Electronic Colloquium on Computational Complexity, Report No. 50 (2019)

NP-Completeness, Proof Systems, and Disjoint NP-Pairs

Titus Dose and Christian Glaßer
Julius-Maximilians-Universität Würzburg

20th March 2019

Abstract

The article investigates the relation between three well-known hypotheses.

H_{union}: the union of disjoint $\leq^p_m$-complete sets for NP is $\leq^p_m$-complete

H_{opps}: there exist optimal propositional proof systems

H_{cpair}: there exist $\leq^{pp}_m$-complete disjoint NP-pairs

The following results are obtained:

- The hypotheses are pairwise independent under relativizable proofs, except for the known implication $H_{opps} \Rightarrow H_{cpair}$.
- Answers to questions by Pudlák in terms of an oracle relative to which $\neg H_{cpair}$, $\neg H_{opps}$, UP has $\leq^p_m$-complete sets, but NP $\cap$ coNP has no $\leq^p_m$-complete sets (i.e., in Pudlák's notation: $\mathsf{DisjNP} \not\Rightarrow \mathsf{UP}$, $\mathsf{CON} \not\Rightarrow \mathsf{UP}$, and $\mathsf{NP} \cap \mathsf{coNP} \not\Rightarrow \mathsf{UP}$).
- The converse of Köbler, Messner, and Torán's implication NEE $\cap$ TALLY $\subseteq$ coNEE $\Rightarrow$ H_{opps} fails relative to an oracle, where NEE $\stackrel{df}{=}$ NTIME$(2^{O(2^n)})$.
- New characterizations of H_{union} and two variants in terms of coNP-completeness and P-producibility of the set of hard formulas of propositional proof systems.

1 Introduction

The three hypotheses studied in this paper came up in the context of fascinating questions. The first one states a simple closure property for the class of NP-complete sets. The second one addresses the existence of optimal propositional proof systems. It is equivalent to state that one can prove the finite consistency of axiomatized theories by proofs of polynomial length [KP89]. The third hypothesis is motivated and also implied by the second one.

Below we explain the context in which these hypotheses came up and discuss further connections to complete sets for promise classes like UP, to the security of public-key cryptosystems, and to complete functions for NPSV, the class of single-valued functions computable by NP-machines. At the end of this section we summarize our results.

Hypothesis H_{union}: unions of disjoint $\leq^p_m$-complete sets for NP are $\leq^p_m$-complete
The beauty of hypothesis H_{union} lies in its simplicity. It states that the class of NP-complete sets is closed under unions of disjoint sets. The question of whether H_{union} holds was raised by Selman [Sel88] in connection with the study of self-reducible sets in NP.[1]

[1] The analog of H_{union} in computability theory holds [Tra07], since the many-one complete c.e. sets are creative [Myh55].

ISSN 1433-8092

An interesting example for a union of disjoint NP-complete sets is the Clique-Coloring pair, which is due to Pudlák [Pud03]:

$$\begin{aligned} C_0 &= \{(G,k) \mid G \text{ is a graph that has a clique of size } k\} \\ C_1 &= \{(G,k) \mid G \text{ is a graph that can be colored with } k-1 \text{ colors}\} \end{aligned}$$

The sets are NP-complete and disjoint, since a clique of size k cannot be colored with $k-1$ colors. C_1 and C_2 are P-separable [Pud03], which means that there exists an $S \in \mathrm{P}$, the separator, such that $C_1 \subseteq S$ and $C_2 \subseteq \overline{S}$. The P-separability of C_1 and C_2 is a result based on deep combinatorial arguments by Lovász [Lov79] and Tardos [Tar88]. It implies that $C_1 \cup C_2$ is NP-complete.

Glaßer et al. [GPSS06, GSTW08] give several equivalent formulations of $\mathrm{H}_{\mathrm{union}}$ (cf. Corollary 3.7) and show that the union of disjoint sets that are $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP is complete with respect to strongly nondeterministic, polynomial-time Turing reducibility. Moreover, the union is also nonuniformly polynomial-time many-one complete for NP under the assumption that NP is not infinitely-often in coNP. Moreover, Glaßer et al. [GHPT14] provide sufficient and necessary conditions for $\mathrm{H}_{\mathrm{union}}$ in terms of certain refuters that distinguish languages $L \in \mathrm{NP}$ with $\mathrm{SAT} \cap L = \emptyset$ from $\overline{\mathrm{SAT}}$.

Hypothesis $\mathrm{H}_{\mathrm{opps}}$: there exist optimal propositional proof systems
Cook and Reckhow [CR79] defined a propositional proof system (pps) as a polynomial-time computable function f whose range is TAUT, the set of tautologies. A pps f is simulated by a pps g, if proofs in g are at most polynomially longer than proofs in f. We say that f is P-simulated by g, if additionally for a given proof in f we can compute in polynomial time a corresponding proof in g. A pps g is optimal (resp., P-optimal) if it simulates (resp., P-simulates) each pps.

The question of whether $\mathrm{H}_{\mathrm{opps}}$ holds was raised by Krajícek and Pudlák [KP89] in an exciting context:[2] Let $\mathrm{Con}_T(n)$ denote the finite consistency of a theory T, which is the statement that T has no proofs of contradiction of length $\leq n$. Krajícek and Pudlák [KP89] showed that $\mathrm{H}_{\mathrm{opps}}$ is equivalent to the statement that there is a finitely axiomatized theory S which proves the finite consistency $\mathrm{Con}_T(n)$ for every finitely axiomatized theory T by a proof of polynomial length in n. In other words, $\mathrm{H}_{\mathrm{opps}}$ expresses that a weak version of Hilbert's program (to prove the consistency of all mathematical theories) is possible [Pud96].

Krajícek and Pudlák [KP89] also show that NE = coNE implies $\mathrm{H}_{\mathrm{opps}}$ and that E = NE implies the existence of P-optimal pps. The converses of these implications do not hold relative to an oracle constructed by Verbitskii [Ver91]. Köbler, Messner, and Torán [KMT03] prove similar implications with weaker assumptions and reveal a connection to promise classes. For $\mathrm{EE} \stackrel{df}{=} \mathrm{DTIME}(2^{O(2^n)})$ and $\mathrm{NEE} \stackrel{df}{=} \mathrm{NTIME}(2^{O(2^n)})$ they show that $\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE}$ implies $\mathrm{H}_{\mathrm{opps}}$, which in turn implies that $\mathrm{NP} \cap \mathrm{SPARSE}$ has $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets. Moreover, $\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE}$ implies the existence of P-optimal pps, which in turn implies that UP has $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets.

Sadowski [Sad02] proves that $\mathrm{H}_{\mathrm{opps}}$ is equivalent to the statement that the class of all easy subsets of TAUT is uniformly enumerable. Beyersdorff [Bey04, Bey06, Bey07, Bey10] investigates connections between disjoint NP-pairs and pps, and in particular studies the hypotheses $\mathrm{H}_{\mathrm{cpair}}$ and $\mathrm{H}_{\mathrm{opps}}$. Pudlák [Pud96, Pud17] provides comprehensive surveys on the finite consistency problem, its connection to propositional proof systems, and related open questions. In a recent paper, Khaniki [Kha18] shows new relations between the conjectures discussed in [Pud17] and constructs two oracles that separate several of these conjectures. Relative to the

[2] The analog of $\mathrm{H}_{\mathrm{opps}}$ in computability theory holds trivially, since there the notion of simulation has no bounds for the length of proofs and hence each proof system is optimal.

first oracle, E = NE and there are no $\leq_m^{pp}$-complete disjoint coNP-pairs. Relative to the second oracle, TFNP = FP and there is no (nonuniform) P-optimal pps.

Hypothesis H_{cpair}: there exist $\leq_m^{pp}$-complete disjoint NP-pairs

Even, Selman, and Yacobi [EY80, ESY84] showed that the security of public-key cryptosystems depends on the computational complexity of promise problems. The latter can be written as disjoint NP-pairs, i.e., pairs (A, B) of disjoint sets $A, B \in$ NP. The Clique-Coloring pair mentioned above is an interesting example for a P-separable disjoint NP-pair. Even, Selman, and Yacobi [EY80, ESY84] conjectured that every disjoint NP-pair has a separator that is not $\leq_T^p$-hard for NP. If the conjecture holds, then there are no public-key cryptosystems that are NP-hard to crack. Grollmann and Selman [GS88] observed that secure public-key cryptosystems exist only if P-inseparable disjoint NP-pairs exist.

The question of whether H_{cpair} holds was raised by Razborov [Raz94] in the context of pps.[3] To explain this connection we need the notions of reducibility and completeness for disjoint NP-pairs. (A, B) polynomial-time many-one reduces to (C, D), written as $(A, B) \leq_m^{pp} (C, D)$, if there is a polynomial-time computable h such that $h(A) \subseteq C$ and $h(B) \subseteq D$. A disjoint NP-pair (A, B) is $\leq_m^{pp}$-complete, if each disjoint NP-pair $\leq_m^{pp}$-reduces to (A, B). Razborov [Raz94] defined for each pps f a corresponding disjoint NP-pair, the canonical pair of f. It is shown that the canonical pair of an optimal pps is a $\leq_m^{pp}$-complete disjoint NP-pair, which proves

$$H_{opps} \Rightarrow H_{cpair}. \tag{1}$$

This means that the open question of whether optimal pps exist can be settled by proving that $\leq_m^p$-complete disjoint NP-pairs do not exist. As we will see, (1) is the only nontrivial implication that relativizably holds between the three hypotheses H_{union}, H_{opps}, H_{cpair} and their negations. For the relationship between H_{cpair} and H_{opps} this is shown by Glaßer et al. [GSSZ04] who construct two oracles such that H_{cpair} holds relative to both oracles, but H_{opps} holds relative to the first one and $\neg H_{opps}$ relative to the second one.

Pudlák [Pud03] further investigates the connection between pps and disjoint NP-pairs and shows that the canonical pair of the resolution proof system is symmetric. Glaßer, Selman, and Sengupta [GSS05] characterize H_{cpair} in several ways, e.g., by the uniform enumerability of disjoint NP-pairs and by the existence of $\leq_m^p$-complete functions in NPSV. Glaßer, Selman, and Zhang [GSZ07] prove that disjoint NP-pairs and pps have identical degree structures. Moreover, they show the following statement, which connects disjoint NP-pairs, pps, and H_{union} [GSZ09]: If NP $\neq$ coNP and each disjoint NP-pair (SAT, B) is strongly polynomial-time many-one equivalent to the canonical pair of a pps, then H_{union} holds.

Our Contribution

The results of this paper improve our understanding on the three hypotheses and their relationships in the following way.

1. Relativized independence of the hypotheses. We show that H_{union}, H_{opps}, and H_{cpair} are pairwise independent under relativizable proofs, except for the known implication $H_{opps} \Rightarrow H_{cpair}$. For any two of these hypotheses and any combination of their truth values there exists an appropriate oracle, except for $H_{opps} \wedge \neg H_{cpair}$ which is impossible. The relativized relationships between H_{opps} and H_{cpair} were settled by Glaßer et al. [GSSZ04]. The remaining ones are obtained from an oracle by Ogiwara and Hemachandra [OH93], an oracle by Homer and Selman [HS92], and three oracles constructed in the present paper. The oracle built in Theorem 7.1 is our most sophisticated result.

2. Answers to questions by Pudlák. The oracle O in Theorem 4.1 answers questions by Pudlák [Pud17], who lists several hypotheses and asks for oracles showing the corresponding

[3] The analog of H_{cpair} in computability theory holds [Rog67, Ch. 7., Thm XII(c)].

relativized hypotheses to be different. We separate several pairs of these hypotheses. Relative to the aforementioned oracle O it holds $\neg \mathrm{H}_{\mathrm{cpair}}$ and UP has $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets, i.e., $\mathsf{DisjNP} \not\Rightarrow \mathsf{UP}$ in the notation of [Pud17]. In particular, relative to this oracle there are no P-optimal pps, but UP has $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets, i.e., $\mathsf{CON} \not\Rightarrow \mathsf{UP}$. This is of particular interest, since $\mathsf{CON} \Leftarrow \mathsf{UP}$ is a theorem [KMT03]. Moreover, relative to the same oracle, UP has $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets, but NP $\cap$ coNP has not, i.e., $\mathsf{NP} \cap \mathsf{coNP} \not\Rightarrow \mathsf{UP}$.

3. Possibility of $\mathrm{H}_{\mathrm{opps}}$ *without* NEE $\cap$ TALLY $\subseteq$ coNEE. The oracle constructed in Theorem 7.1 shows that the converses of the following implications by Krajícek and Pudlák [KP89] and Köbler, Messner, and Torán [KMT03] fail relative to an oracle. For the implications (a) and (b) this was known by Verbitskii [Ver91], for the other implications this is a new result. It tells us that $\mathrm{H}_{\mathrm{opps}}$ might be true under an assumption weaker than NEE $\cap$ TALLY $\subseteq$ coNEE.

(a) [KP89] NE = coNE $\Rightarrow$ $\mathrm{H}_{\mathrm{opps}}$

(b) [KP89] E = NE $\Rightarrow$ there exist P-optimal pps

(c) [KMT03] NEE $\cap$ TALLY $\subseteq$ coNEE $\Rightarrow$ $\mathrm{H}_{\mathrm{opps}}$, where NEE $\stackrel{df}{=}$ NTIME$(2^{O(2^n)})$

(d) [KMT03] NEE$\cap$TALLY $\subseteq$ EE $\Rightarrow$ there exist P-optimal pps, where EE $\stackrel{df}{=}$ DTIME$(2^{O(2^n)})$

4. Characterization of $\mathrm{H}_{\mathrm{union}}$. We characterize $\mathrm{H}_{\mathrm{union}}$ and two variants (one is weaker, the other one stronger) in several ways. For instance, $\mathrm{H}_{\mathrm{union}}$ (resp., its stronger version) is equivalent to the statement that for each propositional proof system, the set of hard formulas is coNP-complete (resp., P-producible). The latter notion was introduced by Hemaspaandra, Hemaspaandra, and Hempel [HHH05] for the study of inverses of NP-problems.

The paper is organized as follows: Section 2 contains the preliminaries. In section 3 we characterize $\mathrm{H}_{\mathrm{union}}$ and two variants. The sections 4–7 contain oracle constructions. Section 8 provides a table summarizing the properties of several oracles. Section 9 concludes the paper and states open questions.

2 Preliminaries

Throughout this paper let Σ be the alphabet $\{0,1\}$. We denote the length of a word $w \in \Sigma^*$ by $|w|$. Let $\Sigma^{\leq n} = \{w \in \Sigma^* \mid |w| \leq n\}$ and $\Sigma^{[m,n]} = \{w \in \Sigma^* \mid m \leq |w| \leq n\}$. The empty word is denoted by ε and the i-th letter of a word w for $0 \leq i < |w|$ is denoted by $w(i)$, i.e., $w = w(0)w(1)\cdots w(|w|-1)$. For $k \leq |w|$ let $\mathrm{pr}_k(w) = w(0)\cdots w(k-1)$ be the length k prefix of w. If v is a prefix of w, then we write $v \sqsubseteq w$. Let $\mathrm{id} : \Sigma^* \to \Sigma^*$ with $\mathrm{id}(x) = x$.

The set of all (resp., positive, negative) integers is denoted by $\mathbb{Z}$ (resp., $\mathbb{Z}^+$, $\mathbb{Z}^-$). Moreover, $\mathbb{N}$ denotes the set of natural numbers and $\mathbb{N}^+$ denotes the set of positive natural numbers. The set of primes is denoted by $\mathbb{P} = \{2,3,5,\ldots\}$, the set of primes $\geq k$ by $\mathbb{P}^{\geq k} = \{n \in \mathbb{P} \mid n \geq k\}$. The logarithm function log denotes the function $\mathbb{N}^+ \to \mathbb{N}$ defined by $n \mapsto \max(\{k \in \mathbb{N} \mid 2^k \leq n\})$.

We identify Σ^* with $\mathbb{N}$ via the polynomial-time-computable, polynomial-time-invertible bijection $w \mapsto \sum_{i<|w|}(1+w(i))2^i$, which is a variant of the dyadic encoding. Hence notations, relations, and operations for Σ^* are transferred to $\mathbb{N}$ and vice versa. In particular, $|n|$ denotes the length of $n \in \mathbb{N}$. We eliminate the ambiguity of the expressions 0^i and 1^i by always interpreting them over Σ^*.

Let $\langle\cdot\rangle : \bigcup_{i\geq 0}\mathbb{N}^i \to \mathbb{N}$ be an injective, polynomial-time-computable, polynomial-time-invertible pairing function such that $|\langle u_1,\ldots,u_n\rangle| = 2(|u_1|+\cdots+|u_n|+n)$.

Given two sets A and B, $A-B$ (resp., $A\triangle B$) denotes the set difference (resp., symmetric difference) between A and B. The complement of a set A relative to the universe U is denoted by $\overline{A} = U - A$. The universe will always be apparent from the context.

Let Pol denote the set of univariate polynomials with coefficients from $\mathbb{N}$. FP, P, and NP denote standard complexity classes [Pap81]. Define co$\mathcal{C} = \{A \subseteq \Sigma^* \mid \overline{A} \in \mathcal{C}\}$ for a class $\mathcal{C}$. Let UP denote the set of problems that can be accepted by a nondeterministic polynomial-time Turing machine that on every input x has at most one accepting path and that accepts if and only if there exists an accepting path. We adopt the following notions from Köbler, Messner, and Torán [KMT03] with the remark that in the literature there exist inequivalent definitions for the double exponential time classes EE and NEE. To avoid confusion we will recall these definitions where appropriate.

$$\begin{aligned} \mathrm{E} &\stackrel{df}{=} \mathrm{DTIME}(2^{O(n)}) & \qquad \mathrm{EE} &\stackrel{df}{=} \mathrm{DTIME}(2^{O(2^n)}) \\ \mathrm{NE} &\stackrel{df}{=} \mathrm{NTIME}(2^{O(n)}) & \qquad \mathrm{NEE} &\stackrel{df}{=} \mathrm{NTIME}(2^{O(2^n)}) \end{aligned}$$

TALLY denotes the class $\{A \mid A \subseteq \{0\}^*\}$.

If $A, B \in \mathrm{NP}$ and $A \cap B = \emptyset$, then we call (A, B) a disjoint NP-pair. The set of all disjoint NP-pairs is denoted by DisjNP.

We also consider all these complexity classes in the presence of an oracle O and denote the corresponding classes by FP^O, P^O, NP^O, and so on. We consider the usual oracle model where the length of queries is *not* bounded, e.g., exponential-time machines can ask queries of exponential length.

A sequence (M_i) is called *standard enumeration* of nondeterministic, polynomial-time oracle Turing machines, if it has the following properties:

1. All M_i are nondeterministic, polynomial-time oracle Turing machines.
2. For all oracles D and all inputs x the computation $M_i^D(x)$ stops within $|x|^i + i$ steps.
3. For every nondeterministic, polynomial-time oracle Turing machine M there exist infinitely many $i \in \mathbb{N}$ such that for all oracles D it holds that $L(M^D) = L(M_i^D)$.
4. There exists a nondeterministic, polynomial-time oracle Turing machine M such that for all oracles D and all inputs x it holds that $M^D(\langle i, x, 0^{|x|^i+i}\rangle)$ simulates the computation $M_i^D(x)$ in the following sense: Each computation path of $M_i^D(x)$ simulates a single path of $M^D(\langle i, x, 0^{|x|^i+i}\rangle)$ by computing its sequence of configurations (i.e., internal state, content of the tapes, positions of the heads).

For every oracle D, the sequence (M_i) represents an enumeration of languages in NP^D. Analogously we define standard enumerations of nondeterministic, polynomial-time Turing machines and deterministic, polynomial-time oracle Turing transducers.

Note that these requirements ensure that $K^D = \{\langle 0^i, 0^j, x\rangle \mid M_i^D(x) \text{ accepts within } j \text{ steps}\}$ is in NP^D for each oracle D.

We define several reducibilities. Let $A, B \subseteq \Sigma^*$. Then $A \leq_{\mathrm{m}}^{\mathrm{p},O} B$ if there exists an $f \in \mathrm{FP}^O$ such that $x \in A \Leftrightarrow f(x) \in B$ for all $x \in \Sigma^*$. We also say $A \leq_{\mathrm{m}}^{\mathrm{p},O} B$ via f. Furthermore $A \leq_{\mathrm{m,li}}^{\mathrm{p},O} B$ if $A \leq_{\mathrm{m}}^{\mathrm{p},O} B$ via some $f \in \mathrm{FP}^O$ such that $|f(x) > |x|$ for all $x \in \Sigma^*$. In this case we say $A \leq_{\mathrm{m,li}}^{\mathrm{p},O} B$ via f.

For disjoint pairs we define specific reducibilities. Let $A, B, C, D \in \Sigma^*$ such that $A \cap B = C \cap D = \emptyset$. Then $(A, B) \leq_{\mathrm{m}}^{\mathrm{pp},O} (C, D)$ (resp., $(A, B) \leq_{\mathrm{m,li}}^{\mathrm{pp},O} (C, D)$) if there exists $f \in \mathrm{FP}^O$ (resp. $f \in \mathrm{FP}^O$ with $|f(x)| > |x|$ for all $x \in \Sigma^*$) with $f(A) \subseteq C$ and $f(B) \subseteq D$. Here we also say $(A, B) \leq_{\mathrm{m}}^{\mathrm{pp},O} (C, D)$ (resp., $(A, B) \leq_{\mathrm{m,li}}^{\mathrm{pp},O} (C, D)$) via f.

In the following we define a stronger reducibility for disjoint pairs: $(A, B) \leq_{\mathrm{sm}}^{\mathrm{p},O} (C, D)$ (resp., $(A, B) \leq_{\mathrm{sm,li}}^{\mathrm{p},O} (C, D)$) if there exists $f \in \mathrm{FP}^O$ (resp. $f \in \mathrm{FP}^O$ with $|f(x)| > |x|$ for all $x \in \Sigma^*$) such that $(A, B) \leq_{\mathrm{m}}^{\mathrm{pp},O} (C, D)$ (resp., $(A, B) \leq_{\mathrm{m,li}}^{\mathrm{pp},O} (C, D)$) via f and $f(\overline{A \cup B}) \subseteq \overline{C \cup D}$.

When we consider these reducibilities without the presence of an oracle O, then we omit O. We use $A \leq_{\mathrm{m}}^{\mathrm{pp}}(C,D)$ as an abbreviation for $(A,\overline{A}) \leq_{\mathrm{m}}^{\mathrm{pp}}(C,D)$.

For a complexity class $\mathcal{C}$ and some problem A, we say that A is $\leq$-hard for $\mathcal{C}$ if for all $B \in \mathcal{C}$ it holds $B \leq A$, where $\leq$ is some reducibility. A is called $\leq$-complete for $\mathcal{C}$ if A is $\leq$-hard for $\mathcal{C}$ and $A \in \mathcal{C}$. Let $\mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ (resp., $\mathrm{NPC}_{\mathrm{m,li}}^{\mathrm{p}}$, $\mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$) be the set of problems that are $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete (resp., $\leq_{\mathrm{m,li}}^{\mathrm{p}}$-complete, $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-complete) for NP, where the reducibility $\leq_{\mathrm{m}}^{\text{io-p/poly}}$ is given in Definition 2.6 below.

If for all $A \in \mathrm{NP}$ it holds $A \leq_{\mathrm{m}}^{\mathrm{pp}}(C,D)$, then we say that (C,D) is $\leq_{\mathrm{m}}^{\mathrm{pp}}$-hard for NP. The analogous holds for the other reducibilities.

Let SAT denote the set of satisfiable formulas and TAUT the set of tautologies. Without loss of generality we assume that each word over Σ^* encodes a propositional formula.

Definition 2.1 ([CR79]) *A function $f \in \mathrm{FP}$ is called* proof system *for the set* $\mathrm{ran}(f)$. *For $f, g \in \mathrm{FP}$ we say that f* is simulated by *g (resp., f* is P-simulated by *g) denoted by $f \leq g$ (resp., $f \leq^{\mathrm{p}} g$), if there exists a function π (resp., a function $\pi \in \mathrm{FP}$) and a polynomial p such that $|\pi(x)| \leq p(|x|)$ and $g(\pi(x)) = f(x)$ for all x. A function $g \in \mathrm{FP}$ is* optimal *(resp.,* P-optimal*), if $f \leq g$ (resp., $f \leq^{\mathrm{p}} g$) for all $f \in \mathrm{FP}$ with* $\mathrm{ran(f)} = \mathrm{ran(g)}$. *Corresponding relativized notions are obtained by using P^O, FP^O, and $\leq^{\mathrm{p},O}$ in the definitions above. A* propositional proof system *(pps) is a proof system for* TAUT.

Remark 2.2 *The notion of a* propositional *proof system has no canonical relativization. However, in view of Corollary 2.4 below, it is reasonable to use the following convention. We say that there exist P^O-optimal (resp., optimal) pps relative to an oracle O, if there exists a $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete $A \in \mathrm{coNP}^O$ that has a P^O-optimal (resp., optimal) proof system.*

The following proposition states the relativized version of a result by Köbler, Messner, and Torán [KMT03], which they show with a relativizable proof.

Proposition 2.3 ([KMT03]) *For every oracle O, if A has a P^O-optimal (resp., optimal) proof system and $B \leq_{\mathrm{m}}^{\mathrm{p},O} A$, then B has a P^O-optimal (resp., optimal) proof system.*

Corollary 2.4 *For every oracle O, if there exists a $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete $A \in \mathrm{coNP}^O$ that has a P^O-optimal (resp., optimal) proof system, then all sets in coNP^O have P^O-optimal (resp., optimal) proof systems.*

Definition 2.5 *For $f \in \mathrm{FP}$ and a polynomial q, a word $y \in \mathrm{ran}(f)$ is q-hard w.r.t. the proof system f if there exists no $x \in \Sigma^{\leq q(|y|)}$ such that $f(x) = y$. The set of elements that are q-hard w.r.t. the proof system f is denoted by f_q, i.e., $f_q = \{y \in \mathrm{ran}(f) \mid y \text{ is } q\text{-hard w.r.t. } f\}$.*

2.1 Infinitely Often P/poly Reducibility

We introduce $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-reducibility, which is used in subsection 3.3 to define the following weakened variant of $\mathrm{H}_{\mathrm{union}}$: the union of disjoint $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets for NP is $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-complete. Although $\leq_{\mathrm{m}}^{\text{io-p/poly}}$ is not transitive (cf. Remark 2.8), we show that the corresponding NP-hardness and NP-completeness notions are robust concepts (cf. Proposition 2.12).

P/poly is the class of sets $A \subseteq \Sigma^*$ for which there exist a $B \in \mathrm{P}$ and a function h such that $|h(n)|$ is polynomially bounded in n and for all x it holds that $x \in A \Leftrightarrow (x, h(|x|)) \in B$. FP/poly is the class of total functions $f : \Sigma^* \to \Sigma^*$ for which there exist a $g \in \mathrm{FP}$ and a function h such that $|h(n)|$ is polynomially bounded in n and for all x it holds that $f(x) = g(x, h(|x|))$. Two total functions $f, g : \Sigma^* \to \Sigma^*$ *agree infinitely often*, written as $f \overset{\mathrm{io}}{=} g$, if for infinitely many n it holds that $\forall x \in \Sigma^n, f(x) = g(x)$. Two sets $A, B \subseteq \Sigma^*$ *agree infinitely often*, written as

$A \overset{\text{io}}{=} B$, if their characteristic functions agree infinitely often. For a class $\mathcal{C}$ of functions or sets let io-$\mathcal{C} = \{A \mid \exists B \in \mathcal{C}, A \overset{\text{io}}{=} B\}$.

For this section fix a standard enumeration $M_0, M_1, \ldots$ of deterministic, polynomial-time oracle Turing machines.

Definition 2.6 *A set $A \subseteq \Sigma^*$ is* infinitely often P/poly reducible *to a set $B \subseteq \Sigma^*$, written as $A \leq_{\text{m}}^{\text{io-p/poly}} B$, if there exists $f \in$ io-FP/poly such that for all x it holds that $x \in A \Leftrightarrow f(x) \in B$.*

It should be mentioned at this point that $\leq_{\text{m}}^{\text{io-p/poly}}$ is an artificial reducibility notion, which emerged from the attempt to express the right-hand side of the known implication $\text{H}_{\text{union}} \Rightarrow \text{NP} \neq \text{coNP}$ as a variant of H_{union}. In Theorem 3.8 we show that this is possible with $\leq_{\text{m}}^{\text{io-p/poly}}$ reducibility.

Remark 2.8 shows that $\leq_{\text{m}}^{\text{io-p/poly}}$ is not transitive, but the following weaker property holds.

Proposition 2.7 *For sets A, B, and C with $A \leq_{\text{m}}^{\text{io-p/poly}} B$ and $B \leq_{\text{m}}^{\text{p}} C$ it holds $A \leq_{\text{m}}^{\text{io-p/poly}} C$.*

Proof Let $f \in$ io-FP/poly and $g \in$ FP such that $A \leq_{\text{m}}^{\text{io-p/poly}} B$ via f and $B \leq_{\text{m}}^{\text{p}} C$ via g. Then there exists $f' \in$ FP/poly with $f \overset{\text{io}}{=} f'$. For h with $h(x) = g(f(x))$ it holds $x \in A \Leftrightarrow h(x)$ for all $x \in \Sigma^*$. Furthermore, for h' with $h'(x) = g(f'(x))$ it holds that $h' \in$ FP/poly and $h \overset{\text{io}}{=} h'$. □

Remark 2.8 *The reducibility $\leq_{\text{m}}^{\text{io-p/poly}}$ is not transitive, which is seen as follows: Assume for the moment that there exists a set $H \subseteq \Sigma^*$ such that $H \notin$ io-P/poly. We show $H \leq_{\text{m}}^{\text{io-p/poly}} HH$ and $HH \leq_{\text{m}}^{\text{io-p/poly}} \{1\}$, but $H \not\leq_{\text{m}}^{\text{io-p/poly}} \{1\}$.*

$H \leq_{\text{m}}^{\text{io-p/poly}} HH$ via the function $f(x) = xx$, which belongs to FP $\subseteq$ io-FP/poly. *Let g be the characteristic function of HH. Note that g agrees with the function $g'(w) = 0$ on all words of odd length. Hence $g \overset{\text{io}}{=} g' \in$ FP $\subseteq$ io-FP/poly and thus $HH \leq_{\text{m}}^{\text{io-p/poly}} \{1\}$ via $g \in$ io-FP/poly. Assume $H \leq_{\text{m}}^{\text{io-p/poly}} \{1\}$ via some $h \in$ io-FP/poly. Let $h' \in$ FP/poly such that $h \overset{\text{io}}{=} h'$. Note that $H' = \{x \mid h'(x) = 1\} \in$ P/poly and $H \overset{\text{io}}{=} H'$. Therefore, $H \in$ io-P/poly, which contradicts our assumption. This shows $H \not\leq_{\text{m}}^{\text{io-p/poly}} \{1\}$.*

It remains to show the existence of a set $H \notin$ io-P/poly. For $n \geq 0$, $i \leq n$, and $v \in \Sigma^{\leq n^{\log n}}$ let $H(n, i, v) = \{w \in \Sigma^n \mid M_i(w, v)$ accepts$\}$, which is the set of words of length n that are accepted by M_i with advice v. For sufficiently large n, the number of sets $H(n, i, v)$ is at most $(n+1) \cdot 2 \cdot 2^{n^{\log n}} < 2^{2^n}$, where the latter is the number of subsets of Σ^n. Hence there exists a set $H_n \subseteq \Sigma^n$ that differs from all $H(n, i, v)$ for $i \leq n$ and $v \in \Sigma^{\leq n^{\log n}}$. Let $H = \bigcup_n H_n$ and observe that $H \notin$ io-P/poly.

Infinitely often P/poly reducibility can be characterized as follows.

Proposition 2.9 *For $A, B \subseteq \Sigma^*$ with $\emptyset \neq B \neq \Sigma^*$ it holds that*

$$A \leq_{\text{m}}^{\text{io-p/poly}} B \iff \exists f \in \text{FP/poly} \exists^\infty n \in \mathbb{N} \forall x \in \Sigma^n (x \in A \Leftrightarrow f(x) \in B).$$

Proof "⇒": There exists an $f \in$ io-FP/poly such that for all x it holds that $x \in A \Leftrightarrow f(x) \in B$. Let $f' \in$ FP/poly such that $f' \overset{\text{io}}{=} f$. Hence for infinitely many n it holds that $\forall x \in \Sigma^n, f'(x) = f(x)$. Thus for infinitely many n it holds that $\forall x \in \Sigma^n (x \in A \Leftrightarrow f'(x) \in B)$.

"⇐": Let $f \in$ FP/poly and $n_1 < n_2 < \cdots$ such that for all $i \geq 1$ it holds that $\forall x \in \Sigma^{n_i} (x \in A \Leftrightarrow f(x) \in B)$. Choose $b_0 \notin B$, $b_1 \in B$, and define f' as follows: If $|x| = n_i$ for some i, then $f'(x) = f(x)$; otherwise if $x \notin A$, then $f'(x) = b_0$; otherwise $f'(x) = b_1$. Hence $f' \overset{\text{io}}{=} f$ and $f' \in$ io-FP/poly. Moreover, for all $x \in \Sigma^*$ it holds that $x \in A \Leftrightarrow f(x) \in B$. □

In the following we argue that $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-hardness for NP and hence also $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-completeness for NP are robust notions. For this purpose, in Proposition 2.12 we show several characterizations of $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-hardness for NP. We start with the definition of paddability and a related notion.

Definition 2.10 ([BH77]) *A set A is* paddable *if there exists a polynomial-time computable, polynomial-time invertible $p(\cdot,\cdot)$ such that for all x, y it holds that $(x \in A \Leftrightarrow p(x,y) \in A)$. Let* $\mathrm{Pad} = \{A \mid A \text{ is paddable}\}$.

Mahaney and Young [MY85] showed that two paddable sets are $\leq_{\mathrm{m}}^{\mathrm{p}}$-equivalent if and only if they are P-isomorphic (i.e., $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ via a polynomial-time computable, polynomial-time invertible bijection f). Hence the paddable $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets for NP are those that are P-isomorphic to SAT. Paddability implies that we can increase the length of an instance without changing its membership. The following notion captures the property that the length can be *precisely* increased without changing membership.

Definition 2.11 *A set A is* homogeneous*, if there exists $h \in \mathrm{FP}$ such that for all x, y it holds that $(x \in A \Leftrightarrow h(x,y) \in A)$ and $|h(x,y)| = |x| + |y|$. Let* $\mathrm{Hom} = \{A \mid A \text{ is homogeneous}\}$.

It is clear that SAT is paddable, but the question of whether SAT is homogenous crucially depends on its specific encoding. The following variant of the canonical NP-complete problem is both, paddable and homogeneous. (Paddability is seen as follows: reduce an instance of K to SAT, use the padding property of SAT, and finally express the satisfiability of the obtained formula by an instance of K.)

$$K = \{0^i 1^j 0^k 1 x \mid i, j, k \in \mathbb{N}, x \in \{0,1\}^*, M_i \text{ accepts } x \text{ within } j \text{ steps}\}$$

We characterize $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-hardness for NP in several ways. Afterwards we explain why in this characterization one statement is missing.

Proposition 2.12 *For a set B, the following statements are equivalent:*

1. *B is $\leq_{\mathrm{m}}^{\text{io-p/poly}}$-hard for* NP.
2. $\exists A \in \mathrm{NP}\mathrm{C}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Hom}$ $\quad \exists f \in \mathrm{FP/poly}\ \exists^{\infty} n \in \mathbb{N}\ \forall x \in \Sigma^n \quad (x \in A \Leftrightarrow f(x) \in B)$
3. $\forall A \in \mathrm{NP}$ $\quad \exists f \in \mathrm{FP/poly}\ \exists^{\infty} n \in \mathbb{N}\ \forall x \in \Sigma^n \quad (x \in A \Leftrightarrow f(x) \in B)$
4. $\exists A \in \mathrm{NP}\mathrm{C}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Pad}$ $\quad \forall q \in \mathrm{Pol}\ \exists f \in \mathrm{FP/poly}\ \exists^{\infty} n \in \mathbb{N}\ \forall x \in \Sigma^{[n,q(n)]} \quad (x \in A \Leftrightarrow f(x) \in B)$
5. $\exists A \in \mathrm{NP}\mathrm{C}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Hom}$ $\quad \forall q \in \mathrm{Pol}\ \exists f \in \mathrm{FP/poly}\ \exists^{\infty} n \in \mathbb{N}\ \forall x \in \Sigma^{[n,q(n)]} \quad (x \in A \Leftrightarrow f(x) \in B)$
6. $\forall A \in \mathrm{NP}$ $\quad \forall q \in \mathrm{Pol}\ \exists f \in \mathrm{FP/poly}\ \exists^{\infty} n \in \mathbb{N}\ \forall x \in \Sigma^{[n,q(n)]} \quad (x \in A \Leftrightarrow f(x) \in B)$

Proof The implications $6 \Rightarrow 3 \Rightarrow 2$, $6 \Rightarrow 5 \Rightarrow 2$, and $6 \Rightarrow 4$ are trivial. Moreover, observe that the implications $1 \Leftrightarrow 3$ follow from Proposition 2.9.

We show $4 \Rightarrow 3$. Choose $A_4 \in \mathrm{NP}\mathrm{C}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Pad}$ according to statement 4. Let $p(\cdot,\cdot)$ be a padding function for A_4, which is invertible in time $r \in \mathrm{Pol}$. To show statement 3, let $A_3 \in \mathrm{NP}$. Choose $g \in \mathrm{FP}$ such that $A_3 \leq_{\mathrm{m}}^{\mathrm{p}} A_4$ via g. Let

$$g'(x) = p(g(x), 0^{r(|x|)+1})$$

and observe that $g' \in \mathrm{FP}$ and $A_3 \leq_{\mathrm{m}}^{\mathrm{p}} A_4$ via g'. Moreover, $|g'(x)| > |x|$, since otherwise $|p(g(x), 0^{r(|x|)+1})| \leq |x|$ contradicting the fact that p is invertible in time r. Choose $q \in \mathrm{Pol}$ such that $|g'(x)| \leq q(|x|)$. According to statement 4, for A_4 and q there exists an $f_4 \in \mathrm{FP/poly}$ with the properties mentioned there. Let $f_3(x) = f_4(g'(x))$, which is in FP/poly. For infinitely many n,

$$\forall x \in \Sigma^{[n,q(n)]}\ \ (x \in A_4 \Leftrightarrow f_4(x) \in B).$$

For each of these n it holds that

$$\forall x \in \Sigma^n \ \ (g'(x) \in \Sigma^{[n,q(n)]} \wedge (x \in A_3 \Leftrightarrow g'(x) \in A_4) \wedge (g'(x) \in A_4 \Leftrightarrow f_4(g'(x)) \in B).$$

Hence, for infinitely many n,

$$\forall x \in \Sigma^n \ \ (x \in A_3 \Leftrightarrow f_3(x) \in B).$$

We show $2 \Rightarrow 6$. Choose $A_2 \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Hom}$ and $f_2 \in \mathrm{FP/poly}$ according to statement 2. Let $h \in \mathrm{FP}$ such that for all x, y it holds that $(x \in A \Leftrightarrow h(x,y) \in A)$ and $|h(x,y)| = |x| + |y|$. To show statement 6, let $A_6 \in \mathrm{NP}$ and $q \in \mathrm{Pol}$, where we may assume $q(n) > n$. Choose $g \in \mathrm{FP}$ and $r \in \mathrm{Pol}$ with $r(n) > n$ such that $|g(x)| \leq r(|x|)$ and $A_6 \leq_{\mathrm{m}}^{\mathrm{p}} A_2$ via g. By assumption, there exist pairwise distinct $n_0, n_1, \ldots \in \mathbb{N}$ such that $(x \in A_2 \Leftrightarrow f(x) \in B)$ for all i and all $x \in \Sigma^{n_i}$. We may assume $n_0 \geq r(q(1))$ and $n_{i+1} \geq r(q(n_i + 1))$. Let $m_i = \max\{m \mid r(q(m)) \leq n_i\}$ and observe that $m_0 < n_0 < m_1 < n_1 < \cdots$. The following function is used as advice for f_6.

$$a(n) = \begin{cases} n_i & \text{if } m_i \leq n \leq q(m_i) \text{ for some } i \\ 0 & \text{otherwise.} \end{cases}$$

Note that $n_i < r(q(m_i + 1))$ and hence $a(n) \in n^{O(1)}$ and $|a(n)| \in O(\log n)$. Let

$$f_6(x) = \begin{cases} f_2(h(g(x), 0^{a(|x|)-|g(x)|})) & \text{if } a(|x|) > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Hence $f_6 \in \mathrm{FP/poly}$. It remains to show $(x \in A_6 \Leftrightarrow f_6(x) \in B)$ for all i and all $x \in \Sigma^{[m_i, q(m_i)]}$. For such x it holds that $m_i \leq |x| \leq q(m_i)$ and $|g(x)| \leq r(q(m_i)) \leq n_i = a(|x|)$. Hence $f_6(x) = f_2(h(g(x), 0^{n_i - |g(x)|}))$ and

$$x \in A_6 \Leftrightarrow g(x) \in A_2 \Leftrightarrow h(g(x), 0^{n_i - |g(x)|}) \in A_2.$$

From $|h(g(x), 0^{n_i - |g(x)|})| = n_i$ it follows that

$$h(g(x), 0^{n_i - |g(x)|}) \in A_2 \Leftrightarrow f_6(x) \in B,$$

which shows $(x \in A_6 \Leftrightarrow f_6(x) \in B)$. □

Remark 2.13 *The following statement cannot appear in Proposition 2.12.*

$$\exists A \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}} \cap \mathrm{Pad} \ \ \exists f \in \mathrm{FP/poly} \ \ \exists^{\infty} n \in \mathbb{N} \ \ \forall x \in \Sigma^n \ \ (x \in A \Leftrightarrow f(x) \in B) \tag{2}$$

The statement actually holds for all $B \subsetneq \mathbb{N}$, which is seen as follows. Choose some $z \notin B$ and let $A = \{ww \mid w \in K\}$, where K is the canonical NP*-complete problem defined above. Observe that A is paddable and $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete for* NP*. The function $f(x) = z$ belongs to* FP *and for all x of odd length it holds that $(x \in A \Leftrightarrow f(x) \in B)$. Therefore, if (2) is equivalent to the statements in Proposition 2.12, then the set $B = \emptyset$ is infinitely often $\leq_{\mathrm{m}}^{\mathrm{p/poly}}$-hard for* NP*. But this is not true, since for $A = \mathbb{N} \in \mathrm{NP}$, for all total functions $f : \mathbb{N} \to \mathbb{N}$, and all $x \in \mathbb{N}$ it holds that $(x \in A \not\Leftrightarrow f(x) \in B)$. This shows that (2) is not equivalent to the statements in Proposition 2.12.*

2.2 Basic Notations and Results for Constructing Oracles

The domain and range of a function t are denoted by $\mathrm{dom}(t)$ and $\mathrm{ran}(t)$, respectively. The support $\mathrm{supp}(t)$ of a real-valued function t is the subset of the domain that consists of all values that t does not map to 0. We say that a partial function t is injective on its support if $t(i,j) = t(i',j') \in \mathrm{supp}(t)$ implies $(i,j) = (i',j')$. If a partial function t is not defined at point x, then $t \cup \{x \mapsto y\}$ denotes the continuation of t that at x has value y.

Let M be a Turing machine. $M^D(x)$ denotes the computation of M on input x with D as an oracle. $L^D(M) = \{x \mid M^D(x) \text{ accepts}\}$ denotes the languages accepted by M with D as an oracle. For a deterministic polynomial-time Turing transducer, depending on the context, $F^D(x)$ either denotes the computation of F on input x with D as an oracle or the output of this computation.

If A is a set, then $A(x)$ denotes the characteristic function at point x, i.e., $A(x)$ is 1 if $x \in A$, and 0 otherwise. An oracle $D \subseteq \mathbb{N}$ is identified with its characteristic sequence $D(0)D(1)\cdots$, which is an ω-word. (In this way, $D(i)$ denotes both, the characteristic function at point i and the i-th letter of characteristic sequence, which are the same.) A finite word w describes an oracle that is partially defined, i.e., only defined for natural numbers $x < |w|$. We can use w instead of the set $\{i \mid w(i) = 1\}$ and write for example $A = w \cup B$, where A and B are sets. For nondeterministic oracle Turing machines M and deterministic oracle Turing transducers F we use the following phrases: A computation $M^w(x)$ *definitely accepts (within t steps)*, if it contains a path that accepts (within t steps) and the queries on this path are $< |w|$. A computation $M^w(x)$ *definitely rejects (within t steps)*, if all paths reject (within t steps) and all queries are $< |w|$. A computation $M^w(x)$ *is defined*, if it definitely accepts or definitely rejects. A computation $F^w(x)$ *is defined*, if all queries are $< |w|$.

For any finite set $Y \subseteq \Sigma^*$, let $\ell(Y) \stackrel{df}{=} \sum_{w \in Y} |w|$. For a path P of some nondeterministic computation, P^{yes} (resp., P^{no}) denotes the set of oracle queries that are answered positively (resp., negatively) along P. Let $P^{\mathrm{all}} = P^{\mathrm{yes}} \cup P^{\mathrm{no}}$, and denote the length of P by $|P|$.

The following lemma and its corollary hold for any standard enumerations of nondeterministic, polynomial-time oracle Turing machines $M_0, M_1, \ldots$ and deterministic, polynomial-time oracle Turing transducers $F_0, F_1, \ldots$.

Lemma 2.14 *For all $i, j \in \mathbb{N}$, and almost all $n \in \mathbb{N}$ and all $D \subseteq \Sigma^*$ there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that at least one of the following statements holds.*

1. $M_i^{D \cup \{x\}}(0^n)$ *rejects*
2. $M_j^{D \cup \{y\}}(0^n)$ *rejects*
3. $M_i^{D \cup \{x,y\}}(0^n)$ *and* $M_j^{D \cup \{x,y\}}(0^n)$ *accept*

Proof Assume that the assertion is wrong, i.e., there are $i, j \in \mathbb{N}$ such that for all $n_0 \in \mathbb{N}$ there is an $n \geq n_0$ and an oracle $D \subseteq \Sigma^{<n}$ such that for all even $x \in \Sigma^n$ and all odd $y \in \Sigma^n$ all three statements are wrong. Fix machines M_i and M_j guaranteed by this assumption.

Let p be a monotone polynomial limiting the running time of M_i and M_j. Choose n_0 such that $2^{2n_0-3} > 2^{n_0} \cdot p(n_0)$. Let $n \geq n_0$ and $D \subseteq \Sigma^{<n}$ such that for all even $x \in \Sigma^n$ and all odd $y \in \Sigma^n$ the three statements are wrong.

As the first statement is wrong, for all even $x \in \Sigma^n$ the computation $M_i^{D \cup \{x\}}(0^n)$ accepts. Since the second statement is wrong as well, for all $y \in \Sigma^n$ the computation $M_j^{D \cup \{y\}}(0^n)$ accepts. Consider the directed graph $G = (\Sigma^n, E_1 \cup E_2)$ with

$$E_1 = \{(x,z) \in (\Sigma^n)^2 \mid x \text{ even}, x \neq z, \text{ the least accepting path of } M_i^{D \cup \{x\}}(0^n) \text{ asks } z\}$$
$$E_2 = \{(y,z) \in (\Sigma^n)^2 \mid y \text{ odd}, y \neq z, \text{ the least accepting path of } M_j^{D \cup \{y\}}(0^n) \text{ asks } z\}$$

Observe $|E_1 \cup E_2| \leq 2^n \cdot p(n)$. Assume that for all even $x \in \Sigma^n$ and all odd $y \in \Sigma^n$ it holds $(x,y) \in E_1 \cup E_2$ or $(y,x) \in E_1 \cup E_2$. Then $|E_1 \cup E_2| \geq 2^{n-1} \cdot 2^{n-1}/2 = 2^{2n-3} > 2^n \cdot p(n) \geq |E_1 \cup E_2|$, a contradiction.

Thus there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that $(x,y) \notin E_1 \cup E_2$ and $(y,x) \notin E_1 \cup E_2$. As $M_i^{D \cup \{x\}}(0^n)$ accepts by the assumption that statement 1 is wrong and the least accepting path of this computation does not ask y (otherwise $(x,y) \in E_1 \cup E_2$), the computation $M_i^{D \cup \{x,y\}}(0^n)$ accepts. Similarly we obtain that $M_j^{D \cup \{x,y\}}(0^n)$ accepts. This contradicts our assumption that statement 3 is wrong and completes the proof. □

Corollary 2.15 *For all $i, j \in \mathbb{N}$, and almost all $n \in \mathbb{N}$ and all $D \subseteq \Sigma^*$ there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that at least one of the following statements holds.*

1. $F_r^{D \cup \{x\}}(0^n) \notin L(M_i^{D \cup \{x\}})$
2. $F_r^{D \cup \{y\}}(0^n) \notin L(M_j^{D \cup \{y\}})$
3. $F_r^{D \cup \{x,y\}}(0^n) \in L(M_i^{D \cup \{x,y\}}) \cap L(M_j^{D \cup \{x,y\}})$

Proof The statement follows by applying Lemma 2.14 to the machines N_i (resp., N_j) that first compute $F_r(0^n)$ and then simulate M_i (resp., M_j) on input $F_r(0^n)$. □

3 Are Unions of Disjoint NP-Complete Sets NP-Complete?

It is difficult to find out whether $\mathrm{H}_{\mathrm{union}}$ is true or not, since any outcome solves a long standing open problem:

$$\begin{array}{lcl} \mathrm{H}_{\mathrm{union}} \text{ is true} & \Rightarrow & \mathrm{NP} \neq \mathrm{coNP} \\ \mathrm{H}_{\mathrm{union}} \text{ is false} & \overset{3.1}{\Rightarrow} & \text{P-inseparable disjoint NP-pairs exist if and only if } \mathrm{P} \neq \mathrm{NP} \end{array}$$

As we expect the right hand sides of both implications to be true, they do not provide evidence for or against $\mathrm{H}_{\mathrm{union}}$. Therefore, researchers approach hypothesis $\mathrm{H}_{\mathrm{union}}$ by proving equivalent, necessary, and sufficient conditions. This section continues this program as follows. In subsection 3.1 we investigate a stronger variant of $\mathrm{H}_{\mathrm{union}}$, in subsection 3.2 the original hypothesis, and in subsection 3.3 a weaker variant. We characterize $\mathrm{H}_{\mathrm{union}}$ and its variants in several ways (e.g., in terms of P-producibility or coNP-completeness of the set of hard formulas of pps) and summarize the corresponding state of knowledge. In particular, within a subsection all hypotheses are equivalent and hence the following implications hold in general.

$$\begin{array}{ccccc} \text{hypotheses in subsect. 3.1} & \Rightarrow & \text{hypotheses in subsect. 3.2} & \Rightarrow & \text{hypotheses in subsect. 3.3} \\ & & \Updownarrow & & \Updownarrow \\ & & \mathrm{H}_{\mathrm{union}} & & \mathrm{NP} \neq \mathrm{coNP} \end{array}$$

Note that under the assumption that all sets in $\mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ are complete w.r.t. length-increasing reductions (which holds for example under the Berman-Hartmanis conjecture), all hypotheses in the subsections 3.1 and 3.2 are equivalent.

Before starting with the proofs of the equivalences, we show the aforementioned implication that under the assumption $\neg\mathrm{H}_{\mathrm{union}}$ it holds that P-inseparable disjoint NP-pairs exist if and only if $\mathrm{P} \neq \mathrm{NP}$.

Proposition 3.1 *If* $\mathrm{H}_{\mathrm{union}}$ *is false, then* P*-inseparable disjoint* NP*-pairs exist if and only if* $\mathrm{P} \neq \mathrm{NP}$.

Proof If $\mathrm{P} = \mathrm{NP}$, then all disjoint NP-pairs are P-separable. It remains to show $\mathrm{P} = \mathrm{NP}$ under the assumption that $\mathrm{H}_{\mathrm{union}}$ is false and all disjoint NP-pairs are P-separable: By [GPSS06], there exists a $B \in \mathrm{NP}$ that is disjoint from SAT such that $\mathrm{SAT} \cup B$ is not $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP. Moreover, there exists an $S \in \mathrm{P}$ such that $\mathrm{SAT} \subseteq S \subseteq \overline{B}$. We claim that $B = \overline{\mathrm{SAT}}$. Otherwise, there exists some $w \in \overline{\mathrm{SAT}} \cup \overline{B}$. Hence $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{SAT} \cup B$ via the reduction that on input x outputs x if $x \in S$ and outputs w otherwise. This contradicts the fact that $\mathrm{SAT} \cup B$ is not $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete. Thus $B = \overline{\mathrm{SAT}}$ and therefore, NP = coNP. By assumption, for each $L \in \mathrm{NP}$, the disjoint NP-pair $(L, \overline{L})$ is P-separable and hence $L \in \mathrm{P}$. This shows $\mathrm{P} = \mathrm{NP}$. □

3.1 Length-Increasing Polynomial-Time Reducibility

We consider the hypothesis that the union of SAT with a disjoint $B \in \mathrm{NP}$ is $\leq^{\mathrm{p}}_{\mathrm{m,li}}$-complete for NP. This is equivalent to say that the union of disjoint sets from $\mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ is $\leq^{\mathrm{p}}_{\mathrm{m,li}}$-complete for NP. We prove several characterizations of this hypothesis, e.g., one in terms of the P-producibility of the set of hard formulas of pps.

Let us define the notion of P-producibility, which was introduced by Hemaspaandra, Hemaspaandra, and Hempel [HHH05], and the notion of a refuter, which was introduced by Kabanets [Kab01].

Definition 3.2 ([HHH05]) *A set* A *is p-producible if and only if there is some* $f \in \mathrm{FP}$ *with* $|f(x)| \geq |x|$ *and* $f(x) \in A$ *for all* x.

Definition 3.3 ([Kab01]) *A* refuter *is a deterministic Turing machine that on an input of length* n *outputs a string of length at least* n. *A refuter* R almost everywhere distinguishes *a language* L *from a language* L' *if for all but finitely many* n, $R(1^n)$ *outputs a string from* $L \Delta L'$.

In the following theorem, the equivalence $1 \Leftrightarrow 4$ was shown in [GHPT14].

Theorem 3.4 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
2. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
3. f_q *is P-producible for all pps* f *and all polynomials* q.
4. *For every language* $L \in \mathrm{NP}$ *that is disjoint from* SAT, *there is a polynomial-time refuter that almost everywhere distinguishes* L *from* $\overline{\mathrm{SAT}}$.

Proof The equivalence $1 \Leftrightarrow 4$ was shown in [GHPT14].

$1 \Rightarrow 2$: Let $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ be disjoint and $f \in \mathrm{FP}$ length-increasing such that $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} A$ via f. Then $B' = f^{-1}(B)$ is in NP since $B' \leq^{\mathrm{p}}_{\mathrm{m,li}} B \in \mathrm{NP}$ via f. Thus, by 1 it follows $\mathrm{SAT} \cup B' \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$. Moreover, $\mathrm{SAT} \cup B' \leq^{\mathrm{p}}_{\mathrm{m,li}} A \cup B$ via f. Hence we obtain $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.

By assumption, $\mathrm{NP} \neq \mathrm{coNP}$. Let f be a pps, q a polynomial, and define

$$B = \{\varphi \mid f(y) = \neg\varphi \text{ for some } y \text{ with } |y| \leq q(|\neg\varphi|)\}.$$

$B \cap \mathrm{SAT} = \emptyset$ and $\mathrm{SAT} \cup B \subsetneq \Sigma^*$. For $A' = 0\mathrm{SAT} \cup 1B$ and $B' = 1\mathrm{SAT} \cup 0B$ it holds $A' \cap B' = \emptyset$ and $A', B' \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$. By 2, $A' \cup B' = \{0,1\}(\mathrm{SAT} \cup B) \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$. In particular

$\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} \{0,1\}(\mathrm{SAT} \cup B)$. As $\mathrm{SAT} \cup B \subsetneq \Sigma^*$, this implies $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{SAT} \cup B$ via an FP-function h_1 with $|x| \leq |h_1(x)|$ for all $x \in \Sigma^*$. Let h_2 be a length-increasing FP-function ensuring $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} \mathrm{SAT}$. Then $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} \mathrm{SAT} \cup B$ via h with $h(x) = h_1(h_2(h_2(x)))$. We claim that f_q is P-producible via the length-increasing function $g(x) = \neg h(x \wedge \neg x)$: As $h(x \wedge \neg x) \notin \mathrm{SAT} \cup B$, $g(x)$ is a tautology. If $g(x) \notin f_q$, then there exists y with $|y| \leq q(|g(x)|)$ and $f(y) = g(x) = \neg h(x \wedge \neg x)$. Hence $h(x \wedge \neg x) \in B$, a contradiction. Thus $g(x) \in f_q$.

$3 \Rightarrow 1$: Choose B according to 1. Consider

$$B' = \{x \mid x \in B \text{ or } \exists z\ |z| \leq |x| \text{ and } x \vee z \in B\}$$

and observe $B' \in \mathrm{NP}$, $B \subseteq B'$, and $B' \cap \mathrm{SAT} = \emptyset$. Let M be an NP-machine with $L(M) = B'$ and running time q for a polynomial q.

Let f be defined as follows and observe that f is a pps.

$$\langle x, z \rangle \mapsto \begin{cases} x & M \text{ accepts } \neg x \text{ on path } z \text{ or } (|z| \geq 2^{|x|} \text{ and } x \text{ is a tautology}) \\ \text{True} & \text{otherwise.} \end{cases}$$

Let q' be a polynomial such that $|\neg x| \leq q'(|x|)$ for every x. Moreover, choose $r(n) = 2 \cdot (q(q'(n)) + n + 1)$. By 3, f_r is P-producible via some $g \in \mathrm{FP}$ with $|g(x)| \geq |x|$. for all x. Consider the length-increasing function $h \in \mathrm{FP}$ with $h(x) = \neg g(x) \vee x$. We show $\mathrm{SAT} \leq^{\mathrm{pp}}_{\mathrm{m,li}} (\mathrm{SAT}, \overline{\mathrm{SAT} \cup B})$ via h, which implies $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} \mathrm{SAT} \cup B$ via h.

As $g(x)$ is a tautology, $x \in \mathrm{SAT} \Leftrightarrow h(x) \in \mathrm{SAT}$. It remains to show that $x \notin \mathrm{SAT} \Rightarrow h(x) \notin B$.

Let $x \notin \mathrm{SAT}$. If $h(x) = \neg g(x) \vee x \in B$, then due to $|x| \leq |\neg g(x)|$ it holds $\neg g(x) \in B'$. Hence, there is some path z such that M accepts $\neg g(x)$ on path z. Thus $|z| \leq q(q'(|g(x)|))$. Consequently, $f(\langle g(x), z \rangle) = g(x)$ and $|\langle g(x), z \rangle| \leq r(|g(x)|)$, in contradiction to $g(x) \in f_r$. □

The following corollary summarizes the state of knowledge on the hypothesis studied in this subsection. It contains the statements from Theorem 3.4 and further equivalent formulations. The statement 3.5.6 is interesting, as it says that all sets in NP can be $\leq^{\mathrm{p}}_{\mathrm{m,li}}$-reduced to SAT in a way that avoids values in B. We do not have a similar characterization in the case of $\leq^{\mathrm{p}}_{\mathrm{m}}$ reducibility. Moreover, statement 3.5.9 shows a connection to the hardness of certain disjoint NP-pairs. As mentioned before, the equivalence $1 \Leftrightarrow 11$ was shown in [GHPT14].

Corollary 3.5 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
2. *There exists* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
3. *For all* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
4. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$.
5. f_q *is P-producible for all pps* f *and all polynomials* q.
6. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *the pair* $(\mathrm{SAT}, \overline{\mathrm{SAT} \cup B})$ *is* $\leq^{\mathrm{pp}}_{\mathrm{m,li}}$*-hard for* NP.
7. *There exists* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *the pair* $(A, \overline{A \cup B})$ *is* $\leq^{\mathrm{pp}}_{\mathrm{m,li}}$*-hard for* NP.
8. *For all* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *the pair* $(A, \overline{A \cup B})$ *is* $\leq^{\mathrm{pp}}_{\mathrm{m,li}}$*-hard for* NP.

9. *For all* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $(\mathrm{SAT}, \emptyset) \leq^{\mathrm{p}}_{\mathrm{sm,li}} (A, B)$.

10. *All disjoint* NP*-pairs* (A, B) *with* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *are* $\leq^{\mathrm{p}}_{\mathrm{sm,li}}$*-hard for* $\mathrm{NP} \times \{\emptyset\}$.

11. *For every language* $L \in \mathrm{NP}$ *that is disjoint from* SAT*, there is a polynomial-time refuter that almost everywhere distinguishes* L *from* $\overline{\mathrm{SAT}}$.

Proof The statements 1, 4, 5, and 11 are equivalent by Theorem 3.4. Moreover, the proof of the implication 3 $\Rightarrow$ 1 of Theorem 3.4 consists of proofs for the implications 5 $\Rightarrow$ 6 and 6 $\Rightarrow$ 1 of this corollary. The following implications are trivial: 2 $\Rightarrow$ 1, 3 $\Rightarrow$ 2, 7 $\Rightarrow$ 2, 8 $\Rightarrow$ 3, and 8 $\Rightarrow$ 7. It holds 9 $\Leftrightarrow$ 10 as $(\mathrm{SAT}, \emptyset)$ is $\leq^{\mathrm{p}}_{\mathrm{sm,li}}$-complete for $\mathrm{NP} \times \{\emptyset\}$. Moreover, 8 $\Leftrightarrow$ 9 holds as SAT is $\leq^{\mathrm{p}}_{\mathrm{m,li}}$-hard for NP and $\mathrm{SAT} \leq^{\mathrm{pp}}_{\mathrm{m,li}} (A, \overline{A \cup B})$ via some function f if and only if $(\mathrm{SAT}, \emptyset) \leq^{\mathrm{p}}_{\mathrm{sm,li}} (A, B)$ via the same function f.

Thus it suffices to prove 6 $\Rightarrow$ 8. Let $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ and $B \in \mathrm{NP}$ be disjoint. Then $\mathrm{SAT} \leq^{\mathrm{p}}_{\mathrm{m,li}} A$ via some length-increasing $f \in \mathrm{FP}$. Define $B' = f^{-1}(B)$. Then $B' \leq^{\mathrm{p}}_{\mathrm{m,li}} B$ via f and thus $B' \in \mathrm{NP}$. Therefore, 6 yields that $(\mathrm{SAT}, \overline{\mathrm{SAT} \cup B'})$ is $\leq^{\mathrm{pp}}_{\mathrm{m,li}}$-hard for NP. Observing $(\mathrm{SAT}, \overline{\mathrm{SAT} \cup B'}) \leq^{\mathrm{pp}}_{\mathrm{m,li}} (A, \overline{A \cup B})$ via f finishes the proof. □

3.2 Polynomial-Time Reducibility

We consider the hypothesis that the union of SAT with a disjoint $B \in \mathrm{NP}$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP. This is equivalent to $\mathrm{H}_{\mathrm{union}}$. We prove several characterizations of $\mathrm{H}_{\mathrm{union}}$, e.g., one in terms of the coNP-completeness of the set of hard formulas of pps.

In the following theorem, the equivalence 1 $\Leftrightarrow$ 2 was shown in [GPSS06].

Theorem 3.6 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.

2. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.

3. f_q *is* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-complete for* coNP *for all pps* f *and all polynomials* q.

Proof "1 $\Leftrightarrow$ 2": Holds by [GPSS06].

"1 $\Rightarrow$ 3": By definition, $f_q = \{x \in \mathrm{TAUT} \mid \neg\exists z \in \Sigma^{\leq q(|x|)} f(z) = x\}$ and hence $f_q \in \mathrm{coNP}$. Let

$$B = \{x \in \Sigma^* \mid \exists z \in \Sigma^{\leq q(|\neg x|)} f(z) = \neg x\}.$$

Observe that $B \in \mathrm{NP}$ and $\mathrm{SAT} \cap B = \emptyset$. By assumption, $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ and hence $\overline{\mathrm{SAT} \cup B}$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP. It holds that

$$\begin{aligned} \overline{\mathrm{SAT} \cup B} \;=\; \overline{\mathrm{SAT}} - B \;&=\; \{x \in \overline{\mathrm{SAT}} \mid \neg\exists z \in \Sigma^{\leq q(|\neg x|)} f(z) = \neg x\} \\ &=\; \{x \in \Sigma^* \mid \neg x \in \mathrm{TAUT} \wedge \neg\exists z \in \Sigma^{\leq q(|\neg x|)} f(z) = \neg x\}. \end{aligned}$$

Thus $x \in \overline{\mathrm{SAT} \cup B} \Leftrightarrow \neg x \in f_q$, which shows $\overline{\mathrm{SAT} \cup B} \leq^{\mathrm{p}}_{\mathrm{m}} f_q$. Hence f_q is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP.

"3 $\Rightarrow$ 1": Let $B \in \mathrm{NP}$ such that $\mathrm{SAT} \cap B = \emptyset$ and let M be a nondeterministic polynomial-time machine that accepts B. Choose a polynomial q such that for all $x \in \Sigma^*$ and all accepting paths y of $M(\neg x)$ it holds that $|\langle x, y\rangle| \leq q(|x|)$. Let

$$f(z) = \begin{cases} x, & \text{if } z = \langle x, y\rangle,\ |y| < 2^{|x|}, \text{ and } y \text{ is an accepting path of } M(\neg x) \\ x, & \text{if } z = \langle x, y\rangle,\ |y| = 2^{|x|}, \text{ and } x \in \mathrm{TAUT} \\ \mathrm{True}, & \text{otherwise.} \end{cases}$$

Observe that f is a pps. By assumption, the set

$$f_q = \{x \in \mathrm{TAUT} \mid \neg\exists z \in \Sigma^{\leq q(|x|)} f(z) = x\}$$

is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP. Observe $f_q \cap \Sigma^{\geq n} = \{x \in \mathrm{TAUT} \mid \neg x \notin B\} \cap \Sigma^{\geq n}$ for sufficiently large $n \in \mathbb{N}$. Hence for all $x \in \Sigma^{\geq n}$ it holds that $x \in f_q \Leftrightarrow \neg x \in \overline{\mathrm{SAT} \cup B}$. In the case $\overline{\mathrm{SAT} \cup B} \neq \emptyset$ this shows $f_q \leq^{\mathrm{p}}_{\mathrm{m}} \overline{\mathrm{SAT} \cup B}$ and hence $\mathrm{SAT} \cup B$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP.

It remains to argue that the case $\overline{\mathrm{SAT} \cup B} = \emptyset$ is not possible. If $\overline{\mathrm{SAT} \cup B} = \emptyset$, then NP = coNP and hence there exists a polynomially bounded pps f'. Thus for some polynomial q' it holds $f'_{q'} = \emptyset$, which is not $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP, in contradiction to our assumption. □

The following corollary summarizes the state of knowledge on the hypothesis $\mathrm{H}_{\mathrm{union}}$. It contains the statements from Theorem 3.6 and further equivalent formulations. The equivalence of statements 1, 3, 5, 7, 10, 11 was shown in [GPSS06].

Corollary 3.7 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
2. *There exists* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
3. *There exists* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
4. *For all* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
5. *For all* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
6. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
7. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
8. f_q *is* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-complete for* coNP *for all pps* f *and all polynomials* q.
9. f_{id} *is* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-complete for* coNP *for all* f *that are proof systems for* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-complete sets for* coNP.
10. *For all paddable* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *with* $A \cap B = \emptyset$ *it holds that* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.
11. *There exists a paddable* $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *such that for all paddable* $B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.

Proof 1, 3, 5, 7, 10, and 11 are equivalent by [GPSS06]. 7 and 8 are equivalent by Theorem 3.6. The implications $5 \Rightarrow 4 \Rightarrow 2 \Rightarrow 3$ and $7 \Rightarrow 6$ are trivial.

"$6 \Rightarrow 4$": We show the contraposition. Let $A \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$ and $B \in \mathrm{NP}$ such that $A \cap B = \emptyset$ and $A \cup B \notin \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$. The sets $0A \cup 1B$ and $1A \cup 0B \cup \{\varepsilon\}$ are disjoint and belong to $\mathrm{NPC}^{\mathrm{p}}_{\mathrm{m,li}}$. Their union is

$$0(A \cup B) \cup 1(A \cup B) \cup \{\varepsilon\} \leq^{\mathrm{p}}_{\mathrm{m}} A \cup B,$$

where the ε is needed for the case $A \cup B = \Sigma^*$. Hence this union is not in $\mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$.

"5⇒9": Let $f \in \mathrm{FP}$ such that $L = \mathrm{ran}(f)$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP. By definition,

$$f_{\mathrm{id}} = \{x \in L \mid \neg\exists z \in \Sigma^{\leq |x|} f(z) = x\}.$$

Let

$$B = \{x \in \Sigma^* \mid \exists z \in \Sigma^{\leq |x|} f(z) = x\}.$$

Observe that $f_{\mathrm{id}} \in \mathrm{coNP}$ and $B \in \mathrm{NP}$. Moreover, $\overline{L}$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP and $\overline{L} \cap B = \emptyset$. Thus our assumption implies that $\overline{L} \cup B$ is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for NP. The observation $f_{\mathrm{id}} = L - B = \overline{\overline{L} \cup B}$ completes the proof.

"$9 \Rightarrow 1$": We prove the contraposition. Let $B \in \mathrm{NP}$ such that $\mathrm{SAT} \cap B = \emptyset$ and $\mathrm{SAT} \cup B \notin \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$. Choose a polynomial q and a nondeterministic machine M that accepts B in time q. Let

$$\mathrm{TAUT}' = \{\langle x, 0^{q(|\neg x|)}\rangle \mid x \in \mathrm{TAUT})\}$$

and observe that TAUT' is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP. Let

$$f'(z) = \begin{cases} \langle x, 0^{q(|\neg x|)}\rangle, & \text{if } z = \langle x, y\rangle,\ |y| = q(|\neg x|),\ y \text{ is an accepting path of } M(\neg x) \\ \langle x, 0^{q(|\neg x|)}\rangle, & \text{if } z = \langle x, y\rangle,\ |y| > q(|\neg x|),\ |y| \geq 2^{|x|}, \text{ and } x \in \mathrm{TAUT} \\ t', & \text{otherwise, where } t' \text{ is a fixed element from } \mathrm{TAUT}'. \end{cases}$$

Observe that f' is a proof system for TAUT'. We claim that

$$f'_{\mathrm{id}} \;=\; \{\langle x, 0^{q(|\neg x|)}\rangle \mid x \in \mathrm{TAUT} \text{ and } \neg x \notin B\} - \{t'\}. \tag{3}$$

"$\subseteq$": Let $x' \in f'_{\mathrm{id}}$. Hence $x' \in \mathrm{TAUT}'$ and $\neg\exists z \in \Sigma^{\leq |x'|} f'(z) = x'$. Thus $x' = \langle x, 0^{q(|\neg x|)}\rangle$ for some $x \in \mathrm{TAUT}$. Assume x' does not belong to the rhs of (3). Note that $x' \neq t'$, since $f'(\varepsilon) = t'$ and $|\varepsilon| < 4 \leq |t'|$. It follows that $\neg x \in B$. Hence $M(\neg x)$ has an accepting path y with $|y| = q(|\neg x|)$. Thus for $z = \langle x, y\rangle$ it holds that $|z| = 2(|x| + q(|\neg x|) + 2) = |x'|$ and $f'(z) = x'$. This contradicts the observation $\neg\exists z \in \Sigma^{\leq |x'|} f'(z) = x'$.

"$\supseteq$": Let x' belong to the rhs of (3). Hence $t' \neq x' = \langle x, 0^{q(|\neg x|)}\rangle$ for some $x \in \mathrm{TAUT}$ and $\neg x \notin B$. It follows that $x' \in \mathrm{TAUT}'$. Assume $x' \notin f'_{\mathrm{id}}$, i.e., $\exists z \in \Sigma^{\leq |x'|} f'(z) = x'$. From $\neg x \notin B$ it follows that $f'(z)$ is not defined according to the first line in the definition of f'. It is also not defined according to the second line, since otherwise $|z| = |\langle x, y\rangle| = 2(|x| + |y| + 2) > 2(|x| + q(|\neg x|) + 2) = |x'|$ contradicting $z \in \Sigma^{\leq |x'|}$. Hence $f'(z)$ is defined according to the third line, but this contradicts $t' \neq x'$.

This finishes the proof of (3). It follows that

$$x' \in f'_{\mathrm{id}} \;\Leftrightarrow\; x' \neq t' \wedge x' = \langle x, 0^{q(|\neg x|)}\rangle \wedge \neg x \in \overline{\mathrm{SAT} \cup B}.$$

Hence $f'_{\mathrm{id}} \leq^{\mathrm{p}}_{\mathrm{m}} \overline{\mathrm{SAT} \cup B}$ (observe that $\mathrm{SAT} \cup B \neq \emptyset$). Therefore, f'_{id} is not $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for coNP. □

3.3 Infinitely Often P/poly Reducibility

We consider the hypothesis that the union of SAT with a disjoint $B \in \mathrm{NP}$ is $\leq^{\text{io-p/poly}}_{\mathrm{m}}$-complete for NP. This is equivalent to say that the union of disjoint sets from $\mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ is $\leq^{\text{io-p/poly}}_{\mathrm{m}}$-complete for NP. We prove several characterizations of this hypothesis, e.g., NP ≠ coNP.

Theorem 3.8 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}^{\text{io-p/poly}}_{\mathrm{m}}$.
2. *For all* $A, B \in \mathrm{NPC}^{\mathrm{p}}_{\mathrm{m}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}^{\text{io-p/poly}}_{\mathrm{m}}$.
3. $\mathrm{NP} \neq \mathrm{coNP}$ *(i.e., polynomially bounded pps do not exist).*

Proof The implication $2 \Rightarrow 3$ can be shown by proving the contraposition: NP = coNP implies $\overline{\text{SAT}} \in \text{NP}$, but $\text{SAT} \cup \overline{\text{SAT}} \notin \text{NPC}_\text{m}^{\text{io-p/poly}}$. We argue for the implication $1 \Rightarrow 2$ and show that from 1 it even follows that for all $A \in \text{NPC}_\text{m}^\text{p}$ and all $B \in \text{NP}$ with $A \cap B = \emptyset$ it holds $A \cup B \in \text{NPC}_\text{m}^{\text{io-p/poly}}$. Let $A \in \text{NPC}_\text{m}^\text{p}$ and $B \in \text{NP}$ be disjoint. Then $\text{SAT} \leq_\text{m}^\text{p} A$ via some $f \in \text{FP}$. Define $B' = f^{-1}(B)$. Then $B' \leq_\text{m}^\text{p} B$ via f and thus $B' \in \text{NP}$. Hence $\text{SAT} \cup B' \in \text{NPC}_\text{m}^{\text{io-p/poly}}$ by 1. Moreover, $\text{SAT} \cup B' \leq_\text{m}^\text{p} A \cup B$ via f. Then by Proposition 2.7, for all C with $C \leq_\text{m}^{\text{io-p/poly}} \text{SAT} \cup B'$ it holds $C \leq_\text{m}^{\text{io-p/poly}} A \cup B$, wherefore $A \cup B \in \text{NPC}_\text{m}^{\text{io-p/poly}}$.

Finally, we consider the implication $3 \Rightarrow 1$. Assume NP $\neq$ coNP. First we show that for each pps f and each polynomial p it holds $\text{TAUT} \cap f_p \neq \emptyset$:

It follows from 3 that $\overline{\text{SAT}} \notin \text{NP}$. Assume there exists a pps f and a polynomial p such that for all $\varphi \in \text{TAUT}$ it holds $\varphi \in f(\Sigma^{\leq p(|\varphi|)})$. Then $B := \{(\varphi, x) \mid \varphi \in \text{TAUT}, f(x) = \varphi\} \in \text{P}$ and $\varphi \in \text{TAUT}$ if and only if there exists some $x \in \Sigma^{\leq p(|\varphi|)}$ with $(\varphi, x) \in B$. Hence $\text{TAUT} \in \text{NP}$ and thus $\overline{\text{SAT}} \in \text{NP}$, which is a contradiction to NP $\neq$ coNP.

Let $B \in \text{NP}$ be disjoint to SAT. We show $\text{SAT} \leq_\text{m}^{\text{io-p/poly}} \text{SAT} \cup B$. According to Proposition 2.12 it suffices to prove the existence of an $f \in \text{FP/poly}$ which for infinitely many $n \in \mathbb{N}$ satisfies $x \in \text{SAT} \Leftrightarrow f(x) \in \text{SAT} \cup B$ for all $x \in \Sigma^n$. We define

$$f(x) = \begin{cases} x \vee \neg w_{|x|} & \text{if } w_{|x|} \neq \varepsilon \\ x & \text{otherwise,} \end{cases}$$

where w_n is the advice string of length n.

Now we construct the advice strings. Let $p_0, p_1, \ldots$ be an enumeration of all polynomials and $f_0, f_1, \ldots$ an enumeration of all pps. Note that we do not require these enumerations to be effective. In the following we construct sets $T_0 \subsetneq T_1 \subsetneq \ldots$ that are subsets of TAUT with at most one element of any length.

1. Let $n = 1$, $i = 0$, and $T_0 = \emptyset$.
2. For $j = 0$ to i:
   (a) Choose the smallest $x \in \Sigma^{\geq n} \cap \text{TAUT}$ in quasi-lexicographical order with $x \notin f_j(\Sigma^{\leq p_i(|x|)})$.
   (b) Set $T_n = T_{n-1} \cup \{x\}$ and $n = |x| + 1$.
3. Increment i and go to step 2.

Note that due to $\text{TAUT} \cap f_p \neq \emptyset$ for each pps f and each polynomial p the step 2(a) can always be executed. Let $T = \lim_{n \in \mathbb{N}} T_n$. By construction, $T \cap f_p \neq \emptyset$ for each pps f and each polynomial p. Now define the advice string w_n to be the unique word of length n in T if T contains a word of length n. Otherwise define $w_n = \varepsilon$.

For a contradiction, assume that for almost all $n \in \mathbb{N}$ there exists $x \in \Sigma^n$ with $x \in \text{SAT} \Leftrightarrow f(x) \notin \text{SAT} \cup B$. As $(x \in \text{SAT} \Leftrightarrow f(x) \in \text{SAT})$ and $\text{SAT} \subseteq \text{SAT} \cup B$, there exists $k \in \mathbb{N}$ such that for all $n \geq k$ there exists a word x_n of length n with $x_n \notin \text{SAT}$ and $f(x_n) \in B$.

Let M be a nondeterministic polynomial-time TM accepting B in time r for a polynomial r. Define the pps

$$f'(x, y, z) = \begin{cases} y & \text{if } M \text{ accepts } (x \vee \neg y) \text{ via path } z,\ |x| = |y| \geq k, \text{ and } 2^{|x|} > |z| \\ x & \text{if } 2^{|x|} \leq |z| \text{ and } x \in \text{TAUT} \\ \text{True} & \text{otherwise.} \end{cases}$$

Let q be a polynomial such that for all $x, y \in \Sigma^n$ for an $n \in \mathbb{N}$ it holds $|x \vee \neg y| \leq q(n)$. We show that all tautologies $y \in T$ have proofs of length $\leq 2 \cdot (2|y| + r(q(|y|)) + 1)$ in f'. It suffices

to show this for each tautology $y \in T$ with $n := |y| \geq k$. Recall $x_n \notin \mathrm{SAT}$, $|x_n| = n$, and $f(x_n) = x_n \vee \neg y \in B$. Choose an accepting path z of M on input $x_n \vee \neg y$. By definition, $f'(x_n, y, z) = y$ and $|(x_n, y, z)| \leq 2 \cdot (2n + r(q(n)) + 1)$, a contradiction as T intersects with f_p for each pps f and each polynomial p. □

The following corollary summarizes the state of knowledge on the hypothesis studied in this subsection. It contains the statements from Theorem 3.8 and further equivalent formulations.

Corollary 3.9 *The following statements are equivalent:*

1. *For all* $B \in \mathrm{NP}$ *with* $\mathrm{SAT} \cap B = \emptyset$ *it holds* $\mathrm{SAT} \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
2. *There exists* $A \in \mathrm{NPC}_{\mathrm{m,li}}^{\mathrm{p}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
3. *There exists* $A \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ *such that for all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
4. *For all* $A \in \mathrm{NPC}_{\mathrm{m,li}}^{\mathrm{p}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
5. *For all* $A \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ *and all* $B \in \mathrm{NP}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
6. *For all* $A, B \in \mathrm{NPC}_{\mathrm{m,li}}^{\mathrm{p}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
7. *For all* $A, B \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ *with* $A \cap B = \emptyset$ *it holds* $A \cup B \in \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.
8. $\mathrm{NP} \neq \mathrm{coNP}$.

Proof By Theorem 3.8, the statements 1, 7, and 8 are equivalent. Furthermore, in the proof of Theorem 3.8 the proof of the implication 1 ⇒ 2 also contains a proof for the implication 1 ⇒ 5 of this corollary. The following implications are trivial: 1 ⇒ 2, 2 ⇒ 3, 4 ⇒ 2, 5 ⇒ 4, and 7 ⇒ 6.

The implication 6 ⇒ 8 can be proven by showing the contraposition. If NP = coNP, then $\mathrm{SAT}, \overline{\mathrm{SAT}} \in \mathrm{NPC}_{\mathrm{m,li}}^{\mathrm{p}}$, but $\mathrm{SAT} \cup \overline{\mathrm{SAT}} = \Sigma^* \notin \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$.

To finish the proof, it suffices to show 3 ⇒ 8. We prove the contraposition. Assume NP = coNP. Let $A \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p}}$ and choose $B = \overline{A} \in \mathrm{coNP} = \mathrm{NP}$. Then $A \cup B = \Sigma^* \notin \mathrm{NPC}_{\mathrm{m}}^{\text{io-p/poly}}$. □

4 An Oracle with P = UP, $\neg \mathrm{H}_{\mathrm{cpair}}$, and no Complete Sets for NP ∩ coNP

In this section we construct an oracle O relative to which (i) P = UP and hence UP has $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets, (ii) $\neg \mathrm{H}_{\mathrm{cpair}}$, and (iii) NP ∩ coNP has no $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets. This answers open questions asked by Pudlák [Pud17], who lists a number of hypotheses and asks for oracles showing that any pairs of corresponding relativized conjectures are different. Our oracle shows that (i) DisjNP does not imply UP in a relativized way and (ii) NP ∩ coNP does not imply UP in a relativized way, where DisjNP is $\neg \mathrm{H}_{\mathrm{cpair}}$ and UP (resp., NP ∩ coNP) is the assertion that UP (resp., NP ∩ coNP) does not have $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets.

In particular, the relativizations of the hypotheses DisjNP and UP are different. Since DisjNP implies several further hypotheses, the following hypotheses are also different from UP relative

to oracle O: CON, $\mathsf{CON} \vee \mathsf{SAT}$, RFN_1[4], and $\mathsf{P} \neq \mathsf{NP}$. We refer to [Pud17] for the definition of these hypotheses and consider CON more closely. CON is the assertion that no P-optimal propositional proof system exists and as it is implied by $\neg \mathrm{H}_{\mathrm{cpair}}$, it holds relative to O. Thus the non-existence of a P-optimal proof system does not imply the non-existence of a $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete set for UP in a relativized way. This is of particular interest as the converse implication holds relative to all oracles [KMT03]. So the relativized hypotheses UP and CON are different, but not independent.

The proof of the following theorem uses ideas by Rackoff [Rac82].

Theorem 4.1 *There exists an oracle O with the following properties.*

1. DisjNP^O *has no pair that is* $\leq^{\mathrm{p},O}_{\mathrm{m}}$*-hard for* $\mathrm{NP}^O \cap \mathrm{coNP}^O$.
2. $\mathrm{P}^O = \mathrm{UP}^O$.

As an immediate consequence we obtain:

Corollary 4.2 *The following holds for the oracle O constructed in Theorem 4.1.*

1. DisjNP^O *has no* $\leq^{\mathrm{pp},O}_{\mathrm{m}}$*-complete pairs.*
2. *Relative to O there are no optimal pps.*
3. $\mathrm{NP}^O \cap \mathrm{coNP}^O$ *has no* $\leq^{\mathrm{p},O}_{\mathrm{m}}$*-complete sets.*
4. UP^O *has* $\leq^{\mathrm{p},O}_{\mathrm{m}}$*-complete sets.*

Proof of Theorem 4.1 Let $M_0, M_1, \ldots$ be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines. Let $F_0, F_1, \ldots$ be a standard enumeration of deterministic, polynomial-time oracle Turing transducers. Choose a $C \subseteq \mathbb{N}$ that is $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete for PSPACE such that all elements in C have odd length. Let $e(0) = 2$ and $e(n+1) = 2^{2^{e(n)}}$ for $n \in \mathbb{N}$. Define the following sets for $p \in \mathbb{P}^{\geq 3}$ and an oracle $D \subseteq \mathbb{N}$.

$$\begin{aligned} A_p^D &= \{0^{e(p^k)} \mid k \geq 1 \text{ and there exists an even } x \in D \text{ such that } |x| = e(p^k)\} \cup \overline{\{0^{e(p^k)} \mid k \geq 1\}} \\ B_p^D &= \{0^{e(p^k)} \mid k \geq 1 \text{ and there exists an odd } x \in D \text{ such that } |x| = e(p^k)\} \end{aligned}$$

Note that if for each $k \geq 1$ it holds

$$\exists \text{ an even } x \in D \cap \Sigma^{e(p^k)} \;\Leftrightarrow\; \neg\exists \text{ an odd } x \in D \cap \Sigma^{e(p^k)},$$

then $A_p^D = \overline{B_p^D}$ and hence $A_p^D \in \mathrm{NP}^D \cap \mathrm{coNP}^D$.

Preview of construction: On the one hand, the construction tries to prevent that $L(M_i)$ and $L(M_j)$ for $i \neq j$ are disjoint. If this is not possible, M_i and M_j inherently accept disjoint sets. In this case, for a suitable $p \in \mathbb{P}^{\geq 3}$, the construction makes sure that A_p is in $\mathrm{NP} \cap \mathrm{coNP}$ and does not $\leq^{\mathrm{p}}_{\mathrm{m}}$-reduce to $(L(M_i), L(M_j))$. This prevents the existence of disjoint NP-pairs that are $\leq^{\mathrm{pp},O}_{\mathrm{m}}$-hard for $\mathrm{NP}^O \cap \mathrm{coNP}^O$. On the other hand, the construction tries to prevent that M_i has the uniqueness property, i.e., for all x, the computation $M_i(x)$ has at most one accepting path. If this is not possible, then M_i inherently has the uniqueness property, which enables us to show that $L(M_i)$ is in P relative to the final oracle.

During the oracle construction we maintain a growing collection of properties that we demand in the further construction. The collection is represented by a function t and if an oracle

[4]Khaniki [Kha18] recently proved $\mathsf{RFN}_1 \Rightarrow \mathsf{CON} \vee \mathsf{SAT}$ and thus the two hypotheses RFN_1 and $\mathsf{CON} \vee \mathsf{SAT}$ are equivalent.

satisfies the properties defined by t, then we call it t-valid. More precisely, we start with the nowhere defined function $t_0 : \mathbb{N} \times \mathbb{N} \to \mathbb{P}^{\geq 3} \cup \{0, 1\}$, which defines no property. We successively continue this function and obtain $t_1, t_2, \ldots$, which have a finite, but growing domain, and which belong to the set

$$\mathcal{T} = \{t : \mathbb{N} \times \mathbb{N} \to \mathbb{P}^{\geq 3} \cup \{0, 1\} \mid \mathrm{dom}(t) \text{ is finite and } t \text{ is injective on } \{x \mid t(x) > 1\}\}.$$

At the end of the construction we reach the total function $t = \lim_{i \to \infty} t_i$.

An oracle $w \in \Sigma^*$ is t-valid, where $t \in \mathcal{T}$, if the following hold:

V1: For all $(i, j) \in \mathrm{dom}(t)$, if $i \neq j$ and $t(i, j) = 0$, then there exists z such that $M_i^w(z)$ and $M_j^w(z)$ definitely accept.
(meaning: $L(M_i^v) \cap L(M_j^v) \neq \emptyset$ for all $v \sqsupseteq w$)

V2: For all $(i, j) \in \mathrm{dom}(t)$, if $i \neq j$ and $t(i, j) = p \in \mathbb{P}^{\geq 3}$, then

1. $A_p^w \cap B_p^w = \emptyset$
2. for all $k \geq 1$ with $|w| > z$ for all z of length $e(p^k)$, there exists $x \in w$ with $|x| = e(p^k)$.

(meaning: relative to the final oracle it holds $A_p = \overline{B_p}$)

V3: For all $(i, j) \in \mathrm{dom}(t)$, if $i = j$ and $t(i, i) = 0$, then there exists z such that $M_i^w(z)$ has more than one path that definitely accepts.
(meaning: M_i^v violates the uniqueness property for all $v \sqsupseteq w$)

V4: If $x < |w|$ and $|x|$ is odd, then $x \in w \Leftrightarrow x \in C$.
(meaning: w and C coincide for words of odd length)

V5: If $x \in w$ and $|x|$ is even, then there exists $n \geq 1$ such that $|x| = e(n)$.
(meaning: if a word in w has even length, then it has length $e(n)$ for some n)

This definition directly implies the following claims.

Claim 4.3 *Let $t, t' \in \mathcal{T}$ such that t' is a continuation of t. If w is t'-valid, then w is t-valid.*

Claim 4.4 *Let $t \in \mathcal{T}$ and $u \sqsubseteq v \sqsubseteq w$ be oracles such that u and w are t-valid. Then v is t-valid.*

Claim 4.5 *For every $t \in \mathcal{T}$ and every t-valid w there exists $b \in \{0, 1\}$ such that wb is t-valid. More precisely, for $z = |w|$ the following holds.*

1. *If $|z|$ is odd, then for each $b \in \{0, 1\}$ it holds that wb is t-valid if and only if $b = C(z)$.*
2. *If $|z|$ is even, then the following holds.*
   (a) *If $|z| = e(p^k)$ for some prime $p \in \mathrm{ran}(t)$ and there exists no word $x \in w$ of length $e(p^k)$, then $w1$ is t-valid.*
   (b) *If $z \neq 1^{e(p^k)}$ for all primes $p \in \mathrm{ran}(t)$ and all $k \geq 1$ or if there exists a word $x \in w$ with $|x| = |z|$, then $w0$ is t-valid.*

Oracle construction: Let t_0 be the nowhere defined function and $w_0 = \varepsilon$, which is t_0-valid. We construct a sequence of partially defined oracles $w_0 \sqsubsetneq w_1 \sqsubsetneq \cdots$ and a sequence $t_0, t_1, \ldots$ of functions from $\mathcal{T}$ such that w_i is t_i-valid and t_{i+1} is a continuation of t_i for all i. The final oracle is $O = \lim_{i \to \infty} w_i$. Each step treats the first task in our task list T and removes this and

possibly other tasks from the list. At the beginning, T is an enumeration of all $(i,j) \in \mathbb{N}^2$ and all $(i,j,r) \in \mathbb{N}^3 - \{(i,i,r) \mid i,r \in \mathbb{N}\}$ in an order having the property that (i,j) appears earlier than (i,j,r). We describe step $s > 0$, which starts with a t_{s-1}-valid oracle w_{s-1} and extends it to a t_s-valid $w_s \supsetneq w_{s-1}$.

- task (i,j) with $i \neq j$: Let $t' = t_{s-1} \cup \{(i,j) \mapsto 0\}$. If there exists a t'-valid $v \supsetneq w_{s-1}$, then let $t_s = t'$, $w_s = v$, and remove all tasks $(i,j,\cdot)$ from T. Otherwise choose $p \in \mathbb{P}^{\geq 3} - \mathrm{ran}(t_{s-1})$ such that $p > |w_{s-1}|$ and let $t_s = t_{s-1} \cup \{(i,j) \mapsto p\}$ and $w_s = w'$ for a t_s-valid $w' \supsetneq w_{s-1}$, which exists by Claim 4.5, since w_{s-1} is t_s-valid by the choice of p.
  (meaning: force $L(M_i^O) \cap L(M_j^O) \neq \emptyset$ if possible, otherwise choose a suitable prime p and make sure that $A_p = \overline{B_p}$ with respect to the final oracle; corresponds to V1 and V2 in the definition of t-valid)

- task (i,i): Let $t' = t_{s-1} \cup \{(i,i) \mapsto 0\}$. If there exists a t'-valid $v \supsetneq w_{s-1}$, then let $t_s = t'$ and $w_s = v$. Otherwise $t_s = t_{s-1} \cup \{(i,i) \mapsto 1\}$ and $w_s = w'$ for a t_s-valid $w' \supsetneq w_{s-1}$, which exists by Claim 4.5, since w_{s-1} is t_s-valid.
  (meaning: destroy the uniqueness property of M_i if possible, otherwise define $t_s(i,i) = 1$, which indicates that M_i inherently has the uniqueness property; corresponds to V3 in the definition of t-valid)

- task (i,j,r) with $i \neq j$: It holds that $t_{s-1}(i,j) = p \in \mathbb{P}^{\geq 3}$. Let $t_s = t_{s-1}$ and choose a t_s-valid $w_s \supsetneq w_{s-1}$ such that for a suitable 0^n at least one of the following holds.
  - $0^n \in A_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_i^{w_s}$
  - $0^n \in B_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_j^{w_s}$

  (meaning: F_r does not realize a reduction $A_p \leq_{\mathrm{m}}^{\mathrm{p}} (L(M_i), L(M_j)))$

Claim 4.6 *For all $s \geq 1$, the construction of w_s and t_s in step s is possible and w_s is t_s-valid.*

Proof For a contradiction, assume that the statement is wrong and choose the smallest step s where the claim fails. There are two cases:

Step s treats task (i,j) for $i,j \in \mathbb{N}$: Hence $t_{s-1}(i,j)$ is not defined, since it can only be defined by the unique treatment of task (i,j). Therefore, t' can be defined as specified, which shows that the construction in step s is possible (cf. description of task (i,j)).

Step s treats task (i,j,r) with $i \neq j$: Here $t_s = t_{s-1}$ and $t_s(i,j) = p \in \mathbb{P}$, since otherwise the earlier task (i,j) had removed (i,j,r). We argue that the choice of the specified t_s-valid w_s is possible, which shows that the construction in step s is possible and which contradicts the assumption.

Choose k large enough such that for $n = e(p^k)$ it holds that n is large enough to apply Corollary 2.15, w_{s-1} is not defined for all words of length $\geq n$ and $e(n+1) > (n^r + r)^{i+j} + i + j$. Choose a t_s-valid $w' \supseteq w_{s-1}$ that is defined for all words of length $< n$ and undefined for all words of length $\geq n$ (w' exists by Claim 4.5). By Corollary 2.15 applied for $D = C \cup w'$, there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that at least one of the statements 1-3 holds.

If statement 1 holds, then define w_s as the minimal $w'' \supsetneq w'$ that satisfies V4, that contains x, and that is defined for all words of length $\leq (n^r + r)^i + i$. The latter makes sure that the computations $F_r^{w_s}(0^n)$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ are defined and will not change when we extend w_s. As $e(n+1) > (n^r + r)^i + i$ and x is the only word of length n in w_s, the oracle w_s satisfies V2. Furthermore, $w_s = w' \cup \{x\} \cup (C \cap \Sigma^{\leq (n^r+r)^i+i})$ when interpreting w' and w_s as sets, i.e., x is the only word of even length that we added to the oracle. Recall that w' is a t_s-valid oracle defined

for all words of length $< n$ and undefined for all other words. We show that w_s is t_s-valid as well. We have already seen that the oracle satisfies V2. It still satisfies V5. Moreover, V4 is satisfied by the definition of w_s. The remaining conditions V1 and V3 are not affected by the extension $w' \sqsubsetneq w_s$. Hence w_s is t_s-valid. $0^n \in A_p^{w_s}$, since $x \in w_s$. The computation $F_r^{w_s}(0^n)$ is defined and by statement 1 of Corollary 2.15, its output is definitely rejected by $M_i^{w_s}$. Thus we have seen that if statement 1 holds, then the construction in step s is possible. For statement 2 this is shown analogously.

It remains to show that statement 3 cannot hold. Otherwise, for $z = F_r^{w' \cup \{x,y\} \cup C}(0^n)$ it holds that $z \in L(M_i^{w' \cup \{x,y\} \cup C}) \cap L(M_j^{w' \cup \{x,y\} \cup C})$. Consider the smallest step s' where $t_{s'}(i,j)$ is defined. This step extends $t_{s'-1}$ such that $t_{s'} = t_{s'-1} \cup \{(i,j) \mapsto p\}$. Thus we have $s' \leq s-1$ and $w_{s'-1} \sqsubsetneq w_{s'} \sqsubseteq w_{s-1} \sqsubseteq w'$. We know that w' is t_s-valid and hence $t_{s'-1}$-valid. Choose the minimal $v \sqsupseteq w'$ that satisfies V4, that contains x and y, and that is defined for all words of length $\leq (n^r + r)^{i+j} + i + j$. Then $M_i^v(z)$ and $M_j^v(z)$ definitely accept. By interpreting w' and v as sets, we have $v = w' \cup \{x, y\} \cup (C \cap \Sigma^{\leq (n^r+r)^{i+j}+i+j})$, i.e., x, y are the only words of even length that we added to the oracle. We know that w' is a $t_{s'-1}$-valid oracle defined for all words of length $< n$ and undefined for all other words. Now we show that v is $t_{s'-1}$-valid as well. Due to $e(n+1) > (n^r + r)^{i+j} + i + j$, v satisfies V2.2. It also satisfies V2.1, since $|x| = |y| = e(p^k)$ with $p \notin \operatorname{ran}(t_{s'-1})$. After adding x, y, and the necessary words from C, the oracle still satisfies V4 and V5 in the definition of $t_{s'-1}$-valid, since $|x| = |y| = e(p^k)$. The remaining conditions V1 and V3 are not affected by the extension $w' \sqsubsetneq v$. Hence v is $t_{s'-1}$-valid and even t'-valid for $t' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$, since $M_i^v(z)$ and $M_j^v(z)$ definitely accept. Therefore, step s' defines $t_{s'} = t'$ and chooses the oracle in an appropriate way (e.g., $w_{s'} = v$), which contradicts $t_{s'}(i,j) = p$. This shows that statement 3 cannot hold.

Thereby we have shown that in the steps treating tasks (i,j,r), the choice of the specified t_s-valid w_s is possible, which contradicts the assumption. □

Let $O = \lim_{s \to \infty} w_s$ be the oracle obtained by the whole construction. It is totally defined, since each step strictly extends the oracle.

Claim 4.7 DisjNP^O *has no pairs that are* $\leq_{\mathrm{m}}^{\mathrm{pp},O}$*-hard for* $\mathrm{NP}^O \cap \mathrm{coNP}^O$.

Proof Assume there exists such a pair $(L(M_i^O), L(M_j^O))$. From $L(M_i^O) \cap L(M_j^O) = \emptyset$ it follows that for all s there is no z such that $M_i^{w_s}(z)$ and $M_j^{w_s}(z)$ definitely accept. Hence $t_s(i,j) \neq 0$ for all s for which $t_s(i,j)$ is defined. Let s be the step that treats task (i,j). Thus for all $s' \geq s$ it holds $t_{s'}(i,j) = p \in \mathbb{P}^{\geq 3}$, which by V2 implies $A_p^O = \overline{B_p^O} \in \mathrm{NP}^O \cap \mathrm{coNP}^O$. Thus there exists an r such that $(A_p^O, B_p^O) \leq_{\mathrm{m}}^{\mathrm{pp},O} (L(M_i^O), L(M_j^O))$ via F_r^O. Let s' be the step that treats task (i,j,r). This step makes sure that for a suitable 0^n at least one of the following holds:

- $0^n \in A_p^{w_{s'}}$, $F_r^{w_{s'}}(0^n)$ is defined, and its output is definitely rejected by $M_i^{w_{s'}}$.
- $0^n \in B_p^{w_{s'}}$, $F_r^{w_{s'}}(0^n)$ is defined, and its output is definitely rejected by $M_j^{w_{s'}}$.

The first (resp., second) assertion implies the first (resp., second) of the two following statements.

- $0^n \in A_p^O$ and $F_r^O(0^n)$ is rejected by M_i^O
- $0^n \in B_p^O$ and $F_r^O(0^n)$ is rejected by M_j^O

This contradicts the choice of r. □

The proof of the following claim is based on a proof by Rackoff [Rac82, Theorem 4].

Claim 4.8 $\mathrm{P}^O = \mathrm{UP}^O$.

Proof Let $L \in \mathrm{UP}^O$ and choose i such that $L = L(M_i^O)$ and M_i^O has the uniqueness property. Moreover, choose the smallest s such that $t_s(i,i)$ is defined and note that $t_s(i,i) = 1$.

Consider the computation of $M_i(x)$, where the oracle is not specified. P is called *potential accepting path* if there exists an oracle D such that P is an accepting path of $M_i^D(x)$. For sets Q, U, W, W' (which will be defined in the following algorithm) we say that P *respects* (Q, U, W, W') if it answers *yes* to questions in $C \cup Q \cup W$, *no* to questions in W', *no* to questions not in $C \cup Q \cup U$, and consistently to questions in $U - (W \cup W')$. Moreover, P^{all} (resp., P^{yes}, P^{no}) denotes the set of all (resp., positively answered, negatively answered) queries of P.

We show that the following algorithm decides L.

```
 1. Input: x ∈ ℕ
 2. Let m = |x|.
 3. If m is not large enough such that m ≥ 4, m^i + i < 2^m,
    and w_{s-1} is undefined for all words of length ≥log m:
 4.    If x ∈ L, then Accept, else Reject.
 5. Let n be the unique number such that e(n − 1) ≤ log m < e(n).
 6. Let Q = {q ∈ O | |q| even and |q| < e(n)}.
 7. If n = p^k for some k ≥ 1 and some p ∈ ran(t_{s-1}) ∩ ℙ^{≥3}:
 8.    Let U = {z ∈ ℕ | |z| = e(n) and z odd} and W = W' = ∅.
 9.    If SEARCH returns True, then Accept.
10.    Let U = {z ∈ ℕ | |z| = e(n) and z even} and W = W' = ∅.
11.    If SEARCH returns True, then Accept.
12.    Reject.
13. If n ≠ p^k for all k ≥ 1 and p ∈ ran(t_{s-1}) ∩ ℙ^{≥3}:
14.    Let U = {z ∈ ℕ | |z| = e(n)} and W = W' = ∅.
15.    If SEARCH returns True, then Accept.
16.    Reject.

17. subroutine SEARCH
18.    For j = 0 to 4(m^i + i):
19.       If there is no potential accepting path respecting (Q, U, W, W'),
          then return False, else let P be such a path.
20.       For each z ∈ P^all with |z| = e(n):
21.          Ask whether z ∈ O.
22.          If z ∈ O − U, then return False.
23.          If z ∈ O ∩ U, then add z to W.
24.          If z ∈ O̅ ∩ U, then add z to W'.
25.       If P still respects (Q, U, W, W'), then return True.
26.    Return False.
```

Observe that once line 5 has been executed, it holds

$$m^i + i < e(n+1). \tag{4}$$

We argue that in presence of oracle O, the algorithm can be implemented as a polynomial time algorithm: It suffices to argue for the lines 6, 7–12, 13–16, and 17–26.

Line 6: Because of line 3 we may assume that m is large enough such that $m^i + i < 2^m$ and w_{s-1} is undefined for all words of length $e(n)$. Hence (4) shows that $M_i(x)$ cannot ask queries of length $\geq e(n+1)$. Recall that each word in $O - C$ has a length $e(j)$ for some j.

Thus the set Q consists of all words in $O - C$ that have length $e(j)$ for some $j \leq n-1$. From $1 + e(n-1) \leq 1 + \log m$ we obtain $2^{1+e(n-1)} \leq 2m$ and hence $|\bigcup_{j=0}^{n-1} \Sigma^{e(j)}| \leq 2m$, which shows that with access to oracle O we can ask "$q \in O$?" for all $q \in \bigcup_{j=0}^{n-1} \Sigma^{e(j)}$ in polynomial time in $|x|$. Hence line 6 only requires polynomial time in $|x|$.

Lines 7–12 and 13–16: Note that we introduce the set U in the lines 8, 10, and 14 only for better readability. These sets never have to be computed explicitly, since it can be easily checked whether some query of $M_i(x)$ is in U.

It remains to argue for the lines 17–26, i.e., subroutine SEARCH. Testing the membership to Q, U, W, and W' is possible in polynomial time without oracle access. Hence, since $C \in$ PSPACE, we can determine in polynomial space without oracle access (whether there exists) a potential accepting path respecting (Q, U, W, W'). As PSPACE $\subseteq \mathrm{P}^C \subseteq \mathrm{P}^O$, the subroutine SEARCH requires polynomial time in $|x|$ when having access to the oracle O.

First we show that if the algorithm accepts, then $x \in L$. This is true, if it accepts in line 4. So assume now that it accepts in the lines 9, 11, or 15. Hence in these lines, SEARCH returns True. We have a closer look at these calls of SEARCH. Recall that O consists of C and elements of even length $e(j)$ for some $j \in \mathbb{N}$. Due to (4) $M_i^O(x)$ cannot ask queries of length $\geq e(n+1)$. Hence $M_i^O(x) = M_i^{C \cup Q \cup (O \cap \Sigma^{e(n)})}(x)$. By the lines 23–24, during the execution of SEARCH it always holds that $W, W' \subseteq U$, $W \subseteq O$, and $W' \subseteq \overline{O}$. Moreover, each time we reach line 25 it holds that

$$P^{\mathrm{all}} \cap \Sigma^{e(n)} \subseteq W \cup W' \cup (\overline{O} - U). \tag{5}$$

Consider the loop 18–25 at the iteration that in line 25 returns True. Hence in line 25 it holds that P respects (Q, U, W, W'). Therefore, on P we have the following cases for queries q and their answers:

- If $|q| < e(n)$, then the answer is $(C \cup Q)(q) = O(q)$.
- If $|q| > e(n)$, then the answer is $C(q) = O(q)$.
- If $|q| = e(n)$ and $q \in W$, then the answer is $1 = O(q)$.
- If $|q| = e(n)$ and $q \in W'$, then the answer is $0 = O(q)$.
- If $|q| = e(n)$ and $q \in \overline{O} - U$, then the answer is $0 = O(q)$.

By (5), the cases $(|q| = e(n) \wedge q \in U - (W \cup W'))$ and $(|q| = e(n) \wedge q \in O - U)$ are impossible. Hence, in the considered execution of line 25, P is an accepting path of $M_i^O(x)$, which implies $x \in L$. This shows that if the algorithm accepts x, then $x \in L$.

It remains to argue that if $x \in L$, then the algorithm accepts x. From now on we assume $x \in L$. Without loss of generality we assume that the algorithm on input x does not stop in line 3. Thus $m \geq 4$, $m^i + i < 2^m$, and w_{s-1} is undefined for all words of length $\geq \log m$ (and thus in particular for all words of length $e(n)$). Thus the number n in line 5 exists. We consider two cases:

Case 1: $4(m^i + i) \geq 2^{e(n)}$.

Assume that the algorithm does not accept, i.e., it rejects. We show that this implies a contradiction. The assumption that the algorithm does not stop in line 4 implies that it stops in the lines 12 or 16. Note that if the algorithm stops in line 12, then $0^{e(n)} \notin A_p^O$ or $0^{e(n)} \notin B_p^O$, since $p \in \mathrm{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3}$ and hence $A_p^O \cap B_p^O = \emptyset$ by V2.1. We have to consider the following cases.

Case 1a: The algorithm stops in line 12 and $0^{e(n)} \notin A_p^O$. Here we continue the argumentation by choosing $U = \{z \in \mathbb{N} \mid |z| = e(n) \text{ and } z \text{ odd}\}$ and having a closer look at the call of SEARCH in line 9, which returns False.

Case 1b: The algorithm stops in line 12 and $0^{e(n)} \notin B_p^O$. Here we continue the argumentation by choosing $U = \{z \in \mathbb{N} \mid |z| = e(n) \text{ and } z \text{ even}\}$ and having a closer look at the call of SEARCH in line 11, which returns False.

Case 1c: The algorithm stops in line 16. Here we continue the argumentation by choosing $U = \{z \in \mathbb{N} \mid |z| = e(n)\}$ and having a closer look at the call of SEARCH in line 15, which returns False.

We argue for the Cases 1a, 1b, and 1c in parallel. Note that in each case it holds $O \cap \Sigma^{e(n)} \subseteq U$. By the lines 23–24, during the considered call of SEARCH it always holds that $W, W' \subseteq U$, $W \subseteq O$, and $W' \subseteq \overline{O}$. As $x \in L$, the computation $M_i^O(x)$ has an accepting path P'. P' respects (Q, U, W, W') each time we reach line 19, since there are the following cases for queries q:

- If $q \in C \cup Q \cup W$, then the answer is $O(q) = 1$, since $C \cup Q \cup W \subseteq O$.
- If $q \in W'$, then the answer is $O(q) = 0$, since $W' \subseteq \overline{O}$.
- If $q \notin C \cup Q \cup U$, then the answer is $O(q) = 0$, since $|q| < e(n+1)$ and $O \cap \Sigma^{<e(n+1)} = C \cup Q \cup (O \cap \Sigma^{e(n)}) \subseteq C \cup Q \cup U$.
- If $q \in U - (W \cup W')$, then multiple queries q are answered consistently by $O(q)$.

Hence the considered call of SEARCH cannot return False in line 19. Moreover, by $O \cap \Sigma^{e(n)} \subseteq U$, it cannot return False in line 22. Thus the considered call of SEARCH returns False in line 26. In particular, the loop 18–25 is executed exactly $4(m^i + i) + 1$ times and in each execution of line 25, P does not respect (Q, U, W, W') anymore. The latter implies that each execution of the loop increases $|W \cup W'|$ at least by 1. Hence, when reaching line 26 it holds $|W \cup W'| > 4(m^i + i) \geq 2^{e(n)}$. This is a contradiction, since $W \cup W' \subseteq U \subseteq \Sigma^{e(n)}$.

Case 2: $4(m^i + i) < 2^{e(n)}$.

Define the following predicate.

$$\begin{aligned}&\textit{All potential accepting paths } P_1, P_2 \textit{ that respect } (Q, U, W, W') \textit{ and that satisfy}\\ &P_1^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset \textit{ and } P_2^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset \textit{ have a query from}\\ &U - (W \cup W') \textit{ in common, i.e., } P_1^{\text{all}} \cap P_2^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset.\end{aligned} \tag{6}$$

We show the following assertions for $Q = \{q \in O \mid |q| \text{ even and } |q| < e(n)\}$.

$$\begin{aligned}&\textit{If } n = p^k \textit{ for } p \in \operatorname{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3} \textit{ and } k \geq 1,\ 0^{e(n)} \notin A_p^O,\ U = \{z \mid |z| = e(n) \text{ and } z \text{ odd}\},\\ &W \subseteq O \cap U,\ W' \subseteq \overline{O} \cap U, \textit{ and } 4(m^i + i) < 2^{e(n)}, \textit{ then (6) holds.}\end{aligned} \tag{7}$$

$$\begin{aligned}&\textit{If } n = p^k \textit{ for } p \in \operatorname{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3} \textit{ and } k \geq 1,\ 0^{e(n)} \notin B_p^O,\ U = \{z \mid |z| = e(n) \text{ and } z \text{ even}\},\\ &W \subseteq O \cap U,\ W' \subseteq \overline{O} \cap U, \textit{ and } 4(m^i + i) < 2^{e(n)}, \textit{ then (6) holds.}\end{aligned} \tag{8}$$

$$\begin{aligned}&\textit{If } n \neq p^k \textit{ for all } p \in \operatorname{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3} \textit{ and all } k \geq 1,\ U = \{z \in \mathbb{N} \mid |z| = e(n)\},\ W \subseteq O \cap U,\\ &W' \subseteq \overline{O} \cap U, \textit{ and } 4(m^i + i) < 2^{e(n)}, \textit{ then (6) holds.}\end{aligned} \tag{9}$$

By symmetry, if suffices to prove (7) and (9). We start with the proof of (7). Suppose there exist potential accepting paths P_1, P_2 that respect (Q, U, W, W'), that satisfy $P_1^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset$ and $P_2^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset$, and that have no query from $U - (W \cup W')$ in common. Hence P_1 and P_2 are different paths. Let $Y = (P_1^{\text{yes}} \cup P_2^{\text{yes}}) \cap \Sigma^{\geq e(n)}$ and $N = (P_1^{\text{no}} \cup P_2^{\text{no}}) \cap \Sigma^{\geq e(n)}$. Note $Y \subseteq U \cup C$ (cf. (4)).

We argue for $Y \cap N = \emptyset$. Assume there exists some $q \in Y \cap N$. Hence $|q| \geq e(n)$. If $|q| > e(n)$, then $q \in Y \subseteq U \cup C$ implies $q \in C$, which contradicts $q \in N$, since both paths respect (Q, U, W, W'). From now on assume $|q| = e(n)$. From the fact that P_1 and P_2 respect (Q, U, W, W') we obtain:

- If $q \notin U$, then it holds that $q \notin P_1^{\text{yes}}$ and $q \notin P_2^{\text{yes}}$, which contradicts $q \in Y$.
- If $q \in W$, then it holds that $q \notin P_1^{\text{no}}$ and $q \notin P_2^{\text{no}}$, which contradicts $q \in N$.
- If $q \in W'$, then it holds that $q \notin P_1^{\text{yes}}$ and $q \notin P_2^{\text{yes}}$, which contradicts $q \in Y$.
- If $q \in U - (W \cup W')$, then $q \in P_1^{\text{yes}} \cap P_2^{\text{no}}$ or $q \in P_1^{\text{no}} \cap P_2^{\text{yes}}$, and hence P_1 and P_2 have a common query from $U - (W \cup W')$, which contradicts the assumption.

This shows $Y \cap N = \emptyset$.

Let $u \sqsupseteq w_{s-1}$ such that $u(z) = O(z)$ for all words z with $|z| < e(n)$ and u is undefined for all other words. According to the Claims 4.3 and 4.4, the oracle u is t_{s-1}-valid. Consider the minimal $v \sqsupsetneq u$ that satisfies V4, that contains all words in Y, that contains at least one word from $U - N$ (which is a nonempty set, since $|N| \leq 2(m^i + i)$, $|U| = 2^{e(n)-1}$, and by assumption $4(m^i + i) < 2^{e(n)}$), and that is defined for all words of length $\leq \max\{m^i + i, e(n)\}$. The nonemptiness of $U - N$ is the reason for the distinction of the Cases 1 and 2. Note that $v \cap N = \emptyset$. Moreover, v contains all words in Q, since these words are in u. The oracle v satisfies V2.1, since u is t_{s-1}-valid, $e(n+1) > \max(e(n), m^i + i)$ (cf. (4)), and the words of even length that we added to the oracle all belong to U (recall $Y \subseteq U \cup C$ for the last property). It also satisfies V2.2, since we added at least one word from $U - N$. Moreover, v satisfies V5, since we only added such words of even length that are in $U \subseteq \Sigma^{e(n)}$. Finally, V1 and V3 are not affected by adding words from U to the oracle. Thus v is t_{s-1}-valid.

P_1 and P_2 respect (Q, U, W, W') and $Y \cap N = \emptyset$. Hence on P_1 and P_2 we have the following cases for queries q and their answers:

- If $|q| < e(n)$, then the answer is $(C \cup Q)(q) = O(q) = u(q) = v(q)$.
- If $|q| \geq e(n)$ and $q \in Y$, then the answer is $1 = v(q)$, since $Y \subseteq v$.
- If $|q| \geq e(n)$ and $q \in N$, then the answer is $0 = v(q)$, since $v \cap N = \emptyset$.

This shows that P_1 and P_2 are two different accepting paths of the computation $M_i^v(x)$. Both paths are definitely accepting, since v is defined for all words of length $\leq m^i + i$. Thus v is t'-valid for $t' = t_{s-1} \cup \{(i, i) \mapsto 0\}$. Hence step s defines $t_s = t'$ and chooses the oracle in an appropriate way (e.g., $w_s = v$), which contradicts $t_s(i, i) = 1$. This proves (7).

In order to prove (9), we only need to simplify the proof of (7): Suppose there exist potential accepting paths P_1, P_2 that respect (Q, U, W, W'), that satisfy $P_1^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset$ and $P_2^{\text{all}} \cap (U - (W \cup W')) \neq \emptyset$, and that have no query from $U - (W \cup W')$ in common. Hence P_1 and P_2 are different paths. Let $Y = (P_1^{\text{yes}} \cup P_2^{\text{yes}}) \cap \Sigma^{\geq e(n)}$ and $N = (P_1^{\text{no}} \cup P_2^{\text{no}}) \cap \Sigma^{\geq e(n)}$. Note $Y \subseteq U \cup C$ (cf. (4)).

We argue for $Y \cap N = \emptyset$. Assume there exists some $q \in Y \cap N$. Hence $|q| \geq e(n)$. If $|q| > e(n)$, then $q \in Y \subseteq U \cup C$ implies $q \in C$, which contradicts $q \in N$, since both paths respect (Q, U, W, W'). From now on assume $|q| = e(n)$, i.e., $q \in U$. From the fact that P_1 and P_2 respect (Q, U, W, W') we obtain:

- If $q \in W$, then it holds that $q \notin P_1^{\text{no}}$ and $q \notin P_2^{\text{no}}$, which contradicts $q \in N$.
- If $q \in W'$, then it holds that $q \notin P_1^{\text{yes}}$ and $q \notin P_2^{\text{yes}}$, which contradicts $q \in Y$.
- If $q \in U - (W \cup W')$, then $q \in P_1^{\text{yes}} \cap P_2^{\text{no}}$ or $q \in P_1^{\text{no}} \cap P_2^{\text{yes}}$, and hence P_1 and P_2 have a common query from $U - (W \cup W')$, which contradicts the assumption.

This shows $Y \cap N = \emptyset$.

Let $u \sqsupseteq w_{s-1}$ such that $u(z) = O(z)$ for all words z with $|z| < e(n)$ and u is undefined for all other words. According to the Claims 4.3 and 4.4, the oracle u is t_{s-1}-valid. Consider the minimal $v \sqsupseteq u$ that satisfies V4, that contains all words in Y, and that is defined for all words of length $\leq \max\{m^i + i, e(n)\}$. Note that $v \cap N = \emptyset$. Moreover, v contains all words in Q, since these words are in u. The oracle v satisfies V2, since u is t_{s-1}-valid, $n \neq p^k$ for all $k \geq 1$ and $p \in \mathrm{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3}$, and $e(n+1) \geq \max\{m^i + i, e(n)\}$. Moreover, v satisfies V5, since we only added such words of even length that are in $U = \Sigma^{e(n)}$. Finally, V1 and V3 are not affected by adding words from U to the oracle. Thus v is t_{s-1}-valid.

P_1 and P_2 respect (Q, U, W, W') and $Y \cap N = \emptyset$. Hence on P_1 and P_2 we have the following cases for queries q and their answers:

- If $|q| < e(n)$, then the answer is $(C \cup Q)(q) = O(q) = u(q) = v(q)$.
- If $|q| \geq e(n)$ and $q \in Y$, then the answer is $1 = v(q)$, since $Y \subseteq v$.
- If $|q| \geq e(n)$ and $q \in N$, then the answer is $0 = v(q)$, since $v \cap N = \emptyset$.

This shows that P_1 and P_2 are two different accepting paths of the computation $M_i^v(x)$. Both paths are definitely accepting, since v is defined for all words of length $\leq m^i + i$. Thus v is t'-valid for $t' = t_{s-1} \cup \{(i, i) \mapsto 0\}$. Hence step s defines $t_s = t'$ and chooses the oracle in an appropriate way (e.g., $w_s = v$), which contradicts $t_s(i, i) = 1$. This proves (9).

We continue to argue that the algorithm accepts x. For this we study two subcases.

Case 2a: Assume $n = p^k$ for some $p \in \mathrm{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3}$ and $k \geq 1$. Then $A_p^O \cap B_p^O = \emptyset$ due to V2.1. Consider the lines 8 and 9 (here $U = \{z \in \mathbb{N} \mid |z| = e(n) \text{ and } z \text{ odd}\}$). Without loss of generality $0^{e(n)} \notin A_p^O$ (otherwise $0^{e(n)} \notin B_p^O$ and it can be argued symmetrically), i.e., O does not contain an even word of length $e(n)$. Hence $O - U$ contains no words of length $e(n)$ and thus the subroutine SEARCH does not return False in line 22. Since $x \in L$, there exists an accepting path P' of $M_i^O(x)$.

Observe that for all $W \subseteq O \cap U$ and $W' \subseteq \overline{O} \cap U$ it holds that P' is a potential accepting path respecting (Q, U, W, W'), which is a consequence of the following possibilities how queries $q \in P'^{\mathrm{all}}$ are answered.

- If $q \in C \cup Q \cup W$, then the answer is *yes*, since $C \cup Q \cup W \subseteq O$.
- If $q \in W'$, then the answer is *no*, since $W' \subseteq \overline{O}$.
- Assume $q \notin C \cup Q \cup U$. As $|q| \leq m^i + i < e(n+1)$ by (4), $q \notin Q \cup U$, and O does not contain an even word of length $e(n)$, it holds that $q \notin O$ or the length of q is odd. In the latter case, as $q \notin C$ and $O(q') = C(q')$ for all words q' of odd length, it holds $q \notin O$. Hence the answer is *no*.
- If $q \in U - (W \cup W')$, then multiple queries q are answered consistently by $O(q)$.

By the lines 23–24, during the execution of SEARCH it always holds that $W \subseteq O \cap U$ and $W' \subseteq \overline{O} \cap U$. Thus, each time we reach line 19 it holds that P' is a potential accepting path respecting (Q, U, W, W'). Hence line 19 does not return False, but chooses some potential accepting path $P = P_1$ that respects (Q, U, W, W'). If $P_1^{\mathrm{all}} \cap (U - (W \cup W')) = \emptyset$, then P_1 still respects (Q, U, W, W') when reaching line 25 (since the loop 20–24 adds only words from U to W or W'), hence SEARCH returns True, the algorithm accepts, and we are done. Otherwise, we have $P_1^{\mathrm{all}} \cap (U - (W \cup W')) \neq \emptyset$. By (7), for each potential accepting path P_2 that respects (Q, U, W, W') and that satisfies $P_2^{\mathrm{all}} \cap (U - (W \cup W')) \neq \emptyset$ it holds that P_1 and P_2 have a query

$q \in U - (W \cup W')$ in common. The lines 23–24 add this query to $W \cup W'$, which decreases $|P_2^{\mathrm{all}} \cap (U - (W \cup W'))|$ at least by 1. Therefore, if SEARCH does not return True within $m^i + i$ iterations of the loop 18–25, then after this number of iterations, for all potential accepting paths P_2 that respect (Q, U, W, W') it holds $P_2^{\mathrm{all}} \cap (U - (W \cup W')) = \emptyset$ and hence the next iteration returns True in line 25. This implies that the loop returns True within $m^i + i + 1$ iterations, which shows that the algorithm accepts.

Case 2b: Assume $n \neq p^k$ for all $p \in \mathrm{ran}(t_{s-1}) \cap \mathbb{P}^{\geq 3}$ and all $k \geq 1$. Consider the lines 14 and 15 (here $U = \Sigma^{e(n)}$). Due to the choice of U, the subroutine SEARCH does not return False in line 22. Since $x \in L$, there exists an accepting path P' of $M_i^O(x)$.

Observe that for all $W \subseteq O \cap U$ and $W' \subseteq \overline{O} \cap U$ it holds that P' is a potential accepting path respecting (Q, U, W, W'), which is a consequence of the following possibilities how queries $q \in P'^{\mathrm{all}}$ are answered.

- If $q \in C \cup Q \cup W$, then the answer is *yes*, since $C \cup Q \cup W \subseteq O$.
- If $q \in W'$, then the answer is *no*, since $W' \subseteq \overline{O}$.
- Assume $q \notin C \cup Q \cup U$. As $|q| \leq m^i + i < e(n+1)$ by (4) and $q \notin Q \cup U$, it holds that $q \notin O$ or the length of q is odd. In the latter case, as $q \notin C$ and $O(q') = C(q')$ for all words q' of odd length, it holds $q \notin O$. Hence the answer is *no*.
- If $q \in U - (W \cup W')$, then multiple queries q are answered consistently by $O(q)$.

By the lines 23–24, during the execution of SEARCH it always holds that $W \subseteq O \cap U$ and $W' \subseteq \overline{O} \cap U$. Thus, each time we reach line 19 it holds that P' is a potential accepting path respecting (Q, U, W, W'). Hence line 19 does not return False, but chooses some potential accepting path $P = P_1$ that respects (Q, U, W, W'). If $P_1^{\mathrm{all}} \cap (U - (W \cup W')) = \emptyset$, then P_1 still respects (Q, U, W, W') when reaching line 25 (since the loop 20–24 adds only words from U to W or W'), hence SEARCH returns True, the algorithm accepts, and we are done. Otherwise, we have $P_1^{\mathrm{all}} \cap (U - (W \cup W')) \neq \emptyset$. By (9), for each potential accepting path P_2 that respects (Q, U, W, W') and that satisfies $P_2^{\mathrm{all}} \cap (U - (W \cup W')) \neq \emptyset$ it holds that P_1 and P_2 have a query $q \in U - (W \cup W')$ in common. The lines 23–24 add this query to $W \cup W'$, which decreases $|P_2^{\mathrm{all}} \cap (U - (W \cup W'))|$ at least by 1. Therefore, if SEARCH does not return True within $m^i + i$ iterations of the loop 18–25, then after this number of iterations for all potential accepting paths P_2 that respect (Q, U, W, W') it holds $P_2^{\mathrm{all}} \cap (U - (W \cup W')) = \emptyset$ and hence the next iteration returns True in line 25. This implies that the loop returns True within $m^i + i + 1$ iterations, which shows that the algorithm accepts. □

This completes the proof of Theorem 4.1. □

5 An Oracle for $\neg \mathrm{H}_{\mathrm{union}}$ and $\neg \mathrm{H}_{\mathrm{cpair}}$

We show that the implication $\neg \mathrm{H}_{\mathrm{union}} \Rightarrow \mathrm{H}_{\mathrm{cpair}}$ cannot be proven in a relativizable way. It follows from (1) that the same holds for the implication $\neg \mathrm{H}_{\mathrm{union}} \Rightarrow \mathrm{H}_{\mathrm{opps}}$.

Theorem 5.1 *There exists an oracle O with the following properties.*

1. DisjNP^O *has no* $\leq_{\mathrm{m}}^{\mathrm{pp},O}$*-complete pairs.*
2. *There are disjoint sets A and B that are* $\leq_{\mathrm{m}}^{\mathrm{p},O}$*-complete for* NP^O *such that $A \cup B$ is not* $\leq_{\mathrm{m}}^{\mathrm{p},O}$*-complete for* NP^O.

Proof Let $M_1, M_2, \ldots$ be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines. Let $F_1, F_2, \ldots$ be a standard enumeration of deterministic, polynomial-time oracle Turing transducers.

Define the following sets for $i, j, k \in \mathbb{N}$, $p \in \mathbb{P}^{\geq 3}$, and an oracle $D \subseteq \mathbb{N}$.

$$\begin{aligned}
K^D &= \{\langle 0^i, 0^j, x\rangle \mid M_i^D(x) \text{ accepts within } j \text{ steps}\} \\
A_p^D &= \{0^{p^k} \mid k \geq 1 \text{ and there exists an even } x \in D \text{ such that } |x| = p^k\} \\
B_p^D &= \{0^{p^k} \mid k \geq 1 \text{ and there exists an odd } x \in D \text{ such that } |x| = p^k\} \\
\Gamma^D &= \{0^n \mid \exists_{y \in \Sigma^n} y \in D\} \in \mathrm{NP}^D \\
\Delta^D &= \{\langle 0^i, 0^j, x\rangle \mid \exists_{y \in \Sigma^{|\langle 0^i, 0^j, x\rangle|}} \langle 0^i, 0^j, x\rangle y \in D\} \in \mathrm{NP}^D
\end{aligned}$$

Observe that K^D is $\leq_{\mathrm{m}}^{\mathrm{p},D}$-complete for NP^D. Moreover, note that for all primes p the sets A_p^D and B_p^D are disjoint if for all $k \in \mathbb{N}^+$ it holds $D \cap \{y \mid |y| = p^k\} \leq 1$.

Preview of construction: On the one hand, the construction tries to prevent that $L(M_i)$ and $L(M_j)$ for $i \neq j$ are disjoint. If this is not possible, M_i and M_j inherently accept disjoint sets. In this case, for a suitable $p \in \mathbb{P}$, the construction makes sure that (A_p, B_p) does not $\leq_{\mathrm{m}}^{\mathrm{pp}}$-reduce to $(L(M_i), L(M_j))$, which prevents the existence of complete disjoint NP-pairs. On the other hand, the construction diagonalizes against all FP-functions ensuring that Γ does not reduce to $K \cup \Delta$. Statement 2 of the theorem is a simple corollary of this result.

Claim 5.2 *For oracles v and w and all $y \leq \min(|v|, |w|)$, if $\mathrm{pr}_y(v) = \mathrm{pr}_y(w)$, then $K^w(y) = K^v(y)$.*

Proof We may assume $y = \langle 0^i, 0^j, x\rangle$ for suitable i, j, x, since otherwise $K^w(y) = K^v(y) = 0$. For each q that is queried within the first j steps of $M_i^w(x)$ or $M_i^v(x)$ it holds that $|q| \leq j < |y|$ and thus $q < y$. Hence these queries are answered the same way relative to w and v, showing that $M_i^w(x)$ accepts if and only if $M_i^v(x)$ accepts. □

During the oracle construction we maintain a growing collection of properties that we demand in the further construction. The collection is represented by a function t and if an oracle satisfies the properties defined by t, then we call it t-valid. More precisely, we start with the nowhere defined function $t_0 : \mathbb{N} \times \mathbb{N} \to \mathbb{P}^{\geq 3} \cup \{0\}$, which defines no property. We successively continue this function and obtain $t_1, t_2, \ldots$, which have a finite, but growing domain. At the end of the construction we reach the total function $t = \lim_{i \to \infty} t_i$.

Let $t \in \mathcal{T} := \{t : \mathbb{N} \times \mathbb{N} \to \mathbb{P} \cup \{0\} \mid t \text{ has finite domain and is injective on } \mathrm{supp}(t)\}$. An oracle $w \in \Sigma^*$ is t-valid, if for all $(i, j) \in \mathrm{dom}(t)$:

V1 If $i \neq j$ and $t(i, j) = 0$, then there exists z such that $M_i^w(z)$ and $M_j^w(z)$ definitely accept.
(meaning: $L(M_i^v) \cap L(M_j^v) \neq \emptyset$ for all $v \sqsupseteq w$)

V2 If $i \neq j$ and $t(i, j) = p \in \mathbb{P}^{\geq 3}$, then for all $k \geq 1$ it holds that $|\{x \in w \mid |x| = p^k\}| \leq 1$.
(meaning: (A_p^w, B_p^w) is a disjoint NP^w-pair)

V3 If $i = j$ and $t(i, i) = 0$, then there is a word 0^n such that $F_i^w(0^n)$ is defined and $0^n \in \Gamma^v \Leftrightarrow F_i^w(0^n) \notin K^v \cup \Delta^v$ for all $v \sqsupseteq w$.
(meaning: there is no $v \sqsupseteq w$ such that F_i^v reduces Γ^v to $K^v \cup \Delta^v$)

V4 $K^w \cap \Delta^w = \emptyset$.

This definition directly implies the following claim.

Claim 5.3 *Let $t, t' \in \mathcal{T}$ such that t' is a continuation of t. If w is t'-valid, then w is t-valid.*

Claim 5.4 *Let $t \in \mathcal{T}$, w be t-valid, and $z = |w|$.*

1. *$w0$ is t-valid.*
2. *If $|z|$ is odd and no prime power, then $w1$ is t-valid.*
3. *If $z = \langle 0^i, 0^j, x\rangle y$ with $\langle 0^i, 0^j, x\rangle \notin K^w$ and $|z| = 2|y|$, then $w1$ is t-valid.*

Proof The statements 1 and 2 directly follow from the definition. Statement 3 follows from Claim 5.2. □

Oracle construction: Let t_0 be the nowhere defined function and $w_0 = \varepsilon$, which is t_0-valid. We construct a sequence of partially defined oracles $w_0 \sqsubsetneq w_1 \sqsubsetneq \cdots$ and a sequence $t_0, t_1, \ldots$ of functions from $\mathcal{T}$ such that w_i is t_i-valid and t_{i+1} is a continuation of t_i for all i. The final oracle is $O = \lim_{i\to\infty} w_i$. Each step treats the first task in our task list T and removes this and possibly other tasks from the list. At the beginning, T consists of an enumeration of all $(i, j) \in \mathbb{N}^2$ and all $(i, j, r) \in \mathbb{N}^3 - \{(i', i', r') \mid i', r' \in \mathbb{N}\}$ in an order having the property that (i, j) appears earlier than (i, j, r) for all i, j, r with $i \neq j$. We describe step $s > 0$, which starts with a t_{s-1}-valid oracle w_{s-1} and extends it to a t_s-valid $w_s \sqsupsetneq w_{s-1}$.

- task (i, j) with $i \neq j$: Let $t' = t_{s-1} \cup \{(i, j) \mapsto 0\}$. If there exists a t'-valid $v \sqsupsetneq w_{s-1}$, then let $t_s = t'$, $w_s = v$, and remove all tasks $(i, j, \cdot)$ from T. Otherwise choose $p \in \mathbb{P}^{\geq 3} - \mathrm{ran}(t_{s-1})$ such that $p > |w_{s-1}|$ and let $t_s = t_{s-1} \cup \{(i, j) \mapsto p\}$ and $w_s = w_{s-1}0$.
  (meaning: force $L(M_i^O) \cap L(M_j^O) \neq \emptyset$ if possible, otherwise choose a suitable prime p and make sure that O contains at most one element of length p^k for all k and hence (A_p^O, B_p^O) is a disjoint NP^O-pair; corresponds to V1 and V2 in the definition of t-valid)
- task (i, i): Let $t' = t_{s-1} \cup \{(i, i) \mapsto 0\}$ and choose a t_s-valid oracle $w_s \sqsupsetneq w_{s-1}$.
  (meaning: F_i^O does not realize a reduction $\Gamma^O \leq_{\mathrm{m}}^{\mathrm{p},O} K^O \cup \Delta^O$)
- task (i, j, r) with $i \neq j$: It holds that $t_{s-1}(i, j) = p \in \mathbb{P}^{\geq 3}$. Let $t_s = t_{s-1}$ and choose a t_s-valid $w_s \sqsupsetneq w_{s-1}$ such that for a suitable 0^n at least one of the following holds.
  - $0^n \in A_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_i^{w_s}$
  - $0^n \in B_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_j^{w_s}$

  (meaning: F_r^O does not realize a reduction $(A_p^O, B_p^O) \leq_{\mathrm{m}}^{\mathrm{pp},O} (L(M_i^O), L(M_j^O)))$

Claim 5.5 *For all $s \geq 1$, the construction of w_s and t_s in step s is possible and w_s is t_s-valid.*

Proof For a contradiction, assume that the statement is wrong and choose the smallest step s where the claim fails. Assume that this step treats a task (i, i). Then $t_{s-1}(i, i)$ is not defined as it can only be defined by the unique treatment of task (i, i). Therefore, t_s can be defined as specified. We argue that the choice of a t_s-valid w_s is possible, which contradicts the assumption.

Choose $n \in \mathbb{N}$ such that n is odd and no prime power, $2^n > n^i + i$, and w_{s-1} is undefined for all words of length n. Define $z = F_i^{w_{s-1}}(0^n)$. We study three cases.

First Case: Assume z is not of the form $\langle 0^i, 0^j, x\rangle$. In particular $z \notin K^v \cup \Delta^v$ for any oracle v. By the choice of n there exists y of length n that is not queried by $F_i^{w_{s-1}}(0^n)$. Then choose w_s to be the minimal oracle $\sqsupsetneq w_{s-1}$ that contains y and is defined for all words of length $\leq n^i + i$. Hence $w_s = w_{s-1} \cup \{y\}$ and as n is odd and no prime power, w_s is t_{s-1}-valid by

Claim 5.4. Since $w_s = w_{s-1} \cup \{y\}$, $F_i^{w_{s-1}}(0^n)$ does not query y, and w_s is defined for all words of length $\leq n^i + i$, it holds $F_i^v(0^n) = z$ for all $v \sqsupseteq w_s$. However, $0^n \in \Gamma^v$ for all $v \sqsupseteq w_s$, since $y \in w_s$. Thus w_s is even t_s-valid, a contradiction.

From now on assume that z is of the form $\langle 0^i, 0^j, x\rangle$, in particular $|z|$ is even by the definition of the pairing function.

Second Case: It holds $|z| \leq n$. As n is odd, it even holds $|z| < n$. First assume $z \in K^{w_{s-1}} \cup \Delta^{w_{s-1}}$. Choose $w_s \sqsupseteq w_{s-1}$ to be the minimal oracle defined for all words of length $\leq n^i + i$, i.e., interpreted as sets, w_{s-1} and w_s are equal. Then by Claim 5.4, w_s is t_{s-1}-valid and it remains to prove that $0^n \in \Gamma^v \Leftrightarrow F_i^v(0^n) \notin K^v \cup \Delta^v$ for all $v \sqsupseteq w_s$. It holds $F_i^v(0^n) = z$ for all $v \sqsupseteq w_s$. We know $z \in K^{w_{s-1}} \cup \Delta^{w_{s-1}}$ and show $z \in K^v \cup \Delta^v$ for all $v \sqsupseteq w_s$: if $z \in K^{w_{s-1}}$, then $z \in K^{w_s}$, since the sets w_{s-1} and w_s are equal. Then by Claim 5.2, $z \in K^v$ for all $v \sqsupseteq w_s$. If $z \in \Delta^{w_{s-1}}$, then $z \in \Delta^v$ even for each $v \sqsupseteq w_{s-1}$. As $0^n \notin \Gamma^v$ for all $v \sqsupseteq w_s$, the oracle w_s is t_s-valid, a contradiction.

Now assume $z \notin K^{w_{s-1}} \cup \Delta^{w_{s-1}}$. Let $y \in \Sigma^n$ be minimal such that it is not queried by $F_i^{w_{s-1}}(0^n)$ (such a word exists by the choice of n). Choose $w_s \sqsupseteq w_{s-1}$ to be the minimal oracle containing y and being defined for all words of length $\leq 2(n^i + i)$, i.e., interpreting the oracles as sets it holds $w_s = w_{s-1} \cup \{y\}$. As n is odd and no prime power, Claim 5.4 states that w_s is t_{s-1}-valid. It remains to show that w_s is even t_s-valid, i.e., $0^n \in \Gamma^v \Leftrightarrow F_i^v(0^n) \notin K^v \cup \Delta^v$ for all $v \sqsupseteq w_s$. Clearly $0^n \in \Gamma^v$ for all such v. Moreover, since $w_s = w_{s-1} \cup \{y\}$, $F_i^{w_{s-1}}(0^n)$ does not query y, and w_s is defined for all words of length $\leq n^i + i$, it holds $F_i^v(0^n) = z$ for all $v \sqsupseteq w_s$. As w_s is defined for all words of length $2(n^i + i) \geq 2|z|$, $w_s = w_{s-1} \cup \{y\}$, and $|y| = n$ is odd, $z \notin \Delta^v$ for all $v \sqsupseteq w_s$. Recall $|z| < n$. As $\mathrm{pr}_z(w_s)$ equals w_{s-1} (when interpreting the oracles as sets), it holds $z \notin K^{\mathrm{pr}_z(w_s)}$. Then Claim 5.2 yields $z \notin K^v$ for all $v \sqsupseteq \mathrm{pr}_z(w_s)$, in particular for all $v \sqsupseteq w_s$. Hence w_s is t_s-valid, a contradiction.

Third Case: It holds $|z| > n$ and z is of the form $\langle 0^i, 0^j, x\rangle$. If $z \in K^{w_{s-1}}$, then choose $w_s \sqsupseteq w_{s-1}$ to be the minimal oracle defined for all words of length $\leq 2(n^i + i)$, i.e., $w_s = w_{s-1}$ when interpreting the oracles as sets. By Claim 5.4, the oracle w_s is t_{s-1}-valid. For all $v \sqsupseteq w_s$, $0^n \notin \Gamma^v$, $z \notin \Delta^v$ (note $2(n^i + i) \geq 2|z|$), and $F_i^v(0^n) = z$. By Claim 5.2, it holds $z \in K^v$ for all $v \sqsupseteq w_s$. Hence w_s is t_s-valid, a contradiction.

We consider the case $z \notin K^{w_{s-1}}$. Choose a word zy for $|y| = |z|$ such that zy is not queried by $F_i^{w_{s-1}}(0^n)$ (such a word exists by the choice of n). Now let $w_s \sqsupseteq w_{s-1}$ be the minimal oracle containing zy and being defined for all words of length $\leq 2(n^i + i)$, i.e., $w_s = w_{s-1} \cup \{zy\}$ when interpreting the oracles as sets. It can be argued as in the case above that $z \notin K^v$ for all $v \sqsupseteq \mathrm{pr}_z(w_s)$. This allows to apply Claim 5.4.3, which (together with Claim 5.4.1) yields that w_s is t_{s-1}-valid. Clearly $0^n \notin \Gamma^v$ for all $v \sqsupseteq w_s$. Furthermore, by the choice of w_s it holds $F_i^v(0^n) = z$ for all $v \sqsupseteq w_s$. However, as $zy \in w_s$, it holds $z \in \Delta^v$ for all $v \sqsupseteq w_s$. Hence w_s is t_s-valid, a contradiction.

Now assume that step s treats a task (i, j) for $i, j \in \mathbb{N}$ and $i \neq j$. Hence $t_{s-1}(i, j)$ is not defined, since it can only be defined by the unique treatment of task (i, j). Therefore, t' and t_s can be defined as specified, which shows that the construction in step s is possible. If a t'-valid $v \sqsupsetneq w_{s-1}$ exists, then w_s is t_s-valid, which contradicts the assumption. Otherwise, $t_s = t_{s-1} \cup \{(i, j) \mapsto p\}$ for a prime p chosen according to the construction above and by Claim 5.4, w_s is t_{s-1}-valid. The choice of p implies that w_s does not contain words of length p^k for $k \geq 1$. Therefore, w_s is also t_s-valid, which contradicts the assumption.

From now on we assume that step s treats a task (i, j, r) with $i \neq j$. Here $t_s = t_{s-1}$ and $t_s(i, j) = p \in \mathbb{P}$, since otherwise the earlier task (i, j) had removed (i, j, r). We argue that the choice of the specified t_s-valid w_s is possible, which shows that the construction in step s is possible and which contradicts the assumption.

We apply Corollary 2.15 for $n = p^k$, where k is chosen large enough such that the corollary

holds for that n and w_{s-1} is not defined for words of length $\geq n$. Consider the minimal $w' \sqsupseteq w_{s-1}$ that is defined for all words of length $< n$. By Claim 5.4, w' is t_s-valid. By Corollary 2.15, there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that at least one of the statements 1-3 holds.

If statement 1 holds, then choose the minimal $w_s \supsetneq w'$ that contains x and that is defined for all words of length $\leq (n^r + r)^i + i$. The latter makes sure that the computations $F_r^{w_s}(0^n)$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ are defined and will not change when we extend w_s. By interpreting w' and w_s as sets, we obtain $w_s = w' \cup \{x\}$, i.e., we added exactly the word x to the oracle. Note that w' is a t_s-valid oracle defined for all words of length $< n$ and undefined for all other words. After adding x, the oracle still satisfies V2 in the definition of t_s-valid, since we only added one word and w' contains no word of this length. The remaining conditions V1, V3, and V4 are not affected by x, since x has odd length. Hence w_s is t_s-valid. $0^n \in A_p^{w_s}$, since $x \in w_s$. The computation $F_r^{w_s}(0^n)$ is defined and by statement 1 of Corollary 2.15, its output is definitely rejected by $M_i^{w_s}$. Thus we have seen that if statement 1 holds, then the construction in step s is possible. For statement 2 this is shown analogously.

It remains to show that statement 3 cannot hold. Otherwise, for $z = F_r^{w' \cup \{x,y\}}(0^n)$ it holds that $z \in L(M_i^{w' \cup \{x,y\}}) \cap L(M_j^{w' \cup \{x,y\}})$. Consider the smallest step s' where $t_{s'}(i,j)$ is defined. This step extends $t_{s'-1}$ such that $t_{s'} = t_{s'-1} \cup \{(i,j) \mapsto p\}$. Thus we have $s' \leq s-1$ and $w_{s'-1} \subsetneq w_{s'} \sqsubseteq w_{s-1} \sqsubseteq w'$. We know that w' is t_s-valid and hence $t_{s'-1}$-valid, by Claim 5.2. Choose the minimal $v \sqsupseteq w'$ that contains x, y and that is defined for all words of length $\leq (n^r + r)^{i+j} + i + j$. Hence $M_i^v(z)$ and $M_j^v(z)$ definitely accept. The interpretation of w' and v as sets illustrates $v = w \cup \{x, y\}$, i.e., we added exactly the words x, y. We know that w' is a $t_{s'-1}$-valid oracle defined for all words of length $< n$ and undefined for all other words. After adding x and y, the oracle still satisfies V2 in the definition of $t_{s'-1}$-valid, since $|x| = p^k \notin \mathrm{ran}(t_{s'-1})$. The remaining conditions V1, V3, and V4 are not affected by x and y, since x and y have odd length. Hence v is $t_{s'-1}$-valid and even t'-valid for $t' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$, since $M_i^v(z)$ and $M_j^v(z)$ definitely accept. Therefore, step s' defines $t_{s'} = t'$ and chooses the oracle in an appropriate way (e.g., $w_{s'} = v$), which contradicts $t_{s'}(i,j) = p$. This shows that statement 3 cannot hold.

Thereby we have shown that in steps treating tasks (i,j,r), the choice of the specified t_s-valid w_s is possible, which contradicts the assumption. □

Recall $O = \lim_{s \to \infty} w_s$ and note that O is totally defined, since each step strictly extends the oracle.

Claim 5.6 DisjNP^O *has no* $\leq_{\mathrm{m}}^{\mathrm{pp},O}$*-complete pairs.*

Proof Assume there exists a $\leq_{\mathrm{m}}^{\mathrm{pp},O}$-complete $(L(M_i^O), L(M_j^O)) \in \mathrm{DisjNP}^O$. From $L(M_i^O) \cap L(M_j^O) = \emptyset$ if follows that for all s there is no z such that $M_i^{w_s}(z)$ and $M_j^{w_s}(z)$ definitely accept. Hence $t_s(i,j) \neq 0$ for all s for which $t_s(i,j)$ is defined. Let s be the step that treats task (i,j). Thus $t_{s'}(i,j) = p \in \mathbb{P}$ for all $s' \geq s$, which implies that $A_p^O \cap B_p^O = \emptyset$. Thus there exists an r such that $(A_p^O, B_p^O) \leq_{\mathrm{m}}^{\mathrm{pp},O} (L(M_i^O), L(M_j^O))$ via F_r^O. Let s' be the step that treats task (i,j,r). This step makes sure that at least one of the two specified properties holds, which implies that at least one of the following holds.

- $0^n \in A_p^O$ and $F_r^O(0^n)$ is rejected by M_i^O
- $0^n \in B_p^O$ and $F_r^O(0^n)$ is rejected by M_j^O

This contradicts the choice of r. □

Claim 5.7 *There exist disjoint sets $A, B \in \mathrm{NPC}_{\mathrm{m}}^{\mathrm{p},O}$ such that $A \cup B$ is not $\leq_{\mathrm{m}}^{\mathrm{p},O}$-hard for NP^O.*

Proof First we show that $K^O \cup \Delta^O$ is not $\leq_{\mathrm{m}}^{\mathrm{p},O}$-hard for NP^O. Assume this is wrong. Then $\Gamma^O \leq_{\mathrm{m}}^{\mathrm{p},O} K^O \cup \Delta^O$ witnessed by some F_i^O for $i \in \mathbb{N}^+$. Let $s \in \mathbb{N}^+$ be the step where the task (i,i) is considered. Then $t_s(i,i) = 0$. As w_s is t_s-valid, for all $v \sqsupseteq w_s$, F_i^v does not reduce Γ^v to $K^v \cup \Delta^v$, a contradiction to the assumption that $\Gamma^O \leq_{\mathrm{m}}^{\mathrm{p},O} K^O \cup \Delta^O$ via F_i^O.

Define $A = 0K^O \cup 1\Delta^O$ and $B = 1K^O \cup 0\Delta^O$. The sets A and B are disjoint and NP^O-complete since $K^O \leq_{\mathrm{m}}^{\mathrm{p}} A$ via $x \mapsto 0x$ and $K^O \leq_{\mathrm{m}}^{\mathrm{p}} B$ via $x \mapsto 1x$. Moreover, $A \cup B = 0(K^O \cup \Delta^O) \cup 1(K^O \cup \Delta^O) \leq_{\mathrm{m}}^{\mathrm{p}} K^O \cup \Delta^O$ via $ax \mapsto x$ for $a \in \{0,1\}$ and thus $A \cup B$ is not $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O. □

This completes the proof of Theorem 5.1. □

6 An Oracle for $\mathrm{H}_{\mathbf{union}}$ and $\neg\mathrm{H}_{\mathbf{cpair}}$

This section shows that the implication $\mathrm{H}_{\mathrm{union}} \Rightarrow \mathrm{H}_{\mathrm{cpair}}$ cannot be proven in a relativizable way. Ogiwara and Hemachandra [OH93] construct an oracle that proves that the converse implication $\mathrm{H}_{\mathrm{cpair}} \Rightarrow \mathrm{H}_{\mathrm{union}}$ cannot be proven in a relativizable way as well. Thus $\mathrm{H}_{\mathrm{union}}$ and $\mathrm{H}_{\mathrm{cpair}}$ are independent of each other under relativizable proofs.

Theorem 6.1 *There exists an oracle O with the following properties.*

1. DisjNP^O *has no $\leq_{\mathrm{m}}^{\mathrm{pp},O}$-complete pairs.*
2. *If A is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O and disjoint to $B \in \mathrm{NP}^O$, then $A \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O.*

Proof [Proof of Theorem 6.1] Let $M_1, M_2, M_3, \ldots$ be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines. Let $F_1, F_2, F_3, \ldots$ be a standard enumeration of deterministic, polynomial-time oracle Turing transducers.

Define the following sets for an oracle $D \subseteq \mathbb{N}$.

$$\begin{aligned} K^D &= \{\langle 0^i, 0^j, x\rangle \mid i > 0 \text{ and } M_i^D(x) \text{ accepts within } j \text{ steps}\} \\ K_\vee^D &= \{\langle z_1, \ldots, z_n\rangle \mid z_1 \in K^D \vee \cdots \vee z_n \in K^D\} \end{aligned}$$

K^D and $K_\vee^D$ are $\leq_{\mathrm{m}}^{\mathrm{p},D}$-complete for NP^D. We construct the oracle such that $K_\vee^O \cup B$ is NP^O-complete for all $B \in \mathrm{NP}^O$ disjoint from $K_\vee^O$ and show that this implies the second statement of the theorem.

For an oracle D let

$$E^D = \{0^n \mid \exists x \in D \text{ such that } |x| = n\}$$

and observe that $E^D \in \mathrm{NP}^D$. Choose $e \in \mathbb{N}$ such that $L(M_e^D) = E^D$ for all oracles D and let $v_n = \langle 0^e, 0^{n^e+e}, 0^n\rangle$. Hence $v_n \in K^D$ if and only if $M_e^D(0^n)$ accepts, i.e., $v_n \in K^D \Leftrightarrow 0^n \in E^D$.

For an oracle D and a prime p define the following sets.

$$\begin{aligned} A_p^D &= \{0^{p^k} \mid k \geq 1 \text{ and there exists an even } x \in D \text{ such that } |x| = p^k\} \\ B_p^D &= \{0^{p^k} \mid k \geq 1 \text{ and there exists an odd } x \in D \text{ such that } |x| = p^k\} \end{aligned}$$

We construct the oracle such that for certain primes p it holds that for each k there is at most one $x \in O$ such that $|x| = p^k$. Hence for these p we have $(A_p^O, B_p^O) \in \mathrm{DisjNP}^O$.

Preview of construction: On the one hand, the construction tries to prevent that M_i and M_j accept disjoint sets. If this is not possible, then $L(M_i)$ and $L(M_j)$ are inherently disjoint. In this case, for a suitable $p \in \mathbb{P}$, the construction makes sure that (A_p, B_p) does not $\leq_{\mathrm{m}}^{\mathrm{pp}}$-reduce to $(L(M_i), L(M_j))$, which prevents the existence of complete disjoint NP-pairs. On the other hand, the construction also tries to prevent that M_i accepts a set disjoint from $K_\vee$. If this is not possible, then M_i inherently accepts a set disjoint from $K_\vee$. In this case, there will be a prime p such that the words v_{p^k} for $k \geq 1$ are neither in K nor in $L(M_i)$. It even holds $\langle v_{p^k}, u_1, \ldots, u_n\rangle \notin L(M_i)$ for all $u = \langle u_1, \ldots, u_n\rangle$ of length $\leq |v_{p^k}|$. This means that the v_{p^k} are difficult instances for M_i, since there is no linear-size proof u that allows M_i to recognize that $v_{p^k} \notin K$. Hence adding a sufficiently large v_{p^k} to an instance u does not change the membership to $K_\vee$, but guarantees that the result is not in $L(M_i)$. This yields a reduction $K_\vee \leq_{\mathrm{m}}^{\mathrm{p}} K_\vee \cup L(M_i)$ and implies that $K_\vee \cup L(M_i)$ is NP-complete.

During the oracle construction we maintain a growing collection of properties that we demand in the further construction. The collection is represented by a function t and if an oracle satisfies the properties defined by t, then we call it t-valid. More precisely, we start with the nowhere defined function $t_0 : \mathbb{N} \times \mathbb{N} \to \mathbb{P} \cup \{0\}$, which defines no property. We successively continue this function and obtain $t_1, t_2, \ldots$, which have a finite, but growing domain. At the end of the construction we reach the total function $\lim_{i\to\infty} t_i$.

Let $t \in \mathcal{T} := \{t : \mathbb{N} \times \mathbb{N} \to \mathbb{P} \cup \{0\} \mid t \text{ has finite domain and is injective on } \mathrm{supp}(t)\}$. An oracle $w \in \Sigma^*$ is t-valid, if for all $(i, j) \in \mathrm{dom}(t)$:

V1: If $i \neq j$ and $t(i, j) = 0$, then $\exists z$ such that $M_i^w(z)$ and $M_j^w(z)$ definitely accept.
(meaning: $L(M_i^v) \cap L(M_j^v) \neq \emptyset$ for all $v \sqsupseteq w$)

V2: If $i \neq j$ and $t(i, j) = p \in \mathbb{P}$, then $\forall k \geq 1$ it holds that $|\{x \in w \mid |x| = p^k\}| \leq 1$.
(meaning: (A_p^w, B_p^w) is a disjoint NP^w-pair)

V3: If $i = j$ and $t(i, i) = 0$, then $\exists n \exists u_0, \ldots, u_n$ such that $M_i^w(\langle u_0, \ldots, u_n\rangle)$ definitely accepts, $u_0 = \langle 0^{i_0}, 0^{j_0}, x_0\rangle$, and $M_{i_0}^w(x_0)$ definitely accepts within j_0 steps.
(meaning: $\langle u_0, \ldots, u_n\rangle \in K_\vee^v \cap L(M_i^v)$ for all $v \sqsupseteq w$)

V4: If $i = j$ and $t(i, i) = p \in \mathbb{P}$, then $\forall k \geq 1$ it holds that $\{x \in w \mid |x| = p^k\} = \emptyset$.
(meaning: for all $k \geq 1$ it holds that $0^{p^k} \notin E^w$ and hence $v_{p^k} \notin K^w$)

This definition leads to the following observations.

Claim 6.2 *Let $t, t' \in \mathcal{T}$ such that t' is a continuation of t. If w is t'-valid, then w is t-valid.*

Claim 6.3 *Let $t \in \mathcal{T}$ and $w \in \Sigma^*$. If w is t-valid, then $w0$ is t-valid.*

Oracle construction: Let t_0 be the nowhere defined function and $w_0 = \varepsilon$, which is t_0-valid. We construct a sequence of partially defined oracles $w_0 \sqsubsetneq w_1 \sqsubsetneq \cdots$ and a sequence $t_0, t_1, \ldots$ of functions from $\mathcal{T}$ such that w_i is t_i-valid and t_{i+1} is a continuation of t_i. The final oracle is $O = \lim_{n\to\infty} w_n$. Each step treats the first task in our task list T and removes this and possibly other tasks from the list. At the beginning, T consists of an enumeration of all $(i, j) \in \mathbb{N}^2$ and all $(i, j, r) \in \mathbb{N}^3 - \{(i, i, r) \mid i, r \in \mathbb{N}\}$ in an order having the property that (i, j) appears earlier than (i, j, r) for all i, j, r with $i \neq j$. We describe step s, which starts with a t_{s-1}-valid oracle w_{s-1} and extends it to a t_s-valid $w_s \sqsupsetneq w_{s-1}$.

- task (i,j) with $i \neq j$: Let $t' = t_{s-1} \cup \{(i,j) \mapsto 0\}$. If there exists a t'-valid $v \sqsupsetneq w_{s-1}$, then let $t_s = t'$, $w_s = v$, and remove all tasks $(i,j,\cdot)$ from T. Otherwise choose $p \in \mathbb{P} - \mathrm{ran}(t_{s-1})$ such that $p > |w_{s-1}|$ and let $t_s = t_{s-1} \cup \{(i,j) \mapsto p\}$ and $w_s = w_{s-1}0$.
(meaning: if possible, force $L(M_i) \cap L(M_j) \neq \emptyset$, otherwise choose a suitable prime p and make sure that the oracle contains at most one element of length p^k for all k and hence (A_p, B_p) is a disjoint NP-pair; corresponds to V1 and V2)

- task (i,i): Let $t' = t_{s-1} \cup \{(i,i) \mapsto 0\}$. If there exists a t'-valid $v \sqsupsetneq w_{s-1}$, then let $t_s = t'$ and $w_s = v$. Otherwise choose $p \in \mathbb{P} - \mathrm{ran}(t_{s-1})$ such that $p > |w_{s-1}|$ and $(3|v_{p^k}| + 2)^i + i < 2^{p^k}$ for all $k \geq 1$, and let $t_s = t_{s-1} \cup \{(i,i) \mapsto p\}$ and $w_s = w_{s-1}0$.
(meaning: if possible, force $K_\vee \cap L(M_i) \neq \emptyset$, otherwise choose a suitable prime p and make sure that the oracle contains no element of length p^k and hence $v_{p^k} \notin K$ for all k; corresponds to V3 and V4)

- task (i,j,r) with $i \neq j$: It holds that $t_{s-1}(i,j) = p \in \mathbb{P}$. Let $t_s = t_{s-1}$ and choose a t_s-valid $w_s \sqsupsetneq w_{s-1}$ such that for a suitable 0^n at least one of the following holds.
  - $0^n \in A_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_i^{w_s}$
  - $0^n \in B_p^{w_s}$, $F_r^{w_s}(0^n)$ is defined, and its output is definitely rejected by $M_j^{w_s}$

  (meaning: F_r does not realize a reduction $(A_p, B_p) \leq_{\mathrm{m}}^{\mathrm{pp}} (L(M_i), L(M_j))$)

Claim 6.4 *For all $s \geq 1$, the construction of w_s and t_s in step s is possible and w_s is t_s-valid.*

Proof We prove the contraposition. Choose the smallest step s where the claim fails. Assume that this steps treats a task (i,j) for $i,j \in \mathbb{N}$. Hence $t_{s-1}(i,j)$ is not defined, since it can only be defined by the unique treatment of task (i,j). Therefore, t' and t_s can be defined as specified, which shows that the construction in step s is possible. If a t'-valid $v \sqsupsetneq w_{s-1}$ exists, then w_s is t_s-valid, which contradicts the assumption. Otherwise, $t_s = t_{s-1} \cup \{(i,j) \mapsto p\}$ for a prime p chosen according to the construction above and by Claim 6.3, w_s is t_{s-1}-valid. The choice of p implies that w_s does not contain words of length p^k for $k \geq 1$. Therefore, w_s is also t_s-valid, which contradicts the assumption.

From now on we assume that step s treats a task (i,j,r) with $i \neq j$. Here $t_s = t_{s-1}$ and $t_s(i,j) = p \in \mathbb{P}$, since otherwise the earlier task (i,j) had removed (i,j,r). We argue that the choice of the specified t_s-valid w_s is possible, which shows that the construction in step s is possible and which contradicts the assumption.

We apply Corollary 2.15 for $n = p^k$, where k is chosen large enough such that the corollary holds for that n and w_{s-1} is not defined for words of length $\geq n$. Consider the minimal $w' \sqsupseteq w_{s-1}$ that is defined for all words of length $< n$. By Claim 6.3, w' is t_s-valid. By Corollary 2.15, there exist an even $x \in \Sigma^n$ and an odd $y \in \Sigma^n$ such that at least one of the statements 1-3 holds.

If statement 1 holds, then choose the minimal $w_s \sqsupsetneq w'$ that contains x and that is defined for all words of length $\leq (n^r + r)^i + i$. The latter makes sure that the computations $F_r^{w_s}(0^n)$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ are defined and will not change when we extend w_s. By interpreting w' and w_s as sets, we obtain $w_s = w' \cup \{x\}$, i.e., we added exactly the word x to the oracle. Note that w' is a t_s-valid oracle defined for all words of length $< n$ and undefined for all other words. After adding x, the oracle still satisfies V2, since we added only one word and w' contains no words of this length. The remaining conditions V1, V3, and V4 are not affected by x, since t_s is injective on its support. Hence w_s is t_s-valid. $0^n \in A_p^{w_s}$, since $x \in w_s$. The computation $F_r^{w_s}(0^n)$ is defined and by statement 1 of Corollary 2.15, its output is definitely rejected by $M_i^{w_s}$. Thus we have seen that if statement 1 holds, then the construction in step s is possible. For statement 2 this is shown analogously.

It remains to show that statement 3 cannot hold. Otherwise, for $z = F_r^{w' \cup \{x,y\}}(0^n)$ it holds that $z \in L(M_i^{w' \cup \{x,y\}}) \cap L(M_j^{w' \cup \{x,y\}})$. Consider the smallest step s' where $t_{s'}(i,j)$ is defined. This step extends $t_{s'-1}$ such that $t_{s'} = t_{s'-1} \cup \{(i,j) \mapsto p\}$. Thus we have $s' \leq s-1$ and $w_{s'-1} \sqsubsetneq w_{s'} \sqsubseteq w_{s-1} \sqsubseteq w'$. We know that w' is t_s-valid and hence $t_{s'-1}$-valid, by Claim 6.2. Choose the minimal $v \sqsupseteq w'$ that contains x, y and that is defined for all words of length $\leq (n^r + r)^{i+j} + i + j$. Hence $M_i^v(z)$ and $M_j^v(z)$ definitely accept. The interpretation of w' and v as sets illustrates $v = w \cup \{x, y\}$, i.e., we added exactly the words x, y. We know that w' is a $t_{s'-1}$-valid oracle defined for all words of length $< n$ and undefined for all other words. After adding x and y, the oracle still satisfies V2 in the definition of $t_{s'-1}$-valid, since $|x| = p^k \notin \mathrm{ran}(t_{s'-1})$. The remaining conditions V1, V3, and V4 are not affected by x and y, since $t_{s'-1}$ is injective on its support. Hence v is $t_{s'-1}$-valid and even t'-valid for $t' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$, since $M_i^v(z)$ and $M_j^v(z)$ definitely accept. Therefore, step s' defines $t_{s'} = t'$ and $w_{s'} = v$, which contradicts $t_{s'}(i,j) = p$. This shows that statement 3 cannot hold.

Thereby we have shown that in steps treating tasks (i,j,r), the choice of the specified t_s-valid w_s is possible, which contradicts the assumption. □

Consider our construction at some step s and assume that $t_s(i,i) = p \in \mathbb{P}$. Thus it was not possible to achieve $K_\vee^{w_s} \cap L(M_i^{w_s}) \neq \emptyset$ and hence $K_\vee^{w_s}$ and $L(M_i^{w_s})$ are disjoint. By V4, w_s does not contain words of length p^k and hence $v_{p^k} \notin K^{w_s}$ for all $k \geq 1$. The following claim asserts that these v_{p^k} are not accepted by $M_i^{w_s}$, even if we add arbitrary information of size at most $|v_{p^k}|$ to the instance. This means that the words v_{p^k} are instances from $\overline{K^{w_s}}$ that are difficult in the sense that there is no proof of size at most $|v_{p^k}|$ that allows $M_i^{w_s}$ to recognize these words.

Claim 6.5 *If $t_s(i,i) = p \in \mathbb{P}$, then for all $k \geq 1$, $n \in \mathbb{N}$, and $u_1, \ldots, u_n \in \mathbb{N}$ with $|\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|$ it does not hold that $M_i^{w_s}(\langle v_{p^k}, u_1, \ldots, u_n \rangle)$ definitely accepts (i.e., is not defined or definitely rejects).*

Proof Assume there exists $k \geq 1$, $n \in \mathbb{N}$, and $u_1, \ldots, u_n \in \mathbb{N}$ such that $|\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|$ and $M_i^{w_s}(\langle v_{p^k}, u_1, \ldots, u_n \rangle)$ definitely accepts. Let l be the minimal path that definitely accepts and choose the smallest word q of length p^k that is not queried on l. Such a word exists, since $|\langle v_{p^k}, u_1, \ldots, u_n \rangle| \leq 3|v_{p^k}| + 2$ by our pairing function and $(3|v_{p^k}| + 2)^i + i < 2^{p^k}$ by the choice of p. Consider the smallest step s' where $t_{s'}(i,i)$ is defined. This step extends $t_{s'-1}$ such that $t_{s'} = t_{s'-1} \cup \{(i,i) \mapsto p\}$. Let w' be the word obtained from w_s by changing the letter $w(q)$ from 0 to 1. Hence $w' = w_s \cup \{q\}$, where w' and w_s are interpreted as sets. By Claim 6.2, w_s is $t_{s'-1}$-valid. Even w' is $t_{s'-1}$-valid: adding q does not affect the properties V1 and V3 in the definition of $t_{s'-1}$-valid, since the mentioned computations definitely accept with oracle $w_{s'-1}$ and $|q| \geq p > |w_{s'-1}|$; and it does not affect V2 and V4, because $|q| = p^k$ and $p \notin \mathrm{ran}(t_{s'-1})$. Choose the minimal $v \sqsupseteq w'$ that is defined for all words of length $\leq p^{ke} + e$. Hence $w_{s'-1} \sqsubsetneq v$ and $v = w_s \cup \{q\}$. By Claim 6.3, v is $t_{s'-1}$-valid. $M_i^v(\langle v_{p^k}, u_1, \ldots, u_n \rangle)$ still definitely accepts on l, since this path does not query q. From $q \in v$ it follows that $0^{p^k} \in E^v = L(M_e^v)$ and hence $M_e^v(0^{p^k})$ definitely accepts within $p^{ke} + e$ steps. By defining $u_0 = v_{p^k}$, $i_0 = e$, $j_0 = p^{ke} + e$, and $x_0 = 0^{p^k}$ we see that $M_i^v(u_0, \ldots, u_n)$ definitely accepts, $u_0 = \langle 0^{i_0}, 0^{j_0}, x_0 \rangle$, and $M_{i_0}^v(x_0)$ definitely accepts within j_0 steps. This shows that v is even t'-valid for $t' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$. Therefore, step s' defines $t_{s'} = t'$ and chooses the oracle $w_{s'}$ in an appropriate way (e.g., $w_{s'} = v$), which contradicts $t_{s'}(i,j) = p$. □

Let $w = \lim_{s \to \infty} w_s$ be the oracle obtained by the whole construction. It is totally defined, since each step strictly extends the oracle.

Claim 6.6 DisjNP^O *has no $\leq_{\mathrm{m}}^{\mathrm{pp},O}$-complete pairs.*

Proof Assume there exists an $\leq_{\mathrm{m}}^{\mathrm{pp},O}$-complete $(L(M_i^O), L(M_j^O)) \in \mathrm{DisjNP}^O$. From $L(M_i^O) \cap L(M_j^O) = \emptyset$ if follows that for all s there is no z such that $M_i^{w_s}(z)$ and $M_j^{w_s}(z)$ definitely accept. Hence $t_s(i,j) \neq 0$ for all s. Let s be the step that treats task (i,j). Thus $t_{s'}(i,j) = p \in \mathbb{P}$ for all $s' \geq s$, which implies that $A_p^O \cap B_p^O = \emptyset$. Thus there exists an r such that $(A_p^O, B_p^O) \leq_{\mathrm{m}}^{\mathrm{pp},O} (L(M_i^O), L(M_j^O))$ via F_r^O. Let s' be the step that treats task (i,j,r). This step makes sure that at least one of two specified properties holds, which implies that at least one of the following holds.

- $0^n \in A_p^O$ and $F_r^O(0^n)$ is rejected by M_i^O
- $0^n \in B_p^O$ and $F_r^O(0^n)$ is rejected by M_j^O

This contradicts the choice of r. □

Claim 6.7 *$K_\vee^O \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O for all $B \in \mathrm{NP}^O$ that are disjoint to $K_\vee^O$.*

Proof Choose i such that $B = L(M_i^O)$ and let s be the step that treats task (i,i). We claim that $t_s(i,i) = p \in \mathbb{P}$. Otherwise there exist $u_0, \ldots, u_n$ such that $M_i^{w_s}(\langle u_0, \ldots, u_n \rangle)$ definitely accepts, $u_0 = \langle 0^{i_0}, 0^{j_0}, x_0 \rangle$, and $M_{i_0}^{w_s}(x_0)$ definitely accepts within j_0 steps. Hence $u_0 \in K^O$, $\langle u_0, \ldots, u_n \rangle \in K_\vee^O$, and $M_i^O(\langle u_0, \ldots, u_n \rangle)$ accepts. This contradicts the assumption $K_\vee^O \cap L(M_i^O) = \emptyset$ and shows $t_s(i,i) = p \in \mathbb{P}$.

It follows that $t_{s'}(i,i) = p \in \mathbb{P}$ for all $s' \geq s$. Thus for all $k \geq 1$, O does not contain elements of length p^k and hence $v_{p^k} \notin K^O$. By Claim 6.5, for all $s' \geq s$, $k \geq 1$, $n \in \mathbb{N}$, and $u_1, \ldots, u_n \in \mathbb{N}$ with $|\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|$ it does not hold that the computation $M_i^{w_{s'}}(\langle v_{p^k}, u_1, \ldots, u_n \rangle)$ definitely accepts. Therefore,

$$\forall k \geq 1, n \in \mathbb{N}, u_1, \ldots, u_n \in \mathbb{N} \text{ with } |\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|, \quad M_i^O(\langle v_{p^k}, u_1, \ldots, u_n \rangle) \text{ rejects.} \quad (10)$$

Let $f(\langle u_1, \ldots, u_n \rangle) = \langle u_0, u_1, \ldots, u_n \rangle$, where $u_0 = v_{p^k}$ for the minimal $k \geq 1$ such that $|\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|$. It holds that $f \in \mathrm{FP} \subseteq \mathrm{FP}^O$. We argue that f reduces $K_\vee^O$ to $K_\vee^O \cup B$. If $\langle u_1, \ldots, u_n \rangle \in K_\vee^O$, then $f(\langle u_1, \ldots, u_n \rangle) \in K_\vee^O$.

Assume now $\langle u_1, \ldots, u_n \rangle \notin K_\vee^O$. From $v_{p^k} \notin K^O$ it follows $f(\langle u_1, \ldots, u_n \rangle) \notin K_\vee^O$. Moreover, $f(\langle u_1, \ldots, u_n \rangle) \notin B = L(M_i^O)$, since otherwise $f(\langle u_1, \ldots, u_n \rangle) = \langle v_{p^k}, u_1, \ldots, u_n \rangle$ is a counterexample for (10).

Hence f reduces $K_\vee^O$ to $K_\vee^O \cup B$, which implies that $K_\vee^O \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O. □

Claim 6.8 *If A is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O and disjoint to $B \in \mathrm{NP}^O$, then $A \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O.*

Proof Otherwise there exist counterexamples A and B. Choose $f \in \mathrm{FP}^O$ such that $K_\vee^O \leq_{\mathrm{m}}^{\mathrm{p},O} A$ via f and let $B' = f^{-1}(B)$. Observe that $B' \in \mathrm{NP}^O$, $K_\vee^O \cap B' = \emptyset$, and $K_\vee^O \cup B' \leq_{\mathrm{m}}^{\mathrm{p},O} A \cup B$ via f. Hence $K_\vee^O \cup B'$ is not $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O, which contradicts Claim 6.7. □

This finishes the proof of Theorem 6.1. □

7 An Oracle for $\mathrm{H}_{\mathrm{union}}$ and $\mathrm{H}_{\mathrm{opps}}$

In this section we construct an oracle O which shows that a relativizable proof of the implication $\mathrm{H}_{\mathrm{opps}} \Rightarrow \neg\mathrm{H}_{\mathrm{union}}$ does not exist. As according to Theorem 5.1 neither the converse implication can be proven in a relativizable way, the two assertions $\mathrm{H}_{\mathrm{cpair}}$ and $\neg\mathrm{H}_{\mathrm{union}}$ are independent of each other under relativizable proofs.

In addition (cf. Corollaries 7.13 and 7.15), relative to O there exists a "super-tally" set in NP − coNP as well as a tally set in NEE − coNEE, where $\mathrm{NEE} \stackrel{df}{=} \mathrm{NTIME}(2^{O(2^n)})$. This is of interest as it shows that the converses of the following implications by Köbler, Messner, and Torán [KMT03] fail relative to O.

- $\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE} \;\Rightarrow\; \mathrm{H}_{\mathrm{opps}}$
- $\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE} \;\Rightarrow\;$ there exist P-optimal pps

Theorem 7.1 *There exists an oracle O with the following properties.*

1. *There exists a P^O-optimal propositional proof system f.*
2. *If A is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O and disjoint to $B \in \mathrm{NP}^O$, then $A \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O.*

Proof Let $M_1, M_3, M_5, \ldots$ be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines. Let $F_2, F_4, F_6, \ldots$ be a standard enumeration of deterministic, polynomial-time oracle Turing transducers.

For $D \subseteq \mathbb{N}$ we define sets K^D, $K_\vee^D$, and E^D similar to those in the proof of Theorem 6.1.

$$\begin{aligned} K^D &= \{\langle 0^i, 0^j, x\rangle \mid i \text{ is odd and } M_i^D(x) \text{ accepts within } j \text{ steps}\} \\ K_\vee^D &= \{\langle z_1, \ldots, z_n\rangle \mid z_1 \in K^D \vee \cdots \vee z_n \in K^D\} \end{aligned}$$

Claim 7.2 *For oracles v and w and all $y \leq \min(|v|, |w|)$, if $\mathrm{pr}_y(v) = \mathrm{pr}_y(w)$, then $K^w(y) = K^v(y)$ and $K_\vee^w(y) = K_\vee^v(y)$.*

Proof It suffices to show $K^w(y) = K^v(y)$. We may assume $y = \langle 0^i, 0^j, x\rangle$ for suitable i, j, x, since otherwise $K^w(y) = K^v(y) = 0$. For each q that is queried within the first j steps of $M_i^w(x)$ or $M_i^v(x)$ it holds that $|q| \leq j < |y|$ and thus $q < y$. Hence these queries are answered the same way relative to w and v, showing that $M_i^w(x)$ accepts if and only if $M_i^v(x)$ accepts. □

K^D and $K_\vee^D$ are $\leq_{\mathrm{m}}^{\mathrm{p},D}$-complete for NP^D and their complements are $\leq_{\mathrm{m}}^{\mathrm{p},D}$-complete for coNP^D. We construct the oracle such that $\overline{K_\vee^D}$ has a P^O-optimal proof system $f \in \mathrm{FP}^O$. As $\overline{K_\vee^O}$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for coNP^O, this implies the first statement of the theorem.

For an oracle D let

$$E^D = \{0^n \mid \exists x \in D \text{ such that } |x| = n\}$$

and observe that $E^D \in \mathrm{NP}^D$. Choose $e \geq 2$ such that $L(M_e^D) = E^D$ for all oracles D and let $v_n = \langle 0^e, 0^{n^e+e}, 0^n\rangle$. Hence $v_n \in K^D$ if and only if $M_e^D(0^n)$ accepts, i.e., $v_n \in K^D \Leftrightarrow 0^n \in E^D$.

For $i \in 2\mathbb{N}^+$ and $x, y \in \mathbb{N}$ let $c(i, x, y) = \langle 0^i, 0^{(|x|^i+i)^{2ie}}, x, y\rangle$. These words are used to encode proofs into the oracle: if the oracle contains the codeword $c(i, x, y)$, then this means $F_i(x) = y$ and $y \notin K_\vee$, i.e., $c(i, x, y)$ is a proof for $y \notin K_\vee$.

Claim 7.3 *The following holds for all oracles w, all $i \in 2\mathbb{N}^+$ and $x, y \in \mathbb{N}$.*

1. *If $c(i, x, y) \leq |w|$, then $F_i^w(x)$ is defined and $F_i^v(x) = F_i^w(x) < |w|$ for all $v \sqsupseteq w$.*
2. *If $c(i, x, y) \leq |w|$, then $F_i^w(x)$ is defined and $F_i^w(x) \in K_\vee^w \Leftrightarrow F_i^v(x) \in K_\vee^v$ for all $v \sqsupseteq w$.*

Proof 1: $F_i^w(x)$ is defined, since for each q queried by $F_i^w(x)$ it holds that $|q| \leq |x|^i + i < |c(i,x,y)|$ and hence $q < c(i,x,y) \leq |w|$. The same argument shows $F_i^v(x) = F_i^w(x) < |w|$. 2: Follows from Claims 7.3.1 and 7.2. □

Preview of construction: On the one hand, the construction tries to prevent that F_i is a proof system for $\overline{K_\vee}$. If this is not possible, then F_i inherently is a proof system for $\overline{K_\vee}$. In this case, the codewords $c(i,x,y)$ are used to encode F_i-proofs into the oracle. These encodings finally yield a P-optimal proof system for $\overline{K_\vee}$. On the other hand, the construction also tries to prevent that M_i accepts a set disjoint from $K_\vee$. If this is not possible, then M_i inherently accepts a set disjoint from $K_\vee$. In this case, there will be a prime p such that the words v_{p^k} for $k \geq 1$ are neither in K nor in $L(M_i)$. It even holds $\langle v_{p^k}, u_1, \ldots, u_n\rangle \notin L(M_i)$ for all $u = \langle u_1, \ldots, u_n\rangle$ of length $\leq |v_{p^k}|$. This means that the v_{p^k} are difficult instances for M_i, since there is no linear-size proof u that allows M_i to recognize that $v_{p^k} \notin K$. Hence adding a sufficiently large v_{p^k} to an instance u does not change the membership to $K_\vee$, but guarantees that the result is not in $L(M_i)$. This yields a reduction $K_\vee \leq_{\mathrm{m}}^{\mathrm{p}} K_\vee \cup L(M_i)$ and implies that $K_\vee \cup L(M_i)$ is NP-complete.

During the construction we maintain a growing list of properties. This list belongs to the set $\mathcal{T} = \{(m_1, \ldots, m_n) \mid n \geq 0,\ m_1, \ldots, m_n \in \mathbb{N}, \text{ and } m_i < m_j \text{ for all } i < j \text{ with } m_j \neq 0\}$. If an oracle satisfies the properties defined by a list t, then we call it t-valid. For a list $t = (m_1, \ldots, m_n)$ and $a \in \mathbb{N}$ let $t(i) = m_i$, $|t| = n$, and $t + a = (m_1, \ldots, m_n, a)$. If the list t is a prefix of the list t', then we write $t \sqsubseteq t'$. We start with the empty list $t_0 = ()$, which defines no property. By successively appending an element we obtain lists t_1, t_2, and so on.

An oracle $w \in \Sigma^*$ is t-valid, where $t \in \mathcal{T}$, if the following holds:

V1: $w \subseteq \{c(i,x,y) \mid i \in 2\mathbb{N}^+ \text{ and } x, y \in \mathbb{N}\} \cup \{v \mid |v| = p^k \text{ for } p \in \mathbb{P}^{\geq 41} \text{ and } k \geq 1\}$
(meaning: the oracle contains only codewords $c(i,x,y)$ and words of length p^k)

V2: For all $c(i,x,y) \in w$ with $i \in 2\mathbb{N}^+$ and $x, y \in \mathbb{N}$ it holds that $F_i^w(x) = y \notin K_\vee^w$.
(meaning: if the oracle contains the codeword $c(i,x,y)$, then $F_i^w(x)$ outputs $y \notin K_\vee^w$; hence $c(i,x,y) \in w$ is a proof for $y \notin K_\vee^w$)

V3: For all positive even $i \leq |t|$ it holds that $t(i) \in 2\mathbb{N}$ and:

(a) If $t(i) = m > 0$, then $c(i,x,y) \in w$ for all $x, y \in \mathbb{N}$ with $F_i^w(x) = y$ and $m \leq c(i,x,y) < |w|$.
(meaning: the oracle maintains codewords for F_i, i.e., if x is large enough and $F_i^w(x)$ outputs y, then w contains a proof for this, namely the codeword $c(i,x,y)$)

(b) If $t(i) = 0$, then there exists x such that $F_i^w(x)$ is defined and outputs $y < |w|$ with $y \in K_\vee^w$.
(meaning: F_i is not a proof system for $\overline{K_\vee}$ relative to all extensions of w)

V4: For all odd $i \leq |t|$ it holds that $t(i) \in \{0\} \cup \mathbb{P}^{\geq 41}$ and:

(a) If $t(i) = p > 0$, then $\{x \in w \mid |x| = p^k \text{ for } k \geq 1\} = \emptyset$ and for all positive even $j < i$ with $t(j) = 0$ it holds that $\{c(j,x,y) \in w \mid x, y \in \mathbb{N} \text{ and } |c(j,x,y)| \geq p\} = \emptyset$.
(meaning: the first part says $0^{p^k} \notin E^w$ and hence $v_{p^k} \notin K^w$ for all $k \geq 1$; the second part says that if F_j is no proof system for $\overline{K_\vee}$ and has a smaller index than M_i, then the oracle contains no codewords $c(j,\cdot,\cdot)$ of length $\geq p$)

(b) If $t(i) = 0$, then there exists $x < |w|$ such that $x \in K_\vee^w$ and $M_i^w(x)$ definitely accepts.
(meaning: M_i is not disjoint from $K_\vee$ relative to all extensions of w)

Claim 7.4 *The following holds in reference to the definition of t-valid.*

1. *In V1, the two sets are disjoint.*
2. *In V2, $F_i^w(x)$ is defined and $F_i^v(x) = y \notin K_\vee^v$ for all $v \sqsupseteq w$.*
3. *In V3a, $F_i^w(x)$ is defined.*
4. *In V3b, $y \in K_\vee^v$ for all $v \sqsupseteq w$.*
5. *In V4b, $x \in K_\vee^v$ for all $v \sqsupseteq w$.*

Proof V1: The union is disjoint, since $|c(i,x,y)|$ is even. V2+V3a: Follows from Claim 7.3. V3b+V4b: Follows from Claim 7.2. □

Claim 7.5 *Let $t, t' \in \mathcal{T}$ such that $t \sqsubseteq t'$. If w is t'-valid, then w is t-valid.*

Proof Follows from the definition of t-valid. □

Claim 7.6 *Let u and w be t-valid. If $u \sqsubseteq v \sqsubseteq w$, then v is t-valid.*

Proof We show that v satisfies V1–V4. When we consider w and v as sets, then $v \subseteq w$. Therefore, v satisfies V1 and V4a. Moreover, $v \sqsubseteq w$ and Claim 7.3 imply that v satisfies V2 and V3a.

Since u is t-valid, it satisfies V3b and V4b. From $u \sqsubseteq v$, Claim 7.4.4, and Claim 7.4.5 it follows that v satisfies V3b and V4b. □

Claim 7.7 *The following holds for all t-valid oracles w and $z = |w|$.*

1. *$w0$ is not t-valid if and only if $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x, y \in \mathbb{N}$ such that $i \leq |t|$, $t(i) > 0$, $z \geq t(i)$, and $F_i^w(x) = y$.*
2. *If $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+, x, y \in \mathbb{N}$ or $|z| = p^k$ for $p \in \mathbb{P}^{\geq 41}, k \geq 1$, then $w1$ satisfies V1.*
3. *If $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+, x, y \in \mathbb{N}$ such that $F_i^w(x) = y \notin K_\vee^w$, then $w1$ satisfies V2.*
4. *$w1$ satisfies V3 and V4b.*

Proof 1. Observe that $w0$ satisfies V1. By Claim 7.4.2, it satisfies V2. By 7.4.4 and 7.4.5, it satisfies V3b and V4b. It also satisfies V4a, since w and $w0$ describe the same sets. Hence $w0$ is not t-valid if and only if it does not satisfy V3a. The latter holds if and only if $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x, y \in \mathbb{N}$ such that $i \leq |t|$, $t(i) > 0$, $z \geq t(i)$, and $F_i^w(x) = y$, since w satisfies V3a, $z \notin w0$, and $F_i^w(x) = F_i^{w0}(x)$ by Claim 7.3.1. 2. Holds by definition. 3.+4. Hold by definition and Claim 7.4. □

Oracle construction: Let $t_0 = ()$ be the empty list and $w_0 = \varepsilon$, which is t_0-valid. We construct a sequence $t_0 \sqsubsetneq t_1 \sqsubsetneq \cdots$ of lists from $\mathcal{T}$ and a sequence $w_0 \sqsubsetneq w_1 \sqsubsetneq \cdots$ of partially defined oracles such that $|t_s| = s$ and w_s is t_s-valid. The final oracle is $O = \lim_{s\to\infty} w_s$. We describe step $s > 0$, which starts with a list t_{s-1} of length $s-1$ and a t_{s-1}-valid w_{s-1} and which defines a list $t_s \sqsupsetneq t_{s-1}$ of length s and a t_s-valid $w_s \sqsupsetneq w_{s-1}$.

- s even: If there is a t_{s-1}-valid $v \sqsupsetneq w_{s-1}$ such that for some x, $F_s^v(x)$ is defined and has an output $y < |v|$ with $y \in K_\vee^v$, then let $w_s = v$ and $t_s = t_{s-1} + 0$. Otherwise choose $b \in \{0,1\}$ such that $w_{s-1}b$ is t_{s-1}-valid, let $w_s = w_{s-1}b$ and $t_s = t_{s-1} + m$ for an even $m > |w_s|$ that is greater than all elements in t_{s-1}.
(meaning: if possible, then force that F_s is not a proof system for $\overline{K_\vee}$ relative to all extensions of v; otherwise, we start to maintain codewords for F_s, i.e., if x is large enough and $F_s(x)$ outputs y, then the oracle contains a proof for this, namely the codeword $c(s,x,y)$)

- s odd: If there is a t_{s-1}-valid $v \sqsupsetneq w_{s-1}$ such that for some $x < |v|$, $x \in K_\vee^v$ and $M_s^v(x)$ definitely accepts, then let $w_s = v$ and $t_s = t_{s-1} + 0$. Otherwise choose $b \in \{0,1\}$ such that $w_{s-1}b$ is t_{s-1}-valid, let $w_s = w_{s-1}b$ and $t_s = t_{s-1} + p$ for some $p \in \mathbb{P}^{\geq 41}$ large enough such that $(16|v_{p^k}|)^s < 2^{p^k}$ for all $k \in \mathbb{N}^+$, $p > |w_s|$, and p is greater than all elements in t_{s-1}.
(meaning: force $L(M_s) \cap K_\vee \neq \emptyset$ if possible; otherwise choose a suitable prime p and make sure that the oracle contains no elements of length p^k and hence $v_{p^k} \notin K$ for all $k \geq 1$; the step corresponds to V4)

The subsequent claims refer to the construction above. We start with a claim showing that the construction is possible and how one can extend a t_s-valid $w \sqsupseteq w_s$ by one bit.

Claim 7.8 *Let $s \in \mathbb{N}$. The choices of w_s and t_s are possible and w_s is t_s-valid. Moreover, for each t_s-valid $w \sqsupseteq w_s$ and $z = |w|$ the following holds.*

1. *If $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x, y \in \mathbb{N}$ such that $i \leq s$, $t_s(i) > 0$, and $z \geq t_s(i)$, then:*
   (a) *if $F_i^w(x) = y$, then $w1$ is t_s-valid and $w0$ is not.*
   (b) *if $F_i^w(x) \neq y$, then $w0$ is t_s-valid and $w1$ is not.*
2. *If $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x, y \in \mathbb{N}$ such that $i \leq s$ and $t_s(i) = 0$, then:*
   (a) *$w0$ is t_s-valid.*
   (b) *if $F_i^w(x) = y \notin K_\vee^w$ and there is no odd i' such that $i < i' \leq s$, $t_s(i') = p \in \mathbb{P}^{\geq 41}$, and $|z| \geq p$, then $w1$ is t_s-valid.*
3. *If $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x, y \in \mathbb{N}$ such that $i > s$, then:*
   (a) *$w0$ is t_s-valid.*
   (b) *if $F_i^w(x) = y \notin K_\vee^w$, then $w1$ is t_s-valid.*
4. *If $|z| = p^k$ for $p \in \mathbb{P}^{\geq 41}$, $p \notin t_s$, and $k \geq 1$, then $w0$ and $w1$ are t_s-valid.*
5. *In all other cases $w0$ is t_s-valid.*

Proof Induction on s. The induction base holds by the definition of t_0 and w_0.

Now assume $s > 0$. By induction hypothesis, the choice of a t_{s-1}-valid w_{s-1} is possible. By the statements 1–5 of the induction hypothesis, the choice of b in step s is possible and hence the choices of w_s and t_s. By construction, w_s is t_{s-1}-valid. We show that w_s is t_s-valid. The following properties hold, since w_s is t_{s-1}-valid: V1, V2, V3 for $i < |t_s|$, and V4 for $i < |t_s|$. It remains to argue for V3 and V4 in case $i = s = |t_s|$. If s is even, then V4 trivially holds, V3(b) holds by construction, and V3(a) trivially holds, since $m = t_s(s) > |w_s|$. If s is odd, then V3 trivially holds, V4(b) holds by construction, and V4(a) trivially holds, since $p = t_s(s) > |w_s|$. Therefore, w_s is t_s-valid. Now let $w \sqsupseteq w_s$ be t_s-valid and $z = |w|$.

1a: By Claim 7.3.1, $F_i^w(x)$ is defined and hence $F_i^{w1}(x) = y$. Then $w0$ is not t_s-valid, since it violates V3a. Consider $w1$. By Claim 7.7, this oracle satisfies V1, V3, and V4b. It also satisfies V4a, since w_s is t_s-valid, $z = c(i, x, y)$ has even length, and $t_s(i) > 0$. Assume $w1$ does not satisfy V2. Hence by Claim 7.7, $y \in K_\vee^w$. As $i \leq s$, the oracle $w \sqsupseteq w_s \sqsupseteq w_{i-1}$ is t_{i-1}-valid. By Claim 7.3.1, $F_i^w(x)$ is defined and has an output $y < |w|$ with $y \in K_\vee^w$. Thus step i defines $t_i(i) = 0$, which contradicts $t_s(i) > 0$.

1b: By Claim 7.3.1, $F_i^w(x)$ is defined and thus $F_i^{w1}(x) = F_i^w(x) \neq y$. Hence $w1$ violates V2 and is not t_s-valid. By Claim 7.7.1, $w0$ is t_s-valid.

2a: Holds by Claim 7.7.1.

2b: By Claim 7.7, $w1$ satisfies V1, V2, V3, and V4b. We show that it satisfies V4a. Let $i' \leq s$ be odd with $t_s(i') = p \in \mathbb{P}^{\geq 41}$. As w is t_s-valid and $c(i, x, y)$ has even length, it holds $\{x \in w1 \mid |x| = p^k \text{ for } k \geq 1\} = \emptyset$. Let $j < i'$ be positive even with $t_s(j) = 0$. We show $z \notin J = \{c(j, x', y') \in w1 \mid x', y' \in \mathbb{N} \text{ and } |c(j, x', y')| \geq p\}$, which implies $J = \emptyset$, since w_s it t_s-valid. If $z \in J$, then $|z| \geq p$ and hence $i' \leq i$, since by assumption, there is no odd i' such that $i < i' \leq s$, $t_s(i') = p \in \mathbb{P}^{\geq 41}$, and $|z| \geq p$. Thus $j < i' \leq i$, which contradicts $z = c(i, x, y) \in J$. Hence $w1$ satisfies V4a and is t_s-valid.

3a: Holds by Claim 7.7.1.

3b: By Claim 7.7, $w1$ satisfies V1, V2, V3, and V4b. It also satisfies V4a, since w_s is t_s-valid, $z = c(i, x, y)$ has even length, and $i > s$.

4: Since $|z|$ is odd, z is not a codeword. By Claim 7.7.1, $w0$ is t_s-valid. Note that $w1$ satisfies V1. By Claim 7.7, $w1$ satisfies V3 and V4b. It satisfies V2 and V4a, since z is not a codeword and $p \notin t_s$.

5: By Claim 7.7.1, only in the case 7.8.1a it holds that $w0$ is not t_s-valid. Hence in the present case $w0$ is t_s-valid. □

Claim 7.9 *Let $k \in \overline{K_\vee^O}$. The following $f \in \mathrm{FP}^O$ is a P^O-optimal proof system for $\overline{K_\vee^O}$.*

$$f(z) = \begin{cases} y & \text{if } z = c(i, x, y) \in O \text{ for } i \in 2\mathbb{N}^+ \text{ and } x, y \in \mathbb{N} \\ k & \text{otherwise} \end{cases}$$

Proof We show $\mathrm{ran}(f) = \overline{K_\vee^O}$. First we argue for $\subseteq$. Let $z \in \mathbb{N}$ with $f(z) \in \overline{K_\vee^O}$. Then $z = c(i, x, y) \in O$ for $i \in 2\mathbb{N}^+, x, y \in \mathbb{N}$. As all finite prefixes of O satisfy V2, $y \notin K_\vee^O$.

Now we argue for $\supseteq$. Let $k' \in \overline{K_\vee^O}$ and $g \in \mathrm{FP}^O$ be a proof system for $\overline{K_\vee^O}$ such that for every $x \in \overline{K_\vee^O}$ there are infinitely many z with $g(z) = x$. Choose $i \in 2\mathbb{N}^+$ such that F_i^O computes g. Hence it holds $t_i(i) > 0$. Let x be greater than $t(i)$ with $F_i^O(x) = k'$. Choose an $s > i$ sufficiently large such that $|w_s| > c(i, x, k')$ and $F_i^{w_s}(x) = k' \in \overline{K_\vee^{w_s}}$. Since w_s is t_s-valid, it holds $c(i, x, k') \in w_s \subseteq O$. Consequently, $k' \in \mathrm{ran}(f)$.

It remains to show that f simulates every other proof system $h \in \mathrm{FP}^O$ for $\overline{K_\vee^O}$. Choose $j \in 2\mathbb{N}^+$ such that F_j^O computes h. Hence $t(j) > 0$. Define

$$\pi(x) = \begin{cases} c(j, x, y) & \text{if } F_j^O(x) = y \text{ and } c(j, x, y) \in O \\ c(i, x', y) & \text{if } F_j^O(x) = y \text{ and } c(j, x, y) \notin O, \text{ where } x' \geq t(i) \text{ is minimal with } F_i^O(x') = y. \end{cases}$$

Then $h(x) = f(\pi(x))$ for all x. If $F_j^O(x) = y$ and $x \geq t(j)$, then $c(j, x, y) \geq t(j)$. Moreover, for a sufficiently large $s > j$ with $c(j, x, y) < |w_s|$ it holds that $F_j^{w_s}(x) = y$ is defined and —as

w_s is t_j-valid— $c(j,x,y) \in w_s \subseteq O$. Thus there exist only finitely many x with $F_j^O(x) = y$ and $c(j,x,y) \notin O$. Hence $\pi \in \mathrm{FP}^O$. □

Since the problem $\overline{K_\vee^O}$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for coNP^O, Claim 7.9 implies the first statement of the theorem.

Claim 7.10 *$M_s^O(\langle v_{p^k}, u_1, \ldots, u_n\rangle)$ rejects for all odd s with $t_s(s) = p \in \mathbb{P}^{\geq 41}$, all $k \in \mathbb{N}^+$, and all $u = \langle u_1, \ldots, u_n\rangle$ with $|u| \leq |v_{p^k}|$.*

Proof We assume that $M_s^O(u')$ accepts for $u' = \langle v_{p^k}, u_1, \ldots, u_n\rangle$ and show a contradiction. Choose $j > s$ large enough such that $M_s^{w_j}(u')$ definitely accepts, $|w_j| > u'$, and $|w_j| > q$ for all q with $|q| = p^k$. By construction, w_j is t_j-valid and hence t_{s-1}-valid. Let r be a definitely accepting path of $M_s^{w_j}(u')$. For r we inductively define the set of queries and their dependencies.

$$Q_0 = \{q \mid q \text{ is queried on } r\} \tag{11}$$

$$Q_{n+1} = \bigcup_{\substack{z \in Q_n \text{ with } z = c(i,x,y),\\ i < s,\, x,y \in \mathbb{N},\, t_{s-1}(i) > 0}} \{q \mid q \text{ is queried by } F_i^{w_j}(x)\} \tag{12}$$

Let $Q = \bigcup_{n\geq 0} Q_n$. It holds that $|Q| < 2^{p^k}$, which is seen as follows: For $m_n = \sum_{q\in Q_n} |q|$ we have $m_{n+1} \leq m_n/2$, since the sum of lengths of queries induced by $z = c(i,x,y)$ is at most $|x|^i + i \leq (|x|^i + i)^{2ie} \leq |z|/2$ by the definition of c and $\langle\cdot\rangle$. Thus the m_n form a geometric series. From $|u'| = |u| + 2|v_{p^k}| + 2 \leq 4|v_{p^k}|$ it follows $|Q| \leq 2m_0 \leq 2(|u'|^s + s) \leq 4|u'|^s \leq (16|v_{p^k}|)^s < 2^{p^k}$, where the latter inequality holds by the choice of p in step s.

Let $\bar{q}$ be the smallest word of length p^k that is not in Q. The word exists, since $|Q| < 2^{p^k}$. By the assumption that $|w_j| > q$ for all q with $|q| = p^k$, it holds in particular $|w_j| > \bar{q}$. By the choice of p in step s we have $p > |w_s|$ and hence $|w_{s-1}| < \bar{q} < |w_j|$. Thus for $v = \mathrm{pr}_{\bar{q}}(w_j)$ it holds that $w_{s-1} \sqsubsetneq v \sqsubsetneq w_j$, where w_{s-1} and w_j are t_{s-1}-valid. By Claim 7.6, v is t_{s-1}-valid. Moreover, $|v| = \bar{q}$, $|\bar{q}| = p^k$, and $p \notin t_{s-1}$, since step s chooses p greater than all elements in t_{s-1}. From Claim 7.8.4 it follows that $v1$ is t_{s-1}-valid.

We show that there exists a t_{s-1}-valid $w' \sqsupseteq v1$ relative to which r is still a definitely accepting path. More precisely, $|w'| = |w_j|$ and for all $q \in Q$ it holds that $q \in w' \Leftrightarrow q \in w_j$. Below we describe how $v1$ is extended bit by bit to w', i.e., how the word $w \sqsupseteq v1 \sqsupseteq w_{s-1}$ constructed so far is extended by one bit b, where z denotes the length of w. We define b and argue that

$$wb \text{ is } t_{s-1}\text{-valid and if } z \in Q \text{ then } b = w_j(z), \tag{13}$$

where we follow the cases in Claim 7.8.

1. $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x,y \in \mathbb{N}$, $i \leq s-1$, $t_{s-1}(i) > 0$: If $F_i^w(x) = y$, then $b = 1$ else $b = 0$.
   Note that $z > \bar{q} > p > t_{s-1}(i)$. By Claim 7.8.1, wb is t_{s-1}-valid. If $z \in Q$, then by (12), $q \in Q$ for all q queried by $F_i^w(x)$. For these q it holds that $q < z = |w|$ and hence $w(q) = w_j(q)$ by (13). Thus $F_i^w(x) = F_i^{w_j}(x)$. We know that w_j is t_{s-1}-valid and $z > t_{s-1}(i) > 0$. From V2 and V3(a) it follows that $z \in w_j \Leftrightarrow F_i^{w_j}(x) = y \Leftrightarrow F_i^w(x) = y \Leftrightarrow b = 1$. Hence $b = w_j(z)$, which proves (13).

2. $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x,y \in \mathbb{N}$, $i \leq s-1$, $t_{s-1}(i) = 0$: Let $b = 0$.
   By Claim 7.8.2, wb is t_{s-1}-valid. Assume $b \neq w_j(z)$, i.e., $z \in w_j$. We are in the situation that w_j is t_j-valid, $s < j$ is odd, $t_j(s) = p$, $i \in 2\mathbb{N}^+$ with $i < s$, and $t_j(i) = 0$. By V4a, the set $\{c(i,x,y) \in w_j \mid x,y \in \mathbb{N} \text{ and } |c(i,x,y)| \geq p\}$ is empty. However, z belongs to this set, as $z = |w| > |v| = \bar{q}$ and hence $|z| \geq p^k \geq p$. This is a contradiction, which shows (13).

3. $z = c(i,x,y)$ for $i \in 2\mathbb{N}^+$, $x,y \in \mathbb{N}$, $i > s-1$: If $z \notin Q \cap w_j$, then $b = 0$ else $b = 1$.
If $b = 0$, then wb is t_{s-1}-valid by Claim 7.8.3. Otherwise, $b = 1$ and $z \in Q \cap w_j$. We show

$$|x|^i + i < p^k. \tag{14}$$

Assume $|x|^i + i \geq p^k$. From $p \geq 41$, $e \geq 2$, $k \geq 1$, and $i \geq s \geq 1$ it follows that $(41 \cdot p^{ke})^s < p^{2ike}$. Moreover, $|v_{p^k}| = 2(e + p^{ke} + e + p^k + 3) \leq 10 \cdot p^{ke}$. Hence we obtain.

$$|c(i,x,y)| > (|x|^i + i)^{2ie} \geq p^{2ike} > (41 \cdot (p^{ke})^s \geq (40 \cdot p^{ke})^s + s \geq (4|v_{p^k}|)^s + s \geq |u'|^s + s.$$

Thus $|z| > |u'|^s + s \geq m_0 \geq m_1 \geq \cdots$ and hence $z \notin Q$, a contradiction. This proves (14).

We know that w_j is t_j-valid. By V2, $F_i^{w_j}(x) = y \notin K_\vee^{w_j}$. By (14), the computation $F_i^{w_j}(x)$ stops within $|x|^i + i < p^k$ steps. Hence it can only ask queries of length $< p^k$ and $|y| < p^k$. Thus $F_i^w(x) = y \notin K_\vee^w$, since w and w_j coincide with respect to all words of length $< p^k$. By Claim 7.8.3, wb is t_{s-1}-valid.

To show the second part of (13) assume $z \in Q$. If $b = 1$, then $z \in Q \cap w_j$ and hence $b = w_j(z)$. If $b = 0$, then $z \notin w_j$ and hence $b = w_j(z)$. This proves (13).

4. $|z| = {p'}^k$ for $p' \in \mathbb{P}^{\geq 41}$, $p' \notin t_s$, $k \geq 1$: Let $b = w_j(z)$.
By Claim 7.8.4, wb is t_{s-1}-valid, which implies (13).

5. Otherwise: Let $b = 0$.
By Claim 7.8.5, wb is t_{s-1}-valid. Assume $b \neq w_j(z)$, i.e., $z \in w_j$. We know that w_j is t_j-valid. From V1 it follows that z must be a word of length ${p'}^k$ for $p' \in \mathbb{P}^{\geq 41}$ and $p' \in t_{s-1}$ (note that the case $p' \notin t_{s-1}$ has already been considered in 4). Choose s' such that $t_{s-1}(s') = p'$ and note that s' is odd. From V4a it follows that $z \notin w_j$, a contradiction which implies (13).

This shows that there exists a t_{s-1}-valid $w' \sqsupseteq v1 \sqsupsetneq w_{s-1}$ such that $|w'| = |w_j| > u'$ and for all $q \in Q$ it holds that $q \in w' \Leftrightarrow q \in w_j$. Hence $M_s^{w'}(u')$ definitely accepts. Moreover, $|v| = \bar{q}$ and hence $\bar{q} \in w'$. From $|\bar{q}| = p^k$ it follows $v_{p^k} \in K^{w'}$ and $u' \in K_\vee^{w'}$. Therefore, step s of the construction defines $t_s = t_{s-1} + 0$ (and chooses for instance $w_s = w'$), which contradicts the assumption $t_s(s) = p \in \mathbb{P}^{\geq 41}$. □

Claim 7.11 *$K_\vee^O \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O for all $B \in \mathrm{NP}^O$ that are disjoint to $K_\vee^O$.*

Proof Choose s odd such that $B = L(M_s^O)$. We claim that $t_s(s) = p \in \mathbb{P}^{\geq 41}$. Otherwise there exists $x \in K_\vee^{w_s}$ such that $M_s^{w_s}(x)$ definitely accepts. Hence $x \in K_\vee^O$ and $M_s^O(x)$ accepts, which contradicts the assumption $K_\vee^O \cap L(M_s^O) = \emptyset$.

Let $f(\langle u_1, \ldots, u_n \rangle) = \langle u_0, u_1, \ldots, u_n \rangle$, where $u_0 = v_{p^k}$ for the minimal $k \geq 1$ such that $|\langle u_1, \ldots, u_n \rangle| \leq |v_{p^k}|$.

It holds that $f \in \mathrm{FP} \subseteq \mathrm{FP}^O$. We argue that f reduces $K_\vee^O$ to $K_\vee^O \cup B$. If $\langle u_1, \ldots, u_n \rangle \in K_\vee^O$, then $f(\langle u_1, \ldots, u_n \rangle) \in K_\vee^O$.

Assume now $\langle u_1, \ldots, u_n \rangle \notin K_\vee^O$. From $t_s(s) = p$ it follows that for all $k \geq 1$, O does not contain elements of length p^k and hence $v_{p^k} \notin K^O$. Therefore, $f(\langle u_1, \ldots, u_n \rangle) \notin K_\vee^O$. Moreover, by Claim 7.10, $f(\langle u_1, \ldots, u_n \rangle) \notin L(M_s^O) = B$. □

The following claim has the same proof as Claim 6.8.

Claim 7.12 *If A is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O and disjoint to $B \in \mathrm{NP}^O$, then $A \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O.*

Proof Otherwise there exist counterexamples A and B. Choose $f \in \mathrm{FP}^O$ such that $K_\vee^O \leq_{\mathrm{m}}^{\mathrm{p},O} A$ via f and let $B' = f^{-1}(B)$. Observe that $B' \in \mathrm{NP}^O$, $K_\vee^O \cap B' = \emptyset$, and $K_\vee^O \cup B' \leq_{\mathrm{m}}^{\mathrm{p},O} A \cup B$ via f. Hence $K_\vee^O \cup B'$ is not $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O, which contradicts Claim 7.11. □

This finishes the proof of Theorem 7.1. □

Corollary 7.13 *For the oracle O constructed in Theorem 7.1 there exists a set $L \in \mathrm{NP}^O - \mathrm{coNP}^O$ with $L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\}$.*

Proof The proof consists of two parts. First, we show the existence of a set $A \in \mathrm{NP}^O - \mathrm{coNP}^O$. Then we "translate" A into a set $L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\}$.

We refer to the proof of Theorem 7.1. Recall $E^O = \{0^n \mid \exists x \in O \text{ with } |x| = n\} \in \mathrm{NP}^O$. Define

$$B = \{0^{p^k} \mid p \in \mathbb{P}^{\geq 41}, \exists i \in \mathbb{N}^+ \; p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}\} \tag{15}$$

and $A = E^O \cap B$. Note that for $p \in \mathbb{P}^{\geq 41}$ and $k \in \mathbb{N}$, due to

$$\frac{2^{2^{(2(i+1)+1)\cdot 2^p}}}{2^{2^{(2i+1)\cdot 2^p}}} > p$$

it holds that if $0^{p^k} \in B$, then in (15) the i is uniquely determined.

Let $0^{p^k} \in B$. Then there exists $i > 0$ such that $p^{k+1} \geq 2^{2^{(2i+1)2^p}} > 2^{2^{2^p \cdot 2}} = 2^{2^{2^p+1}}$. As $p^{k+1} \leq 2^{(\log p+1)\cdot(k+1)}$, we obtain $(\log p + 1) \cdot (k+1) \geq 2^{2^p+1}$, which implies

$$k \geq \frac{2^{2^p+1}}{\log p + 1} - 1 \geq 2^{2^p} \cdot \frac{2^{2^p}}{p} - 1 \geq 2^{2^p} \cdot \frac{2^{2^p}}{2p} \geq 2^{2^p}.$$

This yields

$$\log\log k \geq p. \tag{16}$$

We show $B \in \mathrm{P} \subseteq \mathrm{P}^O$ via the following algorithm (note that this implies $A \in \mathrm{NP}^O$).

1. Input: $w \in \Sigma^*$
2. If w is not of the form 0^{p^k} for some $p \in \mathbb{P}^{\geq 41}$ and $k \in \mathbb{N}$ with $\log\log k \geq p$, then reject.
3. Otherwise, let $t = 2^{2^{2^p}}$ and $j = 0$ and repeat the following until $t > p^k$.
   (a) $t = t^2$
   (b) $j = j + 1$
4. If j is not of the form $2i \cdot 2^p$ for some $i \in \mathbb{N}^+$, then reject.
5. If $t \leq p^{k+1}$, then accept. Otherwise reject.

In step 3, due to (16) it holds $p^k \geq p^{2^{2^p}} \geq 2^{2^{2^p}}$. Therefore, step 3 and as a consequence the complete algorithm works in polynomial time.

Note that for all $j \in \mathbb{N}$ it holds $2^{2^{j+1+2^p}} = \left(2^{2^{j+2^p}}\right)^2$. Thus, before and after each execution of the loop in 3 it holds

$$t = 2^{2^{j+2^p}}. \tag{17}$$

We show that for all w, it holds $w \in B$ if and only if the algorithm accepts on input w.

If $w \in B$, then $w = 0^{p^k}$ for $p \in \mathbb{P}^{\geq 41}$ and $k \in \mathbb{N}$ and there exists a unique $i \in \mathbb{N}^+$ such that $p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}$. Due to (16) the algorithm does not reject in step 2. After step 3 it

holds $t = 2^{2^{(2i+1)\cdot 2^p}}$ (cf. (17)). Because of that and (17), it holds $j = 2i \cdot 2^p$ at this point in time. Consequently, the algorithm accepts in step 5.

Conversely, if the algorithm accepts a word w, then due to step 2 it holds $w = 0^{p^k}$ for $p \in \mathbb{P}^{\geq 41}$ and $k \in \mathbb{N}$. Moreover, because of (17) and step 4 there exists some $i \in \mathbb{N}^+$ such that at the beginning of the execution of step 5 we have $p^k < t = 2^{2^{2i \cdot 2^p + 2^p}} = 2^{2^{(2i+1)\cdot 2^p}}$. As the algorithm accepts in step 5 it holds $2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}$. Hence $w \in B$.

We show $A \notin \text{coNP}^O$. Assume that this is wrong. Then there exists a nondeterministic Turing machine M with running time $n^c + c$ for some constant c such that M accepts $\overline{A}$. Let M' be a nondeterministic polynomial time Turing machine that on input x simulates M on input v_{p^k} if $x = 0^{p^k}$ for $p, k \in \mathbb{N}$ with $0^{p^k} \in B$, and rejects otherwise. There exists an odd s such that $M_s = M'$ and it holds for all $p, k \in \mathbb{N}$ with $0^{p^k} \in B$

$$v_{p^k} \in K^O \Leftrightarrow 0^{p^k} \in E^O \Leftrightarrow 0^{p^k} \in A \Leftrightarrow 0^{p^k} \notin \overline{A} \Leftrightarrow 0^{p^k} \notin L(M^O) \Leftrightarrow v_{p^k} \notin L(M_s^O), \tag{18}$$

which implies $K^O \cap L(M_s^O) = \emptyset$. Therefore, $t_s(s) = p$ for some $p \in \mathbb{P}^{\geq 41}$ and by Claim 7.10

$$M_s^O \text{ rejects } v_{p^k} \text{ for all } k \in \mathbb{N}^+. \tag{19}$$

By V4(a), $\{x \in O \mid |x| = p^k \text{ for } k \geq 1\} = \emptyset$. Therefore, for all $k \geq 1$, it holds $0^{p^k} \notin E^O$. Thus by (18) $v_{p^k} \in L(M_s^O)$ for all $k \in \mathbb{N}^+$ with $0^{p^k} \in B$. Hence, if there exists a $k \in \mathbb{N}$ with $0^{p^k} \in B$, then we obtain a contradiction to (19). We show that such a k exists: choose an arbitrary $i \in \mathbb{N}^+$. Then choose k as the unique number with $p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}$. Then $0^{p^k} \in B$, which shows $A \in \text{NP}^O - \text{coNP}^O$.

Roughly speaking, we now translate A into a set $L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\}$. More precisely, define

$$L = \{0^{2^{2^{(2i+1)\cdot 2^p}}} \mid i, p \in \mathbb{N}^+, \exists k \in \mathbb{N} \text{ such that } 0^{p^k} \in A \text{ and } p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}\}.$$

As $L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\}$, it remains to prove $L \in \text{NP}^O - \text{coNP}^O$. It holds $L \in \text{NP}^O$ as the following NP^O-algorithm accepts L.

1. Input: $w \in \Sigma^*$
2. If w is not of the form $0^{2^{2^m}}$ for some $m \in \mathbb{N}$, reject.
   Otherwise, determine the unique i and p with $(2i+1) \cdot 2^p = m$.
   If $p \notin \mathbb{P}^{\geq 41}$ or $i = 0$, then reject.
3. Compute the unique k such that $p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}$.
4. If $p^k \in A$, accept. Otherwise reject.

It remains to argue for $L \notin \text{coNP}^O$. We show this by proving $A \leq_{\text{m}}^{\text{p}} L$. Consider the following polynomial time algorithm (and note that $\varepsilon \notin L$).

1. Input: $w \in \Sigma^*$
2. If w is not in B, return ε.
3. Otherwise $w = 0^{p^k}$ for $p \in \mathbb{P}^{\geq 41}$ and $k \in \mathbb{N}$. Determine the unique $i \in \mathbb{N}^+$ with $p^k < 2^{2^{(2i+1)\cdot 2^p}} \leq p^{k+1}$ (the above P-algorithm for B illustrates that this is possible in polynomial time) and return $0^{2^{2^{(2i+1)\cdot 2^p}}}$.

If the algorithm terminates in step 2, then the input is not in $B \supseteq A$ and the output is not in L. If it terminates in step 3, then by the definition of A, B, and L the input is in A if and only if the output is in L. □

Proposition 7.14 ([Boo74]) *The following holds for each oracle A and* $\mathrm{NEE}^A \stackrel{df}{=} \mathrm{NTIME}^A(2^{O(2^n)})$.

$$\exists L \in \mathrm{NP}^A - \mathrm{coNP}^A \text{ with } L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\} \;\Leftrightarrow\; \mathrm{NEE}^A \cap \mathrm{TALLY} \not\subseteq \mathrm{coNEE}^A$$

Proof "$\Leftarrow$:" Let $T \in (\mathrm{NEE}^A \cap \mathrm{TALLY}) - \mathrm{coNEE}^A$ and let N be a nondeterministic Turing machine accepting T with oracle A in time $2^{O(2^n)}$. Let $L = \{0^{2^{2^n}} \mid 0^n \in T\}$. Let M be the algorithm that on input x rejects if $x \neq 0^{2^{2^n}}$ for some n and that otherwise simulates N on 0^n. Clearly $L(M^A) = L$. The running time of M on input x is $|x|^{O(1)}$ for the test $x = 0^{2^{2^n}}$ plus $2^{c2^n} = (2^{2^n})^c = |x|^c$ for the simulation of $N(0^n)$. This shows $L \in \mathrm{NP}^A$.

Assume $L \in \mathrm{coNP}^A$ and let M' be a nondeterministic Turing machine accepting $\overline{L}$ with oracle A in polynomial time. Let N' be the algorithm that on input 0^n simulates M' on $0^{2^{2^n}}$ and accepts on all other inputs. Clearly $L(N'^A) = \overline{T}$. The running time of N' on input 0^n is $(2^{2^n})^c = 2^{c2^n}$, which shows $\overline{T} \in \mathrm{NEE}^A$, a contradiction. Hence $L \notin \mathrm{coNP}^A$.

"$\Rightarrow$:" Let $L \in \mathrm{NP}^A - \mathrm{coNP}^A$ with $L \subseteq \{0^{2^{2^n}} \mid n \in \mathbb{N}\}$ and let M be a nondeterministic Turing machine accepting L with oracle A in polynomial time. Let $T = \{0^n \mid 0^{2^{2^n}} \in L\}$. Let N be the algorithm that on input 0^n simulates M on $0^{2^{2^n}}$ and rejects on all other inputs. Clearly $L(N^A) = T$. The running time of N on input 0^n is $(2^{2^n})^c = 2^{c2^n}$, which shows $T \in \mathrm{NEE}^A$.

Assume $T \in \mathrm{coNEE}^A$ and let N' be a nondeterministic Turing machine accepting $\overline{T}$ with oracle A in time $2^{O(2^n)}$. Let M' be the algorithm that on input x accepts if $x \neq 0^{2^{2^n}}$ for some n and that otherwise simulates N' on 0^n. Clearly $L(M'^A) = \overline{L}$. The running time of M on input x is $|x|^{O(1)}$ for the test $x = 0^{2^{2^n}}$ plus $2^{c2^n} = (2^{2^n})^c = |x|^c$ for the simulation of $N'(0^n)$. This shows $\overline{L} \in \mathrm{NP}^A$ and hence $L \in \mathrm{coNP}^A$, which is a contradiction. Hence $T \notin \mathrm{coNEE}^A$ and therefore, $\mathrm{NEE}^A \cap \mathrm{TALLY} \not\subseteq \mathrm{coNEE}^A$. □

The following corollary directly follows from Corollary 2.4, Corollary 7.13, and Proposition 7.14.

Corollary 7.15 *Relative to the oracle O constructed in Theorem 7.1 the following holds.*

1. *Each $A \in \mathrm{coNP}^O$ has a P^O-optimal proof system.*
2. *If A is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O and disjoint to $B \in \mathrm{NP}^O$, then $A \cup B$ is $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete for NP^O.*
3. $\mathrm{NEE}^O \cap \mathrm{TALLY} \not\subseteq \mathrm{coNEE}^O$, *where* $\mathrm{NEE}^O \stackrel{df}{=} \mathrm{NTIME}^O(2^{O(2^n)})$.

Köbler, Messner, and Torán [KMT03] prove the following implications (20) and (22).

$$\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE} \;\Rightarrow\; \mathrm{H}_{\mathrm{opps}} \tag{20}$$

$$\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE} \;\stackrel{?}{\Leftrightarrow}\; \mathrm{NTIME}(2^{O(2^{2^n})}) = \mathrm{coNTIME}(2^{O(2^{2^n})}) \tag{21}$$

$$\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE} \;\Rightarrow\; \exists \text{ a P-optimal pps} \tag{22}$$

$$\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE} \;\stackrel{?}{\Leftrightarrow}\; \mathrm{DTIME}(2^{O(2^{2^n})}) = \mathrm{NTIME}(2^{O(2^{2^n})}) \tag{23}$$

They also mention that the inviting equivalences (21) and (23) are not clear. The usual approach suggests to define for every tally set T the set $L \stackrel{df}{=} \{n \mid 0^n \in T\}$ and to show

$$T \in \mathrm{NEE} \Leftrightarrow L \in \mathrm{NTIME}(2^{O(2^{2^n})}). \tag{24}$$

The equivalence (24) strongly depends on the encoding of numbers:

If we encode numbers in binary representation, then $\Rightarrow$ is clear, but $\Leftarrow$ is not: If on input 0^n for $n = 2^k$ one simulates the $\mathrm{NTIME}(2^{O(2^{2^n})})$ machine on n, then the running time is

$$2^{c2^{2^{|n|}}} = 2^{c2^{2^{1+k}}} = 2^{c2^{2\cdot 2^k}} = 2^{c2^{2n}} \notin 2^{O(2^n)}.$$

If we encode numbers in dyadic representation, then $\Leftarrow$ is clear, but $\Rightarrow$ is not: If on input n for $n = 2 \cdot (2^k - 1)$ one simulates the NEE machine on 0^n, then the running time is

$$2^{c2^n} = 2^{c2^{2\cdot(2^k-1)}} = 2^{c2^{2\cdot(2^{|n|}-1)}} \notin 2^{O(2^{2^{|n|}})}.$$

Further evidence against (21) and (23) is given by Ben-David and Gringauze [BDG98] who state the existence of an oracle relative to which $\mathrm{DTIME}(2^{O(2^{2^n})}) = \mathrm{NTIME}(2^{O(2^{2^n})})$, $\neg \mathrm{H}_{\mathrm{opps}}$, and hence $\mathrm{NEE} \cap \mathrm{TALLY} \not\subseteq \mathrm{coNEE}$. Relative to this oracle, in (21) and (23) the implications $\Leftarrow$ fail.

Corollary 7.15 shows that relative to the oracle from Theorem 7.1, the converses of (20) and (22) fail, i.e., the premises are stronger than the conclusions. It is not clear how to modify these premises such that (20) and (22) become relativizable equivalences. The oracle by Ben-David and Gringauze [BDG98] shows that $\mathrm{NTIME}(2^{O(2^{2^n})}) = \mathrm{coNTIME}(2^{O(2^{2^n})})$ and $\mathrm{DTIME}(2^{O(2^{2^n})}) = \mathrm{NTIME}(2^{O(2^{2^n})})$ are not appropriate choices.

8 Summary of Oracles and their Properties

Table 1 summarizes the properties of several oracles that are relevant to the hypotheses studied in this paper. Some of these properties are obtained by known results, which are compiled in the following theorem to make them quotable in the table.

Theorem 8.1 *The following holds relative to all oracles, where* $\mathrm{EE} = \mathrm{DTIME}(2^{O(2^n)})$ *and* $\mathrm{NEE} = \mathrm{NTIME}(2^{O(2^n)})$.

1. $\exists$ *P-optimal pps* $\Rightarrow$ $\mathrm{H}_{\mathrm{opps}}$
2. $\mathrm{H}_{\mathrm{cpair}}$ $\Rightarrow$ $\exists$ $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-complete disjoint* NP*-pairs*
3. $\mathrm{P} = \mathrm{NP} \Rightarrow \mathrm{UP} = \mathrm{NP} = \mathrm{coNP}$
4. *[KP89]:* $(\mathrm{E} = \mathrm{NE} \Rightarrow \exists$ *P-optimal pps*$)$ *and* $(\mathrm{NE} = \mathrm{coNE} \Rightarrow \mathrm{H}_{\mathrm{opps}})$
5. *[KMT03]:* $(\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE} \Rightarrow \exists$*P-optimal pps*$)$ *and* $(\mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE} \Rightarrow \mathrm{H}_{\mathrm{opps}})$
6. *[Raz94]:* $\mathrm{H}_{\mathrm{opps}} \Rightarrow \mathrm{H}_{\mathrm{cpair}}$
7. $\mathrm{P} = \mathrm{NP} \Rightarrow \mathrm{E} = \mathrm{NE} \Rightarrow \mathrm{EE} = \mathrm{NEE} \Rightarrow \mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{EE}$ *and*
   $\mathrm{NP} = \mathrm{coNP} \Rightarrow \mathrm{NE} = \mathrm{coNE} \Rightarrow \mathrm{NEE} = \mathrm{coNEE} \Rightarrow \mathrm{NEE} \cap \mathrm{TALLY} \subseteq \mathrm{coNEE}$
8. *[KMT03]:* $\mathrm{H}_{\mathrm{opps}} \Rightarrow \mathrm{NP} \cap \mathrm{SPARSE}$ *has* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-complete sets*
9. $\mathrm{H}_{\mathrm{union}} \Rightarrow \mathrm{NP} \neq \mathrm{coNP}$
10. $\mathrm{NP} = \mathrm{coNP} \Rightarrow \exists$ *disjoint* NP*-pairs that are* $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-hard for* NP
11. *[GS88]:* $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP} \Rightarrow \exists$ P-inseparable disjoint NP-pairs
12. *If* $\mathrm{NP} \neq \mathrm{coNP}$ *and all disjoint* NP*-pairs are* P*-separable, then* $\mathrm{H}_{\mathrm{union}}$ *holds.*
13. *If* $\mathrm{P} \neq \mathrm{NP}$ *and all disjoint* NP*-pairs are* P*-separable, then there are no disjoint* NP*-pairs that are* $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-hard for* NP*.*
14. *If all disjoint* NP*-pairs are* P*-separable, then* $\mathrm{H}_{\mathrm{cpair}}$ *holds.*
15. *[ESY84]: If no disjoint* NP*-pair is* $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-hard for* NP*, then* $\mathrm{UP} \neq \mathrm{NP}$ *and* $\mathrm{NP} \neq \mathrm{coNP}$*.*
16. *If there exist disjoint* NP*-pairs that are* $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-hard for* NP*, then there exist* $\leq^{\mathrm{pp}}_{\mathrm{T}}$*-complete disjoint* NP*-pairs.*
17. $\mathrm{EE} \subseteq \mathrm{coNEE}$

	[GSSZ04, T3.8]	[GSSZ04, T6.1]	[GSSZ04, T6.7]	[GSS05, T21]	[OH93, L4.7]	[HS92, T1]	Thm 4.1	Thm 5.1	Thm 6.1	Thm 7.1
$\exists$ P-optimal pps	− 1		− 1	− 1			− 1	− 1	− 1	+
$\exists$ optimal pps / $\mathrm{H_{opps}}$	−	+	−	− 6	+ 4		− 6	− 6	− 6	+ 1
$\mathrm{NPC_m^p}$ closed under disj. union / $\mathrm{H_{union}}$					− 9	+ 12		−	+	+
$\exists \leq_{\mathrm{m}}^{\mathrm{pp}}$-complete disjoint NP-pairs / $\mathrm{H_{cpair}}$	− 2	+ 6	+	−	+ 6	+ 14	−	−	−	+ 6
$\exists \leq_{\mathrm{T}}^{\mathrm{pp}}$-complete disjoint NP-pairs	−	+ 2	+ 2	+ 16	+ 2	+ 2				+ 2
$\exists$ disj. NP-pairs that are $\leq_{\mathrm{T}}^{\mathrm{pp}}$-hard for NP	−	−	−	+ 15	+ 10	− 13				
$\exists$ P-inseparable disjoint NP-pairs	+	+	+		+ 11	−	+ 14	+ 14	+ 14	
P $\neq$ UP						−	−			
P $\neq$ NP	+ 3	+ 7	+ 3	+ 3	+ 3	+	+ 7	+ 7	+ 3	+ 7
UP $\neq$ NP	+	+	+		+	+	+ 7			
NP $\neq$ coNP	+	+	+	+ 7	−	+ 11	+ 7	+ 7	+ 9	+ 9
NP $\cap$ SPARSE has $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets		+ 8	−		+ 8					+ 8
E $\neq$ NE	+ 4	+	+ 4	+ 4			+ 4	+ 4	+ 4	+ 7
NE $\neq$ coNE	+ 4	−	+ 4	+ 4	− 7		+ 4	+ 4	+ 4	+ 7
NEE $\cap$ TALLY $\not\subseteq$ EE	+ 5		+ 5	+ 5			+ 5	+ 5	+ 5	+ 17
NEE $\cap$ TALLY $\not\subseteq$ coNEE	+ 5	− 7	+ 5	+ 5	− 7		+ 5	+ 5	+ 5	+

Table 1: Summary of oracles and their properties. Each column corresponds to the oracle mentioned in the topmost cell. If entries + or − appear without a number, then the corresponding property is mentioned in the oracle construction. Otherwise, the number refers to the argument in Theorem 8.1 that implies the property (sometimes one additionally needs other entries of the same column). We say that there exist P-optimal (resp., optimal) pps relative to an oracle, if relative to this oracle, some $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete $A \in \mathrm{coNP}$ has a P-optimal (resp., optimal) proof system (cf. Remark 2.2). A disjoint NP-pair (A, B) is $\leq_{\mathrm{T}}^{\mathrm{pp}}$-complete, if for every disjoint NP-pair (C, D) and every separator S of (A, B) there exists a separator T of (C, D) such that $T \leq_{\mathrm{T}}^{\mathrm{p}} S$. A disjoint NP-pair (A, B) is $\leq_{\mathrm{T}}^{\mathrm{pp}}$-hard for NP, if for every $C \in \mathrm{NP}$ and every separator S of (A, B) it holds that $C \leq_{\mathrm{T}}^{\mathrm{p}} S$. The double exponential time classes are defined as $\mathrm{EE} = \mathrm{DTIME}(2^{O(2^n)})$ and $\mathrm{NEE} = \mathrm{NTIME}(2^{O(2^n)})$.

9 Conclusion and Open Questions

The main goal of this paper is to investigate the connections between three famous complexity theoretic hypotheses. Regarding the three hypotheses $\mathrm{H_{union}}$, $\mathrm{H_{opps}}$, and $\mathrm{H_{cpair}}$, we have shown that —except for the known implication $\mathrm{H_{opps}} \Rightarrow \mathrm{H_{cpair}}$— any two of the hypotheses are independent under relativized proofs. But what are the connections between the hypotheses if we consider all three at once. At first glance there are 8 possible situations. As it is known that $\mathrm{H_{opps}}$ implies $\mathrm{H_{cpair}}$ in a relativized way, there remain 6 possible situations. Table 1 illustrates that oracles for 4 of the 6 possible situations are already known. This observation leads to the open question of whether there also exist oracles for the remaining two situations. More precisely, we ask:

- Does there exist an oracle O_1 with the following properties?
  Relative to O_1, it holds $\neg \mathrm{H}_{\mathrm{opps}} \wedge \mathrm{H}_{\mathrm{union}} \wedge \mathrm{H}_{\mathrm{cpair}}$, i.e., there exists no optimal pps, unions of disjoint, $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete NP-sets remain complete, and there exist $\leq^{\mathrm{pp}}_{\mathrm{m}}$-complete disjoint NP-pairs.

- Does there exist an oracle O_2 with the following properties?
  Relative to O_2, it holds $\neg \mathrm{H}_{\mathrm{opps}} \wedge \neg \mathrm{H}_{\mathrm{union}} \wedge \mathrm{H}_{\mathrm{cpair}}$, i.e., there exists no optimal pps, there exist disjoint $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete NP-sets whose union is not complete, and there exist $\leq^{\mathrm{pp}}_{\mathrm{m}}$-complete disjoint NP-pairs.

Note that the oracle in [GSSZ04, T6.7] either has the properties requested for O_1 or has the properties requested for O_2. So this oracle answers one of the two open questions, yet we do not know which one.

Furthermore we receive new insights on problems related to the main topic. On the one hand we answer open questions by Pudlák [Pud17] who asked for oracles relative to which the following assumptions do not imply that UP has no $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets: $\neg \mathrm{H}_{\mathrm{cpair}}$, $\neg \mathrm{H}_{\mathrm{opps}}$, and NP $\cap$ coNP has no $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets. On the other hand we show that the converses of Köbler, Messner, and Torán's [KMT03] implications (NEE $\cap$ TALLY $\subseteq$ coNEE $\Rightarrow \mathrm{H}_{\mathrm{opps}}$) and (NEE $\cap$ TALLY $\subseteq$ EE $\Rightarrow$ there exist P-optimal pps) fail relative to an oracle.

References

[BDG98] S. Ben-David and A. Gringauze. On the existence of propositional proof systems and oracle-relativized propositional logic. Technical Report 5, Electronic Colloquium on Computational Complexity, 1998.

[Bey04] O. Beyersdorff. Representable disjoint NP-pairs. In *Proceedings 24th International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 3328 of *Lecture Notes in Computer Science*, pages 122–134. Springer, 2004.

[Bey06] O. Beyersdorff. Disjoint NP-pairs from propositional proof systems. In *Proceedings of Third International Conference on Theory and Applications of Models of Computation*, volume 3959 of *Lecture Notes in Computer Science*, pages 236–247. Springer, 2006.

[Bey07] O. Beyersdorff. Classes of representable disjoint NP-pairs. *Theoretical Computer Science*, 377(1-3):93–109, 2007.

[Bey10] O. Beyersdorff. The deduction theorem for strong propositional proof systems. *Theory of Computing Systems*, 47(1):162–178, 2010.

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

[Boo74] R. V. Book. Tally languages and complexity classes. *Information and Control*, 26:186–194, 1974.

[CR79] S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[ESY84] S. Even, A. L. Selman, and J. Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61:159–173, 1984.

[EY80] S. Even and Y. Yacobi. Cryptocomplexity and NP-completeness. In *Proceedings 7th International Colloquium on Automata, Languages and Programming*, volume 85 of *Lecture Notes in Computer Science*, pages 195–207. Springer, 1980.

[GHPT14] C. Glaßer, J. M. Hitchcock, A. Pavan, and S. Travers. Unions of disjoint np-complete sets. *ACM Trans. Comput. Theory*, 6(1):3:1–3:10, 2014.

[GPSS06] C. Glaßer, A. Pavan, A. L. Selman, and S. Sengupta. Properties of NP-complete sets. *SIAM Journal on Computing*, 36(2):516–542, 2006.

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

[GSS05] C. Glaßer, A. L. Selman, and S. Sengupta. Reductions between disjoint NP-pairs. *Information and Computation*, 200:247–267, 2005.

[GSSZ04] C. Glaßer, A. L. Selman, S. Sengupta, and L. Zhang. Disjoint NP-pairs. *SIAM Journal on Computing*, 33(6):1369–1416, 2004.

[GSTW08] C. Glaßer, A. L. Selman, S. Travers, and K. W. Wagner. The complexity of unions of disjoint sets. *Journal of Computer and System Sciences*, 74(7):1173–1187, 2008.

[GSZ07] C. Glaßer, A. L. Selman, and L. Zhang. Canonical disjoint NP-pairs of propositional proof systems. *Theoretical Computer Science*, 370:60–73, 2007.

[GSZ09] C. Glaßer, A. L. Selman, and L. Zhang. The informational content of canonical disjoint NP-pairs. *International Journal of Foundations of Computer Science*, 20(3):501–522, 2009.

[HHH05] E. Hemaspaandra, L. A. Hemaspaandra, and H. Hempel. All superlinear inverse schemes are conp-hard. *Theoretical Computer Science*, 345(2-3):345–358, 2005.

[HS92] S. Homer and A. L. Selman. Oracles for structural properties: The isomorphism problem and public-key cryptography. *Journal of Computer and System Sciences*, 44(2):287–301, 1992.

[Kab01] V. Kabanets. Easiness assumptions and hardness tests: trading time for zero error. *Journal of Computer and System Sciences*, 63(2):236–252, 2001.

[Kha18] E. Khaniki. New relations and separations of conjectures about incompleteness in the finite domain. Technical Report 64, Institute of Mathematics, Czech Academy of Sciences, 2018.

[KMT03] J. Köbler, J. Messner, and J. Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184(1):71–92, 2003.

[KP89] J. Krajícek and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic*, 54:1063–1079, 1989.

[Lov79] L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[MY85] S. Mahaney and P. Young. Reductions among polynomial isomorphism types. *Theoretical Computer Science*, 39:207–224, 1985.

[Myh55] J. Myhill. Creative sets. *Mathematical Logic Quarterly*, 1(2):97–108, 1955.

[OH93] M. Ogiwara and L. Hemachandra. A complexity theory of feasible closure properties. *Journal of Computer and System Sciences*, 46:295–325, 1993.

[Pap81] C. H. Papadimitriou. On the complexity of integer programming. *Journal of the ACM*, 28(4):765–768, 1981.

[Pud96] P. Pudlák. On the lengths of proofs of consistency. In *Collegium Logicum*, pages 65–86. Springer Vienna, 1996.

[Pud03] P. Pudlák. On reducibility and symmetry of disjoint NP pairs. *Theoretical Computer Science*, 295:323–339, 2003.

[Pud17] P. Pudlák. Incompleteness in the finite domain. *The Bulletin of Symbolic Logic*, 23(4):405–441, 2017.

[Rac82] C. Rackoff. Relativized questions involving probabilistic algorithms. *Journal of the ACM*, 29:261–268, 1982.

[Raz94] A. A. Razborov. On provably disjoint np-pairs. *Electronic Colloquium on Computational Complexity (ECCC)*, 1(6), 1994.

[Rog67] H. Rogers Jr. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, New York, 1967.

[Sad02] Z. Sadowski. On an optimal propositional proof system and the structure of easy subsets of TAUT. *Theoretical Computer Science*, 288(1):181–193, 2002.

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

[Tar88] E. Tardos. The gap between monotone and non-monotone circuit complexity is exponential. *Combinatorica*, 8(1):141–142, 1988.

[Tra07] S. Travers. *Structural Properties of NP-Hard Sets and Uniform Characterisations of Complexity Classes*. PhD thesis, Julius-Maximilians-Universität Würzburg, 2007.

[Ver91] O. V. Verbitskii. Optimal algorithms for conp-sets and the exp =? nexp problem. *Mathematical notes of the Academy of Sciences of the USSR*, 50(2):796–801, Aug 1991.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il