P-Optimal Proof Systems for Each NP-Set but no Complete Disjoint NP-Pairs Relative to an Oracle

Titus Dose
Julius-Maximilians-Universität Würzburg, Germany

Abstract

Pudlák [17] lists several major conjectures from the field of proof complexity and asks for oracles that separate corresponding relativized conjectures. Among these conjectures are:

- DisjNP: The class of all disjoint NP-pairs has no many-one complete elements.
- SAT: NP contains no many-one complete sets that have P-optimal proof systems.
- UP: UP has no many-one complete problems.
- NP ∩ coNP: NP ∩ coNP has no many-one complete problems.

As one answer to this question, we construct an oracle relative to which DisjNP, ¬SAT, UP, and NP∩coNP hold, i.e., there is no relativizable proof for the implication DisjNP∧UP∧NP∩coNP ⇒ SAT. In particular, regarding the conjectures by Pudlák this extends a result by Khaniki [9]. Since Khaniki [9] constructs an oracle showing that the implication SAT ⇒ DisjNP has no relativizable proof, we obtain that the conjectures DisjNP and SAT are independent in relativized worlds, i.e., none of the implications DisjNP ⇒ SAT and SAT ⇒ DisjNP can be proven relativizably.

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, proof systems, disjoint NP-pair, oracle, UP

Digital Object Identifier 10.4230/LIPIcs.MFCS.2019.47

Related Version A full version [4] of the paper is available at `https://arxiv.org/abs/1904.06175`.

1 Introduction

The main motivation for the present paper is an article by Pudlák [17] that is "motivated by the problem of finding finite versions of classical incompleteness theorems", investigates major conjectures in the field of proof complexity, discusses their relations, and draws new connections between the conjectures. Among others, Pudlák conjectures the following assertions (note that within the present paper all reductions are polynomial-time-bounded):

- CON (resp., SAT): coNP (resp., NP) contains no many-one complete sets that have P-optimal proof systems
- $\mathsf{CON}^{\mathsf{N}}$: coNP contains no many-one complete sets that have optimal proof systems, (note that $\mathsf{CON}^{\mathsf{N}}$ is the non-uniform version of CON)
- DisjNP (resp., DisjCoNP): The class of all disjoint NP-pairs (resp., coNP-pairs) has no many-one complete elements,
- TFNP: The class of all total polynomial search problems has no complete elements,
- NP ∩ coNP (resp., UP): NP ∩ coNP (resp., UP, the class of problems accepted by NP machines with at most one accepting path for each input) has no many-one complete elements.

The following figure contains the conjectures by Pudlák and illustrates the state of the art regarding (i) known implications and (ii) separations in terms of oracles that prove the non-existence of relativizable proofs for implications. O denotes the oracle constructed in the present paper.

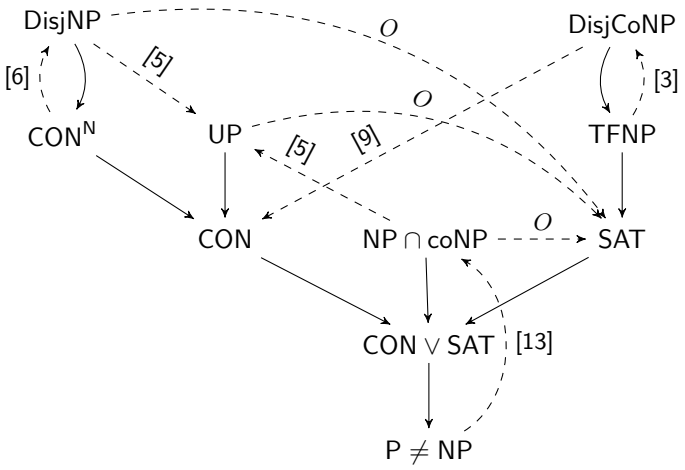

Figure 1 Solid arrows mean implications. All implications in the graphic can be proven with relativizable proofs. A dashed arrow from A to B means that there is an oracle X against the implication $\mathsf{A} \Rightarrow \mathsf{B}$, i.e., relative to X, it holds $\mathsf{A} \wedge \neg\mathsf{B}$. Pudlák [17] also defines the conjecture RFN_1 and lists it between $\mathsf{CON} \vee \mathsf{SAT}$ and $\mathsf{P} \neq \mathsf{NP}$, i.e., $\mathsf{CON} \vee \mathsf{SAT} \Rightarrow \mathsf{RFN}_1 \Rightarrow \mathsf{P} \neq \mathsf{NP}$. Khaniki [9] even shows $\mathsf{CON} \vee \mathsf{SAT} \Leftrightarrow \mathsf{RFN}_1$, which is why we omit RFN_1 in the figure.

The main conjectures of [17] are CON and TFNP. Let us give some background on these conjectures (for details we refer to [16]) and on the notion of disjoint pairs. The first main conjecture CON refers to the notion of proof systems introduced by Cook and Reckhow [2], who define a proof system for a set A to be a polynomial-time computable function whose range is A. The remainder of this paragraph originates from [5]. CON has an interesting connection to some finite version of an incompleteness statement. Denote by $\mathrm{Con}_T(n)$ the finite consistency of a theory T, i.e., $\mathrm{Con}_T(n)$ is the statement that T has no proofs of contradiction of length $\leq n$. Krajícek and Pudlák [12] raise the conjectures CON and CON^N and show that the latter is equivalent to the statement that there is no 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, $\neg\mathsf{CON}^\mathsf{N}$ expresses that a weak version of Hilbert's program (to prove the consistency of all mathematical theories) is possible [15]. Correspondingly, $\neg$CON is equivalent to the existence of a theory S such that, for any fixed theory T, proofs of $\mathrm{Con}_T(n)$ in S can be constructed in polynomial time in n [12].

The conjecture TFNP was raised by Megiddo and Papadimitriou, is implied by the non-existence of disjoint coNP-pairs [1, 17], and implies that no NP-complete set has P-optimal proof systems [1, 17]. It states the non-existence of total polynomial search problems that are complete with respect to polynomial reductions.

The notion of disjoint NP-pairs, i.e., pairs (A, B) with $A \cap B = \emptyset$ and $A, B \in \mathrm{NP}$, was introduced by Grollman and Selman [7] in order to characterize promise problems. Razborov [18] connects it with the concept of propositional proof systems (pps), i.e., proof systems for the set of propositional tautologies TAUT, defining for each pps f a disjoint NP-pair, the so-called canonical pair of f, and showing that the canonical pair of an optimal pps f is complete. Hence, $\mathsf{DisjNP} \Rightarrow \mathsf{CON}^\mathsf{N}$.

In contrast to the many implications only very few oracles were known separating two of the relativized conjectures [17], which is why Pudlák asks for further oracles showing relativized conjectures to be different.

Khaniki [9] partially answers this question: besides proving two of the conjectures to be equivalent, he presents two oracles $\mathcal{V}$ and $\mathcal{W}$ showing that SAT and CON (just as TFNP

and CON) are independent in relativized worlds, which means that none of the two possible implications between the two conjectures has a relativizable proof. To be more precise, relative to $\mathcal{V}$, there exist P-optimal propositional proof systems but no many-one complete disjoint coNP-pairs, where, as mentioned above, the latter implies TFNP and SAT. Relative to $\mathcal{W}$, there exist no P-optimal propositional proof systems and each total polynomial search problem has a polynomial-time solution, where the latter implies ¬SAT [10].

Dose and Glaßer [5] construct an oracle X that also separates some of the above relativized conjectures. Relative to X there exist no many-one complete disjoint NP-pairs, UP has many-one complete problems, and NP ∩ coNP has no many-one complete problems. In particular, relative to X, there do not exist P-optimal propositional proof systems. Thus, among others, X shows that the conjectures CON and UP as well as NP ∩ coNP and UP cannot be proven equivalent with relativizable proofs.

In another paper [3], the author adds one more oracle to this list proving that there is no relativizable proof for the implication TFNP ⇒ DisjCoNP.

Our Contribution

In the present paper we construct an oracle O relative to which

1. The class of all disjoint NP-pairs has no many-one complete elements.
2. NP contains no many-one complete sets that have P-optimal proof systems.
3. UP has no many-one complete problems.
4. NP ∩ coNP has no many-one complete problems.

Indeed, relative to O there even exist no disjoint NP-pairs hard for NP ∩ coNP, which implies both 1 and 4. Among others, the oracle shows that there are no relativizable proofs for the implications NP ∩ coNP ⇒ SAT and UP ⇒ SAT. Let us now focus on the properties 1 and 2 of the oracle. Regarding these, our oracle has similar properties as the aforementioned oracle $\mathcal{W}$ by Khaniki [9]: both oracles show that there is no relativizable proof for the implication CON ⇒ SAT. Relative to Khaniki's oracle $\mathcal{W}$ it even holds that each total polynomial search problem has a polynomial time solution, which implies not only ¬SAT but also that all optimal proof systems for SAT are P-optimal [10]. Regarding Pudlák's conjectures, however, our oracle O extends Khaniki's result as relative to O we have the even stronger result that there is no relativizable proof for the implication DisjNP ⇒ SAT. Since due to the oracle $\mathcal{V}$ by Khaniki [9] none of the implications DisjCoNP ⇒ DisjNP, TFNP ⇒ DisjNP, and SAT ⇒ DisjNP can be proven relativizably, our oracle shows that DisjNP is independent of each of the conjectures DisjCoNP, TFNP, and SAT in relativized worlds, i.e., none of the six possible implications has a relativizable proof.

2 Preliminaries

Major parts of this section are copied from our paper [5] coauthored by Christian Glaßer. 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 $\Sigma^{>n} = \{w \in \Sigma^* \mid |w| > n\}$. 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., $w = w(0)w(1)\cdots w(|w|-1)$. If v is a prefix of w, i.e., $|v| \leq |w|$ and $v(i) = w(i)$ for all $0 \leq i < |v|$, then we write $v \sqsubseteq w$. For any finite set $Y \subseteq \Sigma^*$, let $\ell(Y) \stackrel{df}{=} \sum_{w \in Y} |w|$.

$\mathbb{Z}$ denotes the set of integers, $\mathbb{N}$ denotes the set of natural numbers, and $\mathbb{N}^+ = \mathbb{N} - \{0\}$. The set of primes is denoted by $\mathbb{P} = \{2,3,5,\ldots\}$ and $\mathbb{P}^{\geq 3}$ denotes the set $\mathbb{P} - \{2\}$.

We identify Σ^* with $\mathbb{N}$ via the polynomial-time computable, polynomial-time invertible bijection $w \mapsto \sum_{i<|w|}(1+w(i))2^{|w|-1-i}$, 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, $A - B$ denotes the set 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. Furthermore, the symmetric difference is denoted by $\triangle$, i.e., $A \triangle B = (A - B) \cup (B - A)$ for arbitrary sets A and B.

The domain and range of a function t are denoted by $\mathrm{dom}(t)$ and $\mathrm{ran}(t)$, respectively.

FP, P, and NP denote standard complexity classes [14]. Define $\mathrm{co}\mathcal{C} = \{A \subseteq \Sigma^* \mid \overline{A} \in \mathcal{C}\}$ for a class $\mathcal{C}$. UP is the class of all problems accepted by nondeterministic polynomial-time Turing machines with at most one accepting path for each input. If $A, B \in \mathrm{NP}$ (resp., $A, B \in \mathrm{coNP}$) and $A \cap B = \emptyset$, then we call (A, B) a disjoint NP-pair (resp., a disjoint coNP-pair). The set of all disjoint NP-pairs (resp., coNP-pairs) is denoted by DisjNP (resp., DisjCoNP). 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.

Let M be a Turing machine. $M^D(x)$ denotes the computation of M on input x with D as an oracle. For an arbitrary oracle D we let $L(M^D) = \{x \mid M^D(x) \text{ accepts}\}$. For a deterministic polynomial-time Turing transducer (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.

▶ **Definition 1.** *A sequence $(M_i)_{i\in\mathbb{N}^+}$ 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 $M^D(\langle i, x, 0^{|x|^i+i}\rangle)$ nondeterministically simulates the computation $M_i^D(x)$.*

Analogously we define standard enumerations of deterministic, polynomial-time oracle Turing transducers.

Throughout this paper, we fix some standard enumerations. Let $M_1, M_2, \ldots$ be a standard enumeration of nondeterministic polynomial-time oracle Turing machines. Then for every oracle D, the sequence $(M_i)_{i\in\mathbb{N}^+}$ represents an enumeration of the languages in NP^D, i.e., $\mathrm{NP}^D = \{L(M_i^D) \mid i \in \mathbb{N}\}$, where as usual a computation $M_i^D(x)$ accepts if and only if it has at least one accepting path. Let $F_1, F_2, \ldots$ be a standard enumeration of polynomial time oracle Turing transducers. By the properties of standard enumerations, for each oracle D the following problem is NP^D-complete (in particular it is in NP^D):

$$K^D = \{\langle 0^i, 0^t, x\rangle \mid M_i^D(x) \text{ accepts within } t \text{ steps}\}.$$

Let D be an oracle and $A, B, A', B' \subseteq \Sigma^*$ such that $A \cap B = A' \cap B' = \emptyset$. In this paper we always use the following reducibility for disjoint pairs [18]. (A', B') is polynomially many-one reducible to (A, B), denoted by $(A', B') \leq_{\mathrm{m}}^{\mathrm{pp},D} (A, B)$, if there exists $f \in \mathrm{FP}^D$ with $f(A') \subseteq A$ and $f(B') \subseteq B$. If $A' = \overline{B'}$, then we also write $A' \leq_{\mathrm{m}}^{\mathrm{p},D} (A, B)$ instead of $(A', B') \leq_{\mathrm{m}}^{\mathrm{pp},D} (A, B)$.

We say that (A, B) is $\leq_{\mathrm{m}}^{\mathrm{pp},D}$*-hard* ($\leq_{\mathrm{m}}^{\mathrm{pp},D}$*-complete*) *for* DisjNP^D if $(A', B') \leq_{\mathrm{m}}^{\mathrm{pp},D} (A, B)$ for all $(A', B') \in \mathrm{DisjNP}^D$ (and $(A, B) \in \mathrm{DisjNP}^D$). Moreover, a pair (A, B) is $\leq_{\mathrm{m}}^{\mathrm{p},D}$*-hard for* $\mathrm{NP}^D \cap \mathrm{coNP}^D$ if $A' \leq_{\mathrm{m}}^{\mathrm{p},D} (A, B)$ for every $A \in \mathrm{NP}^D \cap \mathrm{coNP}^D$.

▶ **Definition 2** ([2]). *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.*

The following proposition states the relativized version of a result by Köbler, Messner, and Torán [11], which they show with a relativizable proof.

▶ **Proposition 3** ([11]). *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 4.** *For every oracle O, if there exists a $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete $A \in \mathrm{NP}^O$ that has a P^O-optimal (resp., optimal) proof system, then all sets in NP^O have P^O-optimal (resp., optimal) proof systems.*

Let us introduce some notations that are designed for the construction of oracles [5]. 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 $t(i,j) = t(i',j')$ for $(i,j), (i',j') \in \mathrm{supp}(t)$ implies $(i,j) = (i',j')$. If a partial function t is not defined at point x, then $t \cup \{x \mapsto y\}$ denotes the extension of t that at x has value y.

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 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 $x < |w|$. 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 we use the following phrases: a computation $M^w(x)$ *definitely accepts*, if it contains a path that accepts and the queries on this path are $< |w|$. A computation $M^w(x)$ *definitely rejects*, if all paths reject and all queries are $< |w|$. For a nondeterministic Turing machine M we say that the computation $M^w(x)$ *is defined*, if it definitely accepts or definitely rejects. For a polynomial time oracle transducer F, the computation $F^w(x)$ *is defined*, if all queries are $< |w|$.

3 Oracle Construction

The following lemma is a slightly adapted variant of a result from [5].

▶ **Lemma 5.** *For all $y \leq |w|$ and all $v \sqsupseteq w$ it holds $y \in K^v \Leftrightarrow y \in K^w$.*

▶ **Theorem 6.** *There exists an oracle O such that the following statements hold:*

- DisjNP^O *contains no pairs that are $\leq_{\mathrm{m}}^{\mathrm{p},O}$-hard for $\mathrm{NP}^O \cap \mathrm{coNP}^O$.*
- *Each $L \in \mathrm{NP}^O$ has P^O-optimal proof systems.*
- UP^O *contains no $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete problems.*

Observe that the first of the three statements implies that both DisjNP^O contains no $\leq_{\mathrm{m}}^{\mathrm{pp},O}$-complete pairs and $\mathrm{NP}^O \cap \mathrm{coNP}^O$ contains no $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete problems.

Proof. Let D be a (possibly partial) oracle and p (resp., q) be in $\mathbb{P}_3$ (resp., $\mathbb{P}_1$). We define

$$\begin{aligned} A_p^D &:= \{0^{p^k} \mid k \in \mathbb{N}^+, \exists_{x \in \Sigma^{p^k}} x \in D \text{ and } x \text{ odd}\} \cup \overline{\{0^{p^k} \mid k \in \mathbb{N}^+\}} \\ B_p^D &:= \{0^{p^k} \mid k \in \mathbb{N}^+, \exists_{x \in \Sigma^{p^k}} x \in D \text{ and } x \text{ even}\} \\ C_q^D &:= \{0^{q^k} \mid k \in \mathbb{N}^+, \exists_{x \in \Sigma^{q^k}} x \in D\} \end{aligned}$$

Note that $A_p^D, B_p^D \in \mathrm{NP}^D$ and $A_p^D = \overline{B_p^D}$ if $|\Sigma^{p^k} \cap D| = 1$ for each $k \in \mathbb{N}^+$. In that case $A_p^D \in \mathrm{NP}^D \cap \mathrm{coNP}^D$. Moreover, $C_q^D \in \mathrm{UP}^D$ if and only if $|\Sigma^{q^k} \cap D| \leq 1$ for each $k \in \mathbb{N}^+$.

For the sake of simplicity, let us call a pair (M_i, M_j) an $\mathrm{NP}^D \cap \mathrm{coNP}^D$-machine if $L(M_i^D) = \overline{L(M_j^D)}$. For $i \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$ we write $c(i, x, y) := \langle 0^i, 0^{|x|^i+i}, x, y\rangle$. Thus, $|c(i, x, y)|$ is even. Note that throughout this proof we sometimes omit the oracles in the superscript, e.g., we write NP or A_p instead of NP^D or A_p^D. However, we do not do that in the "actual" proof but only when explaining ideas in a loose way in order to give the reader the intuition behind the occasionally very technical arguments.

Preview of construction. We sketch some of the very basic ideas our construction uses.

1. For all positive $i \neq j$ the construction tries to achieve that (M_i, M_j) is not an NP ∩ coNP-machine. If this is not possible, then $(L(M_i), L(M_j))$ inherently is an NP ∩ coNP-machine. Once we know this, we choose some odd prime p and diagonalize against all FP-functions such that $A_p = \overline{B_p}$ and A_p is not $\leq_{\mathrm{m}}^{\mathrm{p}}$-reducible to $(L(M_i), L(M_j))$.
2. For all $i \geq 1$ the construction intends to make sure that F_i is not a proof system for K. If this is not possible, then F_i inherently is a proof system for K and then we start to encode the values of F_i into the oracle. However, it is important to also allow encodings for functions that are not known to be proof systems for K yet. Regarding the P-optimal proof systems, our construction is based on ideas by Dose and Glaßer [5].
3. For all $i \geq 1$ the construction tries to ensure that M_i is not a UP-machine. If this is not possible, we know that M_i inherently is a UP machine, which enables us to diagonalize against all FP-functions so that C_q for some q that we choose is not reducible to $L(M_i)$.

▷ Claim 7. Let $w \in \Sigma^*$ be an oracle, $i \in \mathbb{N}^+$, and $x, y \in \mathbb{N}$ such that $c(i, x, y) \leq |w|$. Then the following holds.

1. $F_i^w(x)$ is defined and $F_i^w(x) < |w|$.
2. $F_i^w(x) \in K^w \Leftrightarrow F_i^w(x) \in K^v$ for all $v \sqsupseteq w$.

During the construction we maintain a growing collection of requirements that is represented by a partial function belonging to the set

$$\begin{aligned} \mathcal{T} = \Big\{ t : \mathbb{N}^+ \cup (\mathbb{N}^+)^2 \to \mathbb{Z} \mid \mathrm{dom}(t) \text{ is finite, } t \text{ is injective on its support,} \\ - \ t(\mathbb{N}^+) \subseteq \{0\} \cup \mathbb{N}^+ \\ - \ t(\{(i,i) \mid i \in \mathbb{N}^+\}) \subseteq \{0\} \cup \{-q \mid q \in \mathbb{P}_1\} \\ - \ t(\{(i,j) \in (\mathbb{N}^+)^2 \mid i \neq j\}) \subseteq \{0\} \cup \{-p \mid p \in \mathbb{P}_3\} \Big\}. \end{aligned}$$

A partial oracle w is called t-valid for $t \in \mathcal{T}$ if it satisfies the following properties.

V1 For all $i \in \mathbb{N}^+$ and all $x, y \in \mathbb{N}$, if $c(i, x, y) \in w$, then $F_i^w(x) = y \in K^w$.
(meaning: if the oracle contains the codeword $c(i, x, y)$, then $F_i^w(x)$ outputs $y \in K^w$; hence, $c(i, x, y) \in w$ is a proof for $y \in K^w$)

V2 For all distinct $i, j \in \mathbb{N}^+$, if $t(i, j) = 0$, then there exists x such that $M_i^w(x)$ and $M_j^w(x)$ definitely accept.
(meaning: for every extension of the oracle, $(L(M_i), L(M_j))$ is not a disjoint NP-pair.)

V3 For all distinct $i, j \in \mathbb{N}^+$ with $t(i,j) = -p$ for some $p \in \mathbb{P}_3$ and each $k \in \mathbb{N}^+$, it holds (i) $|\Sigma^{p^k} \cap w| \leq 1$ and (ii) if w is defined for all words of length p^k, then $|\Sigma^{p^k} \cap w| = 1$.
(meaning: if $t(i,j) = -p$, then ensure that $A_p = \overline{B_p}$ (i.e., $A_p \in \mathrm{NP} \cap \mathrm{coNP}$) relative to the final oracle.)

V4 For all $i \in \mathbb{N}^+$ with $t(i) = 0$, there exists x such that $F_i^w(x)$ is defined and $F_i^w(x) \notin K^v$ for all $v \sqsupseteq w$.
(meaning: for every extension of the oracle, F_i is not a proof system for K)

V5 For all $i \in \mathbb{N}^+$ and $x \in \mathbb{N}$ with $0 < t(i) \leq c(i, x, F_i^w(x)) < |w|$, it holds $c(i, x, F_i^w(x)) \in w$.
(meaning: if $t(i) > 0$, then from $t(i)$ on, we encode the values of F_i into the oracle.
Note that V5 is not in contradiction with e.g. V3 or V7 as $|c(\cdot,\cdot,\cdot)|$ is even.)

V6 For all $i \in \mathbb{N}^+$ with $t(i,i) = 0$, there exists x such that $M_i^w(x)$ is defined and has two accepting paths.
(meaning: for every extension of the oracle, M_i is not a UP-machine.)

V7 For all $i \in \mathbb{N}^+$ with $t(i,i) = -q \in \mathbb{P}_1$ and each $k \in \mathbb{N}^+$, it holds $|\Sigma^{q^k} \cap w| \leq 1$.
(meaning: if $t(i,i) = -q$, ensure that C_q is in UP.)

▷ Claim 8. Let $t, t' \in \mathcal{T}$ such that t' is an extension of t. For all oracles $w \in \Sigma^*$, if w is t'-valid, then w is t-valid.

▷ Claim 9. Let $t \in \mathcal{T}$ and $u, v, w \in \Sigma^*$ be oracles such that $u \sqsubseteq v \sqsubseteq w$ and both u and w are t-valid. Then v is t-valid.

Oracle construction. Let T be an enumeration of $\bigcup_{i=1}^{3} (\mathbb{N}^+)^i$ having the property that (i,j) appears earlier than (i,j,r) for all $i, j, r \in \mathbb{N}^+$. Each element of T stands for a task. We treat the tasks in the order specified by T and after treating a task we remove it and possibly other tasks from T. We start with the nowhere defined function t_0 and the t_0-valid oracle $w_0 = \varepsilon$. Then we define functions $t_1, t_2, \ldots$ in $\mathcal{T}$ such that t_{i+1} is an extension of t_i and partial oracles $w_0 \sqsubsetneq w_1 \sqsubsetneq w_2 \sqsubsetneq \ldots$ such that each w_i is t_i-valid. Finally, we choose $O = \bigcup_{i=0}^{\infty} w_i$ (note that O is totally defined since in each step we strictly extend the oracle). 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 $w_s \sqsupsetneq w_{s-1}$ (it will be argued later that all these steps are indeed possible). Let us recall that each task is immediately deleted from T after it is treated.

- Task i: Let $t' = t_{s-1} \cup \{i \mapsto 0\}$. If there exists a t'-valid $v \sqsupsetneq w_{s-1}$, then let $t_s = t'$ and $w_s = v$. Otherwise, let $t_s = t_{s-1} \cup \{i \mapsto |w_{s-1}|\}$ and choose $w_s = w_{s-1}b$ for $b \in \{0,1\}$ such that w_s is t_s-valid.
  (meaning: try to ensure that F_i is not a proof system for K. If this is impossible, require that the values of F_i are encoded into the oracle.)
- 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 $t_s = t'$ as well as $w_s = v$ and delete all tasks $(i,j,\cdot)$ from T. Otherwise, let $z = |w_{s-1}|$, choose $p \in \mathbb{P}_3$ greater than $|z|$ and all p' with $p' \in \mathbb{P}^{\geq 3}$ and $-p' \in \mathrm{ran}(t_{s-1})$, let $t_s = t_{s-1} \cup \{(i,j) \mapsto -p\}$, and choose $w_s = w_{s-1}b$ for $b \in \{0,1\}$ such that w_s is t_s-valid.
  (meaning: try to ensure that $(L(M_i), L(M_j))$ is not a disjoint NP-pair. If this is impossible, choose a sufficiently large prime p. It will be made sure later that A_p does not reduce to $(L(M_i), L(M_j))$.)
- Task (i,j,r) with $i \neq j$: It holds $t_{s-1}(i,j) = -p$ for a prime $p \in \mathbb{P}_3$, since otherwise, this task would have been deleted in the treatment of task (i,j). Define $t_s = t_{s-1}$ and choose a t_s-valid $w_s \sqsupsetneq w_{s-1}$ such that for some $n \in \mathbb{N}^+$ one of the following two statements holds:

- $0^n \in A_p^v$ for all $v \sqsupseteq w_s$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ definitely rejects.
- $0^n \in B_p^v$ for all $v \sqsupseteq w_s$ and $M_j^{w_s}(F_r^{w_s}(0^n))$ definitely rejects.

(meaning: make sure that it does not hold $A_p \leq_{\mathrm{m}}^{\mathrm{p}} (L(M_i), L(M_j))$ via F_r)

- 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 $t_s = t'$ as well as $w_s = v$ and delete all tasks $(i,i,\cdot)$ from T. Otherwise, let $z = |w_{s-1}|$, choose $q \in \mathbb{P}_1$ greater than $|z|$ and all p' with $p' \in \mathbb{P}^{\geq 3}$ and $-p' \in \mathrm{ran}(t_{s-1})$, let $t_s = t_{s-1} \cup \{(i,i) \mapsto -q\}$, and choose $w_s = w_{s-1}b$ for $b \in \{0,1\}$ such that w_s is t_s-valid.
  (meaning: try to ensure that M_i is not a UP-machine. If this is impossible, choose a sufficiently large prime q. It will be made sure later that C_q does not reduce to $L(M_i)$.)
- Task (i,i,r): It holds $t_{s-1}(i,j) = -q$ for a prime $q \in \mathbb{P}_1$, since otherwise, this task would have been deleted in the treatment of task (i,i). Define $t_s = t_{s-1}$ and choose a t_s-valid $w_s \sqsupsetneq w_{s-1}$ such that for some $n \in \mathbb{N}^+$ one of the following conditions holds:
  - $0^n \in C_q^v$ for all $v \sqsupseteq w_s$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ definitely rejects.
  - $0^n \notin C_q^v$ for all $v \sqsupseteq w_s$ and $M_i^{w_s}(F_r^{w_s}(0^n))$ definitely accepts.

  (meaning: make sure that it does not hold $C_q \leq_{\mathrm{m}}^{\mathrm{p}} L(M_i)$ via F_r)

We now show that the construction is possible. For that purpose, we first describe how a valid oracle can be extended by one bit such that it remains valid.

▷ Claim 10. Let $s \in \mathbb{N}$ and $w \in \Sigma^*$ be a t_s-valid oracle with $w \sqsupseteq w_s$. It holds for $z = |w|$:

1. If $z = c(i,x,y)$ for $i \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$, $0 < t_s(i) \leq z$, and $F_i^w(x) = y$, then $y \in K^v$ for all $v \sqsupseteq w$.
2. There exists $b \in \{0,1\}$ such that wb is t_s-valid. In detail, the following statements hold.
   a. If $|z|$ is odd and for all $p \in \mathbb{P}$ and $k \in \mathbb{N}^+$ with $-p \in \mathrm{ran}(t_s)$ it holds $|z| \neq p^k$, then $w0$ and $w1$ are t_s-valid.
   b. If there exist $p \in \mathbb{P}_3$ and $k \in \mathbb{N}^+$ with $-p \in \mathrm{ran}(t_s)$ such that $|z| = p^k$, $z \neq 1^{p^k}$, and $w \cap \Sigma^{p^k} = \emptyset$, then $w0$ and $w1$ are t_s-valid.
   c. If there exist $p \in \mathbb{P}_3$ and $k \in \mathbb{N}^+$ with $-p \in \mathrm{ran}(t_s)$ such that $z = 1^{p^k}$ and $w \cap \Sigma^{p^k} = \emptyset$, then $w1$ is t_s-valid.
   d. If there exist $q \in \mathbb{P}_1$ and $k \in \mathbb{N}^+$ with $-q \in \mathrm{ran}(t_s)$ such that $|z| = q^k$ and $w \cap \Sigma^{q^k} = \emptyset$, then $w0$ and $w1$ are t_s-valid.
   e. If $z = c(i,x,y)$ for $i \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$, $0 < t_s(i) \leq z$, and $F_i^w(x) = y$, then $w1$ is t_s-valid and $F_i^{w1}(x) = y$.
   f. In all other cases (i.e., none of the assumptions in (a)–(e) holds) $w0$ is t_s-valid.

In order to show that the above construction is possible, assume that it is not possible and let $s > 0$ be the least number such that it fails in step s.

If step s treats a task $t \in \mathbb{N}^+ \cup (\mathbb{N}^+)^2$, then $t_{s-1}(t)$ is not defined, since the value of t is defined in the unique treatment of the task t. If $t_s(t)$ is chosen to be 0, then the construction clearly is possible. Otherwise, due to the choice of $t_s(t)$, the t_{s-1}-valid oracle w_{s-1} is even t_s-valid and Claim 10 ensures that there exists a t_s-valid $w_{s-1}b$ for some $b \in \{0,1\}$. Hence, the construction does not fail in step s, a contradiction.

For the remainder of the proof that the construction above is possible we assume that step s treats a task $(i,j,r) \in (\mathbb{N}^+)^3$. We treat the cases $i = j$ and $i \neq j$ simultaneously whenever it is possible. Recall that in the case $i = j$ we work for the diagonalization ensuring that $L(M_i)$ is not a complete UP-set and in the case $i \neq j$ we work for the diagonalization ensuring that the pair $(L(M_i), L(M_j))$ is not hard for $\mathrm{NP} \cap \mathrm{coNP}$.

In any case, $t_s = t_{s-1}$ and $t_s(i,j) = -p$ for some $p \in \mathbb{P}^{\geq 3}$ (recall $p \in \mathbb{P}_1$ if $i = j$ and $p \in \mathbb{P}_3$ if $i \neq j$). Let $\gamma(x) = (x^r + r)^{i+j} + i + j$ and choose $n = p^k$ for some $k \in \mathbb{N}^+$ such that

$$2^{2n-2} > 2^{n+1} \cdot \gamma(n) \tag{1}$$

and w_{s-1} is not defined for any word of length n. Note that $\gamma(n)$ is not less than the running time of each of the computations $M_i^D(F_r^D(0^n))$ and $M_j^D(F_r^D(0^n))$ for any oracle D.

We define $u \sqsupseteq w_{s-1}$ to be the minimal t_s-valid oracle that is defined for all words of length $< n$. Such an oracle exists by Claim 10.2. Moreover, for $z \in \Sigma^n$, let $u_z \sqsupsetneq u$ be the minimal t_s-valid oracle that contains z and that is defined for all words of length $\leq \gamma(n)$. By Claim 10.2, such oracles exist and $u_z \cap \Sigma^n = \{z\}$ (in detail, the second part follows from (2b, 2c, and 2f) or (2d and 2f) depending on whether $p \in \mathbb{P}_3$ or $p \in \mathbb{P}_1$, for the first part we also need that each valid oracle can be extended by one bit without losing its validity).

▷ Claim 11. Let $z \in \Sigma^n$.

1. For each $\alpha \in u_z \cap \Sigma^{>n}$ one of the following statements holds.
   - $\alpha = 1^{p'^\kappa}$ for some $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t_s)$ and some $\kappa > 0$.
   - $\alpha = c(i', x, y)$ for some $i', x, y \in \mathbb{N}$ with $i' > 0$, $0 < t_s(i') \leq c(i', x, y)$, $F_{i'}^{u_z}(x) = y$, and $y \in K^{u_z}$.
2. For all $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t_s)$ and all $\kappa > 0$, if $n < p'^\kappa \leq \gamma(n)$, then $u_z \cap \Sigma^{p'^\kappa} = \{1^{p'^\kappa}\}$.

Proof. 1. Let $\alpha \in u_z \cap \Sigma^{>n}$. Moreover, let u' be the prefix of u_z that has length α, i.e., α is the least word that u' is not defined for. In particular, it holds $u' \cap \Sigma^{\leq n} = u_z \cap \Sigma^{\leq n}$ and thus, $z \in u'$. As $u \sqsubseteq u' \sqsubseteq u_z$ and both u and u_z are t_s-valid, Claim 9 yields that u' is also t_s-valid. Let us apply Claim 10.2 to the oracle u'. If one of the cases 2a, 2b, 2d, and 2f can be applied, then $u'0$ is t_s-valid and can be extended to a t_s-valid oracle u'' with $|u''| = |u_z|$ by Claim 10.2. As u'' and u_z agree on all words $< \alpha$ and $\alpha \in u'' - u_z$, we obtain $z \in u''$ and $u'' < u_z$. This is a contradiction to the choice of u_z (recall that u_z is the minimal t_s-valid oracle that is defined for all words of length $\leq \gamma(n)$ and contains z).

Hence, by Claim 10.2, either (i) $\alpha = 1^{p'^\kappa}$ for some $p' \in \mathbb{P}_3$ and $\kappa > 0$ with $-p' \in \mathrm{ran}(t_s)$ or (ii) $\alpha = c(i', x, y)$ for $i', x, y \in \mathbb{N}$, $i' > 0$, $0 < t_s(i') \leq \alpha$, and $F_{i'}^{u'}(x) = y$. In the latter case $F_{i'}^{u'}(x)$ is defined by Claim 7 and $y \in K^v$ for all $v \sqsupseteq u'$ by Claim 10.1, which implies $F_{i'}^{u_z}(x) = y \in K^{u_z}$.

2. As $-p' \in \mathrm{ran}(t_s)$ and u_z is t_s-valid, V3 yields that there exists $\beta \in \Sigma^{p'^\kappa} \cap u_z$. Let β be the minimal element of $\Sigma^{p'^\kappa} \cap u_z$. It suffices to show $\beta = 1^{p'^\kappa}$. For a contradiction, we assume $\beta < 1^{p'^\kappa}$. Let u' be the prefix of u_z that is defined for exactly the words of length $< p'^\kappa$. Then $u \sqsubseteq u' \sqsubseteq u_z$ and both u and u_z are t_s-valid. Then by Claim 9, the oracle u' is t_s-valid as well. By Claim 10.2 u' can be extended to a t_s-valid oracle u'' that satisfies $|u''| = |u_z|$ and $u'' \cap \Sigma^{p'^\kappa} = \{1^{p'^\kappa}\}$. The last property guarantees that $u'' < u_z$ because $\beta \in u_z - u''$ and the oracles u'' and u_z agree on all words smaller than β. As furthermore $z \in u''$, we obtain a contradiction to the choice of u_z. This finishes the proof of Claim 11. ◁

We study the case that for some odd (resp., even) $z \in \Sigma^n$ the computation $M_i^{u_z}(F_r^{u_z}(0^n))$ (resp., $M_j^{u_z}(F_r^{u_z}(0^n))$) rejects. Then it even definitely rejects since u_z is defined for all words of length $\gamma(n)$. If $i \neq j$, then $p \in \mathbb{P}_3$ and since $z \in u_z$, we have $0^n \in A_p^v$ for all $v \sqsupseteq u_z$ (resp., $0^n \in B_p^v$ for all $v \sqsupseteq u_z$ if z is even). Analogously, if $i = j$, then $p \in \mathbb{P}_1$ and as $z \in u_z$, we have $0^n \in C_p^v$ for all $v \sqsupseteq u_z$. Hence, in all these cases we can choose $w_s = u_z$ and obtain a contradiction to the assumption that step s of the construction fails.

Therefore, for the remainder of the proof that the construction is possible we assume the following: For each $z \in \Sigma^n$ odd (resp., even) the computation $M_i^{u_z}(F_r^{u_z}(0^n))$ (resp., $M_j^{u_z}(F_r^{u_z}(0^n))$) definitely accepts.

Let U_z for $z \in \Sigma^n$ odd (resp., $z \in \Sigma^n$ even) be the set of all those oracle queries of the least accepting path of $M_i^{u_z}(F_r^{u_z}(0^n))$ (resp., $M_j^{u_z}(F_r^{u_z}(0^n))$) that are of length $\geq n$. Observe

$\ell(U_z) \leq \gamma(n)$. Moreover, define $Q_0(U_z) := U_z$ and for $m \in \mathbb{N}$, define

$$Q_{m+1}(U_z) := \bigcup_{\substack{c(i',x,y)\in Q_m(U_z)\\ i',x,y\in\mathbb{N},i'>0}} \{q \in \Sigma^{\geq n} \mid q \text{ is queried by } F_{i'}^{u_z}(x)\}.$$

Let $Q(U_z) := \bigcup_{m\in\mathbb{N}} Q_m(U_z)$. Note that all words in $Q(U_z)$ have length $\geq n$.

▷ Claim 12. Let $z \in \Sigma^n$. Then $\ell(Q(U_z)) \leq 2\ell(U_z) \leq 2\gamma(n)$ and for all $q \in Q(U_z)$, $|q| \leq \gamma(n)$.

Proof. We show that for all $m \in \mathbb{N}$, $\ell(Q_{m+1}(U_z)) \leq 1/2 \cdot \ell(Q_m(U_z))$. Then $\sum_{m=0}^{s} 1/2^m \leq 2$ for all $s \in \mathbb{N}$ implies $\ell(Q(U_z)) \leq 2 \cdot \ell(U_z)$. Moreover, from $\ell(U_z) \leq \gamma(n)$ and $\ell(Q_{m+1}(U_z)) \leq 1/2 \cdot \ell(Q_m(U_z))$ the second part of the claim follows.

Let $m \in \mathbb{N}$ and consider an arbitrary element α of $Q_m(U)$. If α is not of the form $c(i', x, y)$ for $i' \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$, then α generates no elements in $Q_{m+1}(U)$. Assume $\alpha = c(i', x, y)$ for $i' \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$. The computation $F_{i'}^{u_z}(x)$ runs for at most $|x|^{i'} + i' < |\alpha|/2$ steps, where "$<$" holds by the definition of $c(\cdot,\cdot,\cdot)$ and the properties of the pairing function $\langle\cdot\rangle$. Hence, the set of queries Q of $F_{i'}^{u_z}(x)$ satisfies $\ell(Q) < |\alpha|/2$. Consequently,

$$\begin{aligned}\ell(Q_{m+1}(U)) &\leq \sum_{\substack{c(i',x,y)\in Q_m(U_z)\\ i',x,y\in\mathbb{N},i'>0}} \ell\big(\{q \in \Sigma^{\geq n} \mid q \text{ is queried by } F_{i'}^{u_z}(x)\}\big)\\ &\leq \sum_{\substack{c(i',x,y)\in Q_m(U_z)\\ i',x,y\in\mathbb{N},i'>0}} |c(i',x,y)|/2 \leq \ell(Q_m(U_z))/2,\end{aligned}$$

which finishes the proof of Claim 12. ◁

For $z, z' \in \Sigma^n$ we say that $Q(U_z)$ and $Q(U_{z'})$ *conflict* if there is a word $\alpha \in Q(U_z) \cap Q(U_{z'})$ in $u_z \triangle u_{z'}$. In that case, we say $Q(U_z)$ and $Q(U_{z'})$ conflict in α. Note that whenever $Q(U_z)$ and $Q(U_{z'})$ conflict in a word α, then $\alpha \in u_z \cup u_{z'}$. The next three claims show that for all $z \in \Sigma^n$ odd and $z' \in \Sigma^n$ even, the sets $Q(U_z)$ and $Q(U_{z'})$ conflict in a word of length n. Indeed, then they conflict in z or z' as these are the only words of length n in $u_z \cup u_{z'}$.

▷ Claim 13. Let $z, z' \in \Sigma^n$ such that z is odd and z' is even. If $Q(U_z)$ and $Q(U_{z'})$ conflict, then they conflict in a word of length n.

Proof. Let α be the least word in which $Q(U_z)$ and $Q(U_{z'})$ conflict. Then $\alpha \in u_z \triangle u_{z'}$. By symmetry, it suffices to consider the case $\alpha \in u_z - u_{z'}$. For a contradiction, assume that $|\alpha| > n$. Then by Claim 11, two situations are possible.

1. Assume $\alpha = 1^{p'^{\kappa}}$ for $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t_s)$ and $\kappa > 0$. Then by Claim 11.2, $\alpha \in u_{z'}$, a contradiction. Hence, $\alpha \neq 1^{p'^{\kappa}}$ for all $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t_s)$ and $\kappa > 0$.

2. Here, $\alpha = c(i', x, y)$ for $i' \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$ with $0 < t_s(i') \leq c(i', x, y)$ and $F_{i'}^{u_z}(x) = y \in K^{u_z}$. By construction, it holds $t_s(i') = t_{s-1}(i') \leq |w_{s-1}| \leq |u| < \alpha$. Thus, $F_{i'}^{u_{z'}}(x) \neq y$, since otherwise, by the t_s-validity of $u_{z'}$ and V5, it would hold $\alpha \in u_{z'}$. Consequently, $F_{i'}^{u_{z'}}(x) \neq F_{i'}^{u_z}(x)$. Hence, there exists a query β that is asked by both $F_{i'}^{u_z}(x)$ and $F_{i'}^{u_{z'}}(x)$ and that is in $u_z \triangle u_{z'}$ (otherwise, both computations would output the same word). By definition of $Q(U_z)$ and $Q(U_{z'})$, it holds $\beta \in Q(U_z) \cap Q(U_{z'})$. Hence, $Q(U_z)$ and $Q(U_{z'})$ conflict in β and $|\beta| \leq |x|^{i'} + i' < |c(i', x, y)| = |\alpha|$, in contradiction to the assumption that α is the least word which $Q(U_z)$ and $Q(U_{z'})$ conflict in. ◁

For showing that for all odd $z \in \Sigma^n$ and all even $z' \in \Sigma^n$ the sets $Q(U_z)$ and $Q(U_{z'})$ conflict, we need one more claim. Let t' be defined such that $\mathrm{dom}(t') = \mathrm{dom}(t_s) - \{(i, j)\}$ and $t'(i', j') = t_s(i', j')$ for $(i', j') \in \mathrm{dom}(t')$. Then u and u_z for $z \in \Sigma^n$ are t'-valid by Claim 8.

▷ Claim 14. Let $t \in \{t', t_s\}$ and $z, z' \in \Sigma^n$ such that $Q(U_z)$ and $Q(U_{z'})$ do not conflict. For each t-valid oracle $v \supsetneq u$ that is defined for exactly the words of length $\leq n$ and that satisfies $v(q) = u_z(q)$ for all $|v| > q \in Q(U_z)$ and $v(q) = u_{z'}(q)$ for all $|v| > q \in Q(U_z)$, there exists a t-valid oracle $v' \supsetneq v$ with $|v'| = |u_z|$, $v'(q) = u_z(q)$ for all $|v'| > q \in Q(U_z)$, and $v'(q) = u_{z'}(q)$ for all $|v'| > q \in Q(U_z)$.

Proof. Let $w \sqsupseteq u$ with $|w| < |u_z|$, $w(q) = u_z(q)$ for all $|w| > q \in Q(U_z)$, and $w(q) = u_{z'}(q)$ for all $|w| > q \in Q(U_{z'})$. Moreover, let $\alpha = |w|$. It suffices to show the following:

- If $\alpha = 0^{p'^\kappa}$ for some $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t)$ and $\kappa > 0$, then there exists a t-valid $w' \supsetneq w$ that is defined for the words of length p'^κ, undefined for all words of greater length, and that satisfies $w'(q) = u_z(q)$ for all $|w'| > q \in Q(U_z)$ and $w'(q) = u_{z'}(q)$ for all $|w'| > q \in Q(U_{z'})$.
  Note that in this case $|w'| \leq |u_z|$ as u_z is defined for exactly the words of length $\leq \gamma(n)$.
- If α is not of length p'^κ for all $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t)$ and all $\kappa > 0$, then there exists $b \in \{0,1\}$ such that wb is t-valid, $wb(q) = u_z(q)$ for all $|wb| > q \in Q(U_z)$ and $wb(q) = u_{z'}(q)$ for all $|wb| > q \in Q(U_{z'})$.

We study three cases.

1. Assume $\alpha = 0^{p'^\kappa}$ for some $p' \in \mathbb{P}_3$ with $-p' \in \mathrm{ran}(t)$ and $\kappa > 0$. Then we let $w' \supsetneq w$ be the minimal oracle that is defined for all words of length p'^κ and contains $1^{p'^\kappa}$, i.e., $w' = w \cup \{1^{p'^\kappa}\}$ when interpreting the oracles as sets. As $u_z \cap \Sigma^{p'^\kappa} = u_{z'} \cap \Sigma^{p'^\kappa} = \{1^{p'^\kappa}\}$ by Claim 11.2, we obtain $w'(q) = u_z(q)$ for all $|w'| > q \in Q(U_z)$ and $w'(q) = u_{z'}(q)$ for all $|w'| > q \in Q(U_{z'})$. Moreover, by Claim 10.2b and Claim 10.2c, the oracle w' is t-valid.
2. Now assume that $\alpha = c(i', x, y)$ for $i' \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$ with $0 < t(i') \leq \alpha$ such that one of the conditions $F_{i'}^{u_z}(x) = y$ and $F_{i'}^{u_{z'}}(x) = y$ holds. By Claim 10.1, then even one of the two conditions $F_{i'}^{u_z}(x) = y \in K^{u_z}$ and $F_{i'}^{u_{z'}}(x) = y \in K^{u_{z'}}$ holds. By symmetry, if suffices to argue for the case $F_{i'}^{u_z}(x) = y \in K^{u_z}$. Recall that the oracles u_z and $u_{z'}$ are t-valid. Hence, by V5 and $0 < t(i') \leq \alpha < |u_z|$, it holds $\alpha \in u_z$. We consider two cases depending on whether $F_{i'}^{w}(x)$ returns y. In any case, if $\alpha \in Q(U_z)$ (resp., $\alpha \in Q(U_{z'})$), then $F_{i'}^{w}(x) = F_{i'}^{u_z}(x)$ (resp., $F_{i'}^{w}(x) = F_{i'}^{u_{z'}}(x)$), since for all queries q of $F_{i'}^{u_z}(x)$ (resp., $F_{i'}^{u_{z'}}(x)$), it holds $q \in Q(U_z)$ (resp., $q \in Q(U_{z'})$), $|q| \leq |x|^{i'} + i' < |\alpha|$, and by assumption, $w(q) = u_z(q)$ (resp., $w(q) = u_{z'}(q)$).
   - **(i)** Assume $F_{i'}^{w}(x) = y$. Choose $b = 1$. As w is t-valid, $0 < t(i') \leq \alpha$, and $F_{i'}^{w}(x) = y$, Claim 10.2e yields that $w1$ is t-valid. As $\alpha \in u_z$, we have $w1(q) = u_z(q)$ for all $|w1| > q \in Q(U_z)$. It remains to show that $w1(q) = u_{z'}(q)$ for all $|w1| > q \in Q(U_{z'})$. If $\alpha \notin Q(U_{z'})$, this trivially holds. If $\alpha \in Q(U_{z'})$, then as observed above, $F_{i}^{u_{z'}}(x) = F_{i}^{w}(x) = y$. Hence, as $u_{z'}$ is t-valid and $0 < t'(i') \leq \alpha < |u_{z'}|$, it holds $\alpha \in u_{z'}$ by V5. Thus, $w1(q) = u_{z'}(q)$ for all $|w1| > q \in Q(U_{z'})$.
   - **(ii)** Assume $F_{i'}^{w}(x) \neq y$. Choose $b = 0$. Then Claim 10.2f states that wb is t-valid. It holds $\alpha \notin Q(U_z)$, since otherwise, as observed above, $F_{i'}^{w}(x) = F_{i'}^{u_z}(x) = y$, which would yield a contradiction. Thus, $wb(q) = u_z(q)$ for all $|wb| > q \in Q(U_z)$. It remains to show $wb(q) = u_{z'}(q)$ for all $|wb| > q \in Q(U_{z'})$. If $\alpha \notin Q(U_{z'})$, this trivially holds and otherwise, it also holds, since as observed above, we have $F_{i'}^{u_{z'}}(x) = F_{i'}^{w}(x) \neq y$, which implies $\alpha \notin u_{z'}$ (by V1, $\alpha \in u_{z'}$ would imply $F_{i'}^{u_{z'}}(x) = y$).
3. We now consider the remaining cases, i.e., we may assume: (i) α is not of length p'^κ for all $p' \in \mathbb{P}_3$ and $\kappa > 0$ with $-p' \in \mathrm{ran}(t)$ and (ii) if $\alpha = c(i', x, y)$ for some $i' \in \mathbb{N}^+$ and $x, y \in \mathbb{N}$ with $0 < t(i') \leq \alpha$, then none of the conditions $F_{i'}^{u_z}(x) = y$ and $F_{i'}^{u_{z'}}(x) = y$ holds.

In this case, it holds $\alpha \notin u_z \cup u_{z'}$ by Claim 11.1. We choose $b = 0$ and obtain that $wb(q) = u_z(q)$ for all $|wb| > q \in Q(U_z)$ and $wb(q) = u_{z'}(q)$ for all $|wb| > q \in Q(U_{z'})$. Moreover, by Claim 10.2, wb is t-valid. This shows Claim 14. ◀

▷ Claim 15. For all odd $z \in \Sigma^n$ and all even $z' \in \Sigma^n$, $Q(U_z)$ and $Q(U_{z'})$ conflict.

Proof. Let us first show that $\alpha \in Q(U_\alpha)$ for all $\alpha \in \Sigma^n$. For a contradiction, assume $\alpha \notin Q(U_\alpha)$ for some $\alpha \in \Sigma^n$. We study the cases $i = j$ and $i \neq j$ separately.

First assume $i = j$. In this case $p \in \mathbb{P}_1$. Let u' be the oracle that is defined for exactly the words of length $\leq n$ and satisfies $u' = u$ when the oracles are considered as sets. Then u' is t_s-valid by Claim 10.2d and u' and u_α agree on all words in $\Sigma^n \cap Q(U_\alpha)$ as $u_\alpha \cap \Sigma^n = \{\alpha\}$ and $\alpha \notin Q(U_\alpha)$. Thus, we can apply Claim 14 to the oracle u' for $z = z' = \alpha$. Hence, there exists a t_s-valid oracle v satisfying $|v| = |u_z|$, $v \cap \Sigma^n = \emptyset$, and $v(q) = u_\alpha(q)$ for all $q \in Q(U_\alpha)$. By the latter property and the fact that $U_\alpha \subseteq Q(U_\alpha)$ contains all queries asked by the least accepting path of $M_i^{u_\alpha}(F_r^{u_\alpha}(0^n))$, this path is also an accepting path of the computation $M_i^v(F_r^v(0^n))$. As v is defined for all words of length $\leq \gamma(n)$, the computation $M_i^v(F_r^v(0^n))$ is defined. Thus, $0^n \notin C_q^{v'}$ for all $v' \sqsupseteq v$ and $M_i^v(F_r^v(0^n))$ definitely accepts, in contradiction to the assumption that step s of the construction fails.

Now let us consider the case $i \neq j$. Here $p \in \mathbb{P}_3$. By symmetry, it suffices to consider the case that α is odd. Let α' be the minimal even element of Σ^n that is not in $Q(U_\alpha)$. Such α' exists as it holds $2^{n-1} > 4(\gamma(n)) > 2\gamma(n)$ by (1), $\ell(Q(U_\alpha)) \leq 2\gamma(n)$ by Claim 12, and hence, $\ell(Q(U_\alpha)) \leq 2\gamma(n) < 2^{n-1} = |\{\alpha'' \in \Sigma^n \mid \alpha'' \text{ even}\}|$. Now choose u' to be the oracle that is defined for exactly the words of length $\leq n$ and that satisfies $u' = u \cup \{\alpha'\}$ when the oracles are considered as sets. Then u' is t_s-valid by Claim 10.2b and Claim 10.2f. Moreover, as $\alpha, \alpha' \notin Q(U_\alpha)$, the oracles u' and u_α agree on all words in $\Sigma^n \cap Q(U_\alpha)$. Thus, we can apply Claim 14 to the oracle u' for $z = z' = \alpha$ and obtain a t_s-valid oracle v that is defined for all words of length $\leq \gamma(n)$ and satisfies both $v \cap \Sigma^n = \{\alpha'\}$ and $v(q) = u_\alpha(q)$ for all $q \in Q(U_\alpha)$. The latter property and the fact that $U_\alpha \subseteq Q(U_\alpha)$ contains all queries asked by the least accepting path of $M_i^{u_\alpha}(F_r^{u_\alpha}(0^n))$ yield that this path is also an accepting path of the computation $M_i^v(F_r^v(0^n))$. As v is defined for all words of length $\leq \gamma(n)$, the computation $M_i^v(F_r^v(0^n))$ definitely accepts. Let us study two cases depending on whether $M_j^v(F_r^v(0^n))$ definitely accepts or definitely rejects (note that this computation is defined as v is defined for all words of length $\leq \gamma(n)$):

- Assume that $M_j^v(F_r^v(0^n))$ definitely accept. Let s' be the step that treats the task (i, j). Hence, $s' < s$ since $t_s(i, j)$ is defined. By Claim 8, the oracle v is $t_{s'-1}$-valid. Now, as both $M_i^v(F_r^v(0^n))$ and $M_j^v(F_r^v(0^n))$ definitely accept, v is even t''-valid for $t'' = t_{s'-1} \cup \{(i, j) \mapsto 0\}$. But then the construction would have chosen $t_{s'} = t''$ and a suitable oracle $w_{s'}$ (e.g., $w_{s'} = v$), a contradiction.
- Assume that $M_j^v(F_r^v(0^n))$ definitely rejects. As $v \cap \Sigma^n = \{\alpha'\}$, it holds $0^n \in B_p^{v'}$ for all $v' \sqsupseteq v$. This is a contradiction to the assumption that step s of the construction fails.

Hence, from now on we may assume that $\alpha \in Q(U_\alpha)$ for all $\alpha \in \Sigma^n$. Moreover, assume there are z odd and z' even such that $Q(U_z)$ and $Q(U_{z'})$ do not conflict. Then let $u' \supsetneq u$ be the minimal oracle that is defined for all words of length $\leq n$ and contains z and z', i.e., interpreting oracles as sets it holds $u' = u \cup \{z, z'\}$. Since $-p \notin \text{ran}(t')$, the oracle u' is t'-valid by Claim 10.2a. If Claim 14 cannot be applied to the oracle u' for z and z', then $z \in Q(U_{z'})$ or $z' \in Q(U_z)$. Since we observed above that $z \in Q(U_z)$ and $z' \in Q(U_{z'})$ and moreover, $u_z \cap \Sigma^n = \{z\}$ and $u_{z'} \cap \Sigma^n = \{z'\}$, in this case $Q(U_z)$ and $Q(U_{z'})$ conflict. Hence, it remains to consider the case that Claim 14 can be applied to the oracle u' for z and z'.

Applying Claim 14, we obtain a t'-valid $v \sqsupseteq u'$ that is defined for all words of length $\leq \gamma(n)$ and that satisfies $v(q) = u_z(q)$ for all $q \in Q(U_z)$ and $v(q) = u_{z'}(q)$ for all $q \in Q(U_{z'})$.

Let s' be the step in which (i,j) is treated. As $t_s(i,j)$ is defined, it holds $s' < s$. Hence, t' is an extension of $t_{s'-1}$ and by Claim 8, v is $t_{s'-1}$-valid. We claim that v is t''-valid for $t'' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$. Once this is proven, we obtain a contradiction as then the construction would have chosen $t_{s'} = t''$ and an appropriate $w_{s'}$ (e.g. $w_{s'} = v$). Then our assumption is wrong and for all odd $z \in \Sigma^n$ and all even $z' \in \Sigma^n$, $Q(U_z)$ and $Q(U_{z'})$ conflict.

It remains to prove that v is t''-valid for $t'' = t_{s'-1} \cup \{(i,j) \mapsto 0\}$. We study two cases.

Case 1: first we assume that $i \neq j$, i.e., it suffices to prove that $M_i^v(F_r^v(0^n))$ and $M_j^v(F_r^v(0^n))$ definitely accept. Recall that $M_i^{u_z}(F_r^{u_z}(0^n))$ and $M_j^{u_{z'}}(F_r^{u_{z'}}(0^n))$ definitely accept. Moreover, $v(q) = u_z(q)$ for all $q \in Q(U_z)$ and $v(q) = u_{z'}(q)$ for all $q \in Q(U_{z'})$ and in particular, v is defined for all words in $Q(U_z) \cup Q(U_{z'})$. This implies that the least accepting paths of $M_i^{u_z}(F_r^{u_z}(0^n))$ and $M_i^{u_z}(F_r^{u_z}(0^n))$ are also accepting paths of the computations $M_i^v(F_r^v(0^n))$ and $M_j^v(F_r^v(0^n))$.

Case 2: assume that $i = j$, i.e., we have to prove that on some input x the computation $M_i^v(x)$ has two accepting paths. As observed above, $z \in Q(U_z)$ and $z' \in Q(U_{z'})$. As $Q(U_z)$ and $Q(U_{z'})$ do not conflict, it holds $z \notin Q(U_{z'})$, which implies $Q(U_z) \neq Q(U_{z'})$. Let $\kappa \in \mathbb{N}$ be minimal such that $Q_\kappa(U_z) \neq Q_\kappa(U_{z'})$ and for a contradiction, assume $\kappa > 0$. Let $\alpha \in Q_\kappa(U_z) \triangle Q_\kappa(U_{z'})$. Without loss of generality, we assume $\alpha \in Q_\kappa(U_z) - Q_\kappa(U_{z'})$. Then there exist $i', x, y \in \mathbb{N}$ with $i' > 0$ such that $c(i', x, y) \in Q_{\kappa-1}(U_z)$ and $F_{i'}^{u_z}(x)$ asks the query α. By the choice of κ, it holds $Q_{\kappa-1}(U_{z'}) = Q_{\kappa-1}(U_z)$ and thus, $c(i', x, y) \in Q_{\kappa-1}(U_{z'})$. Consequently, all queries of $F_{i'}^{u_{z'}}(x)$ are in $Q_\kappa(U_{z'})$. However, $\alpha \notin Q_\kappa(U_{z'})$ and therefore, α cannot be asked by $F_{i'}^{u_{z'}}(x)$. This shows that there is a word $\beta \in u_z \triangle u_{z'}$ asked by both $F_{i'}^{u_z}(x)$ and $F_{i'}^{u_{z'}}(x)$ (otherwise, the two computations would ask the same queries). But then $\beta \in Q_\kappa(U_z) \cap Q_\kappa(U_{z'})$, which implies that $Q(U_z)$ and $Q(U_{z'})$ conflict, a contradiction. Hence, we obtain $\kappa = 0$ and $U_z = Q_0(U_z) \neq Q_0(U_{z'}) = U_{z'}$. Recall that U_z (resp., $U_{z'}$) is the set consisting of all oracle queries of the least accepting path P (resp., P') of the computation $M_i^{u_z}(F_r^{u_z}(0^n))$ (resp., $M_i^{u_{z'}}(F_r^{u_{z'}}(0^n))$). As $u_z(q) = v(q)$ for all $q \in Q(U_z) \supseteq U_z$ and $u_{z'}(q) = v(q)$ for all $q \in Q(U_{z'}) \supseteq U_{z'}$, the paths P and P' are accepting paths of the computation $M_i^v(F_r^v(0^n))$. Finally, P and P' are distinct paths since $U_z \neq U_{z'}$. This finishes the proof that v is t''-valid. Hence, the proof of Claim 15 is complete. ◀

The remainder of the proof that the construction is possible is based on an idea by Hartmanis and Hemachandra [8]. Consider the set

$$\begin{aligned} E &= \{\{z, z'\} \mid z, z' \in \Sigma^n, z \text{ odd} \Leftrightarrow z' \text{ even}, (z \in Q(U_{z'}) \vee z' \in Q(U_z))\} \\ &= \bigcup_{z \in \Sigma^n} \{\{z, z'\} \mid z' \in \Sigma^n, z \text{ odd} \Leftrightarrow z' \text{ even}, z' \in Q(U_z)\}. \end{aligned} \tag{2}$$

Let $z, z' \in \Sigma^n$ such that (z odd $\Leftrightarrow$ z' even). By Claim 15 and Claim 13, $Q(U_z)$ and $Q(U_{z'})$ conflict in a word of length n. Then, as observed above, they conflict in z or z', i.e., $z \in Q(U_{z'})$ or $z' \in Q(U_z)$. This shows $E = \{\{z, z'\} \mid z, z' \in \Sigma^n, z \text{ odd} \Leftrightarrow z' \text{ even}\}$ and thus, $|E| = 2^{2n-2}$. By Claim 12, for each $z \in \Sigma^n$ it holds $|Q(U_z)| \leq \ell(Q(U_z)) \leq 2\gamma(n)$. Consequently,

$$|E| \overset{(2)}{\leq} \sum_{z \in \Sigma^n} |Q(U_z)| \leq 2^n \cdot 2\gamma(n) = 2^{n+1} \cdot \gamma(n) \overset{(1)}{<} 2^{2n-2} = |E|,$$

a contradiction to the assumption that the construction fails in step s treating the task (i,j,r). This shows that the construction is possible and O is well-defined. It remains to show that DisjNP^O contains no pair $\leq_{\mathrm{m}}^{\mathrm{p},O}$-hard for $\mathrm{NP}^O \cap \mathrm{coNP}^O$, each problem in NP^O has P^O-optimal proof systems, and UP^O has no $\leq_{\mathrm{m}}^{\mathrm{p},O}$-complete problem. As the corresponding proofs are rather straightforward, we omit them. This completes the proof of Theorem 6. ◀

References

1 O. Beyersdorff, J. Köbler, and J. Messner. Nondeterministic functions and the existence of optimal proof systems. *Theor. Comput. Sci.*, 410(38-40):3839–3855, 2009. doi:10.1016/j.tcs.2009.05.021.

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

3 T. Dose. Complete Disjoint coNP-Pairs but no Complete Total Polynomial Search Problems Relative to an Oracle. *arXiv e-prints*, pages 1–13, March 2019. arXiv:1903.11860.

4 T. Dose. P-Optimal Proof Systems for Each Set in NP but no Complete Disjoint NP-pairs Relative to an Oracle. *arXiv e-prints*, pages 1–19, April 2019. arXiv:1904.06175.

5 T. Dose and C. Glaßer. NP-completeness, proof systems, and disjoint NP-pairs. Technical Report 19-050, Electronic Colloquium on Computational Complexity (ECCC), 2019.

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

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

8 J. Hartmanis and L. A. Hemachandra. Complexity Classes without Machines: On Complete Languages for UP. *Theor. Comput. Sci.*, 58:129–142, 1988. doi:10.1016/0304-3975(88)90022-9.

9 E. Khaniki. New relations and separations of conjectures about incompleteness in the finite domain. *arXiv e-prints*, pages 1–25, April 2019. arXiv:1904.01362.

10 J. Köbler and J. Messner. Is the Standard Proof System for SAT P-Optimal? In S. Kapoor and S. Prasad, editors, *FSTTCS 2000: Foundations of Software Technology and Theoretical Computer Science*, pages 361–372, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

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

12 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.

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

14 C. M. Papadimitriou. *Computational complexity.* Addison-Wesley, Reading, Massachusetts, 1994.

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

16 P. Pudlák. *Logical Foundations of Mathematics and Computational Complexity - A Gentle Introduction.* Springer monographs in mathematics. Springer, 2013. doi:10.1007/978-3-319-00119-7.

17 P. Pudlák. Incompleteness in the Finite Domain. *The Bulletin of Symbolic Logic*, 23(4):405–441, 2017.

18 A. A. Razborov. On provably disjoint NP-pairs. *Electronic Colloquium on Computational Complexity (ECCC)*, 1(6), 1994.