Electronic Colloquium on Computational Complexity, Report No. 71 (2004)

Simplicity and Strong Reductions

Marcus Schaefer[*]
School of CTI
DePaul University
243 South Wabash Avenue
Chicago, Il 60604, USA
mschaefer@cs.depaul.edu

Stephen Fenner[†]
Department of Computer Science
University of South Carolina
Columbia, SC 29208, USA
fenner@cs.sc.edu

August 11, 2004

Abstract

A set is called NP-*simple* if it lies in NP, and its complement is infinite, and does not contain any infinite subsets in NP. Hartmanis, Li and Yesha [HLY86] proved that no set which is hard for NP under many-one (Karp) reductions is NP-simple unless NP $\cap$ coNP $\subseteq$ SUBEXP. However, we can exhibit a relativized world in which there is an NP-simple set that is complete under Turing (Cook) reductions, even conjunctive reductions. This raises the questions whether the result by Hartmanis, Li and Yesha generalizes to reductions of intermediate strength.

We show that NP-simple sets are not complete for NP under positive bounded truth-table reductions unless UP $\subseteq$ SUBEXP. In fact, NP-simple sets cannot be complete for NP under bounded truth-table reductions under the stronger assumption that UP $\cap$ coUP $\not\subseteq$ SUBEXP (while there is an oracle relative to which there is an NP-simple set conjunctively complete for NP). We present several other results for different types of reductions, and show how to prove a similar result for NEXP which does not require any assumptions. We also prove that all NEXP-complete sets are P-levelable, extending work by Tran [Tra95].

Most of the results are derived by the use of inseparable sets. This technique turns out to be very powerful in the study of truth-table and even (honest) Turing reductions.

Keywords: NP-immune, NP-simple, *btt*-complete, inseparable sets, strong reducibilities, P-levelable.

1 Introduction

In 1944 Post published his epochal paper on *Recursively enumerable sets of positive integers and their decision problems* (reprinted in *The Undecidable* by Davis [Dav65]). With this paper he initiated a line of research in computability theory[1] which has since become famous as Post's program. To settle the question of whether there are incomplete, c.e., noncomputable degrees he pursued a simple, but productive idea: among the c.e. sets reducing to a complete set are sets with very "fat" complements. Thus c.e. sets with very "thin" complements should not be complete,

[*] Most of this work was done while I was visiting Maine as a research assistant to Steve Fenner. I was partially supported by NSF Grant CCR-9501794

[†] Partially supported by NSF Grant CCR-9501794

[1] In this paper we will use the terminology suggested by Soare [Soa96]. That means *computable* instead of recursive, and *computably enumerable (c.e.)* instead of recursively enumerable (r.e.).

ISSN 1433-8092

since strong reductions cannot squeeze the fat complements into the thin complements[2]. Post's program was successfully completed in the seventies by Degtev and Marchenkov who exhibited a thinness property which made a c.e. set incomplete [Odi89, III.5].

A similar approach to incompleteness has been popular in complexity theory since the time the isomorphism conjecture was first suggested by Berman and Hartmanis in 1977: the study of sparse sets. The isomorphism conjecture claims that all NP-complete sets are polynomial time isomorphic. Sparse sets are thin in the sense that they contain only polynomially many strings at every length. Sparseness is invariant under polynomial-time isomorphisms, hence, assuming that the isomorphism conjecture holds, no sparse set can be NP-complete, since SAT (for example) is evidently not sparse (for a recent survey on the completenss of sparse sets see the paper by Cai and Ogihara [CO97]).

There is an alternative and relatively unexplored approach which is closer in spirit to Post's original idea: consider effectively thin sets, like Post's simple and immune sets.

The use of effective thinness notions in complexity theory to obtain results on strong reductions dates back to a paper by Hartmanis, Li and Yesha [HLY86] published in 1986. This paper contains the result that every m-hard (many-one hard) set for NP has an infinite NP subset unless NP $\subseteq$ SUBEXP $= \bigcap_{k=0}^{\infty} \mathrm{DTIME}(2^{n^{1/k}})$. We could also express this as saying that no m-hard set for NP is NP-*immune* (unless, of course, NP $\subseteq$ SUBEXP). In analogy with computability theory we call a set NP-*simple* if it lies in NP and its complement is NP-immune. Hartmanis, Li and Yesha concluded that an NP-simple set cannot be m-hard for NP, unless NP $\cap$ coNP $\subseteq$ SUBEXP. This addressed a question raised earlier by Homer [Hom86] whether NP-complete sets can be NP-simple. This is the question we want to investigate in this paper.

Pursuing the idea that NP-simple sets should not be complete for NP under sufficiently strong reductions we set out to improve upon the initial result by Hartmanis, Li, and Yesha. To achieve this goal we will need assumptions from complexity theory. If we restrict the reductions to be honest we can show that NP-simple sets are neither honest bounded truth-table complete nor honest disjunctively complete unless P = UP, and NP-hypersimple sets cannot be honest Turing complete unless P = UP (NP-hypersimple sets will be introduced in Section 3). The first result was improved by Manindra Agrawal: NP-simple sets are not honest bounded truth-table complete without any assumptions. A weaker version of the second result (where honest d-reductions were forced to be honest on all inputs) was shown by Yamakami [Yam95] (our more liberal version of honest disjunctive reductions will be introduced in Section 5).

Without the honesty constraint we need stronger complexity-theoretic assumptions. The work of Hartmanis, Li and Yesha suggests that SUBEXP plays a central role in the case of reductions that are not honest.

We will establish that NP-simple sets are neither 1-*tt*-complete, nor d-complete, nor positive bounded truth-table complete unless UP $\subseteq$ SUBEXP. The proof for positive *btt*-reductions does not seem to generalize to *btt*-reductions. We therefore take a detour through truth-table reductions: under the stronger assumption that UP $\cap$ coUP $\not\subseteq$ SUBEXP we can show that NP-hypersimple sets are not $o(\log n)$-*tt*-complete for NP. The proof of this result yields that NP-simple sets are not *btt*-complete unless UP $\cap$ coUP $\not\subseteq$ SUBEXP. The last result was claimed by Yamakami [Yam95] (under the weaker hypothesis that NP $\not\subseteq$ SUBEXP), but we are as yet unable to verify the proof. The assumption UP $\cap$ coUP $\not\subseteq$ SUBEXP is not unreasonable; its negation would imply

[2] In compliance with computability rather than complexity theory, we think of m-reductions as the strongest kind of reduction whereas Turing reductions are considered weak.

FACTORING $\in$ SUBEXP which is considered unlikely (FACTORING $\in$ UP $\cap$ coUP by a result of Fellows and Koblitz [FK95]).

The techniques developed for NP-simple sets translate up into the realm of exponential time, and we have some results on EXP and NEXP which do not require any assumptions. We show that no set *btt*-hard for EXP can be NEXP-simple. This result was first shown by Harry Buhrman using a different idea. We will also prove that NEXP-complete sets are P-levelable (improving a result by Tran [Tra95]).

This paper is of interest from a methodological point of view through its use of inseparable sets. In computability theory inseparable sets have been a rich source of results [Odi89, Soa87] and this paper demonstrates that the same can be true for complexity theory. The abundance of results shows that here is a technique waiting to be exploited further. This paper seems to be the first to apply inseparable sets to the study to resource bounded reductions. Inseparability, however, has been used before in complexity theory, and more will be said about that in Section 4.

We review the relevant concepts from complexity theory in Section 2. In Sections 3 and 4 we introduce and discuss the different notions of immunity, simplicity, and inseparability needed in this paper. Sections 5 through 7 deal with increasingly weaker reductions in NP, and Section 8 is devoted to completeness in NEXP. The paper concludes with some remarks on relativizations in Section 9 and a list of (challenging) open problems.

2 Preliminaries

Let ω be the set of natural numbers. Throughout this text Σ will denote the alphabet $\{0,1\}$, and Σ^* the set of all (finite) binary strings. Let $\Sigma^{\leq n}$ denote the set of all binary strings of length at most n. $(\Sigma^*)^{<\omega}$ is the set of all finite tuples of binary strings (we write $()$ for the empty tuple). We use a function $\langle \cdots \rangle \colon (\Sigma^*)^{<\omega} \to \Sigma^*$ to encode any sequence of strings uniquely in a single string (applying a standard pairing function). For a language $L \subseteq \Sigma^*$ we say $L \in \mathrm{DTIME}(f)$ ($L \in \mathrm{NTIME}(f)$) if L is decidable in time $O(f)$ (in nondeterministic time $O(f)$). With this we can define the usual complexity classes:

- $\mathrm{P} = \bigcup_{k=0}^{\infty} \mathrm{DTIME}(n^k)$ (*polynomial time*),
- $\mathrm{NP} = \bigcup_{k=0}^{\infty} \mathrm{NTIME}(n^k)$ (*nondeterministic polynomial time*),
- $\mathrm{SUBEXP} = \bigcap_{k=0}^{\infty} \mathrm{DTIME}(2^{n^{1/k}})$ (*subexponential time*),
- $\mathrm{E} = \bigcup_{k=0}^{\infty} \mathrm{DTIME}(2^{kn})$ (*linear exponential time*),
- $\mathrm{NE} = \bigcup_{k=0}^{\infty} \mathrm{NTIME}(2^{kn})$ (*nondeterministic linear exponential time*),
- $\mathrm{EXP} = \bigcup_{k=0}^{\infty} \mathrm{DTIME}(2^{n^k})$ (*exponential time*), and
- $\mathrm{NEXP} = \bigcup_{k=0}^{\infty} \mathrm{NTIME}(2^{n^k})$ (*nondeterministic exponential time*).

Advice classes (a special case of nonuniform complexity classes) are complexity classes in which the decision algorithm has access to a string called the *advice string* which only depends on the length of the input. For example, any language can be decided in exponential time with one bit of advice (EXP/1): for any set L, code $x \in A$ in the single bit at length x (which can be accessed in exponential time).

Similarly, any language is contained in $\mathrm{P}/2^n$, by just coding membership of the 2^n strings of length n in an advice string of length 2^n. This example illustrates one of the problems with the traditional definition of advice strings. Usually, advice classes are defined in such a way that the advice string counts towards the input size. With that interpretation an algorithm deciding a language in $\mathrm{P}/2^n$ is effectively allowed to take exponential time rather than polynomial time (in the input x that is to be decided). While this does not matter in this particular case, it does make a difference for subexponential advice which we need for this paper.

To avoid this anomaly, we will follow the convention that the advice string is not an input, but instead is accessed like an oracle via random access. That is, a machine taking advice has an additional tape on which the algorithm can write the address of a bit in the advice string, and it will get the answer on the same tape, after entering a special advice string query state. Consequently the advice string will not be considered part of the input. We now say $L \in \mathrm{DTIME}(f)/g$ if there is a sequence of advice strings s_n such that $|s_n| \leq g(n)$ for all n, and an advice machine that runs in time $O(f)$ (independently of the advice strings used) such that the machine decides membership in L correctly if as advice we use the strings s_n.

With this convention we can define $\mathrm{P/subexp} = \bigcap_{\varepsilon>0} \mathrm{P}/2^{n^\varepsilon}$. Note that our new convention does not affect the extension of the popular nonuniform complexity classes such as P/poly, or P/1.

In its most general form a polynomial-time reduction from a set A to a set B is an oracle Turing machine $T^{(\cdot)}$ such that for some polynomial p and all x:

- the computation of $T^B(x)$ terminates in at most $p(|x|)$ steps, and
- $T^B(x) \in \{0,1\}$, and
- $x \in A$ if and only if $T^B(x) = 1$.

Such a reduction is called a *polynomial-time Turing reduction (Cook reduction).* Note that we can assume that the oracle Turing machine fulfills the first two conditions for every oracle by adding a clock and replacing bad outputs (arbitrarily) with a zero.

The stronger reductions we will consider in the rest of the paper are special cases of the polynomial-time Turing reduction. A reduction $T^{(\cdot)}$ is called *positive* if $T^A(x) = 1$ implies $T^B(x) = 1$ for all A and B fulfilling $A \subseteq B$.

The class PF contains the *polynomial-time computable functions*, namely functions that are computed by a Turing-machine running in polynomial time. The notion of a function computable in nondeterministic polynomial time is made precise using the notion of a transducer. A *transducer* is a nondeterministic Turing machine with a read-only input tape, a write-only output tape, and any number of worktapes. We say that a transducer computes a value y on input x if there is an accepting computation of the transducer on input x that terminates with y on the output tape. If there is no accepting computation we say that the transducer does not compute a value on x. Transducers compute relations, also called multi-valued, partial functions. We will use the symbol $\uparrow$ for the undefined value. The collection of multi-valued, partial functions computed by transducers is called NPMV. The collection of single-valued, partial functions computed by transducers is called NPSV (for a survey of these and related notions see [Sel96]).

Some short remarks on notation: honest reductions will be marked by an h added to the the reduction sign. For example $A \leq^{\mathrm{h}}_{\mathrm{btt}} B$ means that A honest bounded truth-table reduces to B.

Furthermore all reductions in this paper (unless stated otherwise) are polynomial time reductions, which is not reflected in the notation.

We use the usual set-theoretic notation. We define the *join* of two sets A and B as $A \oplus B = \{2x : x \in A\} \cup \{2x+1 : x \in B\}$, and use $\dot\cup$ for a disjoint union. The notation $A =^* B$ means that A and B are equal with only finitely many exceptions.

The *domain* of a (partial) function f is the set of values for which the function is defined: $\mathrm{dom}(f) = \{x : f(x) \neq\uparrow\}$. In general we will assume functions to be total. For functions from Σ^* to $(\Sigma^*)^{<\omega}$ we will write $f(x) = (y_1, \ldots, y_m)$. We think of $y_1, \ldots, y_m$ as the queries made by some reduction on input x. The *characteristic function* $\chi_A(x)$ is 1 if $x \in A$, and 0 otherwise. Extending this notation to vectors we obtain the *characteristic vector* $\chi_A(f(x)) = \chi_A(y_1, \ldots, y_m) = (\chi_A(y_1), \ldots, \chi_A(y_m))$ with $f(x)$ as above. Sometimes we want to ignore the order of the elements in $f(x)$, and consider it as a set of its elements. To avoid confusion we introduce the notation $f\{x\} = \{y_1, \ldots, y_m\}$ (when $f(x) = (y_1, \ldots, y_m)$).

We will occasionally refer to concepts from computability without actually defining them, since they only serve as illustration and are not essential. The interested reader will find the missing definitions in either Odifreddi [Odi89] or Soare [Soa87]. As references for complexity theory we mention Balcázar, Diaz, Gabarró [BDG88] and Papadimitriou [Pap94].

3 Immunity and Simplicity

The concepts of immunity and simplicity have a long tradition in computability theory starting with Post's paper [Dav65]. In computability a set is called *immune* if it is infinite and does not contain an infinite c.e. subset. A c.e. set is called *simple* if its complement is immune.

Definition 3.1 *A set is $\mathcal{C}$-*immune *if it is infinite and does not contain an infinite subset which lies in $\mathcal{C}$. A set is $\mathcal{C}$-*simple *if it is in $\mathcal{C}$ and its complement is $\mathcal{C}$-immune.*

If $\mathcal{C}$ is closed under polynomial time isomorphisms, then $\mathcal{C}$-immunity and $\mathcal{C}$-simplicity are invariant under polynomial time isomorphisms. In particular NP-immunity and NP-simplicity can be used to tackle the isomorphism conjecture, and these notions might prove more flexible than sparseness. Historical background on NP-immunity and NP-simplicity can be found in the second volume of Balcázar *et al.* [BDG88] from which the above definition is taken. Note that this book (like some others) abbreviates NP-simple to simple. To avoid confusion with computability theory we will use NP-immune and NP-simple in this paper.

NP-immune sets exist: any immune set (in the sense of computability) is NP-immune. The case with NP-simple sets is more difficult, and the known results are all oracle results. Homer and Maass [HM83] and, later, Balcázar [Bal85] proved that relative to some oracle an NP-simple set exists. Recently it was shown by Vereshchagin [Ver94] that an NP-simple set exists relative to a random oracle. More on this topic can be found in Section 9 on relativizations. Apart from the observation that the existence of an NP-simple set implies that NP $\neq$ coNP, our knowledge about the existence of NP-simple sets is very limited. In particular we do not know of any probable combination of assumptions that would entail the existence (or nonexistence) of an NP-simple set. Homer [Hom86] tried to circumvent the problem by introducing k-simple sets in analogy with the k-creative sets of Joseph and Young [JY85]. We will not pursue this line of research here.

For dealing with bounded truth-table reductions we introduce a variant of NP-immunity. Remember that NPSV is the class of partial single-valued functions computable by an NP-machine.

We call $f : \Sigma^* \to (\Sigma^*)^k$ in NPSV with infinite domain an *honest np-k-array*, if there is a polynomial p such that $p(|y|) \geq |x|$ for all x, and $y \in f\{x\}$ (see Section 2 for an explanation of the notation $f\{x\}$).

Note that it would not have made a difference in the definition if instead of NPSV we had used NPMV. In view of the use we make of this notion, the NPSV definition seems to be the most natural.

Definition 3.2 *A set A is called* NP-k-immune, *if it is infinite and there is no honest np-k-array f such that $A \cap f\{x\} \neq \emptyset$ for all $x \in \mathrm{dom}(f)$.*

The honesty condition implies that NP-1-immunity is the same as NP-immunity. Furthermore it is immediate from the definition that any NP-$(k+1)$-immune set is also NP-k-immune. The interest in NP-k-immunity stems from its connection with NP-simplicity:

Lemma 3.3 *If A is* NP*-simple, then $\overline{A}$ is* NP*-k-immune for every k.*

The computability version of this lemma is a folklore result [FS99, Lemma 2.2] and the lemma itself is implicit in Yamakami's manuscript [Yam95]. For sake of completeness we include a proof.

Proof. Assume that $A \in$ NP, and there is an honest np-k-array $f \in$ NPSV such that $\overline{A} \cap f\{x\} \neq \emptyset$ for all $x \in \mathrm{dom}(f)$. Let $m = \limsup_{x \in \Sigma^*} |A \cap f\{x\}|$. By assumption $0 \leq m < k$. Consider the set $S = \{y : y \in f\{x\}, \text{ and } f\{x\} \setminus \{y\} \text{ contains at least } m \text{ elements in } A\}$. Then S is infinite because f is honest and has infinite domain, $S \in$ NP, since A is in NP and f is an honest function in NPSV. Finally S is a subset of $\overline{A}$ except for finitely many elements, hence A is not NP-simple. □

NP-immunity, NP-k-immunity and NP-simplicity will not carry us beyond bounded truth-table reductions, not surprisingly in view of the situation in computability. The need arises for a new concept which corresponds to hyperimmunity from computability theory. We relax the cardinality condition we introduced for np-k-arrays.

Call a partial NPSV function $f : \Sigma^* \to (\Sigma^*)^{<\omega} \setminus \{()\}$ with infinite domain an *honest np-array*, if there is a polynomial p such that $p(|y|) \geq |x|$ for all x, and $y \in f\{x\}$. In other words f is honest in all outputs.

Definition 3.4 *A set A is called* NP-hyperimmune, *if it is infinite and there is no honest np-array f such that $A \cap f\{x\} \neq \emptyset$ for all $x \in \mathrm{dom}(f)$. Call a set* NP-hypersimple *it is is in* NP *and its complement is* NP*-hyperimmune.*

It is clear from the definition that being NP-hyperimmune implies being NP-k-immune for every k, and hence an NP-hypersimple set is NP-simple, but probably not vice versa, as will be argued in the section on relativizations.

To summarize

$$\text{NP-hyperimmune} \Rightarrow \text{NP-}(k+1)\text{-immune} \Rightarrow \text{NP-}k\text{-immune} \Rightarrow \text{NP-1-immune} = \text{NP-immune},$$

and

$$\text{NP-hypersimple} \Rightarrow \text{NP-simple} \Rightarrow \text{complement is NP-}k\text{-immune}.$$

At this point we should ask how much farther we can take effective thinness. In analogy with computability, we could call a set A NP-*maximal* if it is infinite and has no superset in NP which differs infinitely often from both A and Σ^*. NP-maximal sets, however, do no exist. This follows from a result of Breidbart's on splittings by P-sets: for any infinite, coinfinite and computable set A there is a set $B \in \mathrm{P}$ such that all of $A \cap B$, $A \cap \overline{B}$, $\overline{A} \cap B$ and $\overline{A} \cap \overline{B}$ are infinite. The link to NP-maximality was observed by Homer and Maass [HM83].

4 Inseparability

Inseparability was first used by Rosser [Dav65] in 1936 in connection with extensions of Gödel's Theorem. Since then it has been quite successful as a clean and easy tool to deal with reductions [FS99]. We will see that the same is true for the complexity theoretic setting.

Definition 4.1 *Two disjoint sets A and B are called $\mathcal{C}$-inseparable, if there is no $C \in \mathcal{C}$ for which $A \subseteq C \subseteq \overline{B}$.*

If $\mathcal{C}$ is taken as the class of computable sets, and A and B are required to be c.e., then $\mathcal{C}$-inseparability corresponds to the classical notion of computable inseparability. Here we are interested in NP-sets which are not separated by any set of low time complexity. Grollmann and Selman, for example, showed that there are NP-sets which are not separated by any polynomial time computable set unless $\mathrm{P} = \mathrm{UP}$, which is considered unlikely.

Fact 4.2 (Grollmann and Selman [GS88]) *If* $\mathrm{P} \neq \mathrm{UP}$ *then there are two disjoint* NP*-complete sets which are not separated by any set in* P*.*

We can generalize this result from P to all reasonable classes $\mathcal{C}$, where a nonempty class of subsets of Σ^* is called *reasonable* if it is closed downward under polynomial time truth-table reducibilities for which all queries (on an input) have the same length.

Lemma 4.3 *If* $\mathrm{UP} \not\subseteq \mathcal{C}$ *for a reasonable class $\mathcal{C}$, then there are two disjoint* NP*-complete sets which are $\mathcal{C}$-inseparable.*

Proof. If $\mathrm{UP} \not\subseteq \mathcal{C}$, then we can choose a set $C \in \mathrm{UP} \setminus \mathcal{C}$. Since $C \in \mathrm{UP}$ there is a set $D \in \mathrm{P}$ and a polynomial p such that $x \in C$ if and only if $(\exists y)[|y| = p(|x|)$ and $\langle x, y\rangle \in D]$. Furthermore for all $x \in C$ there is exactly one such y. Now define

$$A = \{\langle x, i, b\rangle : (\exists y)[|y| = p(|x|), \langle x, y\rangle \in D, |i| = \lceil \log p(|x|)\rceil \text{ and } y_i = b\},$$

and

$$B = \{\langle x, i, b\rangle : (\exists y)[|y| = p(|x|), \langle x, y\rangle \in D, |i| = \lceil \log p(|x|)\rceil \text{ and } y_i = \overline{b}\},$$

where y_i is the ith bit of y, interpreting the string i as a number. It is clear from the definition that A and B are disjoint sets in NP (even UP). Furthermore any separator of A and B in $\mathcal{C}$ would allow us to decide C in $\mathcal{C}$ by making a polynomial number of truth-table queries (all of the same length) to the separator.

It is then straightforward to see that $A \times \mathrm{SAT}$ and $B \times \mathrm{SAT}$ are two disjoint NP-complete sets. Suppose there was a separator $C' \in \mathcal{C}$ such that $A \times \mathrm{SAT} \subseteq C' \subseteq \overline{B \times \mathrm{SAT}}$. Let $f(x) = (x, \top)$. Then $C = f^{-1}(C')$ is in $\mathcal{C}$ (since $\mathcal{C}$ is reasonable), and C separates A and B contradicting their construction. This easy way of converting A and B into complete sets was first observed by Dubhashi [Dub89]. Grollmann and Selman [GS88] use a similar construction which additionally allows us to let A (or B) be any specific m-complete set. □

If $\mathcal{C}$ is not reasonable the above construction does not apply, and we have to fall back on a trivial observation (mentioned by Dubhashi). If $A \in \mathrm{NP} \cap \mathrm{coNP} \setminus \mathcal{C}$ then A and $\overline{A}$ are $\mathcal{C}$-inseparable sets in NP.

Lemma 4.4 *If* $\mathrm{NP} \cap \mathrm{coNP} \not\subseteq \mathcal{C}$*, then there are two disjoint sets in* $\mathrm{NP} \cap \mathrm{coNP}$ *which are* $\mathcal{C}$*-inseparable.*

For the purposes of this paper we shift our focus from the inseparable sets themselves to the sets separating them.

Definition 4.5 *We call a set E a $\mathcal{C}$-*separator *if it separates a $\mathcal{C}$-inseparable pair of disjoint sets in* NP*, i.e. there are disjoint sets A and B in* NP *that are $\mathcal{C}$-inseparable and $A \subseteq E \subseteq \overline{B}$. We will write p-*separator *instead of* P*-separator, and s-*separator *for any* $\mathrm{DTIME}(2^{n^\varepsilon})$*-separator (where $\varepsilon > 0$).*

The purpose of p-separators is to deal with honest reductions. The result of Grollmann and Selman tells us that p-separators exist if $\mathrm{UP} \not\subseteq \mathrm{P}$. For reductions that are not necessarily honest we need a stronger kind of separator, a subexponential time separator. However, SUBEXP-separators turn out to be insufficient which is why we introduced the stonger concept of an s-separator. The proof of Lemma 4.3 actually yields the existence of s-separators, under the hypothesis $\mathrm{UP} \not\subseteq \mathrm{SUBEXP}$.

Corollary 4.6 *If* $\mathrm{UP} \not\subseteq \mathrm{SUBEXP}$*, then there are two disjoint* NP*-sets A and B, and an $\varepsilon > 0$ such A and B are* $\mathrm{DTIME}(2^{n^\varepsilon})$*-inseparable, i.e. an s-separator exists.*

Proof. Consider the set C from the proof of Lemma 4.3. Since $C \notin \mathrm{SUBEXP}$, there is an $\varepsilon > 0$ such that $C \notin \mathrm{DTIME}(2^{n^\varepsilon})$. Suppose there was a set $E \in \mathrm{DTIME}(2^{n^{\varepsilon/2}})$ separating A and B as defined in the proof. Then $x \in C$ can be decided by making at most $p(|x|)$ queries to E of length at most $|x| + (\log p(|x|)) + 1$. This would imply $C \in \mathrm{DTIME}(2^{n^\varepsilon})$. □

The relationships between some of the assumptions mentioned above in the case that $\mathcal{C} = \mathrm{P}$ are discussed by Fortnow and Rogers [FR94]. Grollmann and Selman [GS88] showed that a secure public-key cryptosystem exists (i.e. one which cannot be cracked in polynomial time) only if p-separators exist. Homer and Selman [HS92] constructed an oracle relative to which all Σ_2^p complete sets are polynomial time isomorphic, and no p-separators exist. Beigel, Buhrman, and Fortnow [BBF98] showed that there is an oracle relative to which the isomorphism conjecture holds, and p-separators exist. Relative to any oracle for which $\mathrm{P} = \mathrm{PSPACE}$ the isomorphism conjecture is true, and p-separators do no exist.

5 Disjunctive reductions and m-reductions

This section is mainly intended for warming up and serves to illustrate the basic ideas. The case of honest disjunctive reductions is perhaps the easiest result. Our definition of an honest disjunctive reduction might not be considered standard which is why we include it below.

Definition 5.1 *A set A* honest disjunctively reduces (h-d reduces) to B in polynomial time *(or $A \leq_{\rm d}^{\rm h} B$ for short), if there is a polynomial time computable function f such that f maps Σ^* to $(\Sigma^*)^{<\omega} \dot\cup \{\top\}$, and $x \in A$ if and only if $B \cap f\{x\} \neq \emptyset$ or $f(x) = \top$ (for all x), and there is a polynomial p such that $p(|y|) \geq |x|$ for all x, and $y \in f\{x\}$ (i.e. f is a polynomially honest function with regard to its outputs in $(\Sigma^*)^{<\omega}$).*

With this definition it is possible that f is the empty set or equals the constant $\top$. The reduction can exploit this to get around the honesty condition for cases it can decide easily by itself without querying B. This feature is not standard.

Lemma 5.2 *If E is a p-separator, and $E \leq_{\rm d}^{\rm h} M$, then $\overline{M}$ is not* NP*-immune.*

Proof. Let f be the function witnessing the reduction from E to M, and let E separate the two NP sets A and B. Then $f\{x\} \subseteq \overline{M}$ for all $x \in B$. Note that infinitely often $f\{x\} \neq \emptyset$, since otherwise we could separate A and B by a set in P. Since f is polynomially honest in these cases, we can define an infinite NP subset of $\overline{M}$. □

If P $\neq$ UP then there is a p-separator $E \in$ NP (take one of the P-inseparable set). Suppose now that M is NP-hard under honest disjunctive reductions. Then $E \leq_{\rm d}^{\rm h} M$, and $\overline{M}$ is not NP-immune by Lemma 5.2. This establishes the next theorem.

Theorem 5.3 *No set h-d-hard for* NP *has an* NP*-immune complement (let alone is* NP*-simple) unless* P = UP*.*

To eliminate the honesty condition we will make use of the stronger premise that s-separators exist. The next proof illustrates in a nutshell how s-separators are used to force the reduction to be sufficiently honest.

Lemma 5.4 *If E is an s-separator, and $E \leq_{\rm d} M$, where $M \in$* EXP*, then $\overline{M}$ is not* NP*-immune.*

Proof. Let f be the reduction from E to $M \in {\rm DTIME}(2^{n^k})$, and let E be an s-separator with regard to two NP sets A and B which are ${\rm DTIME}(2^{n^\varepsilon})$-inseparable for some $\varepsilon > 0$. Define $g(x)$ to be the largest string in $f\{x\}$. Then $g(x) \in \overline{M}$ for all $x \in B$. There are two cases.

(i) There is a polynomial p and infinitely many $x \in B$ such that $p(|g(x)|) \geq |x|$.

(ii) For every polynomial p there are at most finitely many $x \in B$ for which $p(|g(x)|) \geq |x|$.

In case (i) the set $S = \{y : (\exists x \in B)[p(|y|) \geq |x| \text{ and } y = g(x)\}$ is an infinite NP subset of $\overline{M}$.

In case (ii) consider $p(n) = n^{2k/\varepsilon}$. Let $F = \{x \in B : p(|g(x)|) \geq |x|\}$, and $E' = \{x : p(|g(x)|) < |x|, \text{ and } f\{x\} \subseteq \overline{M}\} \cup F$. By definition $A \subseteq \overline{E'} \subseteq \overline{B}$. If $p(|g(x)|) \leq |x|$ then all strings in $f\{x\}$ have length less than $|x|^{\varepsilon/(2k)}$, hence membership in M for each can be decided in time $2^{|x|^{\varepsilon/2}}$. Hence $f\{x\} \subseteq \overline{M}$ can be decided in time $|f\{x\}|2^{|x|^{\varepsilon/2}} = O(2^{n^\varepsilon})$. Since F is finite this implies that $E' \in {\rm DTIME}(2^{n^\varepsilon})$ contradicting the choice of A and B. □

Lemma 5.4 together with Corollary 4.6 implies the following theorem.

Theorem 5.5 *No set in* EXP *which is d-hard for* NP *can have an* NP*-immune complement unless* UP $\subseteq$ SUBEXP*.*

Corollary 5.6 NP*-simple sets are not d-complete for* NP *unless* UP $\subseteq$ SUBEXP*.*

We can also apply Lemma 5.4 to get a result on m-reductions that will be useful later for dealing with 1-tt-reductions.

Lemma 5.7 *If E is an s-separator, and $E \leq_{\mathrm{m}} M$, where $M \in$ EXP, then neither M nor $\overline{M}$ are* NP*-immune (in particular M is not* NP*-simple).*

Proof. Since $E \leq_{\mathrm{m}} M$ implies $E \leq_{\mathrm{d}} M$ we can apply the last lemma to get that $\overline{M}$ is not NP-immune. Since $\overline{E}$ is an s-separator if E is, and $E \leq_{\mathrm{m}} M$ implies that $\overline{E} \leq_{\mathrm{m}} \overline{M}$, we can conclude that M is not NP-immune. □

Corollary 4.6 allows us to draw the following conclusion.

Corollary 5.8 NP*-simple sets are not m-complete for* NP *unless* UP $\subseteq$ SUBEXP*.*

If instead of Corollary 4.6 we use Lemma 4.4 to guarantee the existence of an s-separator we obtain the result that NP-simple sets are not m-complete for NP unless NP $\cap$ coNP $\subseteq$ SUBEXP which was first shown by Hartmanis, Li and Yesha. In fact they managed to combine sparseness with immunity:

Fact 5.9 (Hartmanis, Li and Yesha [HLY86]) *Every m-hard set for* NP *has a dense subset in* NP *unless* NP $\subseteq$ SUBEXP*.*

A set is *dense* if there is an $\varepsilon > 0$ such that $|A^{\leq n}| \geq 2^{n^{\varepsilon}}$ for almost all n.

6 Bounded truth-table reductions

In this section we tackle honest and positive bounded truth-table reductions. The general case of bounded truth-table reductions will be resolved by different methods in the section on truth-table reductions. Let us first define what we mean by an honest bounded truth-table reduction. For the definition let $[\![F]\!]$ equal 1 if F is true, and 0 otherwise.

Definition 6.1 *A set A* honest bounded truth-table reduces (h-btt reduces) to B in polynomial time *(or $A \leq^{\mathrm{h}}_{\mathrm{btt}} B$ for short), if there are two polynomial time computable functions f and α and $k \in \omega$ such that f maps Σ^* to $(\Sigma^*)^k$, α maps $\Sigma^* \times \{0,1\}^k$ to $\{0,1\}$ such that $x \in A$ if and only if $\alpha(x, f(x)) = 1$ (for all x), and f is a polynomially honest function with regard to all k output values.*

Note that for h-btt reductions it is not necessary to relax the honesty condition as we did for h-d reductions. The reason is that a h-btt reduction can let $\alpha(x, \ldots)$ be one of the two trivial truth-tables (always true, always false) so that we can define $f(x) = (x, \ldots, x) \in (\Sigma^*)^k$ in this case.

Fixing truth-tables

Perhaps the most amazing fact about bounded truth-table reductions is that we can assume that we are dealing with one fixed truth-table, rather than having the truth-table depend on the input. This fact was established (in a computability context) by Fischer [Odi89, Proposition III.8.6.]. Our result here is different. We will establish that if a $\mathcal{C}$-separator *btt*-reduces to a set M, then we can assume that there is another $\mathcal{C}$-separator reducing to M via a fixed truth-table without increasing the norm (number of queries) of the reduction. Fischer's result increases the norm by using additional queries to fix the truth-table. Since we want to draw conclusions about 1-*tt*-reductions we cannot apply his result.

For the sake of clarity we include the definition of a (honest) reduction via a fixed truth-table.

Definition 6.2 *Let E and M be arbitrary sets, let $\alpha\colon \{0,1\}^k \to \{0,1\}$ be a k-ary Boolean function, and let f be computable in polynomial time. We say that E* polynomial time α-reduces to M via f *($f\colon E \le_\alpha M$) if there is a polynomial p such that*

- $(\forall x \in E)\ \alpha(\chi_M(f(x))) = 1$*, and*
- $(\forall x \notin E)\ \alpha(\chi_M(f(x))) = 0$*,*

We say that $E \le_\alpha M$ is there exists such an f. If additionally there is a polynomial p such that $p(|y|) \ge |x|$ for all x and $y \in f\{x\}$ we call the reduction honest *and say that E* honest polynomial time α-reduces to M via f *($f\colon E \le_\alpha^{\mathrm{h}} M$) (We say that $E \le_\alpha^{\mathrm{h}} M$ if there exists such an f.)*

We try to formulate the following lemma as general as possible so it applies to both p-separators and s-separators. Call a class $\mathcal{C}$ *fixable* if $\mathcal{C}$ contains P and is closed under finite union and intersection.

Lemma 6.3 *Suppose E is a $\mathcal{C}$-separator for a fixable class $\mathcal{C}$ and M an arbitrary set. If $E \le_{k\text{-tt}} M$, then there is a $\mathcal{C}$-separator $\widetilde{E}$ and a k-ary Boolean function α such that $\widetilde{E} \le_\alpha M$. As a matter of fact, α will be one of the truth-tables used in the reduction from E to M.*

Proof. Let A and B be two $\mathcal{C}$-inseparable NP sets with $A \subseteq E \subseteq \overline{B}$. Since $E \le_{k\text{-tt}} M$, there is a function $f \in \mathrm{PF}$, and a k-ary Boolean function α_x computable in polynomial time in x and its arguments such that

- $(\forall x \in A)\ \alpha_x(\chi_M(f(x))) = 1$, and
- $(\forall x \in B)\ \alpha_x(\chi_M(f(x))) = 0$.

Let $\ell = 2^{2^k}$ and let $\tau_1, \dots, \tau_\ell$ enumerate all k-ary Boolean functions. For $1 \le i \le \ell$, set $T_i = \{x : \alpha_x = \tau_i\}$. All T_i are in P. We claim that there is an i such that $A \cap T_i$ and $B \cap T_i$ are $\mathcal{C}$-inseparable. Assume this is not the case, namely for each i there is a set $E_i \in \mathcal{C}$ for which $A \cap T_i \subseteq E_i \subseteq \overline{B \cap T_i}$. The set $E = \bigcup_{1 \le i \le \ell} E_i \cap T_i$ lies in $\mathcal{C}$ (since $\mathcal{C}$ is fixable), and it separates A and B (since the T_i are a partition of Σ^*). This contradicts the assumption on A and B, and hence we can fix an i such that $\widetilde{A} = A \cap T_i$ and $\widetilde{B} = B \cap T_i$ are $\mathcal{C}$-inseparable, and let $\alpha = \tau_i$, and $\widetilde{E} = \{x : \alpha(\chi_M(f(x)) = 1\}$.
□

The last result allows us to apply our recently gained knowledge about m-reductions.

Lemma 6.4 *If E is an s-separator, and $E \leq_{\text{1-tt}} M$, where $M \in \mathrm{EXP}$, then M is not* NP*-immune.*

Proof. By Lemma 6.3 we can assume that E reduces to M via a fixed truth-table of norm one. There are four possible truth-tables. We can exclude the constant truth-tables since E is not in P. So either $E \leq_{\text{m}} M$ or $\overline{E} \leq_{\text{m}} M$. In both cases neither M nor $\overline{M}$ are NP-immune by Lemma 5.7. □

This lemma together with Lemma 4.3 implies the following theorem.

Theorem 6.5 *No set in* EXP *which is 1-tt-hard for* NP *is* NP*-immune unless* UP $\subseteq$ SUBEXP*.*

Corollary 6.6 NP*-simple sets are not 1-tt-complete for* NP *unless* UP $\subseteq$ SUBEXP*.*

Honest bounded truth-tables

It is not too difficult to show that a set complete under a fixed honest truth-table reduction cannot be NP-simple unless P = UP and then extend this to arbitrary honest bounded truth-table reductions using Lemma 3.3. Somewhat surprisingly the result is true without any assumptions as shown by Manindra Agrawal, whose proof we include here. The proof exploits the fact that if P $\neq$ NP, then $\overline{\text{SAT}}$ is P-*levelable*, i.e. for every subset $A \in \mathrm{P}$ of $\overline{\text{SAT}}$ there is an infinite set $B \in \mathrm{P}$ which is disjoint from A and is also contained in $\overline{\text{SAT}}$ [BDG88, Volume II].

Theorem 6.7 (Agrawal [Agr97]) *An* NP*-simple set is not honest btt-complete for* NP*.*

Proof. If P = NP there is nothing to prove, since in this case there are no NP-simple sets. Hence we can assume that P $\neq$ NP and therefore $\overline{\text{SAT}}$ is P-levelable. Fix an honest *btt*-reduction from SAT to some NP-simple set A, i.e. $x \in \text{SAT}$ if and only if $\alpha_x(\chi_A(f(x))) = 1$, where f computes k (honest) queries and $\alpha_x : \{0,1\}^k \to \{0,1\}$ is a k-ary truth-table computable in polynomial time in x. For $\alpha : \{0,1\}^k \to \{0,1\}$ define $S_\alpha = \{x : \alpha_x = \alpha\} \in \mathrm{P}$. If there is an α for which $\alpha(1^k) = 0$ and $|\text{SAT} \cap S_\alpha| = \infty$ we are done, since we can define an honest np-k-array intersecting $\overline{A}$ as follows: let $g(x) = f(x)$ for $x \in \text{SAT} \cap S_\alpha$, and undefined otherwise. The function g is in NPSV, has infinite domain, and if it is defined, $g\{x\}$ contains an element of $\overline{A}$ (since $\alpha(1^k)$ is false).

We can therefore assume that for all α for which $\alpha(1^k) = 0$ the set $\text{SAT} \cap S_\alpha$ is finite. Hence $S := \bigcup_{\alpha : \alpha(1^k)=0} S_\alpha \in \mathrm{P}$ is a subset of $\overline{\text{SAT}}$ except for finitely many elements. Since $\overline{\text{SAT}}$ is P-levelable there exists an infinite set $S' \in \mathrm{P}$ which is contained in $\overline{\text{SAT}}$ and is disjoint from S. The disjointness from S implies that $\alpha_x(1^k) = 1$ for all $x \in S'$. However, $\alpha_x(\chi_A(f(x))) = 0$ for all $x \in S' \subseteq \overline{\text{SAT}}$ which implies that $f\{x\}$ must contain an element from $\overline{A}$ for all $x \in S'$ which again gives us an honest np-k-array intersecting $\overline{A}$. □

Positive bounded truth-table reductions

Our eventual aim is to extend the result of the last section from honest *btt*-reductions to arbitrary *btt*-reductions. Along the particular path we have chosen this seems difficult and the best we can do at present is to deal with the class of positive *btt*-reductions, which includes bounded disjunctive and bounded conjunctive reductions. In the next section on *tt*-reductions we take a slightly different approach which leads us to a result for general *btt*-reduction, but requires a stronger hypothesis than UP $\not\subseteq$ SUBEXP.

Intuitively, a reduction is positive, if changing answers to queries from no to yes will never turn an accepting computation into a rejecting one. More precisely for truth-table reductions this means that for every truth-table $\alpha : \{0,1\}^k \to \{0,1\}$ generated on some input it is true that if $v \subseteq w$ (where $\subseteq$ is the partial order that compares v and w componentwise) and $\alpha(v) = 1$, then $\alpha(w) = 1$. We write $A \leq_{\mathrm{pbtt}} B$ if A reduces to B by a positive truth-table reduction.

Lemma 6.8 *If E is an s-separator and $E \leq_{\mathrm{pbtt}} M$, then neither M nor $\overline{M}$ is* NP*-simple.*

The lemma will be a consequence of the following lemma, and the observation that if $A \leq_{\mathrm{pbtt}} B$ then $\overline{A} \leq_{\mathrm{pbtt}} \overline{B}$ by using the complementary truth-table. Given a truth-table α, define the *complementary truth-table* $\overline{\alpha}$ by $\alpha(u) = 1$ if and only if $\overline{\alpha}(\overline{u}) = 0$, where $\overline{u}$ is the componentwise negation of the vector u. If α is positive, and $v \subseteq w$, then $\overline{\alpha}(v) = 1$ implies $\alpha(\overline{v}) = 0$, and hence $\alpha(\overline{w}) = 0$ (since $\overline{w} \subseteq \overline{v}$), and therefore $\overline{\alpha}(w) = 1$ showing that the complementary truth-table is again positive.

Lemma 6.9 *If E is an s-separator and $E \leq_{\mathrm{pbtt}} M$, then $\overline{M}$ is not* NP*-simple.*

Proof. Suppose $\overline{M} \in \mathrm{NP}$. Let A and B be disjoint NP sets which are DTIME(2^{n^ε})-inseparable such that $A \subseteq E \subseteq \overline{B}$, and $E \leq_{k\text{-tt}} M$ via a positive reduction. We can reorder the queries of that reduction such that they are in length nondecreasing order, that is, any query can be written as $(y_1, y_2, \dots, y_k)$ with $|y_1| \leq |y_2| \leq \cdots |y_k|$.

By Lemma 6.3 we can assume that there is a fixed positive truth-table α of arity k and a polynomial time computable function f from Σ^* to $(\Sigma^*)^k$ such that $x \in E$ iff $\alpha(\chi_M(f(x))) = 1$. Note that α is positive, since the reduction from E to M is positive. The reduction f also retains the property that if $f(x) = (y_1, y_2, \dots, y_k)$, then $|y_1| \leq |y_2| \leq \cdots |y_k|$.

Consider the set

$$V = \{v \in \{0,1\}^k : \text{ there are infinitely many } x \in A \text{ for which } v = \chi_M(f(x))\}.$$

We will use the partial order $\subseteq$ on V, where $v \subseteq w$ if $v_i = 1$ implies $w_i = 1$ for all $1 \leq i \leq k$.

For $v \in \{0,1\}^k$ define $A_v = \{x \in A : \chi_M(f(x)) = v\}$. Note that $A =^* \bigcup_{v \in V} A_v$, since A_v is finite for $v \notin V$. By one(v) we denote the position of the rightmost 1 in v. Then $1 \leq \mathrm{one}(v) \leq k$ for $v \in V$, since V does not contain 0^k (otherwise the truth-table would be constantly true since the reduction is positive).

We will prove that for every $v \in V$ either A_v is separable from B by a set in DTIME(2^{n^ε}), or there is an infinite subset of M in NP. If all of the A_v were DTIME(2^{n^ε})-separable from B then $A =^* \bigcup_{v \in V} A_v$ would be DTIME(2^{n^ε})-separable from B which contradicts the assumption (consider the union of the separators). Hence there is an infinite subset of M in NP.

Fix any $v \in V$. Define the set

$$C = \{x \in A : f(x) = (y_1, \dots, y_k), \text{ and for all } 1 \leq j \leq k, \text{if } v_j = 0 \text{ then } y_j \in \overline{M}\}.$$

Then $C \in \mathrm{NP}$, since $\overline{M} \in \mathrm{NP}$, and furthermore C contains A_v.

Let $1 \leq i \leq k$ be minimal such that there is a polynomial p for which the set

$$D_{i,p} = \{x \in A : f(x) = (y_1, \dots, y_k), \text{ and for all } 1 \leq j \leq k, \text{if } v_j = 0 \text{ then } y_j \in \overline{M}, \text{ and } p(|y_i|) \geq |x|\}$$

is infinite. If one(v) $< i$, or i does not exist, then $D_{\mathrm{one}(v),p}$ is finite for any choice of a polynomial p.

In this case we claim that A_v and B are separated by a set in DTIME(2^{n^ε}). Fix $p(n) = n^{2k/\varepsilon}$ (where $M \in$ DTIME(2^{n^k})), and with that choice let

$$C' = \{x : f(x) = (y_1, \dots, y_k),\ \text{and for all}\ 1 \leq j \leq \text{one}(v), \text{if}\ v_j = 0\ \text{then}\ y_j \in \overline{M},\ \text{and}\ p(|y_{\text{one}(v)}|) < |x|\},$$

and $C'' = D_{\text{one}(v),p} \cup C'$.

If $x \in C$, then either $p(|y_{\text{one}(v)}|) < |x|$, or $p(|y_{\text{one}(v)}|) \geq |x|$, hence $x \in D_{\text{one}(v),p} \cup C' = C''$ (where $f(x) = (y_1, \dots, y_k)$). Now $B \cap D_{\text{one}(v),p} = \emptyset$, since $D_{\text{one}(v),p} \subseteq A$. Furthermore $B \cap C' = \emptyset$, since $v \in V$, there are zeroes in v to the right of one(v), and the reduction is positive. Putting things together we have $B \cap C'' = \emptyset$, and therefore $A_v \subseteq C'' \subseteq \overline{B}$. Since $C' \in$ DTIME(2^{n^ε}) (we only have to test $y \in M$ for k values of y where $|y|^{2k/\varepsilon} < |x|$), and $D_{\text{one}(v),p}$ is finite we get that $C'' \in$ DTIME(2^{n^ε}), contradicting that A_v and B are not DTIME(2^{n^ε})-separable.

Hence we can assume that $i \leq \text{one}(v)$ and p exist. Fix them, and define

$$g(x) = \begin{cases} (y_i, \dots, y_k) & \text{if}\ x \in D_{i,p},\ \text{and}\ f(x) = (y_1, \dots, y_k)\}, \\ \uparrow & \text{else.} \end{cases}$$

Then g is an honest np-$(k - i + 1)$-array. If $g\{x\} \cap M \neq \emptyset$ for all but finitely many $x \in \text{dom}(g)$, then Lemma 3.3 assures us that $\overline{M}$ is not NP-simple, and we are done. So suppose for a contradiction that there are infinitely many $x \in \text{dom}(g)$ such that $g\{x\} \cap M = \emptyset$. Then there is a $w \in V$ with $w \subseteq v$ and one$(w) < i$ for which

$$\{x \in A : f(x) = (y_1, \dots, y_k), \chi_M(f(x)) = w,\ \text{and}\ p(|y_i|) \geq |x|\}$$

is infinite. Since i was minimal we can conclude that for all polynomials q, and for almost all $x \in C$ we have $q(|y_{\text{one}(w)}|) < |x|$ where $f(x) = (y_1, \dots, y_k)$. Since C contains A_v we know that for all polynomials q, and for almost all $x \in A_v$ it is true that $q(|y_{\text{one}(w)}|) < |x|$ where $f(x) = (y_1, \dots, y_k)$. Since $\alpha(z) = 1$ for every z with $w \subseteq z$ we can define an s-separator which separates A_v from B as above. Let $q(n) = n^{2k/\varepsilon}$, and

$$C' = \{x : f(x) = (y_1, \dots, y_k),\ \text{and for all}\ 1 \leq j \leq \text{one}(w), \text{if}\ v_j = 0\ \text{then}\ y_j \in \overline{M},\ \text{and}\ q(|y_{\text{one}(w)}|) < |x|\},$$

and $C'' = D_{\text{one}(w),p} \cup C'$. As above C'' witnesses that A_v and B are DTIME(2^{n^ε})-separable which is a contradiction. □

Since s-separators exist, unless UP $\subseteq$ SUBEXP, we obtain the following theorem.

Theorem 6.10 *An* NP-*simple set is not positive btt-hard for* NP *unless* UP $\subseteq$ SUBEXP.

7 Truth-table and Turing reductions

We have already dealt with the special cases of disjunctive and conjunctive reductions earlier on. In this section we will study truth-table and Turing reductions. For these we do not expect results regarding NP-simplicity or even NP-immunity (Section 9 contains a contrary relativization). Instead we will make use of NP-hyperimmunity.

For truth-table reductions we cannot hope to prove the very convenient Lemma 6.3 which allowed us to consider fixed truth-tables only. This makes a new approach necessary. The main inspiration comes from Denisov's proof [Odi89, Exercise III.6.23] that if B is part of a computably inseparable pair of c.e. sets, and B (computably) truth-table reduces to A, then A is not hyperimmune.

As in the bounded case the proof for the honest case is easy and goes through with Turing reductions. We will present this result next. The case for general truth-table reductions is still open, but we present a result for $o(\log n)$-*tt* reductions, which also helps to settle the bounded truth-table case.

Honest Turing reductions

The definition of a honest Turing reduction is quite straightforward.

Definition 7.1 *A set A* honest Turing reduces (h-T reduces) to B in polynomial time *(or $A \leq^{\mathrm{h}}_{\mathrm{T}} B$ for short), if there is a polynomial p and an oracle Turing machine $T^{(\cdot)}$ running in time $p(|x|)$ on input x such that $x \in A$ if and only if $T^B(x) = 1$. Furthermore if $Q(x)$ denotes the set of queries made by T to B in the computation of $T^B(x)$, then $p(|w|) \geq |x|$ for every $w \in Q(x)$, i.e. the machine only makes honest queries.*

Since we have a bound on the running time we can assume that $T^{(\cdot)}$ always halts in at most $p(|x|)$ steps on input x with output 0 or 1 and only makes honest queries regardless of the oracle. The bound on the running time is the main difference between Turing reductions in computability and complexity, and it leads to the fact that in complexity we can deal with Turing reductions using only hyperimmunity, whereas in computability not even maximality is good enough (there are Turing complete maximal sets [Odi89, Soa87]).

Theorem 7.2 *An* NP*-hyperimmune set cannot be honest Turing hard for* NP *unless* P = UP*.*

The theorem follows from the next lemma together with Lemma 4.3, and the observation that P = UP if and only if UP $\subseteq$ P/2 (using self-reducibility). Note that to apply Lemma 4.3 the class P/2 has to be closed under *tt*-reductions making queries of one length only. This is the case since the advice string only depends on the length of the input.

Lemma 7.3 *If E is a* P/2*-separator, and $E \leq^{\mathrm{h}}_{\mathrm{T}} M$, then M is not* NP*-hyperimmune.*

Proof. Let E separate $A, B \in$ NP where A and B are not separated by any set in P/2, and $E \leq^{\mathrm{h}}_{\mathrm{T}} M$. Let T be an oracle Turing machine running in polynomial time $p(n)$ which witnesses the reduction, i.e. $x \in E \Rightarrow T^M(x) = 1$ and $x \in \overline{E} \Rightarrow T^M(x) = 0$. We can assume that $T^{(\cdot)}$ always halts in at most $p(|x|)$ steps on input x outputting 0 or 1, and is honest (with respect to the queries it makes) for all oracles. For an input x let $Q(x)$ be the set of queries made by $T^{\emptyset}(x)$.

There are two cases. First consider the case that there are infinitely many n with $x \in A$, and $y \in B$ of length n such that $T^{\emptyset}(x) = T^{\emptyset}(y)$. Fix such an n, x and y. Since $T^M(x) \neq T^M(y)$ one of these values has to be different from $T^{\emptyset}(x) = T^{\emptyset}(y)$. Therefore $M \cap (Q(x) \cup Q(y))$ cannot be empty. With an NPSV function on an input string $z = xy$, where $|x| = |y|$ we can verify that $x \in A$, $y \in B$, and $T^{\emptyset}(x) = T^{\emptyset}(y)$ and then output $Q(x) \cup Q(y)$, which gives us an honest np-array since the queries in Q are honest.

In the other case we know that for almost all n, and all $x \in A$ and $y \in B$ of length n it is true that $T^{\emptyset}(x) \neq T^{\emptyset}(y)$. We can use this to separate A from B by coding for each length n the possible values of $T^{\emptyset}(x)$ for $x \in A$ of length n. Let $O_n = \{T^{\emptyset}(x) : |x| = n\}$, and

$$s_n = \begin{cases} 00 & \text{if } O_n = \{\}, \\ 01 & \text{if } O_n = \{1\}, \\ 10 & \text{if } O_n = \{0\}, \\ 11 & \text{if } O_n = \{0,1\}. \end{cases}$$

Then $C = \{x : T^{\emptyset}(x) \in O_n\}$ separates A and B (except for finitely many lengths), and can be decided in P/2 (using s_n as advice). □

The theorem can be proved without using nonuniform advice, but we prefer this version because it illustrates the basic structure of the more involved Lemma 7.5.

$o(\log n)$-*tt* reductions

A $o(\log n)$-*tt* reduction is a truth-table reduction which on input x makes at most $o(\log |x|)$ queries. In particular this includes bounded truth table reductions. We establish the following result.

Theorem 7.4 *An* NP*-hyperimmune set cannot be* $o(\log n)$*-tt-hard for* NP *unless* UP ∩ coUP ⊆ SUBEXP*.*

As in the case of honest Turing reductions we will make use of nonuniform complexity classes. Call E a $s[1]$-separator, if E separates two disjoint NP-sets that are not separated by any set in $\mathrm{P}/2^{n^{\varepsilon}}[1]$ (for some $\varepsilon > 0$). $\mathrm{P}/2^{n^{\varepsilon}}[1]$ is the variant of $\mathrm{P}/2^{n^{\varepsilon}}$ in which at most one query to the advice string is allowed (per input).

The most important step in the proof is the next lemma.

Lemma 7.5 *If E is a $s[1]$-separator and $E \leq_{o(\log n)-\mathrm{tt}} M$, then M is not* NP*-hyperimmune.*

Proof. Since $E \leq_{o(\log n)-\mathrm{tt}} M$ there are polynomial time computable functions f and α such that for all x:

$$x \in E \iff \alpha_x(\chi_M(f(x))) = 1.$$

Let $(\Sigma^*)^{\leq n}$ denote the set of all strings of length at most n. Since E is a $s[1]$-separator there is an $\varepsilon > 0$, and two $\mathrm{P}/2^{n^{3\varepsilon}}[1]$-inseparable sets A and B in NP with $A \subseteq E \subseteq \overline{B}$. There are two cases to consider.

First, suppose that there exist infinitely many n for which there are $x \in A$ and $y \in B$ with $|x| = |y| = n$ such that $f\{x\} \cap (\Sigma^*)^{\leq n^{\varepsilon}} = f\{y\} \cap (\Sigma^*)^{\leq n^{\varepsilon}}$, and

$$(\forall F \subseteq (\Sigma^*)^{\leq n^{\varepsilon}})\ [\alpha_x(\chi_F(f(x))) = \alpha_y(\chi_F(f(y)))]. \tag{1}$$

Then we can define an NPSV function as follows. On input $z = xy$, where $|x| = |y| = n$ verify that $x \in A$, $y \in B$, and that $f\{x\} \cap (\Sigma^*)^{\leq n^{\varepsilon}}$ and $f\{y\} \cap (\Sigma^*)^{\leq n^{\varepsilon}}$ are equal. Let D be the set of those queries, i.e. $D = f\{x\} \cap (\Sigma^*)^{\leq n^{\varepsilon}} = f\{y\} \cap (\Sigma^*)^{\leq n^{\varepsilon}}$. Verify that for all $F \subseteq D$ it is true that $\alpha_x(\chi_F(f(x))) = \alpha_y(\chi_F(f(y)))$. If this is the case output $(f\{x\} \cup f\{y\}) \setminus (\Sigma^*)^{\leq n^{\varepsilon}}$.

Note that the algorithm described above is indeed in NPSV, as D is of size at most $\log n$ and we have to check no more than n subsets, each in polynomial time. By assumption the algorithm will try infinitely often to output $(f\{x\} \cup f\{y\}) \setminus (\Sigma^*)^{\leq n^\varepsilon}$, which is honest if nonempty. So we only have to prove that $(f\{x\} \cup f\{y\}) \setminus (\Sigma^*)^{\leq n^\varepsilon}$ contains a string in M. We know that for all $F \subseteq D$ it is true that $\alpha_x(\chi_F(f(x))) = \alpha_y(\chi_F(f(y)))$. But then (1) has to hold, since D contains all the queries f makes on x and y of length at most n^ε. Hence if we let $M' = M \cap (\Sigma^*)^{\leq n^\varepsilon}$ it follows that $\alpha_x(\chi_{M'}(f(x))) = \alpha_y(\chi_{M'}(f(y)))$. At the same time $\alpha_x(\chi_M(f(x))) \neq \alpha_y(\chi_M(f(y)))$ since x belongs to A and y to B. So M' and M have to disagree on a query in $(f\{x\} \cup f\{y\}) \setminus (\Sigma^*)^{\leq n^\varepsilon}$. Since M' is empty above length n^ε it follows that M contains a string in $(f\{x\} \cup f\{y\}) \setminus (\Sigma^*)^{\leq n^\varepsilon}$. Hence M is not NP-hyperimmune.

If the first assumption does not apply, it must be true that for almost all n, and all $x \in A$, $y \in B$ with $|x| = |y| = n$ either the sets $f\{x\} \cap (\Sigma^*)^{\leq n^\varepsilon}$ and $f\{y\} \cap (\Sigma^*)^{\leq n^\varepsilon}$ are not the same, or the truth-tables α_x and α_y are different on a set of strings $F \subseteq D$, where $D = f\{x\} \cap (\Sigma^*)^{\leq n^\varepsilon} = f\{y\} \cap (\Sigma^*)^{\leq n^\varepsilon}$. We can use this knowledge to distinguish between strings from A and B. Call two strings x and y of the same length n *equivalent*, if $f\{x\} \cap (\Sigma^*)^{\leq n^\varepsilon} = f\{y\} \cap (\Sigma^*)^{\leq n^\varepsilon}$, and $\alpha_x(\chi_F(f(x))) = \alpha_y(\chi_F(f(y)))$ for all $F \subseteq D = f\{x\} \cap (\Sigma^*)^{\leq n^\varepsilon}$. By assumption it will not be possible that there are two equivalent strings one of which is in A, and the other one in B. So the strings of length n will be partitioned into a finite number of equivalence classes, none of which intersects both A and B. Every equivalence class is uniquely determined by the set D and a truth-table on the elements of D. D contains at most $\varepsilon \log n$ strings of length at most n^ε, and a truth-table on $|D|$ elements has size at most $2^{\varepsilon \log n} = n^\varepsilon$. Hence we can describe an equivalence class by a string of length at most $n^{2\varepsilon} \varepsilon \log n$ which is less than $n^{3\varepsilon}$ for large enough n.

Using this description as an index into an advice string we can code for each equivalence class the information whether it contains a string in A in a random access advice string of length at most $2^{n^{3\varepsilon}}$ (for inputs of length n). This gives us a separator of A and B in $\mathrm{P}/2^{n^{3\varepsilon}}[1]$ contradicting the assumption. □

The proof of Theorem 7.4 is now completed by the following lemma. If $\mathrm{UP} \cap \mathrm{coUP} \not\subseteq \mathrm{SUBEXP}$, then (by the lemma) there is a set $E \in \mathrm{UP} \cap \mathrm{coUP} \setminus (\mathrm{P/subexp}[1])$. By the definition of P/subexp[1] there is an $\varepsilon > 0$ for which $E \notin \mathrm{P}/2^{n^\varepsilon}[1]$. This makes E a $s[1]$-separator (with $A = \overline{B} = E$), and we can apply Lemma 7.5.

Lemma 7.6 *If* $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{P/subexp}[1]$ *then* $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{SUBEXP}$.

The lemma is an immediate consequence of the techniques developed by Ogihara, Watanabe, Homer and Longpré [HL91, Theorem 5] to deal with reductions to sparse sets.

Proof. We prove the contraposition. Suppose $W \in \mathrm{UP} \cap \mathrm{coUP} \setminus \mathrm{SUBEXP}$. Fix $\varepsilon > 0$ such that $W \notin \mathrm{DTIME}(2^{n^\varepsilon})$. Let $w_1(x)$ be the unique witness for $x \in W$ (of length $|x|^k$), and $w_0(x)$ be the unique witness for $x \notin W$ (assume $|w_0(x)| = |w_1(x)|$). Define a set $L = \{\langle x, w\rangle : w \leq w_1(x) \wedge |w| = n^k\}$. Then $L \in \mathrm{UP}$, $w_1(x)$ serving as a unique witness for $\langle x, w\rangle \in L$. On the other hand $\langle x, w\rangle \notin L$ if and only if either $x \in W$, and $w > w_1(x)$, or $w_0(x)$ witnesses that $x \notin W$. Since the two cases are disjoint this shows $L \in \mathrm{coUP}$, and therefore $L \in \mathrm{UP} \cap \mathrm{coUP}$.

Note that W reduces to L ($x \in W$ if and only if $\langle x, 0^{n^k}\rangle \in L$). We will now show that if $L \in \mathrm{P}/2^{n^{\varepsilon/2}}[1]$, then $W \in \mathrm{DTIME}(2^{n^\varepsilon})$, contradicting the assumption. Hence $L \notin \mathrm{P}/2^{n^{\varepsilon/2}}[1]$, and in particular $L \notin \mathrm{P/subexp}[1]$. Since $L \in \mathrm{UP} \cap \mathrm{coUP}$ this shows that $\mathrm{UP} \cap \mathrm{coUP} \not\subseteq \mathrm{P/subexp}[1]$.

We are left with the proof ot the claim that $L \in \mathrm{P}/2^{n^{\varepsilon/2}}[1]$ implies $W \in \mathrm{DTIME}(2^{n^{\varepsilon}})$. Given an input x consider the 2^{n^k} strings between $\langle x, 0^{n^k}\rangle$ and $\langle x, 1^{n^k}\rangle$, and think of them as ordered from left to right. Let $l = 2^{n^{\varepsilon/2}}$. Split the strings up into $2l$ intervals of the same size (plus or minus one). Now run the following procedure: In every step each interval gets split up into two, and all but $2l$ intervals get eliminated again. To describe the pruning procedure let $y_1 = \langle x, w_1\rangle, \ldots, y_{4l} = \langle x, w_{4l}\rangle$ be the $4l$ strings at the left end of the $4l$ intervals $I_1, \ldots, I_{4l}$ we get after the splitting. Membership of each y_i in L can be decided in polynomial time by making a single query to the l bits of advice (and we can assume that each y_i does query an advice bit). For bit q ($1 \leq q \leq l$) in the advice string, and an answer $a \in \{0, 1\}$, let

$$f(q, a) = \max\{i : \text{the nonuniform algorithm on input } y_i \text{ queries } q, \text{ and given answer } a \text{ accepts}\}.$$

Then f is computable in polynomial time, and $\langle x, w_1(x)\rangle \in I_{f(q,a)}$ for some q and a. (If $i < j$, and I_i and I_j are both accepted by the algorithm for some value of q and a, then I_i cannot contain $\langle x, w_1(x)\rangle$ since otherwise I_j would not contain any string from L. Hence either a was the wrong answer, or I_i does not contain $\langle x, w_1(x)\rangle$. In either case I_i can be eliminated.) Hence one of the $2l$ intervals in $\{I_{f(q,a)} : 1 \leq q \leq l, a \in \{0, 1\}\}$ contains $\langle x, w_1(x)\rangle$.

After at most n^k repetitions of the pruning step, all intervals have size at most one, and the procedure guarantees that the witness $\langle x, w_1(x)\rangle$ is contained in one of the intervals if $x \in W$. Hence all we have to do is check the remaining $2l$ witnesses to decide whether $x \in W$. The whole procedure takes at most $\mathrm{DTIME}(ln^k)$ steps which is in $\mathrm{DTIME}(l^2) = \mathrm{DTIME}(2^{n^{\varepsilon}})$ contradicting the choice of W. □

Remark. We would have liked to prove the theorem under the hypothesis that $\mathrm{UP} \not\subseteq \mathrm{SUBEXP}$. Unfortunately the first existence proof for separators (Lemma 4.3) requires $\mathcal{C}$ to be closed under polynomial time truth-table reducibilities. This we cannot guarantee if only one query to the oracle is allowed. On the other hand if we use the full power of P/subexp (instead of P/subexp[1]) we cannot apply the pruning techniques of Ogihara, Watanabe, Homer and Longpré any longer. So we have to use the second existence proof for separators (Lemma 4.4) which did not pose any requirements on $\mathcal{C}$. □

Bounded truth-tables revisited

Note that the NPSV-function in the proof of Lemma 7.5 outputs $f\{x\} \cup f\{y\}$. In case we start with a bounded truth-table this means that $|f\{x\} \cup f\{y\}| \leq 2k$, and we can conclude that M is not NP-$2k$-immune. Hence $\overline{M}$ is not NP-simple. This establishes the next lemma as a corollary of the proof and thereby the theorem.

Lemma 7.7 *If E is a $s[1]$-separator and $E \leq_{\mathrm{btt}} M$, then M is not* NP*-simple.*

Theorem 7.8 *An* NP*-simple set cannot be btt-complete for* NP *unless* $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{SUBEXP}$.

8 Exponential time

In this section we will test our techniques on EXP and NEXP. One advantage is that we can dispense with hypotheses. But let us first recall what is already known. The following account is based on Buhrman [Buh93]. In his PhD thesis Berman proved that all m-complete sets for EXP are in fact one-to-one, length-increasing m-complete. Hence an m-complete set for EXP will not be P-immune, since for example the tally set $\{0^n : n \in \omega\}$ reduces to it via a one-to-one, length-increasing reduction.

Fact 8.1 (Berman, 1977) *No m-complete set for* EXP *is* P*-immune.*

On the other hand it is easy to construct a counterexample for 2-tt-reductions.

Fact 8.2 (Buhrman [Buh93]) *There is a 2-d-complete set for* EXP *which is* P*-immune.*

The case for NEXP seemed more difficult. It was proved by Homer and Wang [HW94] that every m-complete set for NE and its complement contain dense E∩UP subsets. Finally Tran [Tra95] extended the Berman result to NEXP.

Fact 8.3 (Tran [Tra95]) *No m-complete set for* NEXP *is* P*-immune.*

Since it had been proven earlier by Buhrman, Spaan, and Torenvliet [BST93] that a 1-tt-complete set for NEXP is also m-complete the following corollary was immediate.

Fact 8.4 (Tran [Tra95]) *No 1-tt-complete set for* NEXP *is* P*-immune.*

Again this seems to be the limit.

Fact 8.5 (Buhrman [Buh93]) *There is a 2-d-complete set for* NEXP *which is* P*-immune.*

But not quite. We will show how to extend Tran's result to conjunctive and disjunctive reductions as well as how to strengthen its conclusion.

Definition 8.6 *An infinite set A is called* P-levelable *if for every subset B of A in* P *there is another subset C of A in* P *which is infinite and disjoint from B.*

A P-levelable set is not only not P-immune, it cannot even be written as the union of a set in P and a P-immune set.

Theorem 8.7 *Every c-complete set for* NEXP *is* P*-levelable.*

Proof. Let K be c-complete for NEXP. Then $K \in \mathrm{NTIME}(2^{n^l})$ for some $l \geq 1$.

Fix any subset $S \in \mathrm{P}$ of K. We can assume that l was chosen such that $S \in \mathrm{DTIME}(n^l)$. By a theorem of Žàk [Žák83] there is a tally set $H \in \mathrm{NTIME}(2^{n^{l+2}}) - \mathrm{NTIME}(2^{n^{l+1}})$.

For the rest of the proof fix an effective enumeration $(f_i)_{i\in\omega}$ of all functions in PF such that f_i can be uniformly computed in time $n^i + i$. Define

$$\begin{aligned} A_i = \{0^{\langle i,x\rangle} \quad : \quad & (\exists q \in f_i\{0^{\langle i,x\rangle}\})\, [|q| > \langle i,x\rangle/(ci^2) \text{ and } q \notin S] \\ \text{or} \quad & 0^x \in H\}, \end{aligned}$$

and $A = \bigcup_{i \geq 1} A_i$. We will choose c later. It can be checked that $A \in \mathrm{NTIME}(2^{n^{l+2}})$ and therefore A lies in NEXP. Hence there is a conjunctive reduction f_j from A to K, i.e. for some j the function f_j computes a set of queries in polynomial time, such that $x \in A$ iff $f_j\{x\} \subseteq K$. Consider the set

$$D = \{0^{\langle j,x \rangle} : (\exists q \in f_j\{0^{\langle j,x \rangle}\}) \; [|q| > \langle j,x \rangle/(cj^2) \text{ and } q \notin S]\}.$$

Assume that D is finite. Then for sufficiently large x it is true that $0^x \in H$ iff $f_j\{0^{\langle j,x \rangle}\} \subseteq K$. Furthermore each query $q \in f_j\{0^{\langle j,x \rangle}\}$ fulfills either $q \in S$ or $|q| \leq \langle j,x \rangle/(cj^2) \leq x = |0^x|$ (the middle inequality is made correct by the right choice of c depending on $\langle \cdot, \cdot \rangle$ for large enough x). If $q \in S$, then $q \in K$, and therefore q does not influence the truth-value of $f_j\{0^{\langle j,x \rangle}\} \subseteq K$. Hence we can eliminate queries satisfying $q \in S$ (which only takes polynomial time). The remaining queries have length at most the length of the input, thus we can make those remaining queries to K. Because of the bound on the running time of f_j there can be at most $n^j + j$ queries to K each one taking time $\mathrm{NTIME}(2^{n^l})$. This gives us a decision procedure for H in $\mathrm{NTIME}(2^{n^{l+1}})$ contradicting the choice of H.

Therefore the set D has to be infinite and $f_j\{0^{\langle j,x \rangle}\}$ contains a q with $|q| \geq \langle j,x \rangle/(cj^2)$ and $q \notin S$ for each $x \in D$. Let $S' = \{q : (\exists z)[z < |q| \text{ and } q \in f_j\{0^{\langle j,z \rangle}\} - S]\}$. By definition $S \cap S' = \emptyset$, and S' is decidable in polynomial time. Furthermore $q \in S'$ implies $|q| > z \geq \langle j,z \rangle/(cj^2)$ (the second inequality by choice of c). Hence $0^{\langle j,z \rangle} \in A_j$, and therefore $q \in K$ (being one of the queries in $f_j\{0^{\langle j,z \rangle}\}$). This shows that $S' \subseteq K$ finishing the proof. □

Similarly the following result can be shown.

Theorem 8.8 *The complement of every d-complete set for* NEXP *is* P*-levelable.*

Corollary 8.9 *Every 1-tt-complete set for* NEXP *and its complement is* P*-levelable.*

What can we say about truth-table reductions? Looking at the proof of Agrawal's result (Theorem 6.7) will convince the reader that it also holds for NEXP, and NEXP-complete sets (since we established that all NEXP-complete sets and their complements are P-levelable), hence NEXP-simple sets are not honest *btt*-complete for NEXP. As a matter of fact honesty is not actually needed as we will demonstrate using an approach similar to the one in Lemma 7.5: NEXP-simple sets cannot be *btt*-complete for NEXP.

Another approach to the problem might consist in showing that all *btt*-complete sets for NEXP are honest *btt*-complete. We do not know whether this is true. An indication that exponential time does guarantee some degree of honesty is the following partial result generalizing an earlier result by Ganesan and Homer [GH92] for the 1-*tt* case.

Theorem 8.10 *Every 2-tt-complete set for* NEXP *is exponentially honest 2-tt-complete.*

Proof. This is a variation on a trick by Ganesan and Homer [GH92]. Let A be a 2-*tt*-complete set for NEXP. Fix a 1-1, li-complete set K for NEXP and an effective enumeration $(f_i, \alpha_i)_{i \in \omega}$ of polynomial time 2-tt reductions (f_i computes the two queries and α_i the truth-table).

Define a set M as follows:

```
(01) M: input $(i, x)$
(02)      compute $(q_0, q_1) = f_i(i, x)$
```

```
(03)   if $|q_0| > |q_1|$
(04)     then reject input,
(05)   if $2^{|q_1|} < |(i,x)|$
(06)     then compute $\alpha_i(\chi_A(q_0,q_1))$
(07)          and reject if it accepts and vice versa,
(08)   else if $2^{|q_0|} < |(i,x)|$
(09)     then compute $b = \chi_A(q_0)$ and with that information
(10)     determine the remaining unary truth-table $\alpha(b') := \alpha_i(b,b')$, $b' \in \{0,1\}$;
(11)     if $\alpha$ is
(12)       FALSE then accept,
(13)       TRUE then reject,
(14)       negation, then accept if $q_1 \in A$,
(15)       else, accept if $x \in K$,
(16)   else accept if $x \in K$.
```

We claim that $M \in$ NEXP. In fact up to line (13) everything can be done in exponential time (assuming the enumeration is effective enough); note that the queries made to A in lines (06) and (09) are exponentially small compared to the input. Only in lines (14), (15) and (16) do we need the full power of NEXP to guess accepting paths for A and K. Since A is 2-*tt*-complete there has to be a $j \in \omega$ such that $f_j : M \leq_{\text{2-tt}} A$ via truth-table α_j. We can assume that the queries of f_j are in length-non-decreasing order. Now M on input (j,x) cannot reach lines $(04), (07), (12), (13), (14)$ since in all of these cases we diagonalized the reduction. Hence it always terminates in (15) or (16) meaning that $x \in K$ if and only if $(j,x) \in M$. Furthermore the only two possible cases that can occur are that both queries are large, namely $2^{|q_0|} > |(i,x)|$, in which case f_j is exponentially honest, or q_1 is large: $2^{|q_1|} \geq |(i,x)|$ in which case we end in line (15), and $x \in K$ if and only if $q_1 \in A$ (since the only remaining truth-table is the identity), where q_1 is large enough to be exponentially honest. Hence putting things together we have an exponentially honest 2-*tt*-reduction from K to A which shows that A is exponentially honest 2-*tt*-complete. □

Similar proofs will not work for three queries, since the number of truth-tables becomes too large to handle. We will now return to the approach of Lemma 7.5 which is more successful.

We first have to define a new version of hyperimmunity. An *honest exp-array* is a partial function $f : \Sigma^* \to (\Sigma^*)^{<\omega} \setminus \{()\}$ computable in exponential time and with infinite domain with the following property: there is a polynomial p such that for all x

- $p(|y|) \geq |x|$ for all $y \in f\{x\}$, and
- $|f(x)| \leq p(|x|)$.

Note that compared to np-arrays we only increased the computational power of the function. The output is still restricted to polynomially many strings of polynomial size in the input. We call an infinite set EXP-*hyperimmune* if there is no honest exp-array f such that $f\{x\} \cap A \neq \emptyset$ for all $x \in \text{dom}(f)$.

Lemma 8.11 EXP $\not\subseteq$ P/subexp[1].

Proof. Let $0 < \varepsilon < 1$. We will construct a set E in EXP $\setminus$ P/2^{n^ε}[1]. Let $(f_i)_{i\in\omega}$ be an effective enumeration of all polynomial time advice machines making exactly one query. We will diagonalize machine f_n on the strings of length n. There are 2^n binary strings of length n, but only 2^{n^ε} addressable advice bits. Hence there are two strings x and y ($|x| = |y| = n$) for which f_n queries the same advice bit. Compute $f_n(x)$ and $f_n(y)$ for both answers to the query. Since there are four possibilities for $\chi_E(x, y)$, we can choose one different from the two predicted by f_n. Let $E \setminus \{x, y\} = \emptyset$. Obviously, we can decide E in DTIME(2^{n^2}), and $E \not\in \mathrm{P}/2^{n^\varepsilon}[1]$ by construction. □

Theorem 8.12 *An* EXP*-hyperimmune set cannot be* $o(\log n)$*-tt-hard for* EXP*.*

Proof. The proof is an easy adaptation of the proof of Lemma 7.5. By Lemma 8.11 there is an $E \in \mathrm{EXP}$ which is not in $\mathrm{P}/2^{n^{3\varepsilon}}[1]$ (for some $\varepsilon > 0$). Let $A = E = \overline{B}$, and M be $o(\log n)$-*tt*-hard for EXP. Then $E \leq_{o(\log n)-\mathrm{tt}} M$. The second case of the proof of Lemma 7.5 cannot apply since $E \not\in \mathrm{P}/2^{n^{3\varepsilon}}[1]$. Hence the first case must apply, and we conclude that M is not EXP-hyperimmune (EXP rather than NP, since A and B are in EXP). □

As with Lemma 7.5 the theorem allows us to draw a conclusion for *btt*-reductions (we should note that Lemma 3.3 works for NEXP too). Thus the following theorem is immediate.

Theorem 8.13 (Buhrman [Buh97]) *A* NEXP*-simple set cannot be btt-hard for* EXP*.*

This result was first proved by Buhrman using a different technique.

9 Relativizations

We do not know whether NP-simple sets exist and it seems hard to come up with natural conditions that imply their existence; unconditional existence results would of course imply P $\neq$ NP and would therefore require nonrelativizing techniques. However, it would also require nonrelativizing techniques to show that NP-simple do not exist: Homer and Maass [HM83] constructed an oracle relative to which NP-simple sets exist and Balcázar [Bal85] showed that the oracle can be made computable. It is easy to see that NP-simple sets exist relative to Cohen generic oracles (at the end of this section we will sketch a proof that even NP-hypersimple sets exists for these oracles).

Consider the following hypotheses (all of which we would believe to be true).

(*i*) P $\neq$ UP,

(*ii*) P $\neq$ NP $\cap$ coNP,

(*iii*) There are P-inseparable sets in NP,

(*iv*) NP-simple sets exist.

Then relativizable techniques will not be sufficient to show that (*i*) $\wedge$ (*ii*) $\wedge$ (*iii*) imply (*iv*). Similarly there is no relativizable proof that (*iv*) implies either (*i*), or (*ii*), or (*iii*):

The oracle relative to which (*i*), (*ii*), and (*iii*) are true, and (*iv*) is false, is due to Homer and Selman [HS92, Theorem 2]. They constructed a computable oracle relative to which P $\neq$ UP $\neq$ NP = coNP. (NP-simple sets do not exist since NP = coNP, and any set in NP $\setminus$ P is P-inseparable from its complement which lies in NP.)

For the other direction we have to combine three results from the literature (for references see [FR94]). It is known that if H is an oracle for which $\mathrm{P}^H = \mathrm{PSPACE}^H$, and C is a Cohen generic oracle, then relative to $G \oplus H$ it is true that P = UP (Blum, Imagliazzo), P = NP $\cap$ coNP (Hartmanis, Hemachandra), and P-inseparable sets in NP do not exist (Fortnow, Rogers). Since the proof of existence of NP-simple relative to Cohen generic sets relativizes (see Proposition 9.7), NP-simple sets exist relative to $C \oplus H$.

The first oracle made (*iv*) false by letting NP = coNP. Homer and Maass [HM83] showed that there also is an oracle relative to which no NP-simple sets exist, but NP $\neq$ coNP, so we cannot prove that the existence of NP-simple sets is equivalent to NP $\neq$ coNP by relativizable techniques.

Using other kinds of (generic) oracles we can try to show that the existence or nonexistence of NP-simple sets cannot be linked via relativizable proofs to other complexity-theoretic statements. Let us take for example the isomorphism conjecture. Relative to a random oracle the isomorphism conjecture fails (Kurtz, Mahaney and Royer [KMR95]) and NP-simple sets exist (Vereshchagin [Ver94]). On the other hand the isomorphism conjecture holds relative to an sp-generic oracle (Fenner, Fortnow and Kurtz [FFK96]) and NP-simple sets exist (as we will show presently). Hence the assumption that NP-simple sets exist will not be enough to show the isomorphism conjecture true or false with relativizing techniques. In the other direction we can use an oracle constructed by Beigel, Buhrman, and Fortnow [BBF98] which makes the isomorphism conjecture true, while NP-simple sets do not exist (since NP = coNP). Furthermore the isomorphism conjecture will be false, and NP-simple sets do not exist relative to any oracle making P = PSPACE. Hence the isomorphism conjecture will not prove the existence, or nonexistence of NP-simple sets using relativizable techniques only.

We include a compact definition of all the terms needed in the proof that NP-simple sets exist relative to an sp-generic oracle. However, the reader not familiar with generic oracles is advised to take a closer look at the paper by Fenner, Fortnow and Kurtz for background.

Definition 9.1 (Fenner, Fortnow, Kurtz [FFK96]) *An* iterated polynomial sequence $(a_i)_{i\in\omega}$ *fulfills* $a_0 \geq 2$ *and* $a_{i+1} = p(a_i)$ *for some polynomial* $p(n) \geq n^2$. *We call a partial function* $\sigma : \Sigma^* \to \{0, 1\}$ *a* symmetric perfect forcing condition (sp-condition) *if* σ *is undefined on strings of length* a_i *(for all* i*). A partial function* τ extends σ *if* $\mathrm{dom}(\sigma) \subseteq \mathrm{dom}(\tau)$ *and the two functions agree on* $\mathrm{dom}(\sigma)$.

A set of sp-conditions is called dense *if every sp-condition is extended by some sp-condition in the set. A set is called* sp-generic *if it* meets *every dense definable set of sp-conditions, i.e. A viewed as an infinite characteristic string extends some sp-condition in every dense definable set of sp-conditions.*

The following theorem is essentially due to Stuart Kurtz.

Theorem 9.2 (Kurtz [Kur97]) *Relative to an sp-generic oracle there exists an* NP*-simple set.*

Proof. Let $(M_i)_{i\in\omega}$ be an enumeration of nondeterministic oracle Turing machines such that M_i runs in time $n^i + i$ (independent of the oracle). $L(M_i^X)$ denotes the language accepted by M_i with oracle X. Consider the set

$$S(X) = \{x : (\forall z)[|z| = \lceil \log^2 |x| \rceil \Rightarrow |\{z0^i : 0 \leq i \leq |x| - |z|\} \cap X| \equiv 0 \pmod 2)]\}.$$

Then $S(X) \in \mathrm{coNP}^X$ for all oracles X. We have to prove that $S(X)$ is NP^X-immune for an sp-generic oracle X. To this end we show that $S(X)$ fulfills the requirements

$$(R_i) \quad : \quad L(M_i^X) \text{ is finite or } L(M_i^X) \not\subseteq S(X)$$

if X is sp-generic. Furthermore we have to make sure that $S(X)$ is infinite. Again this is taken care of by the sp-genericity of the oracle X.

Claim 9.3 *For any sp-condition σ and any m there is an sp-condition τ extending σ such that $S(X)$ contains at least m strings for any oracle X extending τ.*

If the claim is true then an sp-generic oracle will make $S(X)$ infinite. To show that the claim holds let some sp-condition σ and an integer m be given. By definition there is an iterated polynomial sequence $(a_i)_{i\in\omega}$ such that σ is undefined at lengths a_i. Let $p(n) \geq n^2$ be the polynomial generating the sequence, i.e. $a_{i+1} = p(a_i)$. Choose k such that $a_k \geq \log m$. Extend σ to τ in such a way that

$$(\forall z)[|z| = \lceil \log^2 a_k \rceil \Rightarrow |\{z0^i : 0 \leq i \leq a_k - |z|\} \cap X| \equiv 0 \pmod 2)],$$

and τ is defined on all strings up to length a_k. This can be done since we have complete control over the strings at length a_k. Note that τ is an sp-condition (a new iterated polynomial sequence could start at a_{k+1}). Furthermore by definition $S(X)$ contains all strings of length a_k of which there are $2^{a_k} \geq m$ many. This finishes the proof of the claim.

Claim 9.4 *For any sp-condition σ there is an sp-condition τ extending σ such that (R_i) is fulfilled for any oracle X extending τ.*

The verification of the claim will finish the proof since the claim implies that the set of sp-conditions forcing (R_i) is dense, and hence will be met by any sp-generic oracle.

To show that the claim is true let an sp-condition σ be given. As above let $(a_i)_{i\in\omega}$ be the iterated polynomial sequence witnessing that σ is an sp-condition, and choose $l \geq i$ such that $n \mapsto n^l + l$ majorizes the polynomial associated with the sequence.

We have to extend σ in such a way that (R_i) will be satisfied. There are two cases. If we can force $L(M_i^X)$ to be finite by extending σ to an sp-condition τ we do so, and (R_i) will be fulfilled. Hence we can assume that we cannot force $L(M_i^X)$ to be finite. In particular this means that for every x there is a $y > x$ such that we can force $y \in L(M_i^X)$. Fix x such that

$$|x| \geq \max\{a_0, 2^{l^2}\} \text{ and}(\log^2|y|)^l + l < |y| \text{ for all } y \text{ with } |y| \geq |x|.$$

Fix $y > x$ and an sp-condition σ' extending σ that forces $y \in L(M_i^X)$. Select an accepting path of $M_i^{\sigma'}$ on y. Along this path M_i can make at most $n^i + i$ oracle queries. Hence we can assume that the domain of σ' is the union of the set of those (polynomially many) queries and the domain of σ. Since the gap between $\log^2|y|$ and $|y|$ is larger than p and $|y| \geq a_0$, there is a k for which $\log^2(|y|) < a_k < |y|$. There are $2^{\lceil \log^2(|y|)\rceil} \geq |y|^{\log|y|} \geq |y|^{l^2} > |y|^l + l$ many strings of length a_k which can be used for coding (namely the extensions by zeroes of strings of length $\lceil \log^2(|y|)\rceil$. Since these are more than are committed already by σ' there is an uncommitted string of length a_k with which we can toggle the parity in such a way that $y \notin S(X)$ for each oracle X extending τ. Since this argument only used a finite extension, τ is still an sp-condition. □

Since we are concerned with the relationship between simplicity and completeness the question we should be asking in this section is whether it is possible for a set to be simple and complete. More precisely, is there a world in which there is an NP-simple *btt*-complete set? Of course, by Theorem 7.8 in such a world UP $\cap$ coUP $\subseteq$ SUBEXP. We leave this question open; it seems to be hard, not least so since it will have to depend on the reduction being dishonest because of Agrawal's result (Theorem 6.7). We do not know how to exploit dishonesty to our advantage.

We can show, however, that the the change from NP-simplicity to NP-hypersimplicity was necessary when removing the bound on the truth-tables. More precisely we construct a relativized world, in which there is an (honest) conjunctively complete NP-simple set, although UP $\not\subseteq$ SUBEXP.

Let $f(n)$ be any positive, monotone, polynomially-bounded, polynomial time computable function such that $\lim_{n\to\infty} f(n) = \infty$. For every $x \in \Sigma^*$, define $\mathit{Query}(x) = \{x10, x100, \ldots, x10^{f(|x|)}\}$.

Lemma 9.5 *Relative to some oracle A, there is a language $L^A \in \mathrm{UP}^A$ which is NE^A-simple (that is, $\overline{L^A}$ is NE^A-immune), and for all $x \in \Sigma^*$,*

$$\mathit{Query}(x) \not\subseteq L^A.$$

Assuming the lemma we can prove the oracle result.

Theorem 9.6 *There is an oracle A such that:* $\mathrm{UP}^A \not\subseteq \mathrm{SUBEXP}^A$ *and there exists an* NP^A*-simple set which is (honest) $f(n)$-c-complete for* NP^A.

Proof. Let A and L^A be as in Lemma 9.5. Note that $L^A \notin \mathrm{SUBEXP}^A$, so $\mathrm{UP}^A \not\subseteq \mathrm{SUBEXP}^A$. Note also that L^A is NP^A-simple and $\mathit{Query}(x) \not\subseteq L^A$ for any x. Let C be some (coinfinite) m-complete set for NP^A, and let

$$S^A = L^A \cup \bigcup_{x \in C} \mathit{Query}(x).$$

Since S^A is a coinfinite superset of L^A, it is also NP^A-simple. Moreover, S^A is $f(n)$-c-complete via the reduction $x \mapsto \mathit{Query}(x)$. □

Proof of Lemma 9.5. Our proof uses forcing and is vaguely reminiscent of a construction by Balcázar [BDG88, Theorem 7.11], but here the construction is complicated by the fact that our L^A must have quite a dense complement, whereas Balcázar *et al.* relied heavily on their set (which is analogous to $\overline{L^A}$) being very sparse.

For all $y \in \Sigma^*$, define $\mathit{Region}(y) = \{yz : |z| = |y|^2\}$. For all $X \subseteq \Sigma^*$ define

$$L^X = \{y \in \Sigma^* : \mathit{Region}(y) \cap X \neq \emptyset\}.$$

Clearly, $L^X \in \mathrm{NP}^X$. We construct an A to make L^A satisfy the conditions of the lemma.

For all $x \in \Sigma^*$ define $\mathit{QueryRegions}(x) = \bigcup_{y \in \mathit{Query}(x)} \mathit{Region}(y)$. By a *condition* we mean a pair (σ, k) such that

- $\sigma\colon \Sigma^* \to \{0,1\}$ is a finite partial characteristic function (a "partial oracle"),
- $k \geq 1$ is an integer (a promise that we will leave at least k strings in $\mathit{Query}(x)$ out of L^A "from now on"),
- for all $x \in \Sigma^*$, either $\mathit{QueryRegions}(x) \cap \mathrm{dom}(\sigma) = \emptyset$ (in which case we require $|\mathit{Query}(x)| \geq k$) or $\mathit{QueryRegions}(x) \subseteq \mathrm{dom}(\sigma)$, and
- for all $y \in \Sigma^*$ there is at most one string $z \in \mathit{Region}(y)$ with $\sigma(z) = 1$. (This will guarantee $L^A \in \mathrm{UP}^A$.)

We partially order the set of conditions as follows: we say condition (τ, ℓ) *extends* condition (σ, k) iff τ extends σ, $\ell \geq k$, and for all x with $\mathit{QueryRegions}(x) \in \mathrm{dom}(\tau) - \mathrm{dom}(\sigma)$,

$$|\mathit{Query}(x) - L^{\tau}| \geq k,$$

where L^{τ} has the obvious meaning.

Fix a nondeterministic oracle TM N, running in time 2^{cn} for some constant c (the same for all oracles). Let $y \in \Sigma^*$ and (σ, k) be some condition. We say that (σ, k) *forces* N *to accept* y if $N(y)$ has an accepting path along which all queries to the oracle are in $\mathrm{dom}(\sigma)$ and are answered according to σ. We say that (σ, k) *forces* N *to reject* y if no extension of (σ, k) forces N to accept y.

Fixing an arbitrary condition (σ, k), we will find an extension (τ, ℓ) that forces N to either (i) accept a member of L^{τ}, or (ii) reject all sufficiently large $y \in \Sigma^*$. Forcing (i) will cause $L(N^A) \cap L^A \neq \emptyset$; (ii) will cause $L(N^A)$ to be finite. In either case, N does not prevent L^A from being NE^A-simple.

Suppose there is no extension of (σ, k) that forces (i). Let τ be the finite function extending σ such that

$$\mathrm{dom}(\tau) = \mathrm{dom}(\sigma) \;\cup\; (\Sigma^*)^{\leq c^2+c} \;\cup\; \bigcup \{\, \mathit{QueryRegions}(x) \;:\; |x| \leq c \;\text{ or }\; |\mathit{Query}(x)| \leq k \} \,,$$

and $\tau(z) = 0$ for all $z \in \mathrm{dom}(\tau) - \mathrm{dom}(\sigma)$. Clearly, τ is finite since $\lim_{|x| \to \infty} |\mathit{Query}(x)| = \infty$, and $(\tau, k+1)$ extends (σ, k). We show that $(\tau, k+1)$ forces (ii). Indeed, suppose not: consider any y with $\mathit{Region}(y) \cap \mathrm{dom}(\tau) = \emptyset$, and suppose there is an extension (υ, ℓ) of $(\tau, k+1)$ that forces N to accept y. We may assume without loss of generality that $\mathit{Region}(y) \subseteq \mathrm{dom}(\upsilon)$. Then $y \notin L^{\upsilon}$, since otherwise (υ, ℓ) would force (i). Because $|y| > c$, N^{υ} does not have time to query all of $\mathit{Region}(y)$, so we let $z \in \mathit{Region}(y)$ be the least string not queried by N^{υ}, and let υ' be identical to υ except that $\upsilon'(z) = 1$. Thus $N^{\upsilon'}(y)$ still accepts, but $y \in L^{\upsilon'}$ (and this is the only y added to L^{υ}). Finally, for each x with $\mathit{QueryRegions}(x) \subseteq \mathrm{dom}(\upsilon) - \mathrm{dom}(\tau)$, we have

$$|\mathit{Query}(x) - L^{\upsilon}| \geq k + 1$$

by the definition of extension of conditions, and thus

$$|\mathit{Query}(x) - L^{\upsilon'}| \geq k$$

for all x with $\mathit{QueryRegions}(x) \subseteq \mathrm{dom}(\upsilon) - \mathrm{dom}(\sigma)$. Therefore, (υ', k) extends (σ, k) and forces (i), contrary to our assumption; hence, $(\tau, k+1)$ forces (ii).

Those familiar with forcing arguments will now note that since the conditions forcing (i) or (ii) above form a dense set, any sufficiently generic set of conditions yields an oracle A with all the desired properties. For those not familiar with these arguments, it is nearly as easy to construct A explicitly. Pick some enumeration $N_1, N_2, \ldots$ of all nondeterministic linear exponential time oracle machines, and let $(\sigma_0, k_0) = (\emptyset, 1)$. Given condition (σ_{i-1}, k_{i-1}), let (σ_i, k_i) be some extending condition that forces (i) or (ii) for $N = N_i$. We thus get a countable chain of conditions, each extended by its successor. Let α be the union of all finite functions in the chain, and let $A = \{z : \alpha(z) = 1\}$. Since all the k_i are positive, it follows that $\mathit{Query}(x) \not\subseteq L^A$ for all x. Furthermore, A never intersects $\mathit{Region}(y)$ in more than one place for any y, so $L^A \in \mathrm{UP}^A$. To see that L^A is NE^A-simple, note that for any i, if $L(N_i) \cap L^A = \emptyset$, then it must be that (σ_i, k_i) forces N_i to reject all y with $\mathit{Region}(y) \cap \mathrm{dom}(\sigma_i) = \emptyset$, and so A preserves these rejections. Thus, $L(N_i)$ is finite. □

It is straightforward to show that NP-hypersimple sets exist relative to standard (Cohen) generic oracles.

Proposition 9.7 *Relative to any (Cohen) generic oracle G, there is an* NP^G*-hypersimple set.*

Sketch of Proof. Here our conditions are finite characteristic functions, partially ordered by extension. For any x, let $\mathit{Region}(x) = \{xy : |y| = |x|\}$. For any oracle X, define

$$L^X = \{x : \mathit{Region}(x) \cap X \neq \emptyset\}.$$

Clearly $L^X \in \mathrm{NP}^X$.

Let M be some polynomial-time deterministic honest oracle transducer, and let σ be any condition and let n be sufficiently large. If there is a τ extending σ that causes M^τ to output a set $\{y_1, \ldots, y_k\}$ on an input x longer than n, then for each i with $1 \leq i \leq k$, $M^\tau(x)$ cannot query all of $\mathit{Region}(y_i)$, so we can alter τ to τ' extending σ so that $M^{\tau'}(x)$ still outputs $\{y_1, \ldots, y_k\}$ but $\{y_1, \ldots, y_k\} \subseteq L^{\tau'}$. Thus either σ forces $\mathrm{dom}(M^G)$ to be finite, or we can extend to a condition that forces $M^G(x) \subseteq L^G$ for some x. □

10 Open Questions

Simplicity is a notion which is as natural as it is elusive. We would like to know about any combination of natural assumptions that implies the existence of an NP-simple set. This might in particular yield an easier proof of Vereshchagin's relativization result. The study of NP-simple sets has been less vigorous than one might hope for, and there seems to be plenty of work left to be done. Inspiration for further investigation might well develop out of the work done in computability theory.

We demonstrated that inseparable sets can be an important technique in complexity theory. But many questions regarding inseparable sets are still open (this by the way is true in computability as well). Are there other assumptions under which inseparable sets exist, other constructions which allow better hypotheses for the results we derive from the existence of inseparable sets? The hardest challenge is to find a complexity-theoretic condition that is necessary and sufficient for the existence of inseparable sets. In this context we should mention a paper by Fenner, Fortnow, Naik and Rogers [FFNR96] which investigates two propositions: Q and Q' which seem to be closely related to inseparable sets.

Are there other applications of inseparable sets in the realm of complexity theory? Possible candidates for closer scrutiny include Selman's p-selectivity, or notions from bounded queries (frequency computation). Inseparable sets have been successfully used to study the computability variants (for examples see [Sch98, FS99]).

We already mentioned that better constructions might allow us to improve upon the hypotheses. What can be done about improving the conclusions, what can we say about general truth-table reductions, what about Turing reductions?

There is a fair amount of work still to be done in the exponential time case. Here is an intriguing conjecture:

Conjecture 10.1 *Every btt-complete set for* NEXP *is exponentially honest btt-complete.*

We supplied some evidence for the conjecture, but more likely than not things will break down as soon as we allow three queries. Is there a set which is 3-*tt*-complete, but not honestly so? Is there an advantage in being dishonest?

We complemented our results by some relativization results like the world in which there is an NP-simple *c*-complete set. Can this result be sharpened to yield an NP-simple *btt*-complete set? This would be a rather remarkable result contradicting our intuition about NP-simple sets. We also showed that in some world NP-hypersimple sets exist, but can they be made complete under Turing (or stronger) reductions?

Finally, where do we go from here? Some initial results in the realm of exponential time have shown that our techniques can be useful higher up. There seems to be room for improvement. We might also ask what happens below NP. Do our techniques apply at all to classes below P? How could we use them to prove results on P-immunity for example? Since the reductions run in polynomial time there does not seem to be a way out unless we restrict ourselves to logspace reductions. Furthermore one might ask whether our method yields new assumptions that will allow separations of reducibilities in the complete degrees.

Acknowledgment. We would like to thank Harry Buhrman and Lance Fortnow for their insights into truth-tables and Steve Homer for his ready supply of papers. Many thanks to Manindra Agrawal for allowing us to include his result on honest bounded truth-tables (Theorem 6.7), Stuart Kurtz for Theorem 9.2, Harry Buhrman for allowing us to use his unpublished manuscript [Buh97], and John Rogers for helpful information on relativizations of the isomorphism conjecture. Further thanks go to Dieter Van Melkebeek, Janos Simon and Sophie Laplante for proofreading. Finally the anonymous referee deserves thanks for pointing out several mistakes and inconsistencies.

References

[Agr97] Manindra Agrawal. Personal communication., 1997.

[Bal85] José L. Balcázar. Simplicity, relativizations and nondeterminism. *SIAM Journal on Computing*, 14(1):148–157, 1985.

[BBF98] Richard Beigel, , Harry Burhman, and Lance Fortnow. NP might not be as easy as detecting unique solutions. In *Proceedings of the 30th ACM Symposium on the Theory of Computing (STOC-98)*, pages 203–208, 1998.

[BDG88] José L. Balcázar, Josep Diaz, and Joaquim Gabarró. *Structural Complexity, vols. I and II.* Springer, Berlin, 1988.

[BST93] Harry Buhrman, Edith Spaan, and Leen Torenvliet. Bounded reductions. In Klaus Ambos-Spies, Steven Homer, and Uwe Schöning, editors, *Complexity Theory: Current Research.* Cambridge University Press, 1993.

[Buh93] Harry Buhrman. *Resource Bounded Reductions.* PhD thesis, University of Amsterdam, 1993.

[Buh97] Harry Buhrman. Complete sets are not simple. Unpublished manuscript., FEB 1997.

[CO97] Jin-Yi Cai and Mitsunori Ogihara. Sparse sets versus complexity classes. In Lane A. Hemaspaandra and Alan L. Selman, editors, *Complexity Theory Retrospective, In Honor of Juris Hartmanis on the Occasion of His Sixtieth Birthday, July 5, 1988*, volume 2, pages 53–80. Springer, 1997.

[Dav65] Martin Davis. *The Undecidable.* Raven Press, New York, 1965.

[Dub89] Devdatt Dubhashi. On p-separability. Technical Report TR89-973, Cornell University, 1989.

[FFK96] Stephen Fenner, Lance Fortnow, and Stuart A. Kurtz. The isomorphism conjecture holds relative to an oracle. *SIAM Journal on Computing*, 25(1):193–206, 1996.

[FFNR96] Stephen A. Fenner, Lance Fortnow, Ashish V. Naik, and John D. Rogers. Inverting onto functions. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (CCC-96)*, pages 213–223. IEEE Computer Society, May24–27 1996.

[FK95] Michael R. Fellows and Neal Koblitz. Self-witnessing polynomial-time complexity and prime facotization. In *Proceedings of the 7th Annual Conference on Structure in Complexity Theory (SCTC '92)*, pages 107–110. IEEE Computer Society Press, 1995.

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

[FS99] Stephen Fenner and Marcus Schaefer. Bounded immunity and btt-reductions. *Mathematical Logic Quarterly*, 45(1):3–21, 1999.

[GH92] Krishnamurthy Ganesan and Steven Homer. Complete problems and strong polynomial reducibilities. *SIAM Journal on Computing*, 21(4):733–742, 1992.

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

[HL91] Steven Homer and Luc Longpré. On reductions of NP sets to sparse sets. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory '91*, pages 79–88, Chicago, IL, USA, June 1991. IEEE Computer Society Press.

[HLY86] Juris Hartmanis, Ming Li, and Yaacov Yesha. Containment, separation, complete sets, and immunity of complexity classes. In *Automata, Languages and Programming, 13th International Colloquium*, volume 226 of *Lecture Notes in Computer Science*, pages 136–145, Rennes, France, 15–19 July 1986. Springer-Verlag.

[HM83] Steven Homer and Wolfgang Maass. Oracle-dependent properties of the lattice of NP-sets. *Theoretical Computer Science*, 24:279–289, 1983.

[Hom86] Steven Homer. On simple and creative sets in NP. *Theoretical Computer Science*, 47:169–180, 1986.

[HS92] Steven Homer and Alan L. Selman. Oracles for structural properties: The isomorphism problem and public-key cryptography. *Journal for Computer and System Sciences*, 44:287–301, 1992.

[HW94] Steven Homer and Jie Wang. Immunity of complete problems. *Information and Computation*, 110(1):119–129, 1994.

[JY85] Deborah Joseph and Paul Young. Some remarks on witness functions for nonpolynomial and noncomplete sets in NP. *Theoretical Computer Science*, 39:225–237, 1985.

[KMR95] Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer. The isomorphism conjecture fails relative to a random oracle. *Journal of the ACM*, 42(2):401–420, 1995.

[Kur97] Stuart A. Kurtz. Personal communication., 1997.

[Odi89] Piergiorgio Odifreddi. *Classical recursion theory.* North-Holland, Amsterdam, 1989.

[Pap94] Christos H. Papadimitriou. *Computational Complexity.* Addison-Wesley, New York, 1994.

[Sch98] Marcus Schaefer. A guided tour of minimal indices and shortest descriptions. *Archives for Mathematical Logic*, 37(8):521–548, 1998.

[Sel96] Alan L. Selman. Much ado about functions. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (CCC-96)*, pages 198–212, Los Alamitos, May 24–27 1996. IEEE Computer Society.

[Soa87] Robert I. Soare. *Recursively Enumerable Sets and Degrees.* Springer, New York, 1987.

[Soa96] Robert I. Soare. Computability and recursiveness. *Bulletin of Symbolic Logic*, 3:284–321, 1996.

[Tra95] Nicholas Tran. On P-immunity of nondeterministic complete sets. In *Proceedings of the 10th Annual Conference on Structure in Complexity Theory '95*, pages 262–263. IEEE Computer Society Press, June 1995.

[Ver94] Nikolai K. Vereshchagin. NP-sets are coNP-immune relative to a random oracle. Technical Report TR501, University of Rochester, Computer Science Department, April 1994.

[Yam95] Tomoyuki Yamakami. Simplicity. Unpublished manuscript, August 1995.

[Žák83] Stanislav Žák. A turing machine time hierarchy. *Theoretical Computer Science*, 26:327–333, 1983.