Electronic Colloquium on Computational Complexity, Report No. 29 (2008)

The Shrinking Property for NP and coNP

Christian Glaßer[*] Christian Reitwießner[†] Victor Selivanov[‡]

January 7, 2008

Abstract

We study the shrinking and separation properties (two notions well-known in descriptive set theory) for NP and coNP and show that under reasonable complexity-theoretic assumptions, both properties do not hold for NP and the shrinking property does not hold for coNP. In particular we obtain the following results.

1. NP and coNP do not have the shrinking property, unless PH is finite. In general, Σ_n^P and Π_n^P do not have the shrinking property, unless PH is finite. This solves an open question from [Sel94a].
2. The separation property does not hold for NP, unless UP $\subseteq$ coNP.
3. The shrinking property does not hold for NP, unless there exist NP-hard disjoint NP-pairs (existence of such pairs would contradict a conjecture by Even, Selman, and Yacobi [ESY84]).
4. The shrinking property does not hold for NP, unless there exist complete disjoint NP-pairs.

Moreover, we prove that the assumption NP $\neq$ coNP is too weak to refute the shrinking property for NP in a relativizable way. For this we construct an oracle relative to which P $=$ NP $\cap$ coNP, NP $\neq$ coNP, and NP has the shrinking property. This solves an open question by Blass and Gurevich [BG84] who explicitly ask for such an oracle.

1 Introduction

The shrinking property and the separation property are well-known notions from descriptive set theory. In this paper we study these notions with respect to complexity classes like NP.

Definition 1.1 *1. A class $\mathcal{C}$ has the* shrinking property*, if for all $A, B \in \mathcal{C}$ there exist disjoint sets $A', B' \in \mathcal{C}$ such that $A' \subseteq A$, $B' \subseteq B$, and $A' \cup B' = A \cup B$.*

2. A class $\mathcal{C}$ has the separation property*, if for all disjoint $A, B \in \mathcal{C}$ there exists an $S \in \mathcal{C} \cap$ co$\mathcal{C}$ that separates A and B.*

[*] Julius-Maximilians-Universität Würzburg, Germany. glasser@informatik.uni-wuerzburg.de

[†] Julius-Maximilians-Universität Würzburg, Germany. reitwiessner@informatik.uni-wuerzburg.de

[‡] A.P. Ershov Institute of Informatics Systems, Siberian Division of the Russian Academy of Sciences, Russia. Supported by RFBR grant 07-01-00543a. vseliv@nspu.ru

ISSN 1433-8092

Both properties were introduced long ago in descriptive set theory (see e.g. [Kec94]) where they play an important role. A simple result states that the class O of open subsets of the Baire space has the shrinking property but does not have the separation property. Later the properties were studied in computability theory (see e.g. [Rog67]) and again it turned out that they are very important, in particular due to their close relation to undecidability of first-order theories. In particular, for many natural theories T the set of the sentences provable in T and the set of the sentences false in a finite model of T are recursively (even effectively) inseparable (see e.g. the survey [ELTT65] for additional details). A simple result states that the class RE of computably enumerable sets has the shrinking property, but does not have the separation property. It turned out (see e.g. [Mos80]) that there is a deep and fruitful analogy between O (and more general classes as e.g. levels of the Borel hierarchy) and RE (and more general classes as e.g. levels of the arithmetical hierarchy). More recently it was shown [Sel98, Sel07] that the shrinking and separation properties are also interesting for the theory of finite automata on infinite words.

Note that the shrinking property is also known as the reduction property (see e.g. [Mos80, Rog67]). We follow Blass and Gurevich [BG84] and use the first name in this paper, because the word “reduction” has also a quite different meaning.

Since there is an analogy between NP and RE, complexity theorists started to study the separation and shrinking properties for NP and coNP. While the separation property was investigated rather comprehensively (see e.g. [GSSZ04, GSS05]), the shrinking property was not considered systematically so far. In this respect, Blass and Gurevich [BG84] and Selivanov [Sel94a] show some first results and identify open questions. As one might expect, the status of both properties in the context of complexity theory is not as clear as in computability theory or descriptive set theory: they turn out to be closely related to some well-known conjectures.

In this paper we continue the study of the separation and shrinking properties in complexity theory, and we give evidence that NP does have these properties. We show that under reasonable complexity-theoretic assumptions (like an infinite PH and UP $\not\subseteq$ coNP) both properties do not hold for NP and the shrinking property does not hold for coNP. Moreover, $\Sigma_{\mathrm{n}}^{\mathrm{P}}$ and $\Pi_{\mathrm{n}}^{\mathrm{P}}$ do not have the shrinking property, unless the PH is finite. This solves an open question from [Sel94a]. We also relate the shrinking and separation properties for NP to other well-known notions. For example, we show that the shrinking property does not hold, unless there exist NP-hard disjoint NP-pairs. The existence of such pairs contradicts a conjecture that is related to security aspects of public-key cryptosystems [ESY84, GS88]. Moreover, the shrinking property does not hold for NP, unless there exist complete disjoint NP-pairs. Such complete pairs are studied because of their relations to the theory of propositional proof systems [Raz94, Pud01]. Finally, we will see that the shrinking property for NP is closely related to selectivity, nondeterministic function classes and inverting polynomial-time computable functions (cf. Corollary 3.2) [HNOS96].

Along with the above-mentioned oracle-independent results, we establish some oracle separations for the discussed notions. In particular, we prove that the assumption NP $\neq$ coNP is too weak to refute the shrinking property for NP in a relativizable way. For this we construct an oracle relative to which NP has the shrinking property and (NP $\cap$ coNP) = P $\neq$ NP. It follows that relative to this oracle, NP $\subseteq$ NPSV-sel and NP $\neq$ coNP. Moreover, with our construction we solve an open problem by Blass and Gurevich [BG84] who explicitly ask for the existence of such an oracle.

In Section 2 we give the background on disjoint NP-pairs and function classes that is needed for our investigations. In Section 3 we establish implication relationships between the discussed notions, while in Section 4 we discuss oracle separations for some of these notions. We conclude in Section 5 by mentioning the remaining open questions.

2 Preliminaries

It is well known and easy to see that the shrinking property for a class $\mathcal{C}$ implies the separation property for the class co$\mathcal{C}$ of complements, but not vice versa. It is obvious that if $\mathcal{C} = \mathrm{co}\mathcal{C}$ and $\mathcal{C}$ is closed under intersection, then the shrinking and separation properties hold for both $\mathcal{C}$ and co$\mathcal{C}$. It is also clear that if $\mathcal{C}$ is closed under intersection, then the shrinking property for $\mathcal{C}$ implies that for any $k \geq 2$ any k-tuple $(A_1, \dots, A_k)$ of $\mathcal{C}$-sets may be "shrinked", i.e., there is a k-tuple $(A'_1, \dots, A'_k)$ of pairwise disjoint $\mathcal{C}$-sets such that $A'_i \subseteq A_i$ for each $i \in \{1, \dots, k\}$ and $A'_1 \cup \cdots \cup A'_k = A_1 \cup \cdots \cup A_k$.

2.1 Disjoint NP-Pairs

Even, Selman, and Yacobi [EY80, ESY84] showed that the security of public-key cryptosystems depends on the computational complexity of certain promise problems. Such problems can be written as pairs of disjoint sets, and it turned out that pairs of disjoint NP-sets are crucially important for the analysis of the cracking problem for public-key cryptosystems.

A *disjoint* NP*-pair* is a pair of nonempty sets A and B such that $A, B \in \mathrm{NP}$ and $A \cap B = \emptyset$. Let DisjNP denote the class of all disjoint NP-pairs. Given a disjoint NP-pair (A, B), a *separator* is a set S such that $A \subseteq S$ and $B \subseteq \overline{S}$ (we say that S *separates* (A, B)). Let $\mathit{Sep}(A, B)$ denote the class of all separators of (A, B).

Fortnow and Rogers [FR94] investigated the existence of disjoint sets in NP (resp., coNP) that are P-inseparable. Grollman and Selman [GS88] showed that certain one-way functions exist if and only if there exists a disjoint NP-pair (A, B) that is P-inseparable (i.e., $\mathit{Sep}(A, B) \cap \mathrm{P} = \emptyset$). The same paper demonstrates that natural reducibility notions for promise problems easily inherit to disjoint NP-pairs. We summarize these notions of reducibilities as follows:

Definition 2.1 ([GS88, Raz94, KMT03]) *Let (A, B) and (C, D) be disjoint pairs.*

1. *(A, B) is* many-one reducible in polynomial-time *to (C, D), $(A, B) \leq_{\mathrm{m}}^{\mathrm{pp}} (C, D)$, if for every separator $T \in \mathit{Sep}(C, D)$, there exists a separator $S \in \mathit{Sep}(A, B)$ such that $S \leq_{\mathrm{m}}^{\mathrm{p}} T$.*
2. *(A, B) is* strongly many-one reducible in polynomial-time *to (C, D), $(A, B) \leq_{\mathrm{sm}}^{\mathrm{pp}} (C, D)$, if there is a polynomial-time-computable total function f such that $f(A) \subseteq C$, $f(B) \subseteq D$, and $f(\overline{A \cup B}) \subseteq \overline{C \cup D}$.*
3. *(A, B) is* Turing reducible in polynomial-time *to (C, D), $(A, B) \leq_{\mathrm{T}}^{\mathrm{pp}} (C, D)$, if for every separator $T \in \mathit{Sep}(C, D)$, there exists a separator $S \in \mathit{Sep}(A, B)$ such that $S \leq_{\mathrm{T}}^{\mathrm{p}} T$.*
4. *(A, B) is* uniformly many-one reducible in polynomial-time *to (C, D), $(A, B) \leq_{\mathrm{um}}^{\mathrm{pp}} (C, D)$, if there exists a polynomial-time computable function f such that for every separator $T \in \mathit{Sep}(C, D)$, there exists a separator $S \in \mathit{Sep}(A, B)$ such that $S \leq_{\mathrm{m}}^{\mathrm{p}} T$ via f.*

5. (A,B) *is* uniformly Turing reducible in polynomial-time *to* (C,D), $(A,B) \leq^{\mathrm{pp}}_{\mathrm{uT}} (C,D)$, *if there exists a polynomial-time oracle Turing machine* M *such that for every separator* $T \in Sep(C,D)$, *there exists a separator* $S \in Sep(A,B)$ *such that* $S \leq^{\mathrm{p}}_{\mathrm{T}} T$ *via* M.

If f and M are as above, then we say that $(A,B) \leq^{\mathrm{pp}}_{\mathrm{um}} (C,D)$ via f and $(A,B) \leq^{\mathrm{pp}}_{\mathrm{uT}} (C,D)$ via M. The next result shows nontrivial relationships between the uniform and non-uniform notions above.

Theorem 2.2 ([GS88, Raz94, GSSZ04]) *For all disjoint pairs* (A,B) *and* (C,D),

$$\begin{array}{rcl} (A,B) \leq^{\mathrm{pp}}_{\mathrm{T}} (C,D) & \Leftrightarrow & (A,B) \leq^{\mathrm{pp}}_{\mathrm{uT}} (C,D) \\ (A,B) \leq^{\mathrm{pp}}_{\mathrm{m}} (C,D) & \Leftrightarrow & (A,B) \leq^{\mathrm{pp}}_{\mathrm{um}} (C,D) \\ & \Leftrightarrow & \textit{there is a polynomial-time-computable total function } f \\ & & \textit{such that } f(A) \subseteq C \textit{ and } f(B) \subseteq D. \end{array}$$

Razborov [Raz94] and Pudlák [Pud01] showed that disjoint NP-pairs are closely related to the theory of propositional proof systems. For example, if optimal propositional proof systems exist, then there exist complete disjoint NP-pairs.

A disjoint pair (A,B) is $\leq^{\mathrm{pp}}_{\mathrm{m}}$-*complete* (resp., $\leq^{\mathrm{pp}}_{\mathrm{sm}}$-*complete,* $\leq^{\mathrm{pp}}_{\mathrm{T}}$-*complete*) for the class DisjNP if $(A,B) \in$ DisjNP and for every disjoint pair $(C,D) \in$ DisjNP, $(C,D) \leq^{\mathrm{pp}}_{\mathrm{m}} (A,B)$ (resp., $(C,D) \leq^{\mathrm{pp}}_{\mathrm{sm}} (A,B)$, $(C,D) \leq^{\mathrm{pp}}_{\mathrm{T}} (A,B)$). Unexpectedly, both versions of m-completeness turn out equivalent:

Theorem 2.3 ([GSS05]) *The following statements are equivalent.*

1. *There exists* $\leq^{\mathrm{pp}}_{\mathrm{m}}$-*complete disjoint* NP-*pair.*
2. *There exists* $\leq^{\mathrm{pp}}_{\mathrm{sm}}$-*complete disjoint* NP-*pair.*

Next we recall some notions of hardness for disjoint NP-pairs.

Definition 2.4 *Let* (A,B) *be a disjoint* NP-*pair and let* $\leq_r$ *be from* $\{\leq^{\mathrm{pp}}_{\mathrm{m}}, \leq^{\mathrm{pp}}_{\mathrm{sm}}, \leq^{\mathrm{pp}}_{\mathrm{T}}, \leq^{\mathrm{pp}}_{\mathrm{um}}, \leq^{\mathrm{pp}}_{\mathrm{uT}}\}$.

1. $X \leq_r (A,B) \overset{df}{\Longleftrightarrow} (X, \overline{X}) \leq_r (A,B)$.
2. (A,B) *is* $\leq^{\mathrm{pp}}_{\mathrm{m}}$-hard for NP $\overset{df}{\Longleftrightarrow}$ $\mathrm{SAT} \leq^{\mathrm{pp}}_{\mathrm{m}} (A,B)$.
3. (A,B) *is* $\leq^{\mathrm{pp}}_{\mathrm{T}}$-hard for NP (NP-hard for short) $\overset{df}{\Longleftrightarrow}$ $\mathrm{SAT} \leq^{\mathrm{pp}}_{\mathrm{T}} (A,B)$.

So a disjoint pair is NP-hard if and only if all its separators are $\leq^{\mathrm{p}}_{\mathrm{T}}$-hard for NP. The following conjecture is due to Even, Selman, and Yacobi.

Conjecture 2.5 ([ESY84]) *There is no* NP-*hard disjoint* NP-*pair.*

If this conjecture is true, then no public-key cryptosystem is NP-hard to crack (see Theorem 2.8 for more consequences). Homer and Selman [HS92] construct a relativized world where P $\neq$ NP, but all disjoint NP-pairs are P-separable. In particular, Conjecture 2.5 holds in this world.

2.2 Function Classes

The study of NP search problems and the difficulty of inverting polynomial-time computable functions led to the notion of partial, multivalued functions that are computable by NP-machines. Partial, because NP-machines do not necessarily accept all inputs, and multivalued, because NP-machines can output different values on different accepting paths.

For each partial, multivalued function f, set-$f(x)$ denotes the *set of values* of f on input x. If $f(x)$ is undefined, then set-$f(x) = \emptyset$.

Definition 2.6 ([BLS84]) *We define some function classes:*

1. NPMV *is the class of partial, multivalued functions f for which there is a nondeterministic polynomial-time machine N such that for every x, it holds that*
   $$\text{set-}f(x) = \{y \,|\, \textit{there is an accepting computation path of } N(x) \textit{ that outputs } y\}$$
2. $\text{NP}k\text{V} \overset{\text{df}}{=} \{f \in \text{NPMV} \,|\, \forall x, |\text{set-}f(x)| \leq k\}$ *where* $k \geq 1$
3. $\text{NPSV} \overset{\text{df}}{=} \text{NP1V}$ *(the class of partial, singlevalued* NPMV*-functions)*
4. $\text{NPbV} \overset{\text{df}}{=} \{f \in \text{NP2V} \,|\, \forall x, \text{set-}f(x) \subseteq \{0,1\}\}$
5. PF *is the class of partial (singlevalued) functions computable in (deterministic) polynomial time.*
6. *For any class of functions $\mathcal{F}$, let $\mathcal{F}_t \overset{\text{df}}{=} \{f \in \mathcal{F} \,|\, f$ is total$\}$.*

For partial, multivalued functions f and g, we say that g is a *refinement* of f, if for all x,

1. $g(x)$ is defined if and only if $f(x)$ is defined, and
2. set-$g(x) \subseteq$ set-$f(x)$.

For function classes $\mathcal{F}$ and $\mathcal{G}$ we write $\mathcal{F} \subseteq_c \mathcal{G}$, if for every $f \in \mathcal{F}$ there exists a $g \in \mathcal{G}$ such that g is a refinement of f.

Selman [Sel94b] gives a systematic comparison of classes of functions that are computed by nondeterministic polynomial-time transducers. Moreover, this paper identifies relations between these function classes and disjoint NP-pairs. A comprehensive overview of function classes can be found in [Sel96].

Fenner et al. [FFNR96] introduced and studied the class NPbV. In particular, the paper investigates and gives several equivalent formulations of the hypotheses $\text{NPMV}_t \subseteq_c \text{PF}$ and $\text{NPbV}_t \subseteq_c \text{PF}$. For example, the latter is equivalent to the hypothesis that all disjoint pairs of coNP-sets are P-separable.

Definition 2.7 ([Sel79, HHO$^+$93, HNOS96]) *Let $\mathcal{F}$ be any class of functions (possibly multivalued and/or partial). A set A is $\mathcal{F}$-*selective *if there is a function $f \in \mathcal{F}$ such that for every x and y it holds that* set-$f(x,y) \subseteq \{x,y\}$ *and*

$$\{x,y\} \cap A \neq \emptyset \quad \Rightarrow \quad \emptyset \neq \text{set-}f(x,y) \subseteq A.$$

By $\mathcal{F}$-sel we denote the class of sets that are $\mathcal{F}$-selective.

The following theorem summarizes known consequences of Conjecture 2.5.

Theorem 2.8 ([ESY84, GS88, Sel94b]) *If Conjecture 2.5 holds, then* $\mathrm{NP} \neq \mathrm{coNP}$*,* $\mathrm{NP} \neq \mathrm{UP}$*,* $\mathrm{NPMV} \not\subseteq_c \mathrm{NPSV}$*, and no public-key cryptosystem is* NP*-hard to crack.*

A polynomial-time computable function f is *honest*, if there is a polynomial q such that for every y in the range of f there exists an x in the domain of f such that $f(x) = y$ and $|x| \leq q(|y|)$.

There are several equivalent formulations of the hypothesis $\mathrm{NPMV} \subseteq_c \mathrm{NPSV}$. Later (in Theorem 3.1) we will show that one can add the shrinking property for NP to this list of equivalent formulations.

Theorem 2.9 ([Sel94b, HNOS96]) *The following are equivalent:*

1. $\mathrm{NPMV} \subseteq_c \mathrm{NPSV}$
2. $\mathrm{NP2V} \subseteq_c \mathrm{NPSV}$
3. $\mathrm{SAT} \in \mathrm{NPSV\text{-}sel}$
4. $\mathrm{NP} \subseteq \mathrm{NPSV\text{-}sel}$
5. *The inverse of every honest, polynomial-time computable function has a refinement in* NPSV*.*

Hemaspaandra et al. [HNOS96] use selectivity to show that the assertions above (e.g. $\mathrm{NPMV} \subseteq_c \mathrm{NPSV}$) imply a collapse of the polynomial-time hierarchy. Their proof relativizes to all oracles [HNOS96]. Naik et al. [NRRS98] improve this result and show that the output-multiplicity hierarchy $\{\mathrm{NP}k\mathrm{V}\}_{k\geq 1}$ is infinite unless the polynomial-time hierarchy collapses.

Theorem 2.10 ([HNOS96]) *If* $\mathrm{NP} \subseteq \mathrm{NPSV\text{-}sel}$ *then* $\mathrm{ZPP}^{\mathrm{NP}} = \mathrm{PH}$*.*

We are going to study the relationships between the following assertions.

Definition 2.11 *Define the following assertions.*

A1 : DisjNP *does not have a* $\leq_{\mathrm{T}}^{\mathrm{pp}}$*-complete disjoint pair.*

A2 : DisjNP *does not have a* $\leq_{\mathrm{m}}^{\mathrm{pp}}$*-complete disjoint pair.*

A3 : *There is no* NP*-hard disjoint* NP*-pair.*

A4 : *The separation property does not hold for* coNP*.*

A4′ : $\mathrm{NPbV}_t \not\subseteq_c \mathrm{NPSV}$.

A5 : $\mathrm{UP} \not\subseteq \mathrm{coNP}$.

A6 : *The* PH *is infinite.*

A7 : *The separation property does not hold for* NP*.*

A8 : *The shrinking property does not hold for* NP*.*

A8′ : NPMV $\not\subseteq_c$ NPSV*.*

A9 : *The shrinking property does not hold for* coNP*.*

A9′ : *There is no disjoint* NP*-pair that is* $\leq_{\mathrm{m}}^{\mathrm{pp}}$*-hard for* NP*.*

A9″ : NP $\neq$ coNP*.*

A10 : *There is a* P*-inseparable, disjoint* NP*-pair.*

The next proposition follows immediately from the remarks at the beginning of this section.

Proposition 2.12 A4 ⇒ A8*,* A7 ⇒ A9*,* $\neg$A9″ ⇒ ($\neg$A4 $\wedge$ $\neg$A7 $\wedge$ $\neg$A8 $\wedge$ $\neg$A9)*.*

Theorem 2.13 ([GSSZ04]) *The following holds.*

1. A1 ⇒ A2 ⇒ A9′
2. A1 ⇒ A3 ⇒ A9′
3. A9′ ⇔ A9″

In the following we establish new relationships between the assertions given in Definition 2.11. Figure 1 gives a summary of the relationships and their relativizability. In particular, we will answer the following open questions:

Open Problem 1 [BG84, problem 3]: *Find an oracle relative to which the shrinking property holds for* NP *but* NP $\neq$ coNP*. Better yet, find an oracle relative to which the shrinking property holds for* NP *and* (NP $\cap$ coNP) = P $\neq$ NP*.*

Open Problem 2 [Sel94a]: *Is there an oracle relative to which the polynomial-time hierarchy does not collapse and for all* $n \geq 1$, $\Sigma_{\mathrm{n}}^{\mathrm{P}}$ *(resp.,* $\Pi_{\mathrm{n}}^{\mathrm{P}}$*) has the shrinking property?*

In Theorem 4.1 we construct the oracle that is asked for in the first problem. The Corollaries 3.3 and 3.8 will tell us that the oracles mentioned in the second problem do not exist.

3 Connections to Reasonable Assumptions

In this section we establish implication relationships between the introduced notions. Our results imply that, under reasonable complexity-theoretic assumptions like an infinite PH and UP $\not\subseteq$ coNP, the shrinking and separation properties do not hold for NP and the shrinking property does not hold for coNP. In particular, we will relate the shrinking and separation properties to well-known notions like the classes $\Sigma_{\mathrm{n}}^{\mathrm{P}}$ and $\Pi_{\mathrm{n}}^{\mathrm{P}}$ of the PH, the function classes NPMV and NPSV, NP-hard disjoint NP-pairs, and complete disjoint NP-pairs.

Moreover, with the Corollaries 3.3 and 3.8 we will solve the open problem in [Sel94a] that is mentioned at the end of Section 2.

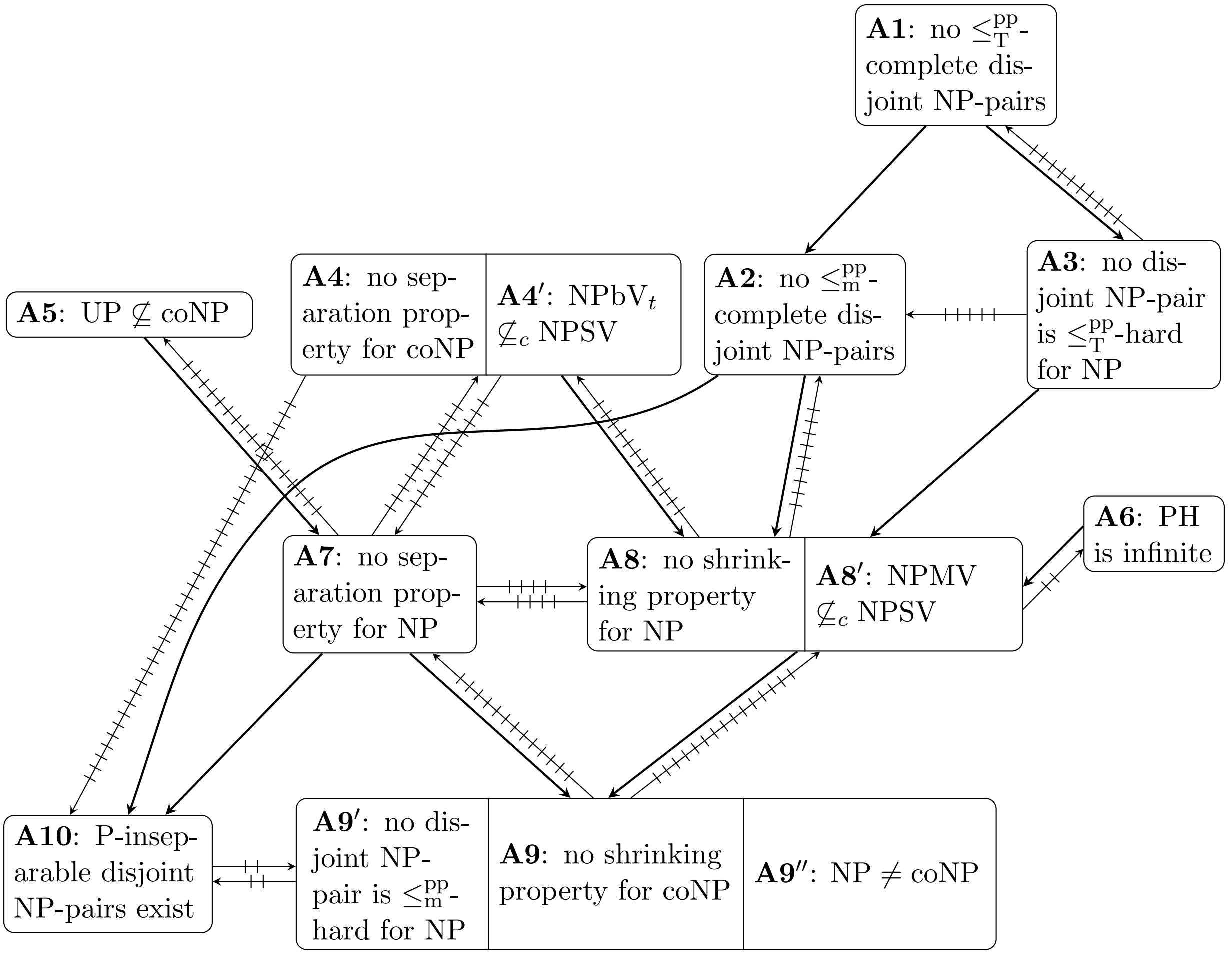
A1: no $\leq_T^{pp}$-complete disjoint NP-pairs
A2: no $\leq_m^{pp}$-complete disjoint NP-pairs
A3: no disjoint NP-pair is $\leq_T^{pp}$-hard for NP
A4: no separation property for coNP
A4′: NPbV$_t$ $\not\subseteq_c$ NPSV
A5: UP $\not\subseteq$ coNP
A6: PH is infinite
A7: no separation property for NP
A8: no shrinking property for NP
A8′: NPMV $\not\subseteq_c$ NPSV
A10: P-inseparable disjoint NP-pairs exist
A9′: no disjoint NP-pair is $\leq_m^{pp}$-hard for NP
A9: no shrinking property for coNP
A9″: NP $\neq$ coNP

Figure 1: Summary of the relations of the assertions A1–A10. Normal arrows denote relativizable implications, crossed-out arrows denote implications that do not hold relative to some oracle. Assertions that share a box are equivalent.

First let us relate the shrinking property for NP to known and well-understood classes of functions that are computable in nondeterministic, polynomial time. As a consequence, the shrinking property for NP is equivalent to all hypotheses mentioned in Theorem 2.9. From a result by Hemaspaandra et al. [HNOS96] it then follows that the shrinking property does not hold for NP, unless the PH collapses to its second level. Later we will see that this evidence is optimal in the sense that relativizable techniques cannot strengthen the collapse to the first level. Moreover, the collapse consequence of the shrinking property for NP solves an open question from [Sel94a].

Theorem 3.1 NP *has the shrinking property if and only if* $\mathrm{NPMV} \subseteq_c \mathrm{NPSV}$ *(*$\mathrm{A8}' \Leftrightarrow \mathrm{A8}$*).*

Proof $\Rightarrow$ By Theorem 2.9 it suffices to show $\mathrm{NP} \subseteq \mathrm{NPSV\text{-}sel}$. Let $L \in \mathrm{NP}$ and let $A \overset{\mathit{df}}{=} \{(x,y) \,|\, x \in L\}$ and $B \overset{\mathit{df}}{=} \{(x,y) \,|\, y \in L\}$. By the shrinking property, there exist disjoint $A', B' \in \mathrm{NP}$ such that $A' \subseteq A$, $B' \subseteq B$, and $A' \cup B' = A \cup B$. Let M_a and M_b be nondeterministic polynomial-time machines such that $A' = L(M_a)$ and $B' = L(M_b)$.

We describe a nondeterministic polynomial-time machine M on input (x,y): The computation starts with a nondeterministic branch. On the left side, we simulate $M_a(x,y)$ such that accepting paths output x. On the right side, we simulate $M_b(x,y)$ such that accepting paths output y.

Let f be the multivalued function computed by M. Observe the following for all x and y.

1. $f \in \mathrm{NPSV}$
2. $\text{set-}f(x,y) \subseteq \{x,y\}$
3. $(x \in L \vee y \in L) \Rightarrow \emptyset \neq \text{set-}f(x,y) \in L$

This shows that L is NPSV-selective.

$\Leftarrow$ Let $A, B \in \mathrm{NP}$ and let f be the multivalued function with values in $\{0,1\}$ that is defined by $(0 \in \text{set-}f(x) \Leftrightarrow x \in A)$ and $(1 \in \text{set-}f(x) \Leftrightarrow x \in B)$. Note that $f \in \mathrm{NPMV}$. Choose $g \in \mathrm{NPSV}$ such that g is a refinement of f.

$$\begin{aligned} A' &\overset{\mathit{df}}{=} \{x \,|\, g(x) = 0\} \\ B' &\overset{\mathit{df}}{=} \{x \,|\, g(x) = 1\} \end{aligned}$$

Since g is singlevalued, A' and B' are disjoint sets in NP. From the fact that g is a refinement of f we obtain $A' \subseteq A$, $B' \subseteq B$, and $A' \cup B' = A \cup B$. So NP has the shrinking property. □

Corollary 3.2 *The following are equivalent:*

1. NP *has the shrinking property*
2. $\mathrm{NPMV} \subseteq_c \mathrm{NPSV}$
3. $\mathrm{NP2V} \subseteq_c \mathrm{NPSV}$
4. $\mathrm{SAT} \in \mathrm{NPSV\text{-}sel}$
5. $\mathrm{NP} \subseteq \mathrm{NPSV\text{-}sel}$

6. *The inverse of every honest, polynomial-time computable function has a refinement in* NPSV.

Proof Follows from the Theorems 2.9 and 3.1. □

The last theorem together with a result by Hemaspaandra et al. [HNOS96] immediately implies a collapse of the PH, if NP has the shrinking property. This solves the $\Sigma_{\mathrm{n}}^{\mathrm{P}}$-part of the open problem in [Sel94a] (the second open problem that is mentioned at the end of Section 2).

Corollary 3.3 *For any $n \geq 1$, the shrinking property for $\Sigma_{\mathrm{n}}^{\mathrm{P}}$ implies $\mathrm{ZPP}^{\Sigma_{\mathrm{n}}^{\mathrm{P}}} = \mathrm{PH}$ (and hence $\mathrm{PH} = \Sigma_{\mathrm{n+1}}^{\mathrm{P}}$). In particular, the shrinking property for* NP *implies $\mathrm{ZPP}^{\mathrm{NP}} = \mathrm{PH}$ (A6 ⇒ A8).*

Proof The Theorems 2.10 and 3.1 are relativizable. □

The following theorem relates the shrinking property for NP to Conjecture 2.5. It follows immediately from the Theorems 2.8, 2.9, and 3.1.

Theorem 3.4 *If* NP *has the shrinking property, then* NP*-hard disjoint* NP*-pairs exist.* (A3 ⇒ A8)

Remark 3.5 *Interestingly, the analog of the last theorem in computability theory is false, i.e., RE has the shrinking property and the analog of Conjecture 2.5 holds: There exists an m-complete disjoint pair (equivalently, an effectively inseparable pair) (A, B) of computably enumerable sets (see e.g. [Rog67]), but every disjoint pair of computably enumerable sets can be separated by some set whose degree is strictly less than $0'$ [Sho60].*

In contrast to NP, the shrinking property for coNP relativizably implies a collapse of the PH to the first level, i.e., NP = coNP.

Theorem 3.6 coNP *has the shrinking property if and only if* NP = coNP. *(A9 ⇔ A9″)*

Proof ⇐ Proposition 2.12.

⇒ Assume that coNP has the shrinking property. We denote the arity of a Boolean formula $F = F(x_1, \ldots, x_n)$ by $|F| = n$. If $m \leq n$ and $a_1, \ldots, a_m \in \{0, 1\}$, then $F(a_1 \cdots a_m)$ denotes the formula $F'(x_{m+1}, \ldots, x_n) \overset{df}{=} F(a_1, \ldots, a_m, x_{m+1}, \ldots, x_n)$.

$$\begin{aligned} A &\overset{df}{=} \{(F, a) \mid F \text{ is a Boolean formula and } a \in \{0,1\}^* \text{ such that } |a| < |F| \text{ and } F(a0) \notin \mathrm{SAT}\} \\ B &\overset{df}{=} \{(F, a) \mid F \text{ is a Boolean formula and } a \in \{0,1\}^* \text{ such that } |a| < |F| \text{ and } F(a1) \notin \mathrm{SAT}\} \end{aligned}$$

Note that $A, B \in$ coNP. By assumption there exist disjoint sets $A', B' \in$ coNP such that $A' \subseteq A$, $B' \subseteq B$, and $A' \cup B' = A \cup B$. Let $M_{A'}$ and $M_{B'}$ be nondeterministic Turing machines such that $L(M_{A'}) = \overline{A'}$ and $L(M_{B'}) = \overline{B'}$.

We describe a nondeterministic algorithm M on input (F, a).

```
1  if |F| < |a| then reject
2  if |F| = |a| then
3     if F(a) = 0 then accept else reject
4  endif
5  do the following nondeterministically
6     simulate $M_{A'}$(F,a) such that accepting paths call M(F,a0)
7     simulate $M_{B'}$(F,a) such that accepting paths call M(F,a1)
```

Observe that M is a nondeterministic polynomial-time algorithm.

Claim 3.7 *For every Boolean formula F it holds that $F \in \overline{\mathrm{SAT}} \Leftrightarrow (F, \varepsilon) \in L(M)$.*

Proof Assume $F \in \overline{\mathrm{SAT}}$. From $A' \cap B' = \emptyset$ it follows that for all $a \in \{0,1\}^*$, $(F,a) \notin A'$ or $(F,a) \notin B'$. Hence, if M on input (F,a) reaches step 5, then one of the simulations $M_{A'}(F,a)$ and $M_{B'}(F,a)$ has accepting paths. These accepting paths cause a continuation of the computation by calling $M(F,a0)$ or $M(F,a1)$. This shows that M on input $M(F,\varepsilon)$ leads to consecutive calls $M(F,a_1)$, $M(F,a_1a_2)$, …, $M(F,a_1a_2\cdots a_{|F|})$. The latter computation accepts in step 3, since $F \in \overline{\mathrm{SAT}}$. Therefore, $(F,\varepsilon) \in L(M)$ which proves the direction from left to right.

Assume now that $(F,\varepsilon) \in L(M)$. Let $n \overset{df}{=} |F|$ and let p be an accepting path of M on (F,ε). Observe that along p there are calls $M(F,a_1)$, $M(F,a_1a_2)$, …, $M(F,a_1a_2\cdots a_n)$ where the a_i are from $\{0,1\}$. $F(a_1\cdots a_n) = 0$, since p accepts. For $i \in [1,n]$ we show

$$F(a_1\cdots a_i) \in \overline{\mathrm{SAT}} \quad \Rightarrow \quad F(a_1\cdots a_{i-1}) \in \overline{\mathrm{SAT}} \qquad (1)$$

Assume that (1) does not hold for some $i \in [1,n]$, i.e., $F(a_1\cdots a_i) \in \overline{\mathrm{SAT}}$ and $F(a_1\cdots a_{i-1}) \in \mathrm{SAT}$.

Case 1: $a_i = 0$. Observe that $(F,a_1\cdots a_{i-1}) \in A - B$. From $A - A' \subseteq B$ it follows that $(F,a_1\cdots a_{i-1}) \in A' - B \subseteq A' - B'$. Hence $M_{A'}(F,a_1\cdots a_{i-1})$ has no accepting paths and $M_{B'}(F,a_1\cdots a_{i-1})$ has accepting paths. So the computation $M(F,a_1\cdots a_{i-1})$ only continues in step 7 with the call of $M(F,a_1\cdots a_{i-1}1)$. This means that $a_i = 1$ which contradicts our assumption in Case 1.

Case 2: $a_i = 1$. We obtain a contradiction analogously to Case 1.

So in both cases we obtain contradictions. This proves (1).

We have already seen that $F(a_1\cdots a_n) = 0$, i.e., $F(a_1\cdots a_n) \in \overline{\mathrm{SAT}}$. The repeated application of (1) yields $F(\varepsilon) \in \overline{\mathrm{SAT}}$, i.e., $F \in \overline{\mathrm{SAT}}$. This shows the direction from right to left and finishes the proof of Claim 3.7. □

Claim 3.7 immediately implies $\overline{\mathrm{SAT}} \in \mathrm{NP}$ and hence $\mathrm{NP} = \mathrm{coNP}$. This proves Theorem 3.6. □

Since the proof of Theorem 3.6 is relativizable, we can solve the $\Pi_{\mathrm{n}}^{\mathrm{P}}$-part of the open problem in [Sel94a]. Together with Corollary 3.3 this completely solves that open problem.

Corollary 3.8 *For any $n \geq 1$, $\Pi_{\mathrm{n}}^{\mathrm{P}}$ has the shrinking property if and only if $\Sigma_{\mathrm{n}}^{\mathrm{P}} = \Pi_{\mathrm{n}}^{\mathrm{P}}$.*

Now let us relate the shrinking property for NP to complete disjoint NP-pairs, a notion that has been studied because of its connections to the theory of propositional proof systems [Raz94].

Theorem 3.9 *If* NP *has the shrinking property, then* DisjNP *has* $\leq_{\mathrm{m}}^{\mathrm{pp}}$*-complete pairs. (*A2 ⇒ A8*)*

Proof Let $A = \{\langle a,b\rangle \mid a \in C\}$ and $B = \{\langle a,b\rangle \mid b \in C\}$ where C is an NP-complete subset of $\{0,1\}^*$ and $\langle,\rangle$ is a polynomial-time-computable bijection between $\{0,1\}^* \times \{0,1\}^*$ and $\{0,1\}^*$. Then (A,B) is a polynomial-time $\leq_{\mathrm{sm}}^{\mathrm{pp}}$-complete pair of NP-sets, i.e., for any pair (E,F) of (not necessarily disjoint) NP-subsets of $\{0,1\}^*$ there is a polynomial-time-computable function $f : \{0,1\}^* \to \{0,1\}^*$ such that $E = f^{-1}(A)$ and $F = f^{-1}(B)$. Indeed, it suffices to set $f(x) = \langle g(x), h(x)\rangle$ where g (resp., h) is a polynomial-time-computable function on $\{0,1\}^*$ satisfying $E = g^{-1}(C)$ (resp., $F = h^{-1}(C)$).

By the shrinking property for NP, there exist disjoint NP-sets A', B' such that $A' \subseteq A$, $B' \subseteq B$, and $A' \cup B' = A \cup B$. Then (A', B') is a desired $\leq_m^{pp}$-complete pair in DisjNP. To see this it suffices to note that if $E \cap F = \emptyset$, then $(E,F) \leq_m^{pp} (A', B')$ via the function f from the preceding paragraph. □

Remark 3.10 *A similar argument shows that if* NP *has the shrinking property then for each* $k \geq 2$ *there is an sm-complete* k*-tuple* $(A_1, \ldots, A_k)$ *of pairwise disjoint* NP*-sets (i.e., for any* k*-tuple* $(B_1, \ldots, B_k)$ *of pairwise disjoint* NP*-sets there is a polynomial-time-computable function* f *such that* $B_i = f^{-1}(A_i)$ *for all* $i \in \{1, \ldots, k\}$*).*

We can relate the separation property for NP to another reasonable conjecture.

Theorem 3.11 *If* UP $\not\subseteq$ coNP*, then the separation property does not hold for* NP *(*A5 ⇒ A7*).*

Proof Let $L \in \mathrm{UP} - \mathrm{coNP}$ and let M be a nondeterministic polynomial-time machine that accepts L in time p. Define a pair $(A,B) \in \mathrm{DisjNP}$ as follows.

$$A \overset{df}{=} \{(x,v) \,\big|\, |v| = p(|x|) \text{ and } \exists w \in \Sigma^{|v|}, w \leq v, M(x) \text{ accepts along path } w\}$$
$$B \overset{df}{=} \{(x,v) \,\big|\, |v| = p(|x|) \text{ and } \exists w \in \Sigma^{|v|}, w > v, M(x) \text{ accepts along path } w\}$$

If $x \in L$, then $M(x)$ has exactly one accepting path which we can determine by a binary search that queries (A,B). This shows $L \leq_{\mathrm{T}}^{\mathrm{pp}} (A,B)$.

Assume that NP has the separation property. So there exists an $S \in \mathrm{NP} \cap \mathrm{coNP}$ such that $A \subseteq S$ and $B \subseteq \overline{S}$. In particular, $L \leq_{\mathrm{T}}^{\mathrm{p}} S$ which shows $L \in \mathrm{P}^{\mathrm{NP} \cap \mathrm{coNP}} = \mathrm{NP} \cap \mathrm{coNP} \subseteq \mathrm{coNP}$. This contradicts our assumption on L. □

Finally, we show that also the separation property for coNP can be equivalently expressed in terms of function classes.

Theorem 3.12 coNP *has the separation property if and only if* $\mathrm{NPbV}_t \subseteq_c \mathrm{NPSV}$*. (*A4 ⇔ A4′*)*

Proof $\Leftarrow$ Let A, B be disjoint sets from coNP and let M_a, M_b be nondeterministic polynomial-time machines such that $\overline{A} = L(M_a)$ and $\overline{B} = L(M_b)$. Let M be the nondeterministic, polynomial-time machine that on input x, simulates the computations $M_a(x)$ and $M_b(x)$ in parallel, where accepting paths output 0 and 1, respectively. Let f be the multivalued function computed by M and observe that $f \in \mathrm{NPbV}_t$. By our assumption, there exists a $g \in \mathrm{NPSV}$ such that g is a refinement of f. Let $A' \overset{df}{=} \{x \mid g(x) = 0\}$ and $B' \overset{df}{=} \{x \mid g(x) = 1\}$. Note that g is a total, singlevalued function with values in $\{0, 1\}$. Therefore, A' and B' are disjoint NP-sets such that $A' \cup B' = \Sigma^*$. So $A' \in \mathrm{NP} \cap \mathrm{coNP}$. Moreover, since g is a refinement of f, $A' \subseteq \overline{A}$ and $B' \subseteq \overline{B}$. Hence $B \subseteq \overline{B'} = A' \subseteq \overline{A}$ which shows that A' separates A and B.

$\Rightarrow$ Let $f \in \mathrm{NPbV}_t$ be computed by the nondeterministic, polynomial-time machine M. Let $A \overset{df}{=} \{x \mid 0 \in \text{set-}f(x)\}$ and $B \overset{df}{=} \{x \mid 1 \in \text{set-}f(x)\}$. Note that $\overline{A}$ and $\overline{B}$ are disjoint sets in coNP. So $(\overline{A}, \overline{B})$ is separated by some $S \in \mathrm{NP} \cap \mathrm{coNP}$, i.e., $\overline{A} \subseteq S \subseteq B$. Let $g(x) \overset{df}{=} c_S(x)$ and observe that $g \in \mathrm{NPSV}$ and that g is a refinement of f. □

We remark that all proofs in this section are relativizable.

4 Oracle Separations

We now concentrate on those implications between the assertions A1–A10 that were left open in Section 3. For most of them we can find oracle constructions showing that the implication in question cannot be established by relativizable proof techniques. Note that an unconditional separation of any two of the assertions A1–A10 immediately implies $\mathrm{P} \neq \mathrm{NP}$ (since if $\mathrm{P} = \mathrm{NP}$, then all our assertions are false and hence pairwise equivalent).

The main result in this section is the construction of an oracle relative to which NP has the shrinking property and $(\mathrm{NP} \cap \mathrm{coNP}) = \mathrm{P} \neq \mathrm{NP}$. This oracle has three applications: First, it provides a relativized world in which some of the open implications do not hold. Second, it shows that the assumption $\mathrm{NP} \neq \mathrm{coNP}$ is too weak to refute the shrinking property for NP with relativizable techniques. Third, with this oracle we solve an open problem by Blass and Gurevich [BG84] who explicitly ask for the existence of such an oracle.

Theorem 4.1 *There exists an oracle O relative to which the following holds:*

1. NP *has the shrinking property.*
2. $\mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$.
3. $\mathrm{UP} \not\subseteq \mathrm{coNP}$.

Proof Overview: We achieve the first part by coding, the second part is reached by diagonalization and coding and the third part is done by diagonalization (which includes a tentative coding).

Fix the alphabet $\Sigma = \{0, 1\}$ and let $M_1, M_2, M_3, \ldots$ be an enumeration of all NP-machines such that the machine M_i runs in time t_i and $t_i(n) \leq n^i + i$.

Coding for part one: For $i, j \in \mathbb{N}$ and $x \in \Sigma^*$ define the injective coding function $\mathrm{code}_1(i, j, x) \overset{df}{=} 0^i 1 0^j 1 0^t 1 x$, where $t = t_i(|x|) + t_j(|x|)$ and

$$A^O_{i,j} \overset{df}{=} \{x \mid \exists y \in 0\Sigma^*, |y| = |\mathrm{code}_1(i, j, x)|, \mathrm{code}_1(i, j, x)y \in O\}$$
$$B^O_{i,j} \overset{df}{=} \{x \mid \exists y \in 1\Sigma^*, |y| = |\mathrm{code}_1(i, j, x)|, \mathrm{code}_1(i, j, x)y \in O\}.$$

We build the oracle O such that the following holds:

$$\text{P1: } \forall i, j \in \mathbb{N}: \quad A^O_{i,j} \cap B^O_{i,j} = \emptyset, A^O_{i,j} \subseteq L(M^O_i), B^O_{i,j} \subseteq L(M^O_j),$$
$$A^O_{i,j} \cup B^O_{i,j} = L(M^O_i) \cup L(M^O_j)$$

Observe that $A^O_{i,j}, B^O_{i,j} \in \mathrm{NP}^O$ and these sets witness the shrinking property for the sets $L(M^O_i)$ and $L(M^O_j)$.

Coding for part two: For $k, i, j \in \mathbb{N}$ and $x \in \Sigma^*$ define the injective coding function $\mathrm{code}_2(k, i, j, x) \overset{df}{=} 0^k 1 0^i 1 0^j 1 0^t 1 x 0^l$, where $t = t_i(|x|) + t_j(|x|)\}$ and l is the smallest $l \in \mathbb{N}$ that fulfills $l \geq \frac{1}{2}|\mathrm{code}_2(k, i, j, x)|$ and $|\mathrm{code}_2(k, i, j, x)| \equiv 1 \pmod 4$. We build the oracle O such that the following holds:

$$\text{P2: } \forall i, j \in \mathbb{N}: \quad L(M^O_i) = \overline{L(M^O_j)} \Rightarrow \exists k \in \mathbb{N}: \quad L(M^O_i) = \{x \mid \mathrm{code}_2(k, i, j, x) \in O\}$$

Note that if P2 holds for O, then the mentioned language $L(M^O_i)$ can be decided in polynomial time relative to O.

We call an oracle O *valid* if it satisfies P1 and P2 and for every $n \equiv 3 \pmod 4$, $|O \cap \Sigma^n| \leq 1$. For $n \in \mathbb{N}$ we call an oracle $O \subseteq \Sigma^*$ an *extension* of $O \cap \Sigma^{\leq n}$. An oracle $O_n \subseteq \Sigma^{\leq n}$ is *valid up to stage n* if there is a valid extension of O_n.

Diagonalization for 2: At the time of coding we do not know if the machines will violate $L(M^O_i) = \overline{L(M^O_j)}$ with a further constructed oracle. So we have to do the coding. If we did this coding for arbitrary pairs of NP-machines, whose languages are not necessarily disjoint, then NP-pairs would be P-separable and hence NP = coNP. This is not what we want. So we try to construct the oracle in such a way that for as many (i, j) as possible $L(M^O_i) \neq \overline{L(M^O_j)}$. This diagonalization is not done by encoding certain strings into the oracle, but rather by choosing suitable finite extensions of the current oracle that are valid up to some further stage.

Diagonalization for 3: The witness language for $\mathrm{UP}^O \not\subseteq \mathrm{coNP}^O$ is $W^O \overset{df}{=} \{0^n \mid n \equiv 3 \pmod 4$ and $\exists y \in \Sigma^n \cap O\}$. We will make sure that there is at most one such y in O and thus $W^O \in \mathrm{UP}^O$. We construct the oracle such that for all $i \in \mathbb{N}$ there exists a stage $n \equiv 3 \pmod 4$ such that $0^n \in W^O \iff M^O_i(0^n)$ accepts. This ensures that $W^O \notin \mathrm{coNP}^O$ and hence $\mathrm{UP}^O \not\subseteq \mathrm{coNP}^O$.

The difficult task is now to combine the codings with the diagonalizations.

We start with an empty oracle and extend it stage-by-stage. Because the codeword is greater than the running time of the machines that need to be simulated, the coding for part one can always be done easily. For the coding for part two, we maintain a list $\mathcal{L} \subseteq \mathbb{N}^3$ that is finite at every stage. Elements are never removed from $\mathcal{L}$ but once in a while, elements are added to $\mathcal{L}$. $(k, i, j) \in \mathcal{L}$ means that for every valid extension O of the current oracle it holds that $L(M^O_i) = \overline{L(M^O_j)}$. Thus in order to fulfill P2, we have to code $L(M^O_i)$ into the oracle once we reach large enough stages (depending on k, which is the parameter from P2).

We now do the main construction.

1) We start with $\mathcal{L} = \emptyset$ and $O = \emptyset$. In each stage, we will fulfill one requirement from $\mathbb{N} \cup (\mathbb{N} \times \mathbb{N})$. The requirement $i \in \mathbb{N}$ means $\overline{L(M_i^O)} \neq W^O$. For the requirement $(i,j) \in \mathbb{N}^2$ we will make sure that either $L(M_i^O) \neq \overline{L(M_j^O)}$ or, if this is not possible, we will choose some sufficiently large $k \in \mathbb{N}$ and add (k,i,j) to $\mathcal{L}$. The latter means we make sure that $L(M_i^O) = \{x \mid \mathrm{code}_2(k,i,j,x) \in O\}$.

2) We do the coding for P1 and P2 until we reach a stage that is large enough such that changes do not affect diagonalizations in earlier stages. Let O_{n-1} be the oracle constructed so far.

3) Suppose (i,j) is the next requirement.
Case 1: There exists a valid extension O of O_{n-1} such that $L(M_i^O) \neq \overline{L(M_j^O)}$. Then we choose a witnessing $x \in L(M_i^O) \oplus \overline{L(M_j^O)}$. Let now $n' \overset{df}{=} \max(n, |x|^{t_i(|x|)+t_j(|x|)})$ and $O_{n'} \overset{df}{=} O \cap \Sigma^{\leq n'}$. Note that $O_{n'}$ is valid up to stage n' and for all valid extensions O of $O_{n'}$ it holds that $L(M_i^O) \neq \overline{L(M_j^O)}$.

Case 2: For all valid extensions O of O_{n-1} it holds that $L(M_i^O) = \overline{L(M_j^O)}$. Here, append (n,i,j) to $\mathcal{L}$.

4) Suppose i is the next requirement.
Leave stage n empty and continue with a tentative construction (coding only) up to stage $n' \overset{df}{=} t_i(n)$. Let this oracle be $O_{n'}$.

Case 1: $M_i^{O_{n'}}(0^n)$ rejects. Here we are done, since $0^n \in \overline{L(M_i^{O_{n'}})}$ but $0^n \notin W^{O_{n'}}$.

Case 2: $M_i^{O_{n'}}(0^n)$ accepts. Here we want to add a word of length n to the oracle, but we have to make sure that $M_i^{O_{n'}}(0^n)$ still accepts after this change. For this, we will collect some words in a set Q^+ (resp. Q^-) that need to stay inside (resp. outside) the oracle. Let p be an accepting path and Q_p^+ (resp. Q_p^-) be the queries asked on p that were answered positively (resp. negatively). We recursively fix the answers to the queries $q \in Q_p^+ \cup Q_p^-$ as follows:

Case 2.1: If $q \in Q_p^+$ then put q in Q^+ and do the following:
Case 2.1.1: If $|q| < n$ then we are done.
Case 2.1.2: $|q| > n$ and q is a codeword for P1. So $q = \mathrm{code}_1(i',j',x')y'$ for some i',j',x',y'. $q \in O_{n'}$ means that if $y' \in 0\Sigma^*$ then $M_{i'}(x')$ accepts, and if $y' \in 1\Sigma^*$ then $M_{j'}(x')$ accepts. We can leave q in the oracle once we make sure that $M_{i'}(x')$ resp. $M_{j'}(x')$ accept. We choose an accepting path and fix its queries recursively.

Case 2.1.3: $|q| > n$ and q is a codeword for P2. So $q = \mathrm{code}_2(k,i',j',x')$ for some x' and $(k,i',j') \in \mathcal{L}$. This means that $M_{i'}^{O_{n'}}(x')$ accepts. Again, we choose an accepting path and fix it recursively. (Note that also with such a modified oracle O, $M_{j'}^O(x')$ rejects, since otherwise O would be an extension where $L(M_{i'})) \neq \overline{L(M_{j'})}$ contradicting $(k,i',j') \in \mathcal{L}$.)

Case 2.2: If $q \in Q_p^-$ then put q in Q^- and do the following: Case 2.2.1: If $|q| > n$ and q is a codeword for P2 such that $q = \mathrm{code}_2(k,i',j',x')$ and $(k,i',j') \in \mathcal{L}$, then proceed analogous to Case 2.1.3 by fixing an accepting path of $M_{j'}(x')$.

Case 2.2.2: Otherwise no dependencies need to be handled.

This procedure terminates after finitely many steps. Furthermore the recursion tree has only polynomial size:

Claim 4.2 *It holds that*

$$\sum_{x \in Q^+ \cup Q^-} |x| \leq 2t_i(n).$$

Proof The running time of the simulated machine is always encoded into the oracle question in unary. Hence the sums of the lengths of the words added to $Q^+ \cup Q^-$ in each recursion step is at least divided by two. So if we sum the lengths of the oracle queries added to $Q^+ \cup Q^-$ in each recursion step, we obtain $t_i(n) + \frac{1}{2}t_i(n) + \frac{1}{4}t_i(n) + \ldots \quad \leq 2t_i(n)$. □

Now we delete the whole tentative construction and start at O_{n-1} again. Choose some $w \in \Sigma^n \setminus Q^-$ (possible by Claim 4.2) and let $O_n \overset{df}{=} O_{n-1} \cup \{w\}$. Now redo the coding until stage n' in such a way that words in Q^+ (resp. Q^-) are put inside (resp. outside) the oracle.

For all $q \in Q^+ \cup Q^-$ we fixed the reason why q is inside or outside O. Also $|Q^+ \cup Q^-| \leq 2t_i(n)$ (cf. Claim 4.2), so the coding is possible and yields an oracle $O_{n'}$ valid up to stage n'. $M_i^{O_{n'}}(0^n)$ still accepts along p, so $0^n \notin \overline{L(M_i^{O_{n'}})}$ and we reached $W^O \neq \overline{L(M_i^O)}$.

5) Continue with step 2).

This completes the construction of O. □

Corollary 4.3 *Relative to the oracle O constructed in Theorem 4.1, all of the following holds.*

$$\neg\text{A1},\ \neg\text{A2},\ \neg\text{A3},\ \neg\text{A4},\ \text{A5},\ \text{A7},\ \neg\text{A8},\ \text{A9},\ \text{A9}',\ \text{A9}'',\ \text{A10},\ \text{ZPP}^{\text{NP}} = \text{PH}$$

Proof From Theorem 4.1 it immediately follows that A5, ¬A8 and A9″ hold relative to O. All implications shown in Figure 1 are relativizable. So we obtain ¬A1, ¬A2, ¬A3, ¬A4, A9, A9′, A9″. From the relativizable Theorems 2.10 and 3.1 we obtain $\text{ZPP}^{\text{NP}} = \text{PH}$. Since A10 trivially follows from A7 in a relativizable way, it remains to show A7.

Assume that A7 does not hold, i.e., NP has the separation property. We already know that ¬A3 relative to O, i.e., there exists a pair $(A, B) \in \text{DisjNP}$ all of whose separators are $\leq_{\text{T}}^{\text{p}}$-hard for NP. By the separation property, (A, B) has a separator $S \in \text{NP} \cap \text{coNP} = \text{P}$ (relative to O). So $S \in \text{P}$ and S is $\leq_{\text{T}}^{\text{p}}$-hard for NP. Therefore, relative to O it holds that P = NP. This contradicts the fact that NP $\neq$ coNP relative to O. This shows A7. □

Recall that Hemaspaandra et al. showed that NP $\subseteq$ NPSV-sel implies a collapse of the polynomial hierarchy to ZPP^{NP}. Our oracle constructed in Theorem 4.1 shows that relativizable techniques cannot strengthen this collapse to NP.

Corollary 4.4 *There exists an oracle relative to which* NP $\subseteq$ NPSV-sel *and* NP $\neq$ coNP.

Proof Follows from the Theorems 4.1 and 3.1. □

Reversely, Corollary 3.3 shows that there is no oracle relative to which NP has the shrinking property and $\Sigma_2^{\text{P}} \neq \Pi_2^{\text{P}}$. In this sense the oracle constructed in Theorem 4.1 is nearly optimal.

Theorem 4.5 ([HS92]) *There exists an oracle O relative to which all of the following holds.*

$$\neg\text{A1},\ \neg\text{A2},\ \text{A3},\ \neg\text{A5},\ \neg\text{A7},\ \text{A8},\ \text{A9},\ \text{A9}',\ \text{A9}'',\ \neg\text{A10}$$

Proof Homer and Selman [HS92] construct an oracle O relative to which $\mathrm{P} \neq \mathrm{NP}$ and all disjoint NP-pairs are P-separable ($\neg$A10) and hence ($\mathrm{NP} \cap \mathrm{coNP}$)-separable. So relative to O, it holds that A3 and $\neg$A7. Grollmann and Selman [GS88] showed (in a relativizable way) that $\mathrm{P} \neq \mathrm{UP}$ implies the existence of P-inseparable disjoint NP-pairs. Hence, relative to O, it holds that $\mathrm{P} = \mathrm{UP}$ and so $\neg$A5.

Moreover, relative to O we have $\neg$A2 which can be seen as follows: Let (A, B) be an arbitrary disjoint NP-pair. We argue that (A, B) is $\leq_{\mathrm{m}}^{\mathrm{pp}}$-complete. For every $(C, D) \in \mathrm{DisjNP}$, since (C, D) is P-separable, there is a separator S of (C, D) that is in P. Therefore, for any separator L of (A, B), S trivially $\leq_{\mathrm{m}}^{\mathrm{p}}$-reduces to L. So $(C, D) \leq_{\mathrm{m}}^{\mathrm{pp}} (A, B)$ and hence (A, B) is $\leq_{\mathrm{m}}^{\mathrm{pp}}$-complete which shows $\neg$A2.

The remaining conditions follow, since all implications shown in Figure 1 relativize. □

We conclude with a summary of other relevant oracle constructions.

Theorem 4.6 *The following oracles are known.*

1. *There exists an oracle relative to which* NP *has the separation property, but* coNP *does not have the separation property.* ($\text{A4} \not\Rightarrow \text{A10}$) *[FR94, Theorem 3.3]*
2. *There exists an oracle relative to which* coNP *has the separation property, but* NP *does not have the separation property.* ($\text{A7} \not\Rightarrow \text{A4}$) *[FR94, Theorem 3.5]*
3. *There exists an oracle relative to which* NP *and* coNP *do not have the separation property and* $\mathrm{UP} \subseteq \mathrm{coNP}$. ($\text{A7} \wedge \text{A4} \not\Rightarrow \text{A5}$) *[FR94, Theorem 3.4]*
4. *There exists an oracle relative to which there are no* NP*-hard disjoint* NP*-pairs, but there exist* $\leq_{\mathrm{m}}^{\mathrm{pp}}$*-complete disjoint* NP*-pairs.* ($\text{A3} \not\Rightarrow \text{A2}$) *[GSSZ04, Theorem 6.1]*
5. *There exists an oracle relative to which* $\mathrm{NP2V} \not\subseteq_c \mathrm{NPSV}$*, but* $\mathrm{NP2V}_t \subseteq_c \mathrm{PF} \subseteq \mathrm{NPSV}$*. In particular,* $\mathrm{NPMV} \not\subseteq_c \mathrm{NPSV}$ *and* $\mathrm{NPbV}_t \subseteq_c \mathrm{NPSV}$*.* ($\text{A8}' \not\Rightarrow \text{A4}'$) *[NRRS98, Corollary 6]*
6. *There exists an oracle relative to which* $\mathrm{NP2V} \not\subseteq_c \mathrm{NPSV}$ *and* $\mathrm{PH} = \Delta_2^{\mathrm{P}}$*. In particular,* $\mathrm{NPMV} \not\subseteq_c \mathrm{NPSV}$ *and* PH *is finite.* ($\text{A8}' \not\Rightarrow \text{A6}$) *[NRRS98, Theorem 5]*
7. *There exists an oracle relative to which* $\mathrm{UP} \neq \mathrm{NP} = \mathrm{PSPACE}$*. In particular,* $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$ *and hence* P*-inseparable disjoint* NP*-pairs exist.* ($\text{A10} \not\Rightarrow \text{A9}''$) *[OH93, Lemma 4.7]*
8. *Relative to a random oracle,* $\mathrm{NP} \neq \mathrm{coNP}$*,* $\mathrm{NP} \neq \mathrm{UP}$*, and* $\mathrm{NPMV} \not\subseteq_c \mathrm{NPSV}$*. In particular, the shrinking property does not hold for* NP*. [BG81, Nai94, NRRS98]*

Figure 1 gives a summary of the oracle results in this section.

5 Conclusions and Open Questions

The results of this paper show that, similar to descriptive set theory and computability theory, the separation and shrinking properties are important also for complexity theory, because they are closely related to many other fundamental notions. In contrast to descriptive set theory and computability theory, these properties are probably false for complexity classes like NP or coNP, because they contradict widely believed conjectures. The negative solution to the problem in [Sel94a] gives a clear evidence that the refinements of the PH studied in [Sel94a] behave probably much worse than the analogous refinements of the Borel hierarchy in descriptive set theory and of the arithmetical hierarchy in computability theory (see [Sel95] for additional details).

Our summary in Figure 1 motivates several open problems. In particular, we would like to know answers for the following questions:

1. Does an infinite PH imply that the separation property does not hold for NP (resp., coNP)?
2. Is there an oracle relative to which A8 $\not\Rightarrow$ A3? By Theorem 2.8 and Corollary 3.3 it suffices to construct an oracle relative to which UP = NP and $\Sigma_2^{\mathrm{P}} \neq \Pi_2^{\mathrm{P}}$. However, it is a known open question whether such a relativized world exists. An even stronger result would be an oracle relative to which A2 $\not\Rightarrow$ A3.

References

[BG81] C. Bennett and J. Gill. Relative to a random oracle $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

[BG84] A. Blass and Y. Gurevich. Equivalence relations, invariants, and normal forms. *SIAM Journal on Computing*, 13(4):682–689, 1984.

[BLS84] R. V. Book, T. Long, and A. L. Selman. Quantitative relativizations of complexity classes. *SIAM Journal on Computing*, 13:461–487, 1984.

[ELTT65] Yu. L. Ershov, I. A. Lavrov, A. D. Taimanov, and M.A. Taitslin. Elementary theories. *Uspechi Matematicheskikh Nauk*, 20(4):37–108, 1965. In Russian, English translation: Russian Mathematical Surveys, 20(4):35–105, 1965.

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

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

[FFNR96] S. Fenner, L. Fortnow, A. Naik, and J. Rogers. On inverting onto functions. In *Proceedings 11th Conference on Computational Complexity*, pages 213–223. IEEE Computer Society Press, 1996.

[FR94] L. Fortnow and J. Rogers. Separability and one-way functions. In *Proceedings of the 5th International Symposium on Algorithms and Computation*, volume 834 of *Lecture Notes in Computer Science*, pages 396–404. Springer Verlag, 1994.

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

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

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

[HHO$^+$93] L. A. Hemachandra, A. Hoene, M. Ogiwara, A. L. Selman, T. Thierauf, and J. Wang. Selectivity. In *Proceedings 5th International Conference on Computing and Information*, pages 55–59. IEEE Computer Society, 1993.

[HNOS96] L. Hemaspaandra, A. Naik, M. Ogihara, and A. L. Selman. Computing solutions uniquely collapses the polynomial hierarchy. *SIAM Journal on Computing*, 25:697–708, 1996.

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

[Kec94] A. S. Kechris. *Classical Descriptive Set Theory.* Springer, New York, 1994.

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

[Mos80] Y. N. Moschovakis. *Descriptive Set Theory.* North Holland, Amsterdam, 1980.

[Nai94] A. Naik. *The structural complexity of intractable search functions.* PhD thesis, State University of New York at Buffalo, 1994.

[NRRS98] A. Naik, J. Rogers, J. Royer, and A. L. Selman. A hierarchy based on output multiplicity. *Theoretical Computer Science*, 207:131–157, 1998.

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

[Pud01] P. Pudlák. On reducibility and symmetry of disjoint NP-pairs. In *Proceedings 26th International Symposium on Mathematical Foundations of Computer Science*, volume 2136 of *Lecture Notes in Computer Science*, pages 621–632. Springer-Verlag, Berlin, 2001.

[Raz94] A. Razborov. On provably disjoint NP-pairs. Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.

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

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

[Sel94a] V. L. Selivanov. Two refinements of the polynomial hierarchy. In *Proceedings 11th Symposium on Theoretical Aspects of Computer Science*, volume 775 of *Lecture Notes in Computer Science*, pages 439–448. Springer Verlag, 1994.

[Sel94b] A. L. Selman. A taxonomy on complexity classes of functions. *Journal of Computer and System Sciences*, 48:357–381, 1994.

[Sel95] V. L. Selivanov. Fine hierarchies and boolean terms. *Journal of Symbolic Logic*, 60:289–317, 1995.

[Sel96] A. L. Selman. Much ado about functions. In *Proceedings 11th Conference on Computational Complexity*, pages 198–212. IEEE Computer Society Press, 1996.

[Sel98] V. L. Selivanov. Fine hierarchy of regular omega-languages. *Theoretical Computer Science*, 191(1-2):37–59, 1998.

[Sel07] V. L. Selivanov. Fine hierarchy of regular aperiodic omega-languages. In *Developments in Language Theory*, volume 4588 of *Lecture Notes in Computer Science*, pages 399–410. Springer, 2007.

[Sho60] J. R. Shoenfield. Degrees of models. *Journal of Symbolic Logic*, 25(3):233–237, 1960.