1, A_2. In a sense, the issue we are raising here, given two m-equivalent disjoint set B_1 and B_2, how complex is the union $B_1 \cup B_2$, is to investigate the converse of that question.

2 Preliminaries

We recall basic notions. Σ denotes a finite alphabet with at least two letters, Σ^* denotes the set of all words, and $|w|$ denotes the length of a word w. A tally set is a subset of 0^*. The language accepted by a machine M is denoted by $L(M)$. The characteristic function of a set A is denoted by c_A. $\overline{L}$ denotes the complement of a language L and co$\mathcal{C}$ denotes the class of complements of languages in $\mathcal{C}$. 1NP [GW86] (also called US [BG82]) is the class of languages L for which there exists a nondeterministic polynomial-time-bounded machine M such that an input x belongs to L if and only if M on input x has exactly one accepting path. In contrast, UP is the class of languages L for which there exists a nondeterministic polynomial-time-bounded machine M such that $L = L(M)$ and on every input x, the machine M on input x has at most one accepting path [Val76]. FP denotes the class of functions computable in deterministic polynomial time. FP/poly is the superclass of FP that consists of all functions f for which there exists a total function $a : 0^* \to \Sigma^*$ such that

- there exists a polynomial p such that for all n, $|a(0^n)| \leq p(n)$, and
- there exists a $g \in$ FP such that for all x, $f(x) = g(x, a(0^{|x|}))$.

The function a is called the advice function.

The symmetric difference of sets A and B is defined as $A \triangle B = (A - B) \cup (B - A)$. The complex version is defined as $\mathcal{C} \oplus \mathcal{D} = \{A \triangle B : A \in \mathcal{C}, B \in \mathcal{D}\}$. For a class of languages $\mathcal{C}$ which is closed under union and intersection, the Boolean hierarchy over $\mathcal{C}$ [WW85] is the family of classes $\mathcal{C}(k)$ and co$^{+}\mathcal{C}(k)$ where $k \geq 1$,

$$\begin{aligned} \mathcal{C}(k) &=_{\mathrm{def}} \overbrace{\mathcal{C} \oplus \mathcal{C} \oplus \cdots \oplus \mathcal{C}}^{k \text{ times}}, \text{ and} \\ \mathrm{co}\mathcal{C}(k) &=_{\mathrm{def}} \left\{\overline{L} : L \in \mathcal{C}(k)\right\}. \end{aligned}$$

The properties of Boolean hierarchies were studied by Köbler, Schöning, and Wagner [KSW87] and Cai et al. [CGH^{+}88].

We recall standard polynomial-time reducibilities [LLS75]. A set B *many-one-reduces* to a set C (*m-reduces* for short; in notation $B \leq_{\mathrm{m}}^{\mathrm{p}} C$) if there exists a total, polynomial-time-computable function f such that for all strings x,

$$x \in B \Leftrightarrow f(x) \in C.$$

A set B *Turing-reduces* to a set C (*T-reduces* for short; in notation $B \leq_{\mathrm{T}}^{\mathrm{p}} C$) if there exists a deterministic polynomial-time-bounded oracle Turing machine M such that for all strings x,

$$x \in B \Leftrightarrow M \text{ with } C \text{ as oracle accepts the input } x.$$

A set B *2-disjunctively truth-table-reduces* to a set C (*2-dtt-reduces* for short; in notation $B \leq_{2\text{-}\mathrm{dtt}}^{\mathrm{p}} C$) if there exists a total, polynomial-time-computable function $f : \Sigma^* \to \Sigma^* \times \Sigma^*$ such that for all strings x,

$$x \in B \Leftrightarrow \text{at least one word from the pair } f(x) \text{ belongs to } C.$$

A set B *non-uniformly many-one-reduces* to a set C (*non-uniformly m-reduces* for short; in notation $B \leq_{\mathrm{m}}^{\mathrm{p/poly}} C$) if there exists a total function $f \in$ FP/poly such that for all strings x,

$$x \in B \Leftrightarrow f(x) \in C.$$

A set B *strongly nondeterministic Turing-reduces* to a set C [Lon78] (*snT-reduces* for short; in notation $B \leq_{\mathrm{snT}}^{\mathrm{p}} C$) if there exists a nondeterministic polynomial-time-bounded oracle Turing machine M that on each computation path outputs exactly one symbol from $\{+, -, ?\}$ such that for all strings x,

$$\begin{aligned} x \in B &\Rightarrow M \text{ on } x \text{ produces at least one } + \text{ and no } - \quad \text{and} \\ x \notin B &\Rightarrow M \text{ on } x \text{ produces at least one } - \text{ and no } +. \end{aligned}$$

If $B \leq_{\mathrm{m}}^{\mathrm{p}} C$ and $C \leq_{\mathrm{m}}^{\mathrm{p}} B$, then we say that B and C are *many-one-equivalent* (*m-equivalent* for short, in notation $B \equiv_{\mathrm{m}}^{\mathrm{p}} C$). Similarly, we define equivalence for other reducibilities. A set B is *many-one-hard* (*m-hard* for short) for a complexity class $\mathcal{C}$ if every $B \in \mathcal{C}$ m-reduces to B. If additionally $B \in \mathcal{C}$, then we say that B is *many-one-complete* (*m-complete* for short) for $\mathcal{C}$. Similarly, we define hardness and completeness for other reducibilities. We use the term $\mathcal{C}$-complete as an abbreviation for m-complete for $\mathcal{C}$.

Schöning [Sch83] defined a set $A \in \mathrm{NP}$ to be *high* for $\Sigma_{\mathrm{k}}^{\mathrm{P}}$ (the k-th level of the polynomial-time hierarchy) if ${\Sigma_{\mathrm{k}}^{\mathrm{P}}}^{A} = \Sigma_{\mathrm{k+1}}^{\mathrm{P}}$. High_k is the class of languages that are high for $\Sigma_{\mathrm{k}}^{\mathrm{P}}$.

Disjoint sets A and B are called *p-separable* if there exists a set $S \in \mathrm{P}$ (the separator) such that $A \subseteq S$ and $B \subseteq \overline{S}$. A set B is *m-mitotic* [AS84] if there exists an $S \in \mathrm{P}$ such that $B \cap S$ and $B \cap \overline{S}$ are m-equivalent to B. B is *p-selective* [Sel79] if there exists a total function $f \in \mathrm{FP}$ (the selector function) such that for all x and y, $f(x,y) \in \{x,y\}$ and if either of x and y belongs to B, then $f(x,y) \in B$.

A is *paddable* [BH77] if there exists $p(\cdot,\cdot)$, a polynomial-time computable, polynomial-time invertible (i.e., there is a $g \in \mathrm{FP}$ such that for all x and y, $g(p(x,y)) = \langle x,y\rangle$) function, such that for all a and x,

$$a \in A \Leftrightarrow p(a,x) \in A.$$

Definition 2.1 *Let A be a set and $\mathcal{C}$ be a complexity class. The* reduction closure *and the* degree *of A (resp., $\mathcal{C}$) are defined as follows.*

$$\begin{aligned}
\mathcal{R}_m^p(A) &=_{\mathrm{def}} \{B \mid B \leq_{\mathrm{m}}^{\mathrm{p}} A\},\\
\mathcal{R}_m^p(\mathcal{C}) &=_{\mathrm{def}} \bigcup_{A \in \mathcal{C}} \mathcal{R}_m^p(A),\\
\deg_{\mathrm{m}}^{\mathrm{p}}(A) &=_{\mathrm{def}} \{B \mid A \equiv_{\mathrm{m}}^{\mathrm{p}} B\},\\
\deg_{\mathrm{m}}^{\mathrm{p}}(\mathcal{C}) &=_{\mathrm{def}} \bigcup_{A \in \mathcal{C}} \deg_{\mathrm{m}}^{\mathrm{p}}(A).
\end{aligned}$$

It is easy to see that whenever a class $\mathcal{C}$ is closed under $\leq_{\mathrm{m}}^{\mathrm{p}}$, it then follows that $\deg_{\mathrm{m}}^{\mathrm{p}}(\mathcal{C}) = \mathcal{R}_m^p(\mathcal{C})$.

Definition 2.2 *Let $\mathcal{C}$ and $\mathcal{M}$ be complexity classes. We define*

$$\begin{aligned}
\mathcal{C} \vee \mathcal{M} &=_{\mathrm{def}} \{A \cup B \mid A \in \mathcal{C}, B \in \mathcal{M}\},\\
\mathcal{C} \dot{\vee} \mathcal{M} &=_{\mathrm{def}} \{A \cup B \mid A \in \mathcal{C}, B \in \mathcal{M}, A \cap B = \emptyset\}.
\end{aligned}$$

Notice that the disjoint union used here is not the same concept as the marked union which is sometimes denoted by $\dot{\cup}$. The reason is that the latter leads to unions of disjoint p-separable sets, which does not have to be the case with $\dot{\vee}$. For instance, for all sets $A, B \in 1\mathrm{NP}$, it holds that $A \dot{\cup} B = 0A \cup 1B \in 1\mathrm{NP}$, implying that 1NP is closed under $\dot{\cup}$. Contrary to that, there exists an oracle relative to which $1\mathrm{NP} \dot{\vee} 1\mathrm{NP} \neq 1\mathrm{NP}$ [GT05].

3 Unions of Disjoint NP-complete Sets are not Easy

In this section we show that unions of disjoint NP-complete sets cannot be too easy. More precisely, we prove the following for disjoint NP-complete sets B and C.

1. $B \cup C$ is high for NP. Equivalently, $B \cup C$ is strongly nondeterministic-Turing-complete for NP [KS97].
2. Under a reasonable hypothesis, $B \cup C$ is non-uniformly many-one-complete for NP.

Our results show that unions of disjoint NP-complete sets remain complete with respect to more general reducibilities. This is evidence that unions of disjoint NP-complete sets retain much of the complexity of their single components.

As a byproduct, we obtain that the levels $1, 2, \ldots$ of the high-hierarchy are closed under disjoint unions with arbitrary NP-sets. Recently, Hitchcock and Pavan [HP06] showed that if NP does not have p-measure 0, then the levels 0 and 1 of the high-hierarchy are different.

3.1 Unions of Disjoint Sets from the High-Hierarchy

Lemma 3.1 *Let $A, B \in \mathrm{NP}$ such that $A \cap B = \emptyset$. Then $\mathrm{NP}^A \subseteq \mathrm{NP}^{A \cup B}$.*

Proof Let M_A and M_B be nondeterministic polynomial-time Turing machines such that $L(M_A) = A$ and $L(M_B) = B$, and let $C \in \mathrm{NP}^A$ via a nondeterministic polynomial-time oracle Turing-machine (NPOTM) M; i.e., $L(M^A) = C$.

We construct a NPTOM N such that $L(N^{A \cup B}) = C$:

N simulates M on input x until M wants to query the oracle A. Say M wants to query A for the string q. Recall that N on its simulation of M cannot query oracle A but only the oracle $A \cup B$. So N queries $A \cup B$ for q.

Case 1: $q \notin A \cup B$: It then follows that $q \notin A$, so N can continue the simulation of M with a negative answer to the query q.

Case 2: $q \in A \cup B$: N branches nondeterministically into two paths. On the first path, it simulates $M_A(q)$, on the second, it simulates $M_B(q)$. Since A and B are disjoint, only one of these two machines produces an accepting path. Then N continues as follows:

- On all accepting paths of $M_A(q)$ (if any), N continues the simulation of M with a positive answer to the query q.
- On all rejecting paths of $M_A(q)$, N rejects.

- On all accepting paths of $M_B(q)$ (if any), N continues the simulation of M with a negative answer to the query q.
- On all rejecting paths of $M_B(q)$, N also rejects.

During its simulation of M, N proceeds in the same way for all of M's queries to A. Observe that since $M_A(q)$ (or $M_B(q)$, respectively) can very well produce more than one accepting path, N will in general perform several parallel simulations of M after a simulation of $M_A(q)$ or $M_B(q)$. As $L(M_A) \cap L(M_B) = \emptyset$, all these parallel simulations are identical. Consequently, it is immediately clear that $N^{A \cup B}(x)$ produces an accepting path if and only if $M^A(x)$ produces an accepting path and hence $L(N^{A \cup B}) = L(M^A) = C$. This proves $C \in \mathrm{NP}^{A \cup B}$ and we obtain $\mathrm{NP}^A \subseteq \mathrm{NP}^{A \cup B}$. □

Theorem 3.2 *Let $k \geq 1$, $A \in \mathrm{High}_k$ and $B \in \mathrm{NP}$ such that $A \cap B = \emptyset$. Then $A \cup B \in \mathrm{High}_k$.*

Proof Let $k \geq 1$, $A \in \mathrm{High}_k$ and $B \in \mathrm{NP}$ such that $A \cap B = \emptyset$. We will show that

$$\Sigma_{\mathrm{k+1}}^{\mathrm{P}} = \Sigma_{\mathrm{k}}^{\mathrm{P}A} \subseteq (\Sigma_{\mathrm{k}}^{\mathrm{P}})^{A \cup B}.$$

Since A is a set from High_k, the first equality follows from the definition. We will argue for $\Sigma_{\mathrm{k}}^{\mathrm{P}A} \subseteq (\Sigma_{\mathrm{k}}^{\mathrm{P}})^{A \cup B}$ by induction over k.

(IB) Let k=1. Then $\Sigma_1^{\mathrm{P}A} = \mathrm{NP}^A \subseteq (\Sigma_1^{\mathrm{P}})^{A \cup B} = \mathrm{NP}^{A \cup B}$ holds due to Lemma 3.1.

(IH) Let us assume that $\Sigma_{\mathrm{k}}^{\mathrm{P}A} \subseteq (\Sigma_{\mathrm{k}}^{\mathrm{P}})^{A \cup B}$ holds for a $k \geq 1$.

(IS) By definition, $(\Sigma_{\mathrm{k+1}}^{\mathrm{P}})^A = (\mathrm{NP}^{\Sigma_{\mathrm{k}}^{\mathrm{P}}})^A$.

Observe that $\left(\mathrm{NP}^{\Sigma_{\mathrm{k}}^{\mathrm{P}}}\right)^A \subseteq \mathrm{NP}^{0A \cup 1O}$ for a suitable set $O \in \Sigma_{\mathrm{k}}^{\mathrm{P}A}$. By the the induction hypothesis, $O \in (\Sigma_{\mathrm{k}}^{\mathrm{P}})^{A \cup B}$. Arguing similarly as in Lemma 3.1, we obtain

$$\mathrm{NP}^{0A \cup 1O} \subseteq (\mathrm{NP}^{\Sigma_{\mathrm{k}}^{\mathrm{P}}})^{A \cup B} = (\Sigma_{\mathrm{k+1}}^{\mathrm{P}})^{A \cup B}.$$

This shows that for all $k \geq 1$, it holds that $\Sigma_{\mathrm{k+1}}^{\mathrm{P}} = \Sigma_{\mathrm{k}}^{\mathrm{P}A} \subseteq (\Sigma_{\mathrm{k}}^{\mathrm{P}})^{A \cup B}$. □

The following corollary is an immediate consequence of Theorem 3.2.

Corollary 3.3 *For all $k \geq 1$, High_k is closed under unions of disjoint sets.*

Corollary 3.4 *Let $A, B \in \mathrm{NPC}$ such that $A \cap B = \emptyset$. Then the set $A \cup B$ is $\leq_{\mathrm{snT}}^{\mathrm{p}}$-complete for NP.*

Proof Since A, B are NP-complete, they obviously are in High_1. Theorem 3.2 yields that $A \cup B$ also is in High_1. However, a set is in in High_1 if and only if it is $\leq_{\mathrm{snT}}^{\mathrm{p}}$-complete for NP [KS97]. □

3.2 Uniformly Hard Languages in NP

In Section 3.1 we showed that the union of a disjoint NP-complete set and an arbitrary NP-set is high for NP. In this section we give further evidence that unions of disjoint NP-complete are not far from being NP-complete. To do so, we assume that NP contains uniformly hard languages, i.e., languages that are uniformly not contained in coNP. After discussing this assumption we show that it implies the following.

- For every NP-complete A and every $B \in \mathrm{NP}$ that is disjoint from A it holds that $A \cup B$ is nonuniformly NP-complete.

Definition 3.5 *Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes, and let A and B be subsets of Σ^*.*

1. $A \overset{\text{i.o.}}{=} B \overset{df}{\Longleftrightarrow}$ *for infinitely many n it holds that* $A \cap \Sigma^n = B \cap \Sigma^n$.
2. $A \overset{\text{i.o.}}{\in} \mathcal{C} \overset{df}{\Longleftrightarrow}$ *there exists* $C \in \mathcal{C}$ *such that* $A \overset{\text{i.o.}}{=} C$.
3. $\mathcal{C} \overset{\text{i.o.}}{\subseteq} \mathcal{D} \overset{df}{\Longleftrightarrow} C \overset{\text{i.o.}}{\in} \mathcal{D}$ *for all* $C \in \mathcal{C}$.

The following proposition is easy to observe.

Proposition 3.6 *Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes, and let A and B be subsets of Σ^*.*

1. $A \overset{\text{i.o.}}{=} B$ *if and only if* $\overline{A} \overset{\text{i.o.}}{=} \overline{B}$.
2. $A \overset{\text{i.o.}}{\in} \mathcal{C}$ *if and only if* $\overline{A} \overset{\text{i.o.}}{\in} \mathrm{co}\mathcal{C}$.
3. $\mathcal{C} \overset{\text{i.o.}}{\subseteq} \mathcal{D}$ *if and only if* $\mathrm{co}\mathcal{C} \overset{\text{i.o.}}{\subseteq} \mathrm{co}\mathcal{D}$.

Proposition 3.7 *The following are equivalent:*

(i) $\mathrm{coNP} \overset{\text{i.o.}}{\not\subseteq} \mathrm{NP}$

(ii) $\mathrm{NP} \overset{\text{i.o.}}{\not\subseteq} \mathrm{coNP}$

(iii) There exists an $A \in \mathrm{NP}$ *such that* $A \overset{\text{i.o.}}{\notin} \mathrm{coNP}$.

(iv) There exists a paddable NP*-complete A such that* $A \overset{\text{i.o.}}{\notin} \mathrm{coNP}$.

Proof The equivalence of (i) and (ii) is by Proposition 3.6. Moreover, from the definition it immediately follows that ¬(ii) ⇒ ¬(iii) and ¬(iii) ⇒ ¬(iv). It remains to show ¬(iv) ⇒ ¬(ii). So we assume that for all paddable NP-complete A it holds that $A \overset{\text{i.o.}}{\in} \mathrm{coNP}$. Choose any $C \in \mathrm{NP}$ and let $B = 0C \cup 1\mathrm{SAT}$. Hence B is paddable and NP-complete. By our assumption $B \overset{\text{i.o.}}{\in} \mathrm{coNP}$. So there exists a $D \in \mathrm{coNP}$ such that

$B \overset{\text{i.o.}}{=} D$. Let $D' = \{w \mid 0w \in D\}$ and note that $D' \in \text{coNP}$. Observe that for every n, if $B \cap \Sigma^{n+1} = D \cap \Sigma^{n+1}$, then $C \cap \Sigma^n = D' \cap \Sigma^n$. Hence $C \overset{\text{i.o.}}{=} D'$ which shows $C \overset{\text{i.o.}}{\in} \text{coNP}$. □

The following results assume the hypothesis that $\text{NP} \overset{\text{i.o.}}{\notin} \text{coNP}$. This is a believable assumption that says that (for sufficiently long formulas) not all tautologies of a given size have short proofs. First we show that unions of disjoint NP-complete sets are nonuniformly many-one complete for NP.

Theorem 3.8 *If* $\text{NP} \overset{\text{i.o.}}{\not\subseteq} \text{coNP}$*, then for every* NP*-complete* A *and every* $B \in \text{NP}$ *that is disjoint to* A *it holds that* $A \cup B$ *is* $\leq_{\text{m}}^{\text{p/poly}}$*-complete for* NP*.*

Proof By assumption, there exists an NP-complete K such that $K \overset{\text{i.o.}}{\notin} \text{coNP}$. Choose $f \in \text{FP}$ such that $K \leq_{\text{m}}^{\text{p}} A$ via f, and choose $g \in \text{FP}$ such that $\{(u,v) \mid u \in K \vee v \in K\} \leq_{\text{m}}^{\text{p}} K$ via g.

$$\text{EASY} =_{\text{def}} \{u \mid \exists v, |v| = |u|, f(g(u,v)) \in B\}$$

EASY belongs to NP. We see $\text{EASY} \subseteq \overline{K}$ as follows: $f(g(u,v)) \in B$ implies $g(u,v) \notin K$ which shows $u \notin K$. Intuitively, EASY is a set of words u that are outside K and that have short proofs for this. (The proof is v together with an accepting path proving $f(g(u,v)) \in B$.) From our assumption $\overline{K} \overset{\text{i.o.}}{\notin} \text{NP}$ it follows that there exists an $n_0 \geq 0$ such that

$$\forall n \geq n_0, \overline{K}^{=n} \not\subseteq \text{EASY}^{=n}.$$

So for every $n \geq n_0$ we can choose a word $w_n \in \overline{K}^{=n} - \text{EASY}$. For $n < n_0$, let $w_n = \varepsilon$. Choose fixed $z_1 \in A \cup B$ and $z_0 \notin A \cup B$ (z_0 exists, since $\text{NP} \overset{\text{i.o.}}{\not\subseteq} \text{coNP}$ implies $\text{NP} \neq \text{coNP}$). We define the reduction that witnesses $K \leq_{\text{m}}^{\text{p/poly}} A \cup B$.

$$h(v) =_{\text{def}} \begin{cases} f(g(w_{|v|}, v)) & : \text{ if } |v| \geq n_0 \\ z_1 & : \text{ if } |v| < n_0 \text{ and } v \in K \\ z_0 & : \text{ if } |v| < n_0 \text{ and } v \notin K \end{cases}$$

Observe that $h \in \text{FP/poly}$ with the advice $n \mapsto w_n$.

We claim that for all v,

$$v \in K \Leftrightarrow h(v) \in A \cup B. \tag{1}$$

This equivalence clearly holds for all v such that $|v| < n_0$. So assume $|v| \geq n_0$ and let $n = |v|$.

If $v \in K$, then $g(w_n, v) \in K$ and hence $f(g(w_n, v)) \in A \subseteq A \cup B$.

If $v \notin K$, then $g(w_n, v) \notin K$ (since $w_n \notin K$). Hence $f(g(w_n, v)) \notin A$. If $f(g(w_n, v)) \in B$, then $w_n \in \text{EASY}$ contradicting the choice of w_n. Therefore, $f(g(w_n, v)) \notin B$. This proves (1) and therefore, $A \cup B$ is $\leq_{\text{m}}^{\text{p/poly}}$-complete for NP. □

4 The Complexity of Disjoint Unions

In this section, we abstract from the main question. We investigate how complex the union of two disjoint[1] equivalent NP sets can be, and we state interesting upper and lower bounds.

For any set A, we define the set $\mathcal{U}(A)$ which is the class of all sets which are m-equivalent to the union of two disjoint sets from the m-degree of A.

Definition 4.1 *For a set A, we define the class*

$$\mathcal{U}(A) =_{\text{def}} \deg_{\text{m}}^{\text{p}}\big(\{C \cup D \,\big|\, C \cap D = \emptyset \wedge C \equiv_{\text{m}}^{\text{p}} D \equiv_{\text{m}}^{\text{p}} A\}\big).$$

The next theorem characterizes the scope of $\mathcal{U}(A)$. We state a technical lemma first.

Lemma 4.2 *Let $\mathcal{K}$ and $\mathcal{M}$ be complexity classes that are closed under $\leq_{\text{m}}^{\text{p}}$. Then the class $\mathcal{K} \dot{\vee} \mathcal{M}$ is closed under $\leq_{\text{m}}^{\text{p}}$ as well.*

Proof We have to show that $A \in \mathcal{R}_m^p(\mathcal{K} \dot{\vee} \mathcal{M})$ implies $A \in \mathcal{K} \dot{\vee} \mathcal{M}$.

Let $A \in \mathcal{R}_m^p(\mathcal{K} \dot{\vee} \mathcal{M})$, hence there exist $f \in \text{FP}, A_1 \in \mathcal{K}, A_2 \in \mathcal{M}$ such that $A_1 \cap A_2 = \emptyset$, and $x \in A \Leftrightarrow f(x) \in A_1 \cup A_2$. For $i \in \{1,2\}$, let $f^{-1}[A_i] =_{\text{def}} \{x : f(x) \in A_i\}$. Observe that for $i \in \{1,2\}$, f reduces $f^{-1}[A_i]$ to A_i. As $\mathcal{K}$ and $\mathcal{M}$ are closed under $\leq_{\text{m}}^{\text{p}}$, it follows that $f^{-1}[A_1] \in \mathcal{K}$ and $f^{-1}[A_2] \in \mathcal{M}$. Moreover $f^{-1}[A_1] \cap f^{-1}[A_2] = \emptyset$. We obtain

$$\begin{aligned} x \in A &\Leftrightarrow f(x) \in A_1 \cup A_2 \\ &\Leftrightarrow \big(f(x) \in A_1\big) \vee \big(f(x) \in A_2\big) \\ &\Leftrightarrow \big(x \in f^{-1}[A_1]\big) \vee \big(x \in f^{-1}[A_2]\big) \\ &\Leftrightarrow x \in f^{-1}[A_1] \cup f^{-1}[A_2]. \end{aligned}$$

Consequently, x is in A if and only if x is in the union of a $\mathcal{K}$-set and a disjoint $\mathcal{M}$-set, hence $A \in \mathcal{K} \dot{\vee} \mathcal{M}$. □

Theorem 4.3 *For all nonempty sets A, it holds that*

$$\deg_{\text{m}}^{\text{p}}(A) \subseteq \mathcal{U}(A) \subseteq \mathcal{R}_m^p(A) \dot{\vee} \mathcal{R}_m^p(A).$$

Proof Let A be a set and $B \in \deg_{\text{m}}^{\text{p}}(A)$. Hence, we have $A \equiv_{\text{m}}^{\text{p}} B \equiv_{\text{m}}^{\text{p}} 0A \cup 1A$. To see that $0A \cup 1A$ is in $\mathcal{U}(A)$, notice that $0A \cap 1A = \emptyset$ and $0A \equiv_{\text{m}}^{\text{p}} 1A \equiv_{\text{m}}^{\text{p}} A$. As B is m-equivalent to A and $0A \cup 1A$, B also is in $\mathcal{U}(A)$.

[1] Note that the main question can easily be solved for non-disjoint unions of NP-complete sets: $0\text{SAT} \cup 1\Sigma^*$ and $0\Sigma^* \cup 1\text{SAT}$ are NP-complete sets whose union is in P.

For the second inclusion, let $E \in \mathcal{U}(A)$. So there exist $C, D \in \mathrm{deg}_{\mathrm{m}}^{\mathrm{p}}(A)$ such that $C \cap D = \emptyset$ and $E \equiv_{\mathrm{m}}^{\mathrm{p}} C \cup D$. It follows that $E \in \mathcal{R}_m^p(C \cup D) \subseteq \mathcal{R}_m^p(\mathrm{deg}_{\mathrm{m}}^{\mathrm{p}}(A) \dot\vee \mathrm{deg}_{\mathrm{m}}^{\mathrm{p}}(A)) \subseteq \mathcal{R}_m^p(\mathcal{R}_m^p(A) \dot\vee \mathcal{R}_m^p(A))$. By Lemma 4.2, this is equal to $\mathcal{R}_m^p(A) \dot\vee \mathcal{R}_m^p(A)$. □

Let A be a set and B and C be disjoint sets that are m-equivalent to A. In the next sections we will study the following phenomena:

- For some A, the union $B \cup C$ is always m-equivalent to A, no matter how B and C are chosen.
- For some A, the union $B \cup C$ can be less complex than A.
- For some A, the union $B \cup C$ can be more complex than A.

4.1 Disjoint Sets Whose Union is At Most as Hard as the Single Components

In the following section, we consider m-equivalent, disjoint sets whose union is at most as complex as the single components. We prove that two extremes can occur:

- Unions of disjoint, m-equivalent NP sets can be equivalent to their single components (Theorem 4.8).
- Unions of disjoint, m-equivalent NP sets can be very easy, e.g. in P (Theorem 4.15).

Definition 4.4 *We say that a set A is* m-idempotent *if the following holds for all sets B and C:*

$$(A \equiv_{\mathrm{m}}^{\mathrm{p}} B \equiv_{\mathrm{m}}^{\mathrm{p}} C) \wedge (B \cap C = \emptyset) \Longrightarrow A \equiv_{\mathrm{m}}^{\mathrm{p}} B \cup C.$$

Observe that a set A is m-idempotent if and only if $\mathrm{deg}_{\mathrm{m}}^{\mathrm{p}}(A) = \mathcal{U}(A)$; that is, the first inclusion in Theorem 4.3 is an equality. Furthermore, it is clear that whenever a set A is m-idempotent, the same holds for all sets $B \in \mathrm{deg}_{\mathrm{m}}^{\mathrm{p}}(A)$.

It turns out that our main question can be formulated equivalently with the notion of m-idempotence.

Proposition 4.5 SAT *is m-idempotent if and only if the union of two disjoint* NP*-complete sets always is* NP*-complete.*

So it is open whether the sets in the highest degree of NP are m-idempotent. A more general question is to ask whether there exists a set $A \in \mathrm{NP}$ such that the sets in the m-degree of A are m-idempotent. In other words, this is the question whether there is a set A in NP that has the least possible scope for $\mathcal{U}(A)$. Observe that such a set A must be in NP $-$ P. Otherwise $0\Sigma^* \equiv^{\mathrm{p}}_{\mathrm{m}} 1^*\Sigma^* \equiv^{\mathrm{p}}_{\mathrm{m}} A$, which would imply that $\Sigma^* \equiv^{\mathrm{p}}_{\mathrm{m}} A$. This is a contradiction because A is nontrivial.

The next theorem states that the notion of p-selectivity can help us to find m-idempotent sets. More precisely, p-selectivity implies m-idempotence for any set outside P.

Theorem 4.6 *Let $A \notin \mathrm{P}$. If A is p-selective, then A is m-idempotent.*

Proof Let A be a p-selective set outside P.

Claim 4.7 *For all disjoint $B, C \in \deg^{\mathrm{p}}_{\mathrm{m}}(A)$ it holds that the pair (B, C) is p-separable.*

Proof of the claim. Let $B, C \in \deg^{\mathrm{p}}_{\mathrm{m}}(A)$ such that $B \cap C = \emptyset$. Let $g, h \in \mathrm{FP}$ such that $B \leq^{\mathrm{p}}_{\mathrm{m}} A$ via g and $C \leq^{\mathrm{p}}_{\mathrm{m}} A$ via h. Furthermore, let $f \in \mathrm{FP}$ be the selector of A. We now define a set $S \in \mathrm{P}$ which separates the pair (B, C). Let

$$S =_{\mathrm{def}} \{x \,|\, f(g(x), h(x)) = g(x)\}.$$

Since $f, g, h \in \mathrm{FP}$, S clearly is in P. It remains to show that S separates (B, C), this means that for all x, it must hold that

$$\begin{aligned} x \in B &\quad \Rightarrow x \in S \\ x \in C &\quad \Rightarrow x \in \overline{S}. \end{aligned}$$

Let $x \in B$. Then $g(x) \in A$. Moreover, $h(x) \notin A$ since B and C are disjoint. Consequently, $f(g(x), h(x)) = g(x)$ and $x \in S$. If $x \in C$, $h(x) \in A$ and $g(x) \notin A$. We obtain $f(g(x), h(x)) = h(x)$ and $x \notin S$. This proves our claim.

Hence, we have shown that all disjoint $B, C \in \deg^{\mathrm{p}}_{\mathrm{m}}(A)$ are p-separable. We argue that this implies that A is m-idempotent. Let $B, C \in \deg^{\mathrm{p}}_{\mathrm{m}}(A)$ such that $B \cap C = \emptyset$ and $C \leq^{\mathrm{p}}_{\mathrm{m}} B$ via $f \in \mathrm{FP}$. We have to show that $B \cup C \equiv^{\mathrm{p}}_{\mathrm{m}} B$. Clearly,

$$g(x) =_{\mathrm{def}} \begin{cases} x, & \text{if } x \in S \\ f(x), & \text{if } x \notin S \end{cases}$$

yields $B \cup C \leq^{\mathrm{p}}_{\mathrm{m}} B$.

Let us assume that $C = \overline{B}$. This implies $A \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$, because $A \equiv^{\mathrm{p}}_{\mathrm{m}} B \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{B} \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$. From [Sel79] it then follows that $A \in \mathrm{P}$. This is a contradiction, so $C \neq \overline{B}$. Hence, there exists $c \in \overline{B \cup C}$. Defining

$$h(x) =_{\mathrm{def}} \begin{cases} x, & \text{if } x \in S \\ c, & \text{if } x \notin S \end{cases}$$

we obtain $x \in B \Leftrightarrow h(x) \in B \cup C$, thus $B \leq^{\mathrm{p}}_{\mathrm{m}} B \cup C$ and $B \cup C \equiv^{\mathrm{p}}_{\mathrm{m}} B$. From this, it follows that $B \cup C \equiv^{\mathrm{p}}_{\mathrm{m}} A$. This finishes our proof. □

The proof of Theorem 4.6 does also show that every degree having the property that all pairs of disjoint sets are p-separable is m-idempotent.

Claim 4.7 then states that this holds in particular for degrees of p-selective sets. Moreover, if all pairs of disjoint sets in NP were p-separable, it would follow that P = UP [GS88] and that all sets in NP are m-idempotent. We refer to Fortnow and Rogers [FR02] for an analysis of this hypothesis.

The next theorem gives a positive answer to the more general question whether NP contains m-idempotent sets under the assumption that NE $\neq$ coNE.

Theorem 4.8 *If* $\mathrm{NE} \neq \mathrm{coNE}$*, there exists* $A \in \mathrm{NP} - \mathrm{coNP}$ *such that* A *is m-idempotent.*

Proof We assume that $\mathrm{NE} \neq \mathrm{coNE}$. This implies the existence of a tally set $T \in \mathrm{NP} - \mathrm{coNP}$ [BWSD77]. It then follows [Sel79] that there exists $A \equiv_{\mathrm{T}}^{\mathrm{p}} T$ such that $A \in \mathrm{NP}$ and A is p-selective. Suppose that $A \in \mathrm{NP} \cap \mathrm{coNP}$. Since $\mathrm{NP} \cap \mathrm{coNP}$ is closed under $\leq_{\mathrm{T}}^{\mathrm{p}}$-reducibility, this implies that $T \in \mathrm{NP} \cap \mathrm{coNP}$. As $T \in \mathrm{NP} - \mathrm{coNP}$, this is a contradiction. It follows that $A \in \mathrm{NP} - \mathrm{coNP}$. So we have identified a p-selective set in $\mathrm{NP} - \mathrm{coNP}$. In particular, $A \notin \mathrm{P}$. By Theorem 4.6, A is m-idempotent. □

The complexity class EXP contains m-idempotent sets unconditionally.

Theorem 4.9 *There exists an m-idempotent set* $A \in \mathrm{EXP}$.

Proof We first prove that there exists a tally set in $\mathrm{EXP} - \mathrm{P}$. We use a standard diagonalization argument. Let $M_1, M_2, \ldots$ be an enumeration of all deterministic polynomial-time Turing machines. For all $i \geq 1$, let the running time of machine M_i be bounded by polynomial p_i. For technical reasons, we choose an enumeration of machines and polynomials such that for all $i \geq 1$, $p_i(i) \leq 2^i - 1$.

Define

$$H =_{\mathrm{def}} \{0^i \mid M_i \text{ accepts } 0^i \text{ after at most } 2^i \text{ steps}\}.$$

Obviously, H is a tally set in EXP. We now prove that $H \notin \mathrm{P}$. We suppose, for the sake of contradiction, that there exists an $x \geq 1$ such that M_x accepts H. We construct a Turing machine D as follows: On input 0^i, D simulates M_x on input 0^i. D accepts the input 0^i if and only if M_x rejects 0^i.

Such a machine clearly exists, so there exists $y \geq 1$ such that $D = M_y$. The running time of M_y on an input 0^n can be bounded by $p_x(n) + 1 \leq p_y(n)$.

We now run M_y on input 0^y. M_y then starts a simulation of M_x on input 0^y.

Let us assume that M_x accepts 0^y. By the definition of H, it must hold that M_y accepts 0^y after at most 2^y steps. Nevertheless, we have designed M_y to reject whenever M_x accepts, so this is a contradiction. Hence, M_x rejects 0^y. Similarly, it follows that M_y does not accept 0^y after at most 2^y steps. Since we know that M_y on input y halts within

$p_x(y) + 1 \leq 2^y$ steps, it follows that M_y rejects 0^y within $p_y(y)$ steps. Again, this is a contradiction.

Consequently, no such machine M_x can exist, hence $H \notin \mathrm{P}$.

Since H is a tally set, it follows [Sel79] that there exists $A \equiv_{\mathrm{T}}^{\mathrm{p}} H$ such that A is p-selective. It is easy to see that $A \in \mathrm{EXP} - \mathrm{P}$. Together with Theorem 4.6, this implies that A is m-idempotent. □

We have shown that there are sets in EXP for which the first inclusion in Theorem 4.3 is an equality. Under a reasonable assumption, we have shown the same for NP. We now take a look at the second inclusion. The next proposition states that for nontrivial sets, at least one of the two inclusions has to be strict.

Proposition 4.10 *If $A \neq \emptyset$ and $A \neq \overline{\emptyset}$, it holds that* $\deg_{\mathrm{m}}^{\mathrm{p}}(A) \subsetneq \mathcal{R}_m^p(A)$.

Proof Let $A \neq \emptyset$ and $A \neq \overline{\emptyset}$ be a set. By definition, $\deg_{\mathrm{m}}^{\mathrm{p}}(A) \subseteq \mathcal{R}_m^p(A)$. Since $A \neq \overline{\emptyset}$, it is clear that $\emptyset \in \mathcal{R}_m^p(A)$. If $\deg_{\mathrm{m}}^{\mathrm{p}}(A)$ contained the empty set, it would follow that $A = \emptyset$, contradicting our assumption. □

We will show that there exists a set $A \in \mathrm{NP}$ such that $\deg_{\mathrm{m}}^{\mathrm{p}}(A) \subsetneq \mathcal{U}(A) = (\mathcal{R}_m^p(A) \dot{\vee} \mathcal{R}_m^p(A)) - \{\emptyset\}$ under the assumption that $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$. We first prove that a set A cannot be m-idempotent if $\mathcal{R}_m^p(A)$ is closed under boolean operations.

Theorem 4.11 *If $\mathcal{R}_m^p(A)$ is closed under boolean operations then $\mathcal{U}(A) = \mathcal{R}_m^p(A) - \{\emptyset\}$.*

Proof As $\mathcal{R}_m^p(A)$ is closed under boolean operations, it is easy to see that $\mathcal{R}_m^p(A) = \mathcal{R}_m^p(A) \dot{\vee} \mathcal{R}_m^p(A) = \mathcal{R}_m^p(A) \vee \mathcal{R}_m^p(A)$. Hence it follows from Theorem 4.3 that we only have to show $\mathcal{R}_m^p(A) \subseteq \mathcal{U}(A)$.

Let $E \in \mathcal{R}_m^p(A)$ and Σ be an alphabet such that $A \cup E \subseteq \Sigma^*$, let $a \notin \Sigma$ be a new letter, and let $\Delta =_{\mathrm{def}} \Sigma \cup \{a\}$. Say $E \leq_{\mathrm{m}}^{\mathrm{p}} A$ via function $h \in \mathrm{FP}$. Since $\mathcal{R}_m^p(A)$ is closed under complementation it follows that $\overline{A} \leq_{\mathrm{m}}^{\mathrm{p}} A$, say via function $h' \in \mathrm{FP}$, and hence $\overline{A} \equiv_{\mathrm{m}}^{\mathrm{p}} A$. Let $a_0, e_0 \in \Sigma^*$ such that $a_0 \notin A$ and $e_0 \notin E$.

We will define sets $A_0, A_1 \subseteq \Delta^*$ such that

- $A_0 \cap A_1 = \emptyset$,
- $A_0 \cup A_1 \equiv_{\mathrm{m}}^{\mathrm{p}} E$,
- $A_0 \equiv_{\mathrm{m}}^{\mathrm{p}} A_1 \equiv_{\mathrm{m}}^{\mathrm{p}} A$.

Notice that this implies $E \in \mathcal{U}(A)$.

We define $A_1 =_{\mathrm{def}} aA \cup E$ and $A_0 =_{\mathrm{def}} a(\Sigma^* - A)$. Clearly, $A_0 \cap A_1 = \emptyset$.

Claim 4.12 $A_0 \cup A_1 \equiv^{\mathrm{p}}_{\mathrm{m}} E$

Proof of the claim. It holds that $A_0 \cup A_1 = a\Sigma^* \cup E$. Let $f_1 : \Delta^* \to \Sigma^*$ be defined by

$$f_1(x) =_{\mathrm{def}} \begin{cases} x, & \text{if } x \in \Sigma^* \\ e_0, & \text{otherwise.} \end{cases}$$

Observe that $x \in a\Sigma^* \cup E \Leftrightarrow f_1(X) \in E$. As f_1 clearly is in FP, we have shown $A_0 \cup A_1 \leq^{\mathrm{p}}_{\mathrm{m}} E$. For the other direction, let $f_2 : \Sigma^* \to \Delta^*$ be defined by $f_2(x) = x$. Again, it is easy to see that $x \in E \Leftrightarrow f_2(x) \in a\Sigma^* \cup E$ and $f_2 \in \mathrm{FP}$. This proves the claim.

Claim 4.13 $A_0 \equiv^{\mathrm{p}}_{\mathrm{m}} A_1 \equiv^{\mathrm{p}}_{\mathrm{m}} A$

Proof of the claim. We will define functions $f_3, f_4, f_5 \in \mathrm{FP}$ such that $A_0 \leq^{\mathrm{p}}_{\mathrm{m}} A_1$ via f_3, $A_1 \leq^{\mathrm{p}}_{\mathrm{m}} A$ via f_4, and $A \leq^{\mathrm{p}}_{\mathrm{m}} A_0$ via f_5.

Define $f_3 : \Delta^* \to \Delta^*$ by

$$f_3(x) =_{\mathrm{def}} \begin{cases} ah'(z), & \text{if } x = az \text{ where } z \in \Sigma^* \\ e_0, & \text{otherwise.} \end{cases}$$

If $x \in A_0$, there exists $z \in \Sigma^* - A$ such that $x = az$. As h' reduces $\overline{A}$ to A, $ah'(z)$ is in A_1. If $x \notin A_0$, it either is of the form $x = az'$ where $z' \in A$ or $x \in \Delta^* - a\Sigma^*$. In the first case, $h'(z') \in \Sigma^* - A$, so $ah'(z) \notin A_1$. In the second case $f_3(x) = e_0 \notin A_1$. Obviously, $f_3 \in \mathrm{FP}$, hence $A_0 \leq^{\mathrm{p}}_{\mathrm{m}} A_1$.

Define $f_4 : \Delta^* \to \Sigma^*$ by

$$f_4(x) =_{\mathrm{def}} \begin{cases} z, & \text{if } x = az \text{ where } z \in \Sigma^* \\ h(x), & \text{if } x \in \Sigma^* \\ a_0, & \text{otherwise.} \end{cases}$$

If $x \in A_1$, either $x = az$ where $z \in A$ or $x \in E$. In the first case, $f_4(x) = z \in A$. In the second case, $f_4(x) = h(x) \in A$ since h reduces E to A. If $x \notin A_1$, we distinguish three cases:

1. Assume $x \in a(\Sigma^* - A)$, i.e. there exists $z' \in \Sigma^* - A$ such that $x = az'$. Then $f_4(x) = z' \notin A$.
2. Assume $x \in \Sigma^* - E$. Then $f_4(x) = h(x) \notin A$.
3. Assume $x \in (\Delta^* a \Delta^*) - (a\Sigma^*)$. Then $f_4(x) = a_0 \notin A$.

Together with $f_4 \in \mathrm{FP}$, we obtain $A_1 \leq^{\mathrm{p}}_{\mathrm{m}} A$.

Define $f_5 : \Sigma^* \to \Delta^*$ by $f_5(x) = ah'(x)$. If $x \in A$ then $h'(x) \in \Sigma^* - A$ hence $f_5(x) = ah'(x) \in a(\Sigma^* - A) \subseteq A_0$. If $x \notin A$ then $h'(x) \in A$ and hence $f_5(x) = ah'(x) \in A_0$. Obviously, $f_5 \in \mathrm{FP}$. This proves our claim.

As argued above, we have now shown that $E \in \mathcal{U}(A)$. This proves $\mathcal{R}^p_m \subseteq \mathcal{U}(A)$. Altogether, we obtain $\mathcal{U}(A) = \mathcal{R}^p_m A$. □

Corollary 4.14 *Let A be a set. If $\mathcal{R}^p_m(A)$ is closed under boolean operations, then A is not m-idempotent.*

Proof Follows immediately from Proposition 4.10 and Lemma 4.11. □

Consequently, no complete problem for a deterministic Turing-machine time or space complexity class can be m-idempotent. By Theorem 4.6, this also implies that no complete problem for a deterministic Turing-machine time or space complexity class except P can be p-selective.

The next theorem shows that unions of disjoints sets in NP can be much easier than the single components. In particular, there exists a degree $\deg^{\mathrm{p}}_{\mathrm{m}}(A)$ in $\mathrm{NP} - \mathrm{P}$ such that all intermediate degrees can be reached by unions from disjoint sets from $\deg^{\mathrm{p}}_{\mathrm{m}}(A)$.

Theorem 4.15 *If* $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$*, then there exists a set* $A \in (\mathrm{NP} \cap \mathrm{coNP}) - \mathrm{P}$ *such that* $\mathcal{U}(A) = \mathcal{R}^p_m(A) - \{\emptyset\} = \mathcal{R}^p_m(A) \dot{\vee} \mathcal{R}^p_m(A) - \{\emptyset\}$.

Proof By Lemma 4.11, it suffices to show under the assumption $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$, that there exists a set $A \in (\mathrm{NP} \cap \mathrm{coNP}) - \mathrm{P}$ such that $\mathcal{R}^p_m(A)$ is closed under boolean operations.

Let us assume that $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$. Then there exists a set $D \in (\mathrm{NP} \cap \mathrm{coNP}) - \mathrm{P}$. Let c_D be the characteristic function of D. We now define a set A which has the desired properties. We define

$$\begin{aligned} A \;=_{\mathrm{def}}\; \{H(x_1,\dots,x_n), w_1,\dots,w_n \mid\, & H \text{ is a boolean formula with variables} \\ & x_1,\dots,x_n \text{ and } H(c_D(w_1),\dots,c_D(w_n)) = 1\}. \end{aligned}$$

It remains to show that

(1) $A \in (\mathrm{NP} \cap \mathrm{coNP}) - \mathrm{P}$,

(2) $B \in \mathcal{R}^p_m(A)$ implies $\overline{B} \in \mathcal{R}^p_m(A)$,

(3) $B, C \in \mathcal{R}^p_m(A)$ implies $B \cup C \in \mathcal{R}^p_m(A)$.

We first argue for (1). A cannot be in P since it obviously holds that $D \leq^{\mathrm{p}}_{\mathrm{m}} A$. We have to show that $A \in \mathrm{NP} \cap \mathrm{coNP}$. Let $M_1 and M_2$ be nondeterministic machines such that the following holds for all x:

$$\begin{aligned} x \in D \;&\Leftrightarrow\; M_1 \text{ on input } x \text{ has (at least) one accepting path} \\ &\Leftrightarrow\; M_2 \text{ on input } x \text{ has no accepting paths.} \end{aligned}$$

Clearly, this implies that for all inputs x, precisely one of the machines M_1, M_2 produces an accepting path when running on input x. We informally describe a nondeterministic algorithm which decides A in polynomial time:

On input $\big(H(x_1,\dots,x_n), w_1,\dots,w_n\big)$ do the following:

```
1. $i := 1$
2. Nondeterministically simulate $M_1$ and $M_2$ on input $w_i$.
3. On all nondeterministic paths of $M_1$ and $M_2$:
    (a) If the current path is rejecting, terminate the computation on
        this path.
    (b) If the current path accepts, set $c_i := 1$ if the path belongs to
        $M_1$, set $c_i := 0$ if it belongs to $M_2$.
    (c) If $i < n$, set $i := i + 1$ and goto 2.
    (d) If $i = n$, evaluate $H(c_1, \dots, c_n)$
    (e) Accept if and only if $H(c_1, \dots, c_n) = 1$.
```

Observe that the algorithm runs in polynomial time and produces an accepting path if and only if the input $\big(H(x_1, \dots, x_n), w_1, \dots, w_n\big)$ is in A. So we obtain $A \in \mathrm{NP}$. To see that $A \in \mathrm{coNP}$, note that $\overline{A} \leq^{\mathrm{p}}_{\mathrm{m}} A$ via the function $f(H(x_1, \dots, x_n), w_1, \dots, w_n) =_{\mathrm{def}} (\neg H(x_1, \dots, x_n), w_1, \dots, w_n)$. Hence, $A \in (\mathrm{NP} \cap \mathrm{coNP}) - \mathrm{P}$.

We now prove (2) and (3). Let $B \leq^{\mathrm{p}}_{\mathrm{m}} A$ and $C \leq^{\mathrm{p}}_{\mathrm{m}} A$ via functions g_1, g_2, that means $x \in B \Leftrightarrow g_1(x) \in A$ and $x \in C \Leftrightarrow g_2(x) \in A$ holds for all x. Clearly, the function f defined above reduces $\overline{B}$ to B. It remains to show that $B \cup C \leq^{\mathrm{p}}_{\mathrm{m}} A$. This is accomplished by the function h, which is defined as follows.

$$h(x) =_{\mathrm{def}} \big(H_1 \vee H_2(x_1, \dots, x_m, x'_1, \dots, x'_n), w_1, \dots, w_m, w'_1, \dots, w'_n\big),$$

where

$$\big(H_1(x_1, \dots, x_n), w_1, \dots, w_n\big) =_{\mathrm{def}} g_1(x) \text{ and } \big(H_2(x'_1, \dots, x'_m), w'_1, \dots, w'_m\big) =_{\mathrm{def}} g_2(x).$$

It now holds that

$$\begin{aligned} x \in B \cup C & \Leftrightarrow (g_1(x) \in A) \vee (g_2(x) \in A) \\ & \Leftrightarrow h(x) \in A. \end{aligned}$$

Function h is computable in polynomial time. We obtain $B \cup C \leq^{\mathrm{p}}_{\mathrm{m}} A$ via function h and hence $B \cup C \in \mathcal{R}^p_m(A)$. This finishes our proof. □

By Proposition 4.10, the set A in Theorem 4.15 cannot be m-idempotent. Informally, the reason is that unions of sets in the degree of A can be too *easy* to be in the degree of A. As stated before, the question whether unions of NP-complete sets can be less than NP-complete is still open.

In the next section, we will show that the opposite can occur also, i.e. unions of equivalent sets can be harder than the original sets.

4.2 Disjoint Sets whose Union is Harder than the Single Components

Buhrman, Hoene, and Torenvliet [BHT98] showed unconditionally that there exists an $A \in \mathrm{EXP} - \mathrm{P}$ such that A is not EXP-complete and not m-idempotent. Recall that due to Corollary 4.14, no EXP-complete problem can be m-idempotent.

Theorem 4.16 *[BHT98] Let C be m-complete for* EXP*. Then C can be split into A and B such that*

- *$A, B \in \mathrm{EXP}$,*
- *$A \equiv^{\mathrm{p}}_{\mathrm{m}} B$,*
- *$A {\leq^{\mathrm{p}}_{\mathrm{m}}} A \cup B$,*
- *$A \cup B$ does not m-reduce to A, that means A, B are not m-complete for* EXP*.*

Corollary 4.17 *There exists $A \in \mathrm{EXP}$ such that*

$$\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(A) \subsetneq \mathcal{U}(A) \subsetneq \mathcal{R}^p_m(A) \,\dot\vee \mathcal{R}^p_m(A) = \mathrm{EXP},$$

hence A is not m-idempotent.

Proof Let C be m-complete for EXP. By Theorem 4.16, C can be split into sets $A, B \in \mathrm{EXP}$ such that $A \equiv^{\mathrm{p}}_{\mathrm{m}} B$, $A{\leq^{\mathrm{p}}_{\mathrm{m}}}A \cup B$, and $A \cup B$ does not m-reduce to A. Hence, $A \cup B \in \mathcal{R}^p_m(A) \,\dot\vee \mathcal{R}^p_m(A) - \mathcal{U}(A)$. As $C = A \cup B$ is NP-complete and $A \equiv^{\mathrm{p}}_{\mathrm{m}} B$, it follows that $\mathcal{R}^p_m(A) \,\dot\vee \mathcal{R}^p_m(A) = \mathrm{EXP}$. □

In this case, the union of sets in $\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(A)$ can be harder than A. We will identify degrees in Θ^{P}_2 for which the same holds. After this, we will construct such sets within NP.

The *chromatic number* of a graph G (in notation $\mathrm{cn}(G)$) is the smallest number k such G is k-colorable.

Definition 4.18 *Let $\mathrm{cn}(G)$ be the chromatic number of a graph G, and let $k \geq 1$. Then*

$$\mathrm{COLOR}_k =_{\mathrm{def}} \{(G, a_1, \ldots, a_k) \mid G \text{ is a graph, } a_1 < \cdots < a_k \text{ and } \mathrm{cn}(G) \in \{a_1, \ldots, a_k\}\}.$$

It is known that COLOR_k is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for $\mathrm{NP}(2k)$ [CGH+88].

Theorem 4.19 *If the boolean hierarchy over* NP *does not collapse to the second level, then there exist $A, B \in \mathrm{NP}(2)$ such that*

- *$A \equiv^{\mathrm{p}}_{\mathrm{m}} B$,*
- *$A {\le}^{\mathrm{p}}_{\mathrm{m}} A \cup B$,*
- *$A \cup B$ does not m-reduce to A.*

Proof

We prove a stronger statement: For every $k \geq 1$, there exist disjoint sets A and B such that A and B are $\mathrm{NP}(2k)$-complete and $A \cup B$ is $\mathrm{NP}(4k)$ complete. We consider variants of the well known graph coloring problem.

Let $k \geq 1$. Then COLOR_{2k} can be partitioned into $\mathrm{L{-}COLOR}_{2k} \subseteq \mathrm{COLOR}_{2k}$ and $\mathrm{R{-}COLOR}_{2k} \subseteq \mathrm{COLOR}_{2k}$, where

$$\begin{aligned} \mathrm{L{-}COLOR}_{2k} &=_{\mathrm{def}} \{(G, a_1, \ldots, a_{2k}) \,\big|\, a_1 < \cdots < a_{2k} \text{ and } \mathrm{cn}(G) \in \{a_1, \ldots, a_k\}\}, \\ \mathrm{R{-}COLOR}_{2k} &=_{\mathrm{def}} \{(G, a_1, \ldots, a_{2k}) \,\big|\, a_1 < \cdots < a_{2k} \text{ and } \mathrm{cn}(G) \in \{a_k, \ldots, a_{2k}\}\}. \end{aligned}$$

It is easy to see that the following holds for all $k \geq 1$:

- $\mathrm{COLOR}_k \equiv^{\mathrm{p}}_{\mathrm{m}} \mathrm{L{-}COLOR}_{2k} \equiv^{\mathrm{p}}_{\mathrm{m}} \mathrm{R{-}COLOR}_{2k}$.
- $\mathrm{L{-}COLOR}_{2k} \cap \mathrm{R{-}COLOR}_{2k} = \emptyset$.
- $\mathrm{L{-}COLOR}_{2k} \cup \mathrm{R{-}COLOR}_{2k} = \mathrm{COLOR}_{2k}$.

In particular, COLOR_2 (which is m-complete for $\mathrm{NP}(4)$) does neither m-reduce to $\mathrm{L{-}COLOR}_2$ nor to COLOR_1 (which are m-complete for $\mathrm{NP}(2)$) unless the boolean hierarchy collapses to $\mathrm{NP}(2)$. □

Corollary 4.20 *There exist $A, B \in \mathrm{NP}(2)$ such that*

- *$A \equiv^{\mathrm{p}}_{\mathrm{m}} B$,*
- *$A {\le}^{\mathrm{p}}_{\mathrm{m}} A \cup B$,*
- *$A \cup B$ does not m-reduce to A.*

unless the polynomial-time hierarchy collapses.

Under the assumption that the boolean hierarchy over NP does not collapse, it follows that $\deg^{\mathrm{p}}_{\mathrm{m}}(\mathrm{COLOR}_1) \subsetneq \mathcal{U}(\mathrm{COLOR}_1)$. Hence, the $\mathrm{NP}(2)$-complete sets are not m-idempotent. This indicates that the converse of Corollary 4.14 does not hold.

The next theorem states that COLOR_1 is an example for which $\mathcal{U}(\mathrm{COLOR}_1)$ lies strictly between $\deg^{\mathrm{p}}_{\mathrm{m}}(\mathrm{COLOR}_1)$ and $\mathcal{R}^p_m(\mathrm{COLOR}_1) \dot{\vee} \mathcal{R}^p_m(\mathrm{COLOR}_1) = \mathrm{NP}(2) \dot{\vee} \mathrm{NP}(2)$.

We first prove a lemma.

Lemma 4.21 *For all sets A, the following are equivalent:*

1. $\mathcal{U}(A) \cap \mathrm{P} \neq \emptyset$
2. $\mathcal{U}(A) \supseteq \mathrm{P} - \{\emptyset\}$
3. $A \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$.

Proof Let A be a set.

For the implication from item 1 to item 2, assume that there exists a set $B \in \mathcal{U}(A) \cap \mathrm{P}$. By definition, $\mathcal{U}(A)$ contains all sets in $\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(B) = \mathrm{P} - \{\emptyset\}$, i.e. $\mathcal{U}(A) \supseteq \mathrm{P} - \{\emptyset\}$. For the implication from 2 to 3, assume that $\mathcal{U}(A) \supseteq \mathrm{P} - \{\emptyset\}$. Hence, there exists $E \in \mathrm{P} - \{\emptyset\}$ such that $E \in \mathcal{U}(A)$. So there exist sets C and D such that $C \equiv^{\mathrm{p}}_{\mathrm{m}} D \equiv^{\mathrm{p}}_{\mathrm{m}} A$, $C \cap D = \emptyset$, and $E \equiv^{\mathrm{p}}_{\mathrm{m}} C \cup D$. Observe that $C \cup D \in \mathrm{P}$ and $\overline{C \cup D} \cap D = \emptyset$. Therefore, it is easy to see that $\overline{C} = \overline{C \cup D} \cup D \equiv^{\mathrm{p}}_{\mathrm{m}} D$. We now have $A \equiv^{\mathrm{p}}_{\mathrm{m}} C \equiv^{\mathrm{p}}_{\mathrm{m}} D \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{C}$. We conclude $A \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$. For the implication from 3 to 1, we assume $A \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$. Hence, $A \neq \emptyset$. Let $a \in A$. Trivially, $A \equiv^{\mathrm{p}}_{\mathrm{m}} A - \{a\} \equiv^{\mathrm{p}}_{\mathrm{m}} \overline{A}$. Therefore, $\{a\} = A - \{a\} \cup \overline{A} \in \mathcal{U}(A)$. □

Since COLOR_1 is m-complete for $\mathrm{NP}(2)$, it follows that $\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(\mathrm{COLOR}_1) = \{A \,|\, A \text{ is m-complete for } \mathrm{NP}(2)\}$ and $\mathcal{R}^p_m(\mathrm{COLOR}_1) \dot{\vee} \mathcal{R}^p_m(\mathrm{COLOR}_1) = \mathrm{NP}(2) \dot{\vee} \mathrm{NP}(2)$.

Theorem 4.22 *If the boolean hierarchy over* NP *does not collapse to* NP(2)*, it holds that*

$$\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(\mathrm{COLOR}_1) \subsetneq \mathcal{U}(\mathrm{COLOR}_1) \subsetneq \mathcal{R}^p_m(\mathrm{COLOR}_1) \dot{\vee} \mathcal{R}^p_m(\mathrm{COLOR}_1).$$

Proof Due to Theorem 4.3 and Theorem 4.19 it suffices to show that there exists $D \in \mathcal{R}^p_m(\mathrm{COLOR}_1) \dot{\vee} \mathcal{R}^p_m(\mathrm{COLOR}_1) = \mathrm{NP}(2) \dot{\vee} \mathrm{NP}(2)$ such that $D \notin \mathcal{U}(\mathrm{COLOR}_1)$. Clearly, $\mathrm{NP}(2) \dot{\vee} \mathrm{NP}(2)$ contains P, so let $D \in \mathrm{P}$. As we assumed that the boolean hierarchy does not collapse to NP(2), it follows that $\mathrm{NP}(2) \neq \mathrm{coNP}(2)$ and hence $\mathrm{COLOR}_1 \not\equiv^{\mathrm{p}}_{\mathrm{m}} \overline{\mathrm{COLOR}_1}$. From Lemma 4.21 we then obtain $\mathcal{U}(\mathrm{COLOR}_1) \cap \mathrm{P} = \emptyset$. Consequently, $D \notin \mathcal{U}(\mathrm{COLOR}_1)$. □

Corollary 4.23 *It holds that*

$$\mathrm{deg}^{\mathrm{p}}_{\mathrm{m}}(\mathrm{COLOR}_1) \subsetneq \mathcal{U}(\mathrm{COLOR}_1) \subsetneq \mathcal{R}^p_m(\mathrm{COLOR}_1) \dot{\vee} \mathcal{R}^p_m(\mathrm{COLOR}_1)$$

unless the polynomial-time hierarchy collapses.

We now start our search inside NP. We prove under a stronger assumption that there exist m-equivalent disjoint sets E and F in NP such that $E \cup F$ is harder than E.

In other words, we show under this assumption that there exists $E \in \mathrm{NP} - \mathrm{coNP}$ such that $\mathcal{U}(E) \not\subseteq \mathcal{R}^p_m(E)$. We then explain that the existence of such a set E separates 2-dtt-reducibility from m-reducibility within NP. Consequently, it is not surprising that we need a stronger assumption to prove our result.

In order to formulate our assumption, we need the notion of *immunity*.

Definition 4.24 *A set L is* immune *to a complexity class $\mathcal{C}$, or $\mathcal{C}$-*immune*, if L is infinite and no infinite subset of L belongs to $\mathcal{C}$. A set L is* bi-immune *to a complexity class $\mathcal{C}$, or $\mathcal{C}$-*bi-immune*, if both L and $\overline{L}$ are $\mathcal{C}$-immune.*

Theorem 4.25 *If* NP *has* NP ∩ coNP*-bi-immune sets and* NP ∩ coNP *has* P*-bi-immune sets, then there exist disjoint sets $E, F \in \mathrm{NP} - \mathrm{coNP}$ such that $E \equiv^{\mathrm{p}}_{\mathrm{m}} F$, but $E \cup F \not\leq^{\mathrm{p}}_{\mathrm{m}} E$.*

Proof Let A be a P-immune set in NP ∩ coNP and let B be an NP ∩ coNP-bi-immune set in NP. We use the tower function

$$t(n) =_{\mathrm{def}} \begin{cases} 2 & : \text{ if } n = 0 \\ 2^{2^{t(n-1)}} & : \text{ otherwise.} \end{cases}$$

Let $C =_{\mathrm{def}} \{0^{t(n)} \mid n \in \mathbb{N}\}$ and $B' =_{\mathrm{def}} B \cap C$. So B' is in NP. We argue that both sets, B' and $C - B'$ are NP ∩ coNP-immune: B' is infinite, since otherwise a finite modification of C yields an infinite, polynomial-time-decidable subset of $\overline{B}$. Also, B' cannot contain an infinite subset from NP ∩ coNP, since this would be an infinite subset of B. $C - B'$ is infinite, since otherwise a finite modification of C yields an infinite, polynomial-time-decidable subset of B. Finally, $C - B'$ cannot contain an infinite subset from NP ∩ coNP, since this would be an infinite subset of $\overline{B}$.

$$\begin{aligned} B'_1 &=_{\mathrm{def}} B' \cap A \\ B'_2 &=_{\mathrm{def}} B' \cap \overline{A} \end{aligned}$$

B'_1 and B'_2 are disjoint sets in NP. We argue that both sets are infinite: If B'_1 is finite, then $X =_{\mathrm{def}} (A \cap C) - B'_1$ is in NP ∩ coNP and is a subset of $C - B'$. From the NP ∩ coNP-immunity of $C - B'$ it follows that X is finite and hence $A \cap C$ is finite. So a finite modification of C yields an infinite, polynomial-time-decidable subset of $\overline{A}$ which contradicts the P-immunity of $\overline{A}$. Therefore, B'_1 is infinite. If we replace A by $\overline{A}$ in the argumentation above, then this shows the infinity of B'_2.

We define the sets asserted in the theorem:

$$\begin{aligned} E &=_{\mathrm{def}} B'_1 \cup 0B'_2 \\ F &=_{\mathrm{def}} 0B'_1 \cup B'_2 \end{aligned}$$

Note that both sets are subsets of $C \cup 0C$, and observe that E and F are disjoint sets in NP. Moreover, the following equivalences hold.

$$\begin{aligned} 0^{t(n)} \in E &\Leftrightarrow 0^{t(n)+1} \in F \\ 0^{t(n)} \in F &\Leftrightarrow 0^{t(n)+1} \in E \end{aligned}$$

Therefore, the following reduction function witnesses both reductions, $E \leq^{\mathrm{p}}_{\mathrm{m}} F$ and $F \leq^{\mathrm{p}}_{\mathrm{m}} E$.

$$f(x) =_{\mathrm{def}} \begin{cases} x & : \text{ if } x \notin C \cup 0C \\ 0^{t(n)+1} & : \text{ if } x = 0^{t(n)} \text{ for some } n \\ 0^{t(n)} & : \text{ if } x = 0^{t(n)+1} \text{ for some } n \end{cases}$$

This shows $E \equiv^{\mathrm{p}}_{\mathrm{m}} F$. Hence, if one of the sets E and F belongs to coNP, then both do so. So assume $E \in \mathrm{coNP}$. Then $B'_1 = E \cap C \in \mathrm{NP} \cap \mathrm{coNP}$ and hence we found an infinite set in NP ∩ coNP that is a subset of B'. This contradicts the NP ∩ coNP-immunity of B'. Therefore, $E, F \in \mathrm{NP} - \mathrm{coNP}$. It remains to show $E \cup F \not\leq^{\mathrm{p}}_{\mathrm{m}} E$.

Assume $E \cup F \leq^{\mathrm{p}}_{\mathrm{m}} E$ via reduction function $f \in \mathrm{FP}$.

Case 1: For infinitely many n, $\{f(0^{t(n)}), f(0^{t(n)+1})\} \not\subseteq \{0^{t(n)}, 0^{t(n)+1}\}$.

Consider the following algorithm which works on input x. The algorithm can end in three different states: Either the input is accepted, or it is rejected, or the algorithm tells that the decision procedure failed.

```
1. if $x \notin \{0^{t(n)} \mid n \in \mathbb{N}\}$ then reject
2. determine n such that $x = 0^{t(n)}$
3. if $\{f(0^{t(n)}), f(0^{t(n)+1})\} \subseteq \{0^{t(n)}, 0^{t(n)+1}\}$ then output "failed"
4. if $f(0^{t(n)}) \notin \{0^{t(n)}, 0^{t(n)+1}\}$ then $y := 0^{t(n)}$ else $y := 0^{t(n)+1}$
5. if $|f(y)| \geq t(n-1) + 2$ then reject
6. if $f(y) \in E$ then accept else reject
```

Observe that this is a polynomial-time algorithm: For this end it is enough to argue for line 6. Here $|y| \leq t(n-1) + 2 = (\log\log|x|) + 2$ and therefore, the nondeterministic computation for "$y \in E$" can be simulated in deterministic, polynomial time in $|x|$.

Claim 4.26 *For almost all x,*

- *if the algorithm accepts x, then $x \in B'$, and*
- *if the algorithm rejects x, then $x \notin B'$.*

Clearly, if the algorithm rejects in line 1, then $x \notin B'$. If the algorithm rejects in line 5, then $f(y) \notin \{0^{t(n)}, 0^{t(n)+1}\}$. Since f is computable in polynomial time, $|f(y)| < t(n+1)$. Moreover, note that $0^{t(n)}$ and $0^{t(n)+1}$ are the only possible strings that have a length in $[t(n-1)+2, t(n+1)-1]$ and that belong to E. Hence $f(y) \notin E$ and therefore, $y \notin E \cup F = B' \cup 0B'$. It follows that $x \notin B'$. Finally, assume the algorithm stops in step 6. Here the algorithm accepts if and only if $y \in E \cup F = B' \cup 0B'$ which in turn is equivalent to $x \in B'$. This proves Claim 4.26.

By our assumption in Case 1, for infinitely many n, $\{f(0^{t(n)}), f(0^{t(n)+1})\} \not\subseteq \{0^{t(n)}, 0^{t(n)+1}\}$. Therefore, for infinitely many n, the algorithm does not return "failed" on input $0^{t(n)}$. So at least one of the following is true:

(i) For infinitely many n, the algorithm accepts $0^{t(n)}$.

(ii) For infinitely many n, the algorithm rejects $0^{t(n)}$.

In case of (i), let

$$X =_{\text{def}} \{0^{t(n)} \mid \text{the algorithm accepts } 0^{t(n)}\},$$

otherwise let

$$X =_{\text{def}} \{0^{t(n)} \mid \text{the algorithm rejects } 0^{t(n)}\}.$$

Note that $X \in \mathrm{P}$ and $X \subseteq C$. By Claim 4.26, either $C \subseteq B'$ or $C \subseteq C - B'$. This contradicts the P-immunity of B' and $C - B'$. Therefore, Case 1 cannot happen.

Case 2: For almost all n, $\{f(0^{t(n)}), f(0^{t(n)+1})\} \subseteq \{0^{t(n)}, 0^{t(n)+1}\}$.

Claim 4.27 *For almost all n, $f(0^{t(n)}) = f(0^{t(n)+1}) = 0^{t(n)}$ or $f(0^{t(n)}) = f(0^{t(n)+1}) = 0^{t(n)+1}$.*

If not, then for infinitely many n, either $f(0^{t(n)}) = 0^{t(n)}$ and $f(0^{t(n)+1}) = 0^{t(n)+1}$, or $f(0^{t(n)}) = 0^{t(n)+1}$ and $f(0^{t(n)+1}) = 0^{t(n)}$. Hence at least one of the following sets is infinite.

$$\begin{aligned} X &=_{\text{def}} \{0^{t(n)} \mid f(0^{t(n)}) = 0^{t(n)} \text{ and } f(0^{t(n)+1}) = 0^{t(n)+1}\} \\ Y &=_{\text{def}} \{0^{t(n)} \mid f(0^{t(n)}) = 0^{t(n)+1} \text{ and } f(0^{t(n)+1}) = 0^{t(n)}\} \end{aligned}$$

Note that $X, Y \in \mathrm{P}$. We argue that both sets, X and Y, are subsets of $C - B'$: Let $0^{t(n)} \in X \cup Y$. At least one of the strings $0^{t(n)}$ and $0^{t(n)+1}$ is not contained in E. Therefore, since f reduces $E \cup F$ to E, at least one of the strings $0^{t(n)}$ and $0^{t(n)+1}$ is not contained in $E \cup F = B' \cup 0B'$. Hence both strings, $0^{t(n)}$ and $0^{t(n)+1}$, are not contained in B'. Therefore, either X or Y is an infinite subset of $C - B'$. This contradicts the P-immunity of $C - B'$ and proves Claim 4.27.

Claim 4.28 *(E, F) is p-separable.*

Choose the greatest n that does not satisfy Claim 4.27. Define the separator as

$$S =_{\text{def}} \{0^{t(m)} \mid m > n, f(0^{t(m)}) = 0^{t(m)}\} \cup \{0^{t(m)+1} \mid m > n, f(0^{t(m)}) = 0^{t(m)+1}\} \cup (E \cap \Sigma^{\leq t(n)+1}).$$

Note that $S \in \mathrm{P}$. We show that S separates (E, F).

Assume $x \in E$. Then $x = 0^{t(m)}$ or $x = 0^{t(m)+1}$ for some m. If $m \leq n$, then $x \in S$ and we are done. Otherwise, $m > n$ and hence by the choice of n, $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)}$ or $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)+1}$. If $x = 0^{t(m)}$, then we must have $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)}$ and hence $x \in S$. If $x = 0^{t(m)+1}$, then we must have $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)+1}$ and hence $x \in S$.

Assume $x \in F$. So $x \notin E$ and $x = 0^{t(m)}$ or $x = 0^{t(m)+1}$ for some m. If $m \leq n$, then $x \notin S$ and we are done. Otherwise, $m > n$ and hence by the choice of n, $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)}$ or $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)+1}$. If $x = 0^{t(m)}$, then we must have $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)+1}$ and hence $x \notin S$. If $x = 0^{t(m)+1}$, then we must have $f(0^{t(m)}) = f(0^{t(m)+1}) = 0^{t(m)}$ and hence $x \notin S$. This proves Claim 4.28.

Since $B_1' \subseteq E$ and $B_2' \subseteq F$, any separator for (E, F) is also a separator for (B_1', B_2'). So by Claim 4.28, (B_1', B_2') is p-separable via some separator $S \in \mathrm{P}$.

Note that $B_1' \subseteq S \cap C$ and $B_2' \subseteq C - S$. So both sets $S \cap C$ and $C - S$ are infinite sets in P. By A's P-immunity, no finite modification of $S \cap C$ can be a subset of A. Therefore, $S \cap C \cap \overline{A}$ is an infinite set in $\mathrm{NP} \cap \mathrm{coNP}$. We argue that $S \cap C \cap \overline{A} \subseteq C - B'$: If not, then there exists an $x \in S \cap C \cap \overline{A}$ such that $x \in B'$. So $x \in S$ while S separates (B_1', B_2'). Therefore, $x \in B_1'$ and hence $x \in A$ which is a contradition. This shows that $S \cap C \cap \overline{A}$ is an infinite subset of $C - B'$. This contradicts the $\mathrm{NP} \cap \mathrm{coNP}$-immunity of $C - B'$. So also Case 2 leads to a contradiction. This shows $E \cup F \not\leq_{\mathrm{m}}^{\mathrm{p}} E$. □

We now show that Theorem 4.25 separates 2-dtt-reducibility from m-reducibility within NP:

Corollary 4.29 *If* NP *has* $\mathrm{NP} \cap \mathrm{coNP}$*-bi-immune sets and* $\mathrm{NP} \cap \mathrm{coNP}$ *has* P*-bi-immune sets, then there exists* $A, B \in \mathrm{NP} - \mathrm{coNP}$ *such that such that* $A \leq_{2-\mathrm{dtt}}^{\mathrm{p}} B$*, but* $A \not\leq_{\mathrm{m}}^{\mathrm{p}} B$*.*

Proof Let E and F be the sets asserted in Theorem 4.25. Define $A =_{\mathrm{def}} E \cup F$ and $B =_{\mathrm{def}} E$. So $A \in \mathrm{NP}$ and $B \in \mathrm{NP} - \mathrm{coNP}$. If $A \in \mathrm{coNP}$, then $A \in \mathrm{NP} \cap \mathrm{coNP}$ and hence $E \in \mathrm{coNP}$ which contradicts Theorem 4.25. Therefore, $A, B \in \mathrm{NP} - \mathrm{coNP}$. $A \not\leq_{\mathrm{m}}^{\mathrm{p}} B$ follows immediately from Theorem 4.25. Let $F \leq_{\mathrm{m}}^{\mathrm{p}} E$ via reduction $f \in \mathrm{FP}$. Then $g(x) =_{\mathrm{def}} x \vee f(x)$ witnesses $A \leq_{2-\mathrm{dtt}}^{\mathrm{p}} B$. □

References

[Agr02] M. Agrawal. Pseudo-random generators and structure of complete degrees. In *IEEE Conference on Computational Complexity*, pages 139–147, 2002.

[AS84] K. Ambos-Spies. P-mitotic sets. In E. Börger, G. Hasenjäger, and D. Roding, editors, *Logic and Machines*, volume 171 of *Lecture Notes in Computer Science*, pages 1–23. Springer Verlag, 1984.

[BG82] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 82:80–88, 1982.

[BH77] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 6:305–322, 1977.

[BHT98] H. Buhrman, A. Hoene, and L. Torenvliet. Splittings, robustness, and structure of complete sets. *SIAM Journal on Computing*, 27:637–653, 1998.

[BV97] D. Boneh and R. Venkatesan. Rounding in lattices and its cryptographic applications. In *SODA*, pages 675–681, 1997.

[BWSD77] R. V. Book, C. Wrathall, A. L. Selman, and D. P. Dobkin. Inclusion complete tally languages and the hartmanis-berman conjecture. *Mathematical Systems Theory*, 11:1–8, 1977.

[CGH$^+$88] J.-Y. Cai, T. Gundermann, J. Hartmanis, L. A. Hemachandra, V. Sewelson, K. W. Wagner, and G. Wechsung. The boolean hierarchy I: Structural properties. *SIAM Journal on Computing*, 17:1232–1252, 1988.

[FR02] L. Fortnow and J. Rogers. Separability and one-way functions. *Computational Complexity*, 11(3-4):137–157, 2002.

[GPSZ05] C. Glaßer, A. Pavan, A. L. Selman, and L. Zhang. Redundancy in complete sets. Technical Report 05-068, Electronic Colloquium on Computational Complexity (ECCC), 2005.

[GS88] J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.

[GT05] C. Glaßer and S. Travers. Machines that can output empty words. Technical Report 147, Electronic Colloquium on Computational Complexity (ECCC), 2005.

[GW86] T. Gundermann and G. Wechsung. Nondeterministic Turing machines with modified acceptance. In *Proceedings 12th Symposium on Mathematical Foundations of Computer Science*, volume 233 of *Lecture Notes in Computer Science*, pages 396–404. Springer Verlag, 1986.

[HP06] J. Hitchcock and A. Pavan. Comparing reductions to NP-complete sets. Technical Report TR06-039, Electronic Colloquium on Computational Complexity, 2006.

[KS97] J. Köbler and U. Schöning. High sets for NP. In *Advances in Algorithms, Languages, and Complexity*, pages 139–156, 1997.

[KSW87] J. Köbler, U. Schöning, and K. W. Wagner. The difference and the truth-table hierarchies for NP. *RAIRO Inform. Théor.*, 21:419–435, 1987.

[LLS75] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial time reducibilities. *Theoretical Computer Science*, 1:103–123, 1975.

[Lon78] T. J. Long. *On some Polynomial Time Reducibilities.* PhD thesis, Purdue University, Lafayette, Ind., 1978.

[Sch83] U. Schöning. A low and a high hierarchy within NP. *Journal of Computer and System Sciences*, 27(1):14–28, 1983.

[Sel79] A. L. Selman. P-selective sets, tally languages, and the behavior of polynomial-time reducibilities on NP. *Mathematical Systems Theory*, 13:55–65, 1979.

[Sel88] A. L. Selman. Natural self-reducible sets. *SIAM Journal on Computing*, 17(5):989–996, 1988.

[Val76] L. G. Valiant. Relative complexity of checking and evaluation. *Information Processing Letters*, 5:20–23, 1976.

[WW85] K. W. Wagner and G. Wechsung. On the boolean closure of NP. In *Proceedings International Conference on Fundamentals of Computation Theory*, volume 199 of *Lecture Notes in Computer Science*, pages 485–493. Springer-Verlag, 1985.