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

**Titus Dose**  
Julius-Maximilians-Universität Würzburg, Germany

**Christian Glaßer**  
Julius-Maximilians-Universität Würzburg, Germany

---

**Abstract**

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

\[ H_{\text{union}}: \text{the union of disjoint } \leq_{\text{NP}} \text{-complete sets for NP is } \leq_{\text{NP}} \text{-complete} \]

\[ H_{\text{opps}}: \text{there exist optimal propositional proof systems} \]

\[ H_{\text{pair}}: \text{there exist } \leq_{\text{pp}} \text{-complete disjoint NP-pairs} \]

The following results are obtained:

- The hypotheses are pairwise independent under relativizable proofs, except for the known implication \( H_{\text{opps}} \Rightarrow H_{\text{pair}} \).
- An answer to Pudlák's question for an oracle relative to which \( \neg H_{\text{pair}} \), \( \neg H_{\text{opps}} \), and UP has \( \leq_{\text{NP}} \)-complete sets.
- The converse of Köbler, Messner, and Torán's implication \( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} \Rightarrow H_{\text{opps}} \) fails relative to an oracle, where \( \text{NEE} = \text{NTIME}(2^{O(2^n)}) \).
- New characterizations of \( H_{\text{union}} \) and two variants in terms of coNP-completeness and p-producibility of the set of hard formulas of propositional proof systems.

2012 ACM Subject Classification  
Theory of computation → Problems, reductions and completeness;  
Theory of computation → Proof complexity; Theory of computation → Oracles and decision trees

Keywords and phrases  
NP-complete, propositional proof system, disjoint NP-pair, oracle

Digital Object Identifier  
10.4230/LIPIcs.STACS.2020.9

Related Version  

**Funding**  
Titus Dose: supported by the German Academic Scholarship Foundation.

---

**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 the existence of a finitely axiomatized theory that proves the finite consistency of each finitely axiomatized theory by a proof of polynomial length [25]. 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.
The beauty of hypothesis $H_{\text{union}}$ lies in its simplicity. It states that the class of NP-complete sets is closed under unions of disjoint sets. The question of whether $H_{\text{union}}$ holds was raised by Selman [37] in connection with the study of self-reducible sets in NP.\footnote{The analog of $H_{\text{union}}$ in computability theory holds [39], since the many-one complete c.e. sets are creative [27].}

An interesting example for a union of disjoint NP-complete sets is the Clique-Coloring pair, which is due to Pudlák [31]:

$C_0 = \{(G,k) \mid G \text{ is a graph that has a clique of size } k\}$

$C_1 = \{(G,k) \mid G \text{ is a graph that can be colored with } k-1 \text{ colors}\}$

The sets are NP-complete and disjoint, since a clique of size $k$ cannot be colored with $k-1$ colors. $C_0$ and $C_1$ are P-separable [31], which means that there exists an $S \in P$, the separator, such that $C_0 \subseteq S$ and $C_1 \subseteq \overline{S}$. The P-separability of $C_0$ and $C_1$ is a result based on deep combinatorial arguments by Lovász [26] and Tardos [38]. It implies that $C_0 \cup C_1$ is NP-complete.

Glaßer et al. [14, 17] give several equivalent formulations of $H_{\text{union}}$ and show that the union of disjoint sets that are $\leq^p_m$-complete for NP is complete with respect to strongly non-deterministic, 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. [13] provide sufficient and necessary conditions for $H_{\text{union}}$ in terms of refuters that distinguish languages $L \in \text{NP}$ with $\text{SAT} \cap L = \emptyset$ from $\text{SAT}$.

**Hypothesis $H_{\text{opps}}$: there exist optimal propositional proof systems**

Cook and Reckhow [6] define a propositional proof system (pps) as a polynomial-time computable function $f$ whose range is TAUT, the set of tautologies. If $f(x) = y$, then $x$ is a proof for $y$. 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 $H_{\text{opps}}$ holds was raised by Krajíček and Pudlák [25] in an exciting context.\footnote{The analog of $H_{\text{opps}}$ in computability theory holds trivially, since there the notion of simulation does not have any bounds for the length of proofs and hence each proof system is optimal.} Let $\text{Con}_T(n)$ denote the finite consistency of a theory $T$, which is the statement that $T$ does not have proofs of contradiction of length $\leq n$. Krajíček and Pudlák [25] showed that $H_{\text{opps}}$ is equivalent to the statement that there is a finitely axiomatized theory $S$ that proves the finite consistency $\text{Con}_T(n)$ for each finitely axiomatized theory $T$ by a proof of polynomial length in $n$. In other words, $H_{\text{opps}}$ expresses that a weak version of Hilbert’s program (to prove the consistency of all mathematical theories) is possible [30].

Krajíček and Pudlák [25] also show that NE = coNE implies $H_{\text{opps}}$ 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 [40]. Köbler, Messner, and Torán [24] prove similar implications with weaker assumptions and reveal a connection to promise classes. For $\text{EE} \not\equiv \text{DTIME}(2^{O(2^n)})$ and $\text{NEE} \not\equiv \text{NTIME}(2^{O(2^n)})$ they show that $\text{NEE} \cap \text{TALLY} \subseteq \text{coNEE}$ implies $H_{\text{opps}}$, which in turn implies that NP $\cap$ SPARSE has $\leq^p_m$-complete sets. Moreover, $\text{NEE} \cap \text{TALLY} \subseteq \text{EE}$ implies the existence of P-optimal pps, which in turn implies that UP has $\leq^p_m$-complete sets.
Sadowski [36] proves that $H_{\text{opps}}$ is equivalent to the statement that the class of all easy subsets of $\text{TAUT}$ is uniformly enumerable. Beyersdorff [2, 3, 4, 5] investigates connections between disjoint $\text{NP}$-pairs and pps, and in particular studies the hypotheses $H_{\text{cpair}}$ and $H_{\text{opps}}$. Pudlák [30, 32] provides comprehensive surveys on the finite consistency problem, its connection to propositional proof systems, and related open questions. In a recent paper, Khaniki [23] shows new relations between the conjectures discussed in [32] and constructs two oracles that separate several of these conjectures. In a couple of further papers [9, 8, 7], one of the authors also builds oracles separating several of the conjectures in [32].

**Hypothesis $H_{\text{cpair}}$: there exist $\leq_{\text{pp}}$-complete disjoint $\text{NP}$-pairs**

Even, Selman, and Yacobi [12, 11] show that the security of public-key cryptosystems depends on the computational complexity of certain promise problems. The latter can be written as disjoint $\text{NP}$-pairs, i.e., pairs $(A, B)$ of disjoint sets $A, B \in \text{NP}$. The Clique-Coloring pair mentioned above is an interesting example for a $P$-separable disjoint $\text{NP}$-pair. Even, Selman, and Yacobi [12, 11] conjecture that every disjoint $\text{NP}$-pair has a separator that is not $\leq_{\text{p}}$-hard for $\text{NP}$. If the conjecture holds, then there are no public-key cryptosystems that are $\text{NP}$-hard to crack. Großmann and Selman [20] observe that secure public-key cryptosystems exist only if $P$-inseparable disjoint $\text{NP}$-pairs exist.

The question of whether $H_{\text{cpair}}$ holds was raised by Razborov [34] in the context of pps. To explain this connection we need the notions of reducibility and completeness for disjoint $\text{NP}$-pairs.

$$(A, B) \leq_{\text{pp} m} (C, D),$$

if there is a polynomial-time computable $h$ such that $h(A) \subseteq C$ and $h(B) \subseteq D$. A disjoint $\text{NP}$-pair $(A, B)$ is $\leq_{\text{pp} m}$-complete, if each disjoint $\text{NP}$-pair $\leq_{\text{pp} m}$-reduces to $(A, B)$. Razborov [34] defines for each pps $f$ a corresponding disjoint $\text{NP}$-pair, the canonical pair of $f$. He shows that the canonical pair of an optimal pps is an $\leq_{\text{pp} m}$-complete disjoint $\text{NP}$-pair, i.e.,

$$H_{\text{opps}} \Rightarrow H_{\text{cpair}}. \quad (1)$$

This means that the open question of whether optimal pps exist can be settled by proving that $\leq_{\text{pp} m}$-complete disjoint $\text{NP}$-pairs do not exist. As we will see, (1) is the only nontrivial implication between the three hypotheses and their negations that holds relative to all oracles. For the relationship between $H_{\text{cpair}}$ and $H_{\text{opps}}$ this is shown by Glaßer et al. [16] who construct two oracles such that $H_{\text{cpair}}$ holds relative to both oracles, but $H_{\text{opps}}$ holds relative to the first one and $\neg H_{\text{opps}}$ relative to the second one.

Pudlák [31] further investigates the connection between pps and disjoint $\text{NP}$-pairs and shows that the canonical pair of the resolution proof system is symmetric. Glaßer, Selman, and Sengupta [15] characterize $H_{\text{cpair}}$ in several ways, e.g., by the uniform enumerability of disjoint $\text{NP}$-pairs and by the existence of $\leq_{\text{pp} m}$-complete functions in $\text{NPSV}$. Glaßer, Selman, and Zhang [18] prove that disjoint $\text{NP}$-pairs and pps have identical degree structures. Moreover, they show the following statement, which connects disjoint $\text{NP}$-pairs, pps, and $H_{\text{union}}$ [19]: If $\text{NP} \neq \text{coNP}$ and each disjoint $\text{NP}$-pair $(\text{SAT}, B)$ is strongly polynomial-time many-one equivalent to the canonical pair of a pps, then $H_{\text{union}}$ holds.

**Our Contribution**

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

---

3 The analog of $H_{\text{cpair}}$ in computability theory holds [35, Ch. 7., Thm XII(c)].
1. **Relativized independence of the hypotheses.** We show that \( H_{\text{union}}, H_{\text{opps}}, \) and \( H_{\text{cpair}} \) are pairwise independent under relativizable proofs (except for the known implication \( H_{\text{opps}} \Rightarrow H_{\text{cpair}} \)). For each two of these hypotheses and every combination of their truth values there exists an appropriate oracle, except for \( H_{\text{opps}} \land \neg H_{\text{cpair}} \) which is impossible. The relativized relationships between \( H_{\text{opps}} \) and \( H_{\text{cpair}} \) were settled by Glaßer et al. [16]. The remaining ones are obtained from an oracle by Ogiwara and Hemachandra [28], an oracle by Homer and Selman [22], and three oracles constructed in the present paper.

2. **Answer to a question by Pudlák.** The oracle in Theorem 11 answers a question by Pudlák [32] who asks for an oracle relative to which \( \neg H_{\text{cpair}} \) and \( U \) has \( \leq_p \text{-complete sets} \), i.e., \( \text{DisjNP} \not\equiv \text{UP} \) in the notation of [32] (see subsection 4.1 for definitions). In particular, relative to this oracle there are no P-optimal pps, but \( U \) has \( \leq_p \text{-complete sets} \), i.e., \( \text{CON} \not\equiv \text{UP} \). This is interesting, since \( \text{CON} \equiv \text{UP} \) is a theorem [24].

3. **Possibility of \( H_{\text{opps}} \) without \( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} \).** The oracle constructed in Theorem 12 shows that the converses of the following implications by Krajíček and Pudlák [25] and Köbler, Messner, and Torán [24] fail relative to an oracle. For the implications (a) and (b) this was known by Verbitskii [40], for the other implications this is a new result. It tells us that \( H_{\text{opps}} \) might be possible under assumptions weaker than \( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} \).

   (a) [25] \( \text{NE} = \text{coNE} \Rightarrow H_{\text{opps}} \)
   (b) [25] \( E = \text{NE} \Rightarrow \) there exist P-optimal pps
   (c) [24] \( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} \Rightarrow H_{\text{opps}}, \) where \( \text{NEE} \not\equiv \text{NTIME}(2^{O(2^n)}) \)
   (d) [24] \( \text{NEE} \cap \text{TALLY} \subseteq \text{EE} \Rightarrow \) there exist P-optimal pps, where \( \text{EE} \not\equiv \text{DTIME}(2^{O(2^n)}) \)

4. **Characterization of \( H_{\text{union}} \).** We characterize \( H_{\text{union}} \) and two variants (one is weaker, the other one stronger) in several ways. For instance, \( H_{\text{union}} \) (resp., its stronger version) is equivalent to the statement that for each pps, the set of hard formulas is \( \text{coNP} \)-complete (resp., \( p \)-productive). The latter notion was introduced by Hemaspaandra, Hemaspaandra, and Hempel [21] for the study of inverses of NP-problems.

### 2 Preliminaries

Throughout this paper let \( \Sigma \) be the alphabet \( \{0, 1\} \). We denote the length of a word \( w \in \Sigma^* \) by \( |w| \). The empty word is denoted by \( \varepsilon \) 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 \( \text{pr}_k(w) = w(0) \cdots w(k-1) \) be the length \( k \) prefix of \( w \). If \( v \) is a prefix (resp., proper prefix) of \( w \), then we write \( v \subseteq w \) (resp., \( v \subset w \)). A function \( f : \Sigma^* \to \Sigma^* \) is length-increasing, if \( |f(x)| > |x| \) for all \( x \in \Sigma^* \). \( N \) (resp., \( N^+ \)) denotes the set of natural numbers (resp., positive natural numbers). The set of primes is denoted by \( P = \{2, 3, 5, \ldots\} \), the set of primes \( \geq k \) by \( P_{\geq k} = \{n \in P \mid n \geq k\} \). We identify \( \Sigma^* \) with \( N \) 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 \( \Sigma^* \) are transferred to \( N \) and vice versa. In particular, \( |n| \) denotes the length of \( n \in N \). We eliminate the ambiguity of the expressions 0’ and 1’ by always interpreting them over \( \Sigma^* \).

Let \( \langle \cdot \rangle : \bigcup_{\geq 0} \mathbb{N}^n \to N \) 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 \( B \), \( A - B = \{a \in A \mid a \notin B\} \). The complement of \( A \) relative to the universe \( U \) is denoted by \( \overline{A} = U - A \). The universe will always be apparent from the context.

\( \text{FP} \), \( P \), and \( \text{NP} \) denote standard complexity classes [29]. Define \( \text{coC} = \{A \subseteq \Sigma^* \mid \overline{A} \in C\} \) for a class \( C \). Let \( \text{UP} \) denote the set of problems that can be accepted by a non-deterministic 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. TALLY denotes the class \( \{ A \mid A \subseteq \{0\}^* \} \). We adopt the following notions from Köbler, Messer, and Torán [24] 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.

\[
\begin{align*}
E & \equiv \text{DTIME}(2^{O(n)}) \\
\text{NE} & \equiv \text{NTIME}(2^{O(n)}) \\
\text{NEE} & \equiv \text{NTIME}(2^{O(2^n)})
\end{align*}
\]

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

Let \( M \) be an oracle Turing machine. \( M^P(x) \) denotes the computation of \( M \) on input \( x \) with \( D \) as an oracle. For an arbitrary oracle \( D \) we let \( L(M^D) = \{ x \mid M^D(x) \text{ accepts} \} \), where as usual if \( M \) is nondeterministic, the computation \( M^D(x) \) accepts if and only if it has at least one accepting path. For a deterministic polynomial-time oracle Turing transducer \( F \) (i.e., a Turing machine computing a function), 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 \( A, B \in \text{NP} \) and \( A \cap B = \emptyset \), then we call \( (A, B) \) a disjoint \( \text{NP} \)-pair. The set of all disjoint \( \text{NP} \)-pairs is denoted by \( \text{DisNP} \).

We use the following reducibilities for sets \( A, B \subseteq \Sigma^* \). \( A \leq_m^p B \) if there exists an \( f \in \text{FP} \) such that \( x \in A \iff f(x) \in B \). \( A \leq_{m,i}^p B \) if \( A \leq_{m,i}^p B \) via some length-increasing \( f \in \text{FP} \). For disjoint \( \text{NP} \)-pairs \( (A, B) \) and \( (C, D) \) we define specific reducibilities. \( (A, B) \leq_{m}^p (C, D) \) (resp., \( (A, B) \leq_{m,i}^p (C, D) \)) if there exists an \( f \in \text{FP} \) (resp., a length-increasing \( f \in \text{FP} \)) with \( f(A) \subseteq C \) and \( f(B) \subseteq D \). We use \( A \leq_{m}^p (C, D) \) as an abbreviation for \( (A, \overline{A}) \leq_{m}^p (C, D) \) and analogous notations for other reducibilities.

When we consider reducibilities in the presence of an oracle \( O \), we write \( \leq_{m}^{p, O} \), \( \leq_{m,i}^{p, O} \), \( \leq_{m}^{p, O} \), and \( \leq_{m,i}^{p, O} \) to indicate that the reduction function has access to \( O \).

For a complexity class \( C \) and some problem \( A \), we say that \( A \) is \( \leq \)-hard for \( C \) if for all \( B \in C \) it holds \( B \leq A \), where \( \leq \) is some reducibility. A is called \( \leq \)-complete for \( C \) if it is \( \leq \)-hard for \( C \) and \( A \in C \). Let \( \text{NCP}^p_{m} \) (resp., \( \text{NPC}^p_{m} \), \( \text{NCP}^i_{m} \)) be the set of problems that are \( \leq_{m}^{p} \)-complete (resp., \( \leq_{m,i}^{p} \)-complete, \( \leq_{m,i}^{i-o/poly} \)-complete) for \( \text{NP} \), where the reducibility \( \leq_{m,i}^{i-o/poly} \) is given in Definition 6 below. If for all \( A \in \text{NP} \) it holds \( A \leq_{m}^{p} (C, D) \), then we say that \( (C, D) \) is \( \leq_{m,i}^{p, O} \)-hard for \( \text{NP} \).

Let \( \text{SAT} \) denote the set of satisfiable formulas and \( \text{TAUT} \) the set of tautologies. Without loss of generality, we assume that each word over \( \Sigma^* \) encodes a propositional formula.

**Definition 1** ([6]). A function \( f \in \text{FP} \) is called a proof system for the set \( \text{ran}(f) \).

For \( f, g \in \text{FP} \) we say that \( f \) is simulated by \( g \) (resp., \( f \) is \( P \)-simulated by \( g \)) denoted by \( f \leq g \) (resp., \( f \leq P g \)) if there is a function \( \pi \) (resp., \( \pi \) a function \( \pi \in \text{FP} \)) and a polynomial \( p \) such that \( |\pi(x)| \leq p(|x|) \) and \( g(\pi(x)) = f(x) \) for all \( x \). A function \( g \in \text{FP} \) is optimal (resp., \( P \)-optimal), if \( f \leq g \) (resp., \( f \leq P g \)) for all \( f \in \text{FP} \) with \( \text{ran}(f) = \text{ran}(g) \). Corresponding relativized notions are obtained by using \( \text{PO}, \text{FP}^O, \) and \( \leq_{m,i}^{O, O} \) in the definitions above. A propositional proof system (pps) is a proof system for \( \text{TAUT} \).

**Remark 2.** The notion of a propositional proof system does not have a canonical relativization. However, in view of Corollary 4 below, it is reasonable to use the following convention. We say that there exist \( \text{PO} \)-optimal (resp., \( \text{PO} \)-optimal) pps relative to an oracle \( O \), if there exists a \( \leq_{m,i}^{O, O} \)-complete \( A \in \text{coNP}^O \) that has a \( \text{PO} \)-optimal (resp., \( \text{PO} \)-optimal) proof system.
The following proposition states the relativized version of a result by Köbler, Messner, and Torán [24], which they show with a relativizable proof.

**Proposition 3** ([24]). For every oracle $O$, if $A$ has a $P^O$-optimal (resp., optimal) proof system and $0 \neq B \leq^O_{\text{m}} A$, then $B$ has a $P^O$-optimal (resp., optimal) proof system.

**Corollary 4.** For every oracle $O$, if there exists a $\leq^O_{\text{m}}$-complete $A \in \text{coNP}^O$ that has a $P^O$-optimal (resp., optimal) proof system, then all non-empty sets in $\text{coNP}^O$ have $P^O$-optimal (resp., optimal) proof systems.

**Definition 5.** For $f \in \text{FP}$ and a polynomial $q$, a word $y \in \text{ran}(f)$ is $q$-hard w.r.t. the proof system $f$ if there does not exist $x \in \Sigma^{|y|}$ 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., $f_q = \{y \in \text{ran}(f) \mid y$ is $q$-hard w.r.t. $f\}$.

We introduce $\leq^\text{io-poly}_{\text{m}}$-reducibility, which we use to study a weakened variant of $H_{\text{union}}$: the union of disjoint $\leq^\text{io-poly}_{\text{m}}$-complete sets for $\text{NP}$ is $\leq^\text{io-poly}_{\text{m}}$-complete.

$\text{P/poly}$ is the class of sets $A \subseteq \Sigma^*$ for which there exist a $B \in \text{P}$ and a function $h : \mathbb{N} \to \Sigma^*$ such that $|h(n)|$ is polynomially bounded in $n$ and for all $x$ it holds that $x \in A \iff (x, h(|x|)) \in B$. $\text{FP/poly}$ is the class of total functions $f : \Sigma^* \to \Sigma^*$ for which there exist a $g \in \text{FP}$ and a function $h : \mathbb{N} \to \Sigma^*$ 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 $f \equiv g$, 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 $A \equiv B$, if their characteristic functions agree infinitely often. For a class $C$ of functions or sets let $\text{io-C} = \{A \mid \exists B \in C, A \equiv B\}$.

**Definition 6.** A set $A \subseteq \Sigma^*$ is infinitely often $\text{P/poly}$ reducible to a set $B \subseteq \Sigma^*$, written as $A \leq^\text{io-poly}_{\text{m}} B$, if there exists an $f \in \text{io-FP/poly}$ such that for all $x$ it holds that $x \in A \iff f(x) \in B$.

It should be mentioned that $\leq^\text{io-poly}_{\text{m}}$ is an artificial reducibility notion (e.g., it is not transitive), which emerged from the attempt to express the right-hand side of the known implication $H_{\text{union}} \Rightarrow \text{NP} \neq \text{coNP}$ as a variant of $H_{\text{union}}$. In Theorem 10 we show that this is possible with $\leq^\text{io-poly}_{\text{m}}$ reducibility.

In our oracle constructions we use the following notations: If a partial function $t$ is not defined at point $x$, then $t \cup \{x \mapsto y\}$ denotes the extension $t'$ of $t$ that at $x$ has value $y$ and satisfies $\text{dom}(t') = \text{dom}(t) \cup \{x\}$.

If $A$ is a set, then $A(x)$ denotes the characteristic function at point $x$, i.e., $A(x) = 1$ 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 $\omega$-word. In this way, $D(i)$ denotes both, the characteristic function at point $i$ and the $i$-th letter of the characteristic sequence, which are the same. A finite word $w$ describes an oracle that is partially defined, i.e., only defined for natural numbers $x < |w|$. Occasionally, we 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. In particular, for an oracle Turing machine $M$, the notation $M^w(x)$ refers to $M^{\{i \mid w(i) = 1\}}(x)$ (hence, oracle queries that $w$ is not defined for are answered by “no”). Using $w$ instead of $\{i \mid w(i) = 1\}$ additionally allows us to define the following notion: for a nondeterministic oracle Turing machine $M$, the computation $M^w(x)$ definitely accepts if it contains a path that accepts and all queries on this path are $< |w|$. The computation $M^w(x)$ definitely rejects if all paths reject and all queries are $< |w|$. We say that the computation $M^w(x)$ is definite if it definitely accepts or definitely rejects. Similarly, for a deterministic oracle Turing transducer $F$, the computation $F^w(x)$ is definite if all its queries are $< |w|$.
3 Are Unions of Disjoint NP-Complete Sets NP-Complete?

It is difficult to find out whether \( H_{\text{union}} \) is true or not, since each outcome solves a long standing open problem:

\[
\begin{align*}
H_{\text{union}} \text{ is true} & \Rightarrow \text{NP} \neq \text{coNP} \\
H_{\text{union}} \text{ is false} & \Rightarrow \text{P-inseparable disjoint NP-pairs exist if and only if } \text{P} \neq \text{NP}
\end{align*}
\]

Therefore, researchers approach the hypothesis \( H_{\text{union}} \) by proving equivalent, necessary, and sufficient conditions. This section continues this program as follows. In subsection 3.1 we investigate a stronger variant of \( H_{\text{union}} \), in 3.2 the original hypothesis, and in 3.3 a weaker variant. We characterize \( H_{\text{union}} \) and its variants in several ways, e.g., in terms of p-producibility or coNP-completeness of the set of hard formulas of pps. Within each subsection all hypotheses are equivalent and hence the following implications hold.

- hypotheses in subsect. 3.1 \( \Rightarrow \) hypotheses in subsect. 3.2 \( \Rightarrow \) hypotheses in subsect. 3.3

\[
\begin{align*}
\Downarrow & \\
H_{\text{union}} & \quad \text{NP} \neq \text{coNP}
\end{align*}
\]

Note that under the assumption that all sets in NPC\(_m\) 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.

3.1 Length-Increasing Polynomial-Time Reducibility

Consider the hypothesis that the union of SAT with a disjoint \( B \in \text{NP} \) is \( \leq^p_{\text{m,li}} \)-complete for NP. We show that this hypothesis can be characterized in terms of the p-producibility of the set of hard formulas of pps. The notion of p-producibility was introduced by Hemaspaandra, Hemaspaandra, and Hempel [21].

- Definition 7 ([21]). A set \( A \) is p-producible if and only if there is some \( f \in \text{FP} \) with \( |f(x)| \geq |x| \) and \( f(x) \in A \) for all \( x \).

- Theorem 8. The following statements are equivalent:
  1. For all \( B \in \text{NP} \) with \( \text{SAT} \cap B = \emptyset \) it holds \( \text{SAT} \cup B \in \text{NPC}_{\text{m,li}} \).
  2. For all \( A, B \in \text{NPC}_{\text{m,li}} \) with \( A \cap B = \emptyset \) it holds \( A \cup B \in \text{NPC}_{\text{m,li}} \).
  3. \( f_q \) is p-producible for all pps \( f \) and all polynomials \( q \).

Proof. 1 \( \Rightarrow \) 2: Let \( A, B \in \text{NPC}_{\text{m,li}} \) be disjoint and \( \text{SAT} \leq^p_{\text{m,li}} A \) via a length-increasing \( f \in \text{FP} \). \( B' = f^{-1}(B) \) is in NP and disjoint to SAT and hence \( \text{SAT} \cup B' \in \text{NPC}_{\text{m,li}} \).

\( \text{SAT} \cup B' \leq^p_{\text{m,li}} A \cup B \) via \( f \) and thus \( A \cup B \in \text{NPC}_{\text{m,li}} \).

2 \( \Rightarrow \) 3: By assumption, \( \text{NP} \neq \text{coNP} \). Let \( f \) be a pps, \( q \) a polynomial, and define

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

\( B \cap \text{SAT} = \emptyset \) and \( \text{SAT} \cup B \subseteq \Sigma^* \). For \( A' = \emptyset \text{SAT} \cup B \) and \( B' = 1\text{SAT} \cup 0B \) it holds \( A' \cap B' = \emptyset \) and \( A', B' \in \text{NPC}_{\text{m,li}} \). By 2, \( A' \cup B' = \{0, 1\}(\text{SAT} \cup B) \in \text{NPC}_{\text{m,li}} \). In particular, \( \text{SAT} \leq^p_{\text{m,li}} (\text{SAT} \cup B) \). Hence \( \text{SAT} \leq^p_{\text{m,li}} A \cup B \) via \( h_1 \in \text{FP} \) with \( |x| \leq |h_1(x)| \). Let \( h_2 \in \text{FP} \) be length-increasing such that \( \text{SAT} \leq^p_{\text{m,li}} \text{SAT} \) via \( h_2 \). Thus \( \text{SAT} \leq^p_{\text{m,li}} A \cup B \) via \( h(x) = h_1(h_2(x)) \). We claim that \( f_q \) is p-producible via the length-increasing \( g(x) = \neg h(x \land \neg x) \): As \( h(x \land \neg x) \not\in \text{SAT} \cup B \), \( g(x) \) is a tautology. If \( g(x) \not\in f_q \), then there exists \( y \) with \( |y| \leq q(|g(x)|) \) and \( f(y) = g(x) = \neg h(x \land \neg x) \). Hence \( h(x \land \neg x) \in B \), a contradiction.
We consider the hypothesis that the union of $\Sigma$ and $\overline{\Sigma}$ is $\text{NP}$-complete, i.e., $\Sigma \cup \overline{\Sigma}$ is $\text{NP}$-complete. We argue for $\text{1} \Rightarrow \text{3.2 Polynomial-Time Reducibility}$.

Let $q'$ be a polynomial such that $|\neg x| \leq q'(|x|)$. Choose $r(n) = 2 \cdot (q(q'(n)) + n + 1)$. By 3, $f_r$ is $p$-producible via some $g \in \text{FP}$ with $|g(x)| \geq |x|$. Consider the length-increasing $h \in \text{FP}$ with $h(x) = \neg g(x) \lor x$. We show $\text{SAT} \leq_{\text{m}, \text{h}} \text{SAT} \cup B$ via $h$, which implies $\text{SAT} \leq_{\text{m}, \text{h}} \text{SAT} \cup B \cup \text{SAT}$. If $g(x)$ is a tautology, $x \in \text{SAT} \iff h(x) \in \text{SAT}$. It remains to show $x \notin \text{SAT} \Rightarrow h(x) \notin \text{SAT}$. Let $x \notin \text{SAT}$. If $h(x) = \neg g(x) \land x \notin \text{SAT}$, then due to $|x| \leq |\neg g(x)|$, it holds $\neg g(x) \in \text{B}$. Hence there is some path $z$ such that $M$ accepts $\neg g(x)$ on path $z$. Thus $|z| \leq q'(q(|g(x)|))$. Consequently, $f(|g(x)|) = g(x)$ and $|q(z)| = r(|g(x)|)$, in contradiction to $g(x) \in f_r$.

### 3.2 Polynomial-Time Reducibility

We consider the hypothesis that the union of $\text{SAT}$ with a disjoint $B \in \text{NP}$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{NP}$. This is equivalent to $\text{H}_{\text{union}}$. We prove one more characterization stating that for each other $f$ the set of formulas hard for $f$ is $\text{coNP}$-complete. In the following theorem, the equivalence $1 \iff 2$ was shown in [14].

**Theorem 9.** The following statements are equivalent:

1. For all $B \in \text{NP}$ with $\text{SAT} \cap B = \emptyset$ it holds $\text{SAT} \cup B \in \text{NP}^p$.
2. For all $A, B \in \text{NP}^p$ with $A \cap B = \emptyset$ it holds $A \cup B \in \text{NP}^p$.
3. $f_q$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{coNP}$ for all $f$ and all polynomials $q$.

**Proof.** We argue for $\text{1} \Rightarrow \text{3}$. By definition, $f_q = \{x \in \text{TAUT} | \neg \exists z \in \Sigma \leq q(|x|) f(z) = x\}$ and hence $f_q \subseteq \text{coNP}$. Let $B = \{x \in \Sigma | \exists z \in \Sigma \leq q(|x|) f(z) = \neg x\}$.

Observe that $B \in \text{NP}$ and $\text{SAT} \cap B = \emptyset$. By assumption, $\text{SAT} \cup B \subseteq \text{NP}^p$ and hence $\text{SAT} \cup B$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{coNP}$. Note $\text{SAT} \cup B = \{x \in \Sigma | \neg x \in \text{TAUT} \land \neg \exists z \in \Sigma \leq q(|x|) f(z) = \neg x\}$. Thus $x \in \text{SAT} \cup B \iff \neg x \in f_q$ and hence $f_q$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{coNP}$.

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

Let

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

Observe that $f$ is a pps. By assumption, the set $f_q = \{x \in \text{TAUT} | \neg \exists z \in \Sigma \leq q(|x|) f(z) = x\}$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{coNP}$. Observe $f_q \cap \Sigma^{\geq n} = \{x \in \text{TAUT} | \neg x \notin B \cap \Sigma^{\geq n}\}$ for sufficiently large $n \in \mathbb{N}$. Hence for all $x \in \Sigma^{\geq n}$ it holds that $x \notin f_q \iff x \notin \text{SAT} \cup B$. In the case $\text{SAT} \cup B \neq \emptyset$ this shows $f_q \leq_{\text{m}} \text{SAT} \cup B$ and hence $\text{SAT} \cup B$ is $\leq_{\text{m}} \text{NP}$-complete for $\text{NP}$.

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

$\blacksquare$
3.3 Infinitely Often P/poly Reducibility

Consider the hypothesis that the union of SAT with a disjoint \( B \in \text{NP} \) is \( \leq_{\text{m}, \text{p}}^{\text{pp}} \)-complete for NP. We show that this hypothesis is equivalent to \( \text{NP} \neq \text{coNP} \).

\( \blacktriangleright \) Theorem 10. The following statements are equivalent:
1. For all \( B \in \text{NP} \) with \( \text{SAT} \cap B = \emptyset \) it holds \( \text{SAT} \cup B \in \text{NP}^{\text{io-p/poly}} \).
2. For all \( A, B \in \text{NP}^{\text{io-p/poly}} \) with \( A \cap B = \emptyset \) it holds \( A \cup B \in \text{NP}^{\text{io-p/poly}} \).
3. \( \text{NP} \neq \text{coNP} \) (i.e., polynomially bounded pps do not exist).

4 Oracle Constructions

4.1 An Oracle for \( \text{P} = \text{UP} \) and \( \neg \text{H}_{\text{cpair}} \)

We construct an oracle \( O \) relative to which \( \text{P} = \text{UP} \) and \( \neg \text{H}_{\text{cpair}} \). This answers open questions by Pudlák [32], who lists several conjectures and asks for equivalence proofs and oracles relative to which conjectures are different. Among these are:

\[
\begin{align*}
\text{DisjNP} & \equiv \text{“there are no } \leq_{\text{m}, \text{p}}^{\text{pp}} \text{-complete disjoint NP-pairs (i.e., } \neg \text{H}_{\text{cpair}} \text{“)}
\text{CON} & \equiv \text{“there are no P-optimal propositional proof systems“}
\text{SAT} & \equiv \text{“NP-complete sets do not have P-optimal proof systems”}
\text{UP} & \equiv \text{“UP does not have } \leq_{\text{m}, \text{p}}^{\text{pp}} \text{-complete sets“}
\text{NP} \cap \text{coNP} & \equiv \text{“NP } \cap \text{coNP does not have } \leq_{\text{m}, \text{p}}^{\text{pp}} \text{-complete sets“}
\end{align*}
\]

Relative to \( O \), \( \text{DisjNP} \) and \( \text{NP} \cap \text{coNP} \) hold, but \( \text{UP} \) does not. Hence \( \text{DisjNP} \) and \( \text{NP} \cap \text{coNP} \) do not imply \( \text{UP} \). Moreover, relative to \( O \), also the following conjectures mentioned by Pudlák [32] do not imply \( \text{UP} \) (as they are implied by \( \text{DisjNP} \) relative to all oracles): \( \text{CON} \), \( \text{CON} \lor \text{SAT} \), and \( \text{P} \neq \text{NP} \). The fact that relative to \( O \), \( \text{CON} \) does not imply \( \text{UP} \) is of particular interest as the converse implication holds relative to all oracles.

\( \blacktriangleright \) Theorem 11. There exists an oracle \( O \) with the following properties.
1. \( \text{DisjNP}^{\text{O}} \) does not have \( \leq_{\text{m}, \text{O}}^{\text{pp}} \)-complete pairs.
2. \( \text{NP}^{\text{O}} \cap \text{coNP}^{\text{O}} \) does not have \( \leq_{\text{m}, \text{O}}^{\text{pp}} \)-complete sets.
3. \( \text{P}^{\text{O}} = \text{UP}^{\text{O}} \).

Sketch of the construction: For simplicity, we argue only for 1 and 3. Let \( M_0, M_1, \ldots \) be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines and let \( F_0, F_1, \ldots \) be a standard enumeration of deterministic, polynomial-time oracle Turing transducers. We assume that for all \( i \) the running times of \( M_i \) and \( F_i \) are bounded by the polynomial \( n^i + i \). Adopting an idea by Baker, Gill and Solovay [1], we start with a PSPACE-complete oracle that consists of words of odd length. During the construction we add words of lengths \( e(n) \) to the oracle, where \( e(0) = 2 \) and \( e(n+1) = 2^{2^{e(n)}} \). Since \( e(n) \) is even, the PSPACE-complete set that we started with will not be damaged.

On the one hand, the construction tries to prevent that \( L(M_i) \) and \( L(M_j) \) are disjoint. If this is not possible, then \( M_i \) and \( M_j \) inherently accept disjoint sets. In this case, we make sure that there exists a disjoint NP-pair \( (A_{ij}, B_{ij}) \) that does not \( \leq_{\text{m}, \text{p}}^{\text{pp}} \)-reduce to \( (L(M_i), L(M_j)) \). This prevents the existence of complete disjoint NP-pairs. On the other hand, we try to prevent that \( M_i \) has the uniqueness property “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 allows us to show \( L(M_i) \in \text{P} \).
On the technical side, we maintain a growing collection \( t \) of properties that we demand in the further construction. If an oracle satisfies the properties defined by \( t \), then we call it \( t \)-valid. The collection \( t \) contains properties of the following style:

**V1:** The oracle constructed so far guarantees that \( L(M_i) \cap L(M_j) \neq \emptyset \) for all extensions of the oracle.

**V2:** It is impossible to reach \( L(M_i) \cap L(M_j) \neq \emptyset \) and for the oracle constructed so far we have \( A_{ij} \cap B_{ij} = \emptyset \). (In the future we restrict to extensions that maintain this property.)

**V3:** The oracle constructed so far guarantees that for all extensions of the oracle, \( M_i \) does not have the uniqueness property.

**V4:** It is impossible to destroy the uniqueness property of \( M_i \).

The construction successively settles the following tasks:
- **task (i, j):** If possible, then realize V1 for the pair \((L(M_i), L(M_j))\), otherwise, V2 holds.
- **task i:** If possible, then realize V3 for \( M_i \), otherwise, V4 holds.
- **task (i, j, r):** Make sure that \( F_r \) does not realize a reduction \( (A_{ij}, B_{ij}) \leq_{pp}^{m}(L(M_i), L(M_j)) \).

The tasks \((i, j)\) and \((i, j, r)\) make sure that relative to the final oracle, \( L(M_i) \cap L(M_j) \neq \emptyset \) or \((L(M_i), L(M_j))\) is not \( \leq_{pp}^{m}\)-complete. The task \( i \) ensures that machines having the uniqueness property are very special. An adaption of an argument by Rackoff [33] yields that these machines accept sets in \( P \), hence \( P = UP \).

### 4.2 An Oracle for \( H_{\text{union}} \) and \( H_{\text{opps}} \)

This section constructs an oracle \( O \) relative to which the implication \( H_{\text{opps}} \Rightarrow \neg H_{\text{union}} \) is false. Theorem 22 provides the analogous for the converse implication.

In addition, relative to \( O \) there exists a tally set in \( \text{NEE} - \text{coNEE} \), where \( \text{NEE} \equiv \text{NTIME}(2^{O(2^n)}) \). It shows that two conditions which are sufficient for the existence of an optimal (resp., a \( P \)-optimal) \( \text{pp} \) [24] are not necessary relative to \( O \).

**Theorem 12.** There exists an oracle \( O \) with the following properties.

1. There exists a \( P^O \)-optimal propositional proof system \( f \).
2. If \( A \) is \( \leq_{pp}^{m} \)-complete for \( \text{NP}^O \) and disjoint from \( B \in \text{NP}^O \), then \( A \cup B \) is \( \leq_{pp}^{m} \)-complete for \( \text{NP}^O \).
3. \( \text{NEE}^O \cap \text{TALLY} \not\subseteq \text{coNEE}^O \), where \( \text{NEE}^O \equiv \text{NTIME}^O(2^{O(2^n)}) \).

**Proof.** We only prove statements 1 and 2. Statement 3 follows (in a nontrivial way) from the construction below. Let \( M_1, M_2, M_3, \ldots \) be a standard enumeration of nondeterministic, polynomial-time oracle Turing machines. Let \( F_2, F_3, F_4, \ldots \) be a standard enumeration of deterministic, polynomial-time oracle Turing transducers. We assume that the running time of \( M_i \) for \( i \) odd (resp., \( F_j \) for \( j > 0 \) even) is bounded by the polynomial \( n^i + i \) (resp., \( n^j + j \)).

For a (possibly partial) oracle \( D \) we define sets \( K_D \) and \( K_D^P \).

\[
K_D = \{ \langle 0^i, 0^j, x \rangle \mid i \text{ is odd and } M_D(x) \text{ accepts within } j \text{ steps} \}
\]

\[
K_D^P = \{ (z_1, \ldots, z_n) \mid z_1 \in K_D \lor \cdots \lor z_n \in K_D \}
\]

**Claim 13.** For partial oracles \( v \) and \( w \) and all \( y \leq \min(|v|, |w|) \), if \( pr_y(v) = pr_y(w) \), then \( K_D^w(y) = K_D^v(y) \) and \( K_D^w(y) = K_D^v(y) \).

**Proof.** It suffices to show \( K_D^w(y) = K_D^v(y) \). We may assume \( y = \langle 0^i, 0^j, x \rangle \) for suitable \( i, j, x \), since otherwise, \( K_D^w(y) = K_D^v(y) = 0 \). For each \( q \) that is queried within the first \( j \) steps of \( M_D^v(x) \) or \( M_D^i(x) \) 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 \( M_D^v(x) \) accepts within \( j \) steps if and only if \( M_D^i(x) \) accepts within \( j \) steps. \( \triangleright \)
\( K^D \) and \( K_V \) are \( \leq_{m}^{D} \)-complete for \( NP^D \) and their complements are \( \leq_{m}^{D} \)-complete for \( coNP^D \). We construct the oracle such that \( K_P^D \) has a \( P^{G} \)-optimal proof system \( f \in \mathcal{F} \). As \( K^D \) is \( \leq_{m}^{D} \)-complete for \( coNP^D \), this implies the first statement of the theorem.

For a (possibly partial) oracle \( D \) let

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

and observe that \( E^D \in NP^D \). Choose \( e \geq 2 \) such that \( L(M^D) = E^D \) for all (possibly partial) oracles \( D \) and let \( \nu_n = (0^e, 0^{n^* + e}, 0^9) \). Hence \( \nu_n \in K^D \) if and only if \( M^D(0^n) \) accepts, i.e., \( \nu_n \in K^D \Leftrightarrow 0^n \in E^D \).

For \( i \in 2N^+ \) and \( x, y \in \mathbb{N} \) let \( c(i, x, y) = (0^i, 0^{(|x|^i + i)2^{iu}}) \). 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 \( y \notin K_V \), i.e., \( c(i, x, y) \) is a proof for \( y \notin K_V \).

\( \triangleright \) Claim 14. The following holds for all partial oracles \( w_i \), all \( i \in 2N^+ \) and \( x, y \in \mathbb{N} \).

1. If \( c(i, x, y) \leq |w| \), then \( F_i^w(x) \) is definite and \( F_i^w(x) = F_i^w(x) < |w| \) for all \( v \supseteq w \).
2. If \( c(i, x, y) \leq |w| \), then \( F_i^w(x) \) is definite and \( F_i^w(x) = F_i^w(x) \in K^w \Leftrightarrow F_i^w(x) \in K^w \) for all \( v \supseteq w \).

Proof. 1: \( F_i^w(x) \) is definite, 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 \( F_i^w(x) = F_i^w(x) < |w| \).

Preview of construction: On the one hand, the construction tries to prevent that \( F_i \) is a proof system for \( K_V \). If this is not possible, then \( F_i \) inherently is a proof system for \( K_V \). 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 \( K_V \). On the other hand, the construction also tries to prevent that \( M_i \) accepts a set disjoint from \( K_V \). If this is not possible, then \( M_i \) inherently accepts a set disjoint from \( K_V \). 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 \( L(M_i) \). Even holds \( (v_{p,k}, u_1, \ldots, u_n) \notin L(M_i) \) for all \( u = (u_1, \ldots, u_n) \) 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 \( K_V \), but guarantees that the result is not in \( L(M_i) \). This yields a reduction \( K_V \leq_{m}^{P} K_V \cup L(M_i) \) and implies that \( K_V \cup L(M_i) \) is \( NP \)-complete.

During the construction we maintain a growing list of properties. This list belongs to the set \( T = \{ (m_1, \ldots, m_n) \mid n \geq 0, m_1, \ldots, m_n \in \mathbb{N}, \text{ and } m_i < m_j \text{ for all } i < j \} \).

If a partial 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 \( t(i) = m_i, \text{ } |t| = n, \text{ and } t + a = (m_1, \ldots, m_n, a) \). If the list \( t \) is a prefix of the list \( t' \), then we write \( t \subseteq t' \). We start with the empty list \( t_0 = () \) which defines no property. By successively appending an element we obtain lists \( t_1, t_2, \text{ and so on.} \)

A partial oracle \( w \in \Sigma^* \) is \( t \)-valid, where \( t \in T \), if the following holds:

**V1:** \( w \subseteq \{ c(i, x, y) \mid i \in 2N^+ \text{ and } x, y \in \mathbb{N} \} \cup \{ v \mid |v| = p^k \text{ for } p \in \mathbb{P}^{2N} \text{ and } k \geq 1 \} \)

(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 \( i \in 2N^+ \) and \( x, y \in \mathbb{N} \) it holds that \( F_i^w(x) = y \notin K_V \).

(meaning: if the oracle contains the codeword \( c(i, x, y) \), then \( F_i^w(x) \) outputs \( y \notin K_V \), hence \( c(i, x, y) \in w \) is a proof for \( y \notin K_V \))

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

\text{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 \( F^w_t(x) \) is definite and outputs \( y < |w| \) with \( y \in K^w_v \).

(meansing: \( F_t \) is not a proof system for \( \overline{K^w_v} \) 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 \( \{c(j, x, y) \in w \mid x, y \in \mathbb{N} \text{ and } |c(j, x, y)| = p\} = \emptyset \).

(meansing: the first part says \( 0^p \not\in E^w \) and hence \( v_{p^k} \not\in K^w \) for all \( k \geq 1 \); the second part says that if \( F_t \) is not a proof system for \( \overline{K^w_v} \) and has a smaller index than \( M_t \), 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 \( x \in K^w_v \) and \( M^w_t(x) \) definitely accepts.

(meansing: \( M_t \) is not disjoint from \( K^w_v \) relative to all extensions of \( w \))

\( \triangleright \) **Claim 15.** The following holds in reference to the definition of \( t \)-valid.

1. In \( V1 \), the two sets are disjoint.
2. In \( V2 \), \( F^w_t(x) \) is definite and \( F^w_t(x) = y \notin K^w_v \) for all \( v \equiv w \).
3. In \( \mathcal{V}3a \), \( F^w_t(x) \) is definite.
4. In \( V3b \), \( y \in K^w_v \) for all \( v \equiv w \).
5. In \( V4b \), \( x \in K^w_v \) for all \( v \equiv w \).

**Proof.** \( V1 \): The union is disjoint, since \( |c(i, x, y)| \) is even. \( V2 + V3a \): Follows from Claim 14. \( V3b + V4b \): Follows from Claim 13. \( \triangleright \)

\( \triangleright \) **Claim 16.** Let \( u \) and \( w \) be \( t \)-valid. If \( u \not\subseteq v \subseteq w \), 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, \( v \not\subseteq w \) and Claim 14 imply that \( v \) satisfies \( V2 \) and \( V3a \). Since \( u \) is \( t \)-valid, it satisfies \( V3b \) and \( V4b \). From \( u \subseteq v \), Claim 15.4, and Claim 15.5 it follows that \( v \) satisfies \( V3b \) and \( V4b \). \( \triangleright \)

**Oracle construction:** Let \( t_0 = () \) be the empty list and \( w_0 = \varepsilon \), which is \( t_0 \)-valid. We construct a sequence \( t_0 \subseteq t_1 \subseteq \cdots \) of lists from \( \mathcal{V} \) and a sequence \( w_0 \subseteq w_1 \subseteq \cdots \) 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 \( t_s \not\subseteq t_{s-1} \) of length \( s \) and a \( t_{s-1} \)-valid \( w_s \not\subseteq w_{s-1} \).

- \( s \) even: If there is a \( t_{s-1} \)-valid \( v \not\subseteq w_{s-1} \) such that for some \( x \), \( F^w_t(x) \) is definite and has an output \( y < |v| \) with \( y \in K^w_v \), 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 \( t_s = t_{s-1} + b \) for an even \( m > |w_s| \) that is greater than all elements in \( t_{s-1} \).

  (meaning: possible, force that \( F_t \) is not a proof system for \( \overline{K^w_v} \) 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 \( v \not\subseteq w_{s-1} \) such that for some \( x < |v| \), \( x \in K^w_v \) and \( M^w_t(x) \) definitely accepts, then let \( w_s = v \) and \( t_s = t_{s-1} + 0 \). Otherwise, let \( w_s = w_{s-1}b \) for \( b \in \{0, 1\} \) such that \( w_{s-1}b \) is \( t_{s-1} \)-valid and \( t_s = t_{s-1} + p \) for \( p \in \mathbb{P} \geq 41 \) large enough such that \( (16|v_{p,k}|)^p < 2^{9^p} \) for all \( k \in \mathbb{N}^+ \), \( p > |w_s| \), and \( p \) is greater than all elements in \( t_{s-1} \).

  (meaning: force \( L(M_t) \cap K^w_v \neq \emptyset \) if possible; otherwise, choose a suitable prime \( p \) and make sure that the oracle contains no elements of length \( p^k \) and hence \( v_{p,k} \not\in K^w \) for all \( k \geq 1 \); the step corresponds to \( V4 \))

The subsequent claims refer to the construction above. We start by showing that the construction is possible and how one can extend a \( t_s \)-valid \( w \not\subseteq w_s \) by one bit. The proof can be found in [10].
\[ \text{where we follow the cases in Claim 17.} \]

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 \( z \geq |w| \) the following holds.
   a. if \( F^{_{y_1}}(x) = y \), then \( w_1 \) is \( t_s \)-valid and \( w_0 \) is not.
   b. if \( F^{_{y_1}}(x) \neq y \), then \( w_0 \) is \( t_s \)-valid and \( w_1 \) 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. \( w_0 \) is \( t_s \)-valid.
   b. if \( F^{_{y_1}}(x) = y \notin K^{_{y_1}} \) 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 \( w_1 \) 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. \( w_0 \) is \( t_s \)-valid.
   b. if \( F^{_{y_1}}(x) = y \notin K^{_{y_1}} \), then \( w_1 \) 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 \( w_0 \) and \( w_1 \) are \( t_s \)-valid.

5. In all other cases \( w_0 \) is \( t_s \)-valid.

\[ \text{Claim 18.} \quad M^{_{Q_0}}(v_{j^*}, u_1, \ldots, u_n) \text{ rejects for all odd } s \text{ with } t_s(s) = p \in \mathbb{P}^{\geq 41}, \text{ all } k \in \mathbb{N}^+, \text{ and all } u = (u_1, \ldots, u_n) \text{ with } |u| \leq |v_{j^*}|. \]

Proof. We assume that \( M^{_{Q_0}}(u') \) accepts for \( u' = (v_{j^*}, u_1, \ldots, u_n) \) and show a contradiction. Choose \( j > s \) large enough such that \( M^{_{Q_0}}(u') \) 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 \( M^{_{Q_0}}(u') \). For \( r \) we inductively define the set of queries and their dependencies.

\[
Q_0 = \{ q \mid q \text{ is queried on } r \} \\
Q_{n+1} = \bigcup_{z \in Q_n \text{ with } z = c(i, x, y), i < s, x, y \in \mathbb{N}, t_{s-1}(i) > 0} \{ q \mid q \text{ is queried by } F^{_{w_j}}(x) \}
\]

Let \( Q = \bigcup_{n \geq 0} Q_n \). It holds that \( |Q| < 2p^k \), 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 \( |x|^i + i \leq (|x|^i + i)2^{n+1} \leq |z|/2 \) by the definition of \( c \) and \( \langle \ldots \rangle \). Thus the \( m_n \) form a geometric series. From \( |v'| = |v| + 2|v_{j^*}| + 2 \leq 4|v_{j^*}| \) it follows \( |Q| \leq 2m_0 \leq 2(|u'|^* + s) \leq 4|u|^* \leq (16|v_{j^*}|)^* < 2p^k \), where the latter inequality holds by the choice of \( p \) in step \( s \).

Let \( \tilde{q} \) be the smallest word of length \( p^k \) that is not in \( Q \). The word exists, since \( |Q| < 2p^k \). By the assumption that \( |w_j| > q \) for all \( q \) with \( |q| = p^k \), it holds in particular \( |w_j| > \tilde{q} \). By the choice of \( p \) in step \( s \) we have \( p > |w_s| \) and hence \( w_{s-1} \) is \( t_{s-1} \)-valid, \( t_{s-1} \)-valid. Thus for \( v = \text{pr}_{\tilde{q}}(w_j) \) it holds that \( w_{s-1} \not\subseteq v \subseteq w_j \), where \( w_{s-1} \) and \( w_j \) are \( t_{s-1} \)-valid. By Claim 16, \( v \) is \( t_{s-1} \)-valid. Moreover, \( |v| = \tilde{q}, |\tilde{q}| = p^k \), and \( p \notin t_{s-1} \), since step \( s \) chooses \( p \) greater than all elements in \( t_{s-1} \). From Claim 17.4 it follows that \( v_1 \) is \( t_{s-1} \)-valid.

We show that there is a \( t_{s-1} \)-valid \( w' \subseteq v_1 \) 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 \( v_1 \) is extended bit by bit to \( w' \), i.e., how the word \( w \supseteq v_1 \supseteq w_{s-1} \) constructed so far is extended by one bit \( b \), where \( z \) denotes the length of \( w \). We define \( b \) and argue that

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

where we follow the cases in Claim 17.
1. \( z = c(i, x, y) \) for \( i \in 2\mathbb{N}^+, x, y \in \mathbb{N}, i \leq s - 1, t_s(i) > 0 \): If \( F_i^w(x) = y \), then \( b = 1 \) else \( b = 0 \). Note that \( z > q > p > t_s(i) \). By Claim 17.1, \( wb \) is \( t_{s-1} \)-valid. If \( z \in Q \), then by (3), \( q \in Q \) for all \( q \) queried by \( F_i^w(x) \). For these \( q \) it holds that \( q < z = |w| \) and hence \( w(q) = w_i(q) \) by (4). 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 \( z \in w_j \iff F_i^{w_j}(x) = y \iff F_i^w(x) = y \iff b = 1 \). Hence \( b = w_j(z) \), which proves (4).

2. \( z = c(i, x, y) \) for \( i \in 2\mathbb{N}^+, x, y \in \mathbb{N}, i \leq s - 1, t_s(i) = 0 \): Let \( b = 0 \). By Claim 17.2, \( wb \) 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 \( z = |w| > |w| = \bar{q} \) and hence \( |z| \geq p^k \geq p \). This is a contradiction, which shows (4).

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 17.3. Otherwise, \( b = 1 \) and \( z \in Q \cap w_j \).

We show \( |x|^t + i < p^k \): Assume \( |x|^t + i \geq p^k \). From \( p \geq 41, e \geq 2, k \geq 1 \), and \( i \geq s \geq 1 \) it follows that \( (41 \cdot p^k)^s < p^{2k^e} \). Moreover, \( |v|_p = 2(e + p^k + e + p^k + 3) \leq 10 \cdot p^k \).

Hence we obtain

\[
|c(i, x, y)| > (|x|^t + i)^{2e} \geq p^{2k^e} > (41 \cdot (p^k)^s)^s \geq (4 \cdot p^k)^s + s \geq |u|^s + s.
\]

Thus \( |z| > |u|^s + s \geq m_0 \geq m_1 \geq \cdots \) and hence \( z \notin Q \), a contradiction. This proves \( |z|^t + i < p^k \).

We know that \( w_j \) is \( t_j \)-valid. By V2, \( F_i^{w_j}(x) = y \notin K_j^{w_j} \). By \( |x|^t + i < p^k \), the computation \( F_i^{w_j}(x) \) stops within \( |x|^t + i < p^k \) steps. Hence it can only ask queries of length \( < p^k \) and \( |y| < p^k \). Thus \( F_i^{w_j}(x) = y \notin K_j^{w_j} \), since \( w \) and \( w_j \) coincide with respect to all words of length \( < p^k \). By Claim 17.3, \( wb \) is \( t_{s-1} \)-valid.

To show the second part of (4) 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 (4).

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 17.4, \( wb \) is \( t_{s-1} \)-valid, which implies (4).

5. Otherwise: Let \( b = 0 \). By Claim 17.5, \( wb \) is \( t_{s-1} \)-valid. Assume \( b \neq w_j(z) \), i.e., \( z \notin w_j \). 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 \( p' \notin t_{s-1} \) (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 (4).

This shows that there exists a \( t_{s-1} \)-valid \( w' \subseteq v \subseteq w_{s-1} \) such that \( |w'| = |w_j| > |w' \) and for all \( q \in Q \) it holds that \( q \in w' \iff q \in w_j \). Hence \( M_w^{w_j}(w') \) definitely accepts. Moreover, \( |w| = q \) and hence \( q \in w' \). From \( |q| = p^k \) it follows \( v_p \in K_w^{w'} \) and \( w' \in K_w^{w'} \). 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 19. \( K_q \cup B \) is \( \leq_m \)-complete for \( NP^O \) for all \( B \in NP^O \) that are disjoint to \( K_q \).

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

Let \( f((u_1, \ldots, u_n)) = (u_0, u_1, \ldots, u_n) \), where \( u_0 = v_p \) for the minimal \( k \geq 1 \) such that \( |(u_1, \ldots, u_n)| \leq |v_p|^k \).

It holds that \( f \in FP \subseteq FP^O \). We argue that \( f \) reduces \( K_q^s \) to \( K_q^s \cup B \). If \( (u_1, \ldots, u_n) \in K_q^s \), then \( f((u_1, \ldots, u_n)) \in K_q^s \).
Assume now \( \langle u_1, \ldots, u_n \rangle \notin K^O \). 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, \( f(\langle u_1, \ldots, u_n \rangle) \notin K^O \). Moreover, by Claim 18, \( f(\langle u_1, \ldots, u_n \rangle) \notin L(M^O_s) = B \).

\[ \sqcap \]

\[ \Delta \]

**Claim 20.** If \( A \) is \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \) and disjoint to \( B \in \text{NP}^O \), then \( A \cup B \) is \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \).

**Proof.** Otherwise, there are counterexamples \( A \) and \( B \). Choose \( f \in \text{FP}^O \) such that \( K^O \leq_{\text{PP}}^O A \) via \( f \) and let \( B' = f^{-1}(B) \). Observe \( B' \in \text{NP}^O \), \( K^O \cap B' = \emptyset \), and \( K^O \cup B' \leq_{\text{PP}}^O A \cup B \) via \( f \). Hence \( K^O \cup B' \) is not \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \), which contradicts Claim 19.

\[ \sqcap \]

**Claim 21.** \( K^O \) has \( \text{PO} \)-optimal proof systems.

The straightforward proof of this claim is left due to space restrictions. As \( K^O \) is \( \leq_{\text{PP}}^O \)-complete for \( \text{coNP}^O \), the first statement of the theorem holds. This finishes the proof of Theorem 12.

Köbler, Messner, and Torán [24] prove the following implications (5) and (6).

\[
\begin{align*}
\text{NEE} \cap \text{TALLY} & \subseteq \text{coNEE} \quad \Rightarrow \quad \text{H}_{\text{opps}} \quad (5) \\
\text{NEE} \cap \text{TALLY} & \subseteq \text{EE} \quad \Rightarrow \quad \exists \text{ P-optimal pps} \quad (6)
\end{align*}
\]

Relative to the oracle \( O \) constructed above, the converses of (5) and (6) fail, i.e., the premises are stronger than the conclusions. This supports the hope that one can weaken the premises in (5) and (6).

### 4.3 Further Oracles

We briefly discuss two further oracles.

**Theorem 22.** There exists an oracle \( O \) with the following properties.

1. \( \text{DisjNP}^O \) does not have \( \leq_{\text{PP}}^O \)-complete pairs (and hence \( \neg \text{H}_{\text{opps}} \) relative to \( O \)).
2. There are disjoint sets \( A \) and \( B \) that are \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \) such that \( A \cup B \) is not \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \).

The construction of this oracle is simpler than the other constructions. In order to achieve statement 1, we proceed similarly as for the oracle in Theorem 11. \( \neg \text{H}_{\text{union}} \) can be achieved by a straightforward diagonalization.

The following theorem shows that the implication \( \text{H}_{\text{union}} \Rightarrow \text{H}_{\text{cpair}} \) cannot be proven in a relativizable way. Ogiwara and Hemachandra [28] construct an oracle that proves that the converse implication \( \text{H}_{\text{cpair}} \Rightarrow \text{H}_{\text{union}} \) cannot be proven relativizably as well.

**Theorem 23.** There exists an oracle \( O \) with the following properties.

1. \( \text{DisjNP}^O \) does not have \( \leq_{\text{PP}}^O \)-complete pairs (and hence \( \neg \text{H}_{\text{opps}} \) relative to \( O \)).
2. If \( A \) is \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \) and disjoint to \( B \in \text{NP}^O \), then \( A \cup B \) is \( \leq_{\text{PP}}^O \)-complete for \( \text{NP}^O \).

The construction of this oracle has similarities to the constructions in the Theorems 11 and 12. However, there are less dependencies and thus, the construction is less complicated. Roughly speaking, we achieve \( \neg \text{H}_{\text{cpair}} \) in the same way as in Theorem 11 and \( \text{H}_{\text{union}} \) can be obtained similarly as in Theorem 12.
Table 1: Summary of oracles and their properties. Each column corresponds to the oracle mentioned in the topmost cell. We say that there exist P-optimal (resp., optimal) pps relative to an oracle, if relative to this oracle, some \( \leq_p \) complete \( A \in \text{coNP} \) has a P-optimal (resp., optimal) proof system (cf. Remark 2). A disjoint NP-pair \((A, B)\) is \( \leq_p \) 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 \( T \leq_p S \). A disjoint NP-pair \((A, B)\) is \( \leq_p \) hard for NP, if for every \( C \in \text{NP} \) and every separator \( S \) of \((A, B)\) it holds that \( C \leq_p S \). The double exponential time classes are defined as \( \text{EE} = \text{DTIME}(2^{2^{O(n)}}) \) and \( \text{NEE} = \text{NTIME}(2^{2^{O(n)}}) \).

<table>
<thead>
<tr>
<th>Property</th>
<th>[16, \text{T3.8}]</th>
<th>[16, \text{T6.1}]</th>
<th>[16, \text{T6.7}]</th>
<th>[28, \text{L4.7}]</th>
<th>Thm 11</th>
<th>Thm 12</th>
<th>Thm 22</th>
<th>Thm 23</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \exists ) P-optimal pps</td>
<td>false</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( \exists ) optimal pps / ( H_{\text{opps}} )</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( \text{NPC}<em>n ) closed under disj. union / ( H</em>{\text{union}} )</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( \exists ) ( \leq_p )-complete disjoint NP-pairs / ( H_{\text{pair}} )</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \exists ) ( \leq_p )-complete disjoint NP-pairs</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \exists ) disjoint NP-pairs that are ( \leq_p )-hard for NP</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \exists ) P-inseparable disjoint NP-pairs</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( P \neq \text{UP} )</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \text{NP} \neq \text{coNP} )</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( \text{NP} \cap \text{PAR} ) has ( \leq_m )-complete sets</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( E \neq \text{NE} )</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \text{NE} \neq \text{coNE} )</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} )</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} )</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

5 Conclusion and Open Questions

The main goal of this paper is to investigate the hypotheses \( H_{\text{union}}, H_{\text{opps}}, \) and \( H_{\text{pair}} \). We have shown that – except for the known implication \( H_{\text{opps}} \Rightarrow H_{\text{pair}} \) – each two of these hypotheses are independent under relativizable 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 \( H_{\text{opps}} \) implies \( H_{\text{pair}} \), relative to all oracles, there remain 6 possible situations. Table 1 illustrates that oracles for 4 of the 6 possible situations are known. This leads to the open question: do 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 \( O_1 \), \( \neg H_{\text{opps}} \land H_{\text{union}} \land H_{\text{pair}} \), i.e., there are no optimal pps, unions of disjoint, \( \leq_p \)-complete NP-sets remain complete, and there are \( \leq_{\text{m}} \)-complete disjoint NP-pairs.

- Does there exist an oracle \( O_2 \) with the following properties?
  - Relative to \( O_2 \), \( H_{\text{opps}} \land \neg H_{\text{union}} \land H_{\text{pair}} \), i.e., there is no optimal pps, unions of disjoint \( \leq_p \)-complete NP-sets are not always \( \leq_{\text{m}} \)-complete, and \( \text{DisjNP} \) has \( \leq_{\text{m}} \)-complete elements.

Furthermore we receive new insights on problems related to the main topic. On the one hand, we answer an open question by Pudlák [32] who asks for an oracle relative to which neither \( \neg H_{\text{pair}} \) nor \( \neg H_{\text{opps}} \) implies that UP does not have \( \leq_{\text{m}} \)-complete elements (cf. Theorem 11). On the other hand, we show that the converses of Köbler, Messner, and Torán’s [24] implications (\( \text{NEE} \cap \text{TALLY} \subseteq \text{coNEE} \Rightarrow H_{\text{opps}} \) and \( \text{NEE} \cap \text{TALLY} \subseteq \text{EE} \Rightarrow \) there exist P-optimal pps) fail relative to an oracle.
References


