INAUGURAL - DISSERTATION

zur

Erlangung der Doktorwürde

der

Naturwissenschaftlich-Mathematischen Gesamtfakultät

der

Ruprecht - Karls - Universität

Heidelberg

vorgelegt von

Timur Bakibayev

aus Karagandinskaya

Tag der mündlichen Prüfung: 10.03.2010

Weak Completeness Notions For Exponential Time

Gutachter: Prof. Dr. Klaus Ambos-Spies

Prof. Dr. Serikzhan Badaev

Abstract

The standard way for proving a problem to be intractable is to show that the problem is hard or complete for one of the standard complexity classes containing intractable problems. Lutz (1995) proposed a generalization of this approach by introducing more general *weak* hardness notions which still imply intractability. While a set A is hard for a class C if *all* problems in C can be reduced to A (by a polynomial-time bounded many-one reduction) and complete if it is hard and a member of C, Lutz proposed to call a set A weakly hard if a *nonnegligible* part of C can be reduced to A and to call A weakly complete if in addition $A \in$ C. For the exponential-time classes E = DTIME(2^{lin}) and EXP = DTIME(2^{poly}), Lutz formalized these ideas by introducing resource bounded (Lebesgue) measures on these classes and by saying that a subclass of E is negligible if it has measure 0 in E (and similarly for EXP). A variant of these concepts, based on resource bounded Baire category in place of measure, was introduced by Ambos-Spies (1996) where now a class is declared to be negligible if it is meager in the corresponding resource bounded sense.

In our thesis we introduce and investigate new, more general, weak hardness notions for E and EXP and compare them with the above concepts from the literature.

The two main new notions we introduce are nontriviality, which may be viewed as the most general weak hardness notion, and strong nontriviality. In case of E, a set A is E-nontrivial if, for any $k \geq 1$, A has a predecessor in E which is $2^{k \cdot n}$ complex, i.e., which can only be computed by Turing machines with run times exceeding $2^{k \cdot n}$ on infinitely many inputs; and A is strongly E-nontrivial if there are predecessors which are almost everywhere $2^{k \cdot n}$ complex.

Besides giving examples and structural properties of the E-(non)trivial and strongly E-(non)trivial sets, we separate all weak hardness concepts for E, compare the corresponding concepts for E and EXP, answer the question whether (strongly) E-nontrivial sets are typical among the sets in E (or among the computable sets, or among all sets), investigate the degrees of the (strongly) E-nontrivial sets, and analyze the strength of these concepts if we replace the underlying *p*-*m*-reducibility by some weaker polynomial-time reducibilities.

Zusammenfassung

Will man zeigen, dass ein Problem zwar algorithmisch lösbar, aber nur schwer (d.h. nicht in Polynomialzeit) lösbar ist, so macht man dies meist dadurch, dass man das Problem als hart oder vollständig für eine Komplexitätsklasse nachweist, die schwer lösbare Probleme enthält. Lutz (1995) schlug eine Verallgemeinerung dieses Ansatzes vor, die auf *schwachen* Härte- bzw. Vollständigkeitsbegriffen basiert. Während eine Menge A hart (oder schwer) für eine Komplexitätsklasse C ist, wenn alle Probleme aus C auf A reduziert werden können (mittels einer polynomialzeit-bechränkten many-one-Reduktion) und A vollständig für C ist, wenn zusätzlich A selbst in C liegt, nennt Lutz eine Menge A schwach hart, falls ein *nicht zu vernachlässigender* Teil der Probleme aus C auf A reduzierbar ist, und schwach vollständig, wenn wiederum zusätzlich $A \in \mathrm{C}$ gilt. Im Falle der Exponentialzeit-Klassen $\mathrm{E} = \mathrm{DTIME}(2^{lin})$ und $\mathrm{EXP} = \mathrm{DTIME}(2^{poly})$ formalisierte Lutz diese Ideen, indem er geeignete ressourcenbeschränkte Varianten des Lebesgue-Maßes auf diesen Klassen einführte und Teilklassen von E vernachlässigbar nennt, falls diese Maß 0 in E haben (und entsprechend für EXP). Eine Variante dieser Konzepte, in der das Lebesgue-Maß durch Baire-Kategorie ersetzt ist, wurde von Ambos-Spies (1996) vorgeschlagen. Hier sind die vernachlässigbaren Teilklassen diejenigen, die - im entsprechenden ressourcenbeschränkten Sinne - mager sind.

In unserer Dissertation führen wir neue, allgemeinere schwache Härtebegriffe für E und EXP ein und vergleichen diese mit den oben genannten Konzepten aus der Literatur.

Die zwei wichtigsten der von uns neu eingeführten Konzepte sind die Nichttrivialität, die als das allgemeinste schwache Härtekonzept angesehen werden kann, und die starke Nichttrivialität. Im Falle der Klasse E ist eine Menge A E-nichttrivial, falls es für jedes $k \geq 1$ eine Menge aus E gibt, die auf A reduzierbar ist und $2^{k \cdot n}$-komplex ist, d.h. nur von Turingmaschinen erkannt werden kann, deren Laufzeit auf unendlich vielen Eingaben die Schranke $2^{k \cdot n}$ überschreitet; und A ist stark E-nichttrivial, falls diese einen fast überall $2^{k \cdot n}$-komplexen Vorgänger in E besitzt.

In unserer Arbeit geben wir Beispiele für E-(nicht)triviale und stark E-(nicht)triviale Mengen an, untersuchen deren Eigenschaften, trennen alle schwachen Vollständigkeitsbegriffe für E, vergleichen die entsprechenden Begriffe für E und EXP, beantworten die Frage, ob (stark) E-nichttriviale Mengen typisch sind (im Bezug auf E, im Bezug auf die entscheidbaren Mengen und im Bezug auf alle Mengen), untersuchen die (p-m-)Grade der (stark) E-(nicht)trivialen Mengen, und analysieren die Stärke der Varianten der schwachen Härtebegriffe, bei denen die zugrundegelegte p-m-Reduzierbarkeit durch allgemeinere Polynomialzeit-Reduzierbarkeiten ersetzt ist.

Contents

CHAPTER 1

Introduction

Hardness and completeness notions are among the most important concepts of computability theory and computational complexity theory. So, in computability theory, noncomputability of a (decision) problem is usually shown by proving it to be complete or hard for the class of the computably enumerable problems. In complexity theory the most popular completeness notion is completeness for the nondeterministic polynomial-time class NP introduced by Cook (1971) and Karp (1972). By Cook's Thesis, a set is feasibly computable if it can be computed by a polynomial-time bounded deterministic Turing machine. So, assuming P $\neq$ NP, NP-complete problems are intractable, i.e., computable in theory but not feasibly computable.

Though intractability of an NP-complete problem is based on the P $\neq$ NP-assumption, this notion is so popular since there are hundreds of interesting problems which have been shown to be NP-complete (see Garey and Johnson (1979)). In order to show a problem to be *provably* intractable, however, it has to be shown to be hard for a complexity class C for which it has been shown that it is not contained in P.

The most interesting classes here are the exponential-time classes E $=$ DTIME(2^{lin}) and EXP $=$ DTIME(2^{poly}). Here E is considered to be the least, sufficiently closed, complexity class inside of which the basic diagonalizations over polynomial computable sets and functions can be carried out, while the larger class EXP is the least deterministic time class which is known to contain the nondeterministic polynomial-time class NP. So these classes are quite important in structural complexity theory though there are much less problems which are complete for these classes than there are NP-complete problems.

Before we further discuss completeness and hardness, let us look at the definition of theses concepts. The standard completeness and hardness notions in computational complexity theory designed for proving intractability results are based on polynomial-time bounded reductions. The most popular and most simple reducibility here is the polynomial-time bounded version of many-one reducibility (*p*-*m*-reducibility for short) introduced by Karp (1972). Here a set A is *p*-*m*-reducible to a set B ($A \leq_m^p B$) via f if f is a polynomial-time computable function and, for any string x, $x \in A$ if and only if $f(x) \in B$. Then a set A is hard for a class C (under *p*-*m*-reducibility) if any set $C \in$ C is *p*-*m*-reducible to A, and A is complete for C if A is hard for C and in addition a member of C. The crucial observation which makes hardness and the underlying *p*-*m*-reducibility such a useful tool is that intractability is preserved upwards by $\leq_m^p$, i.e., for sets A and B such that A is intractable and $A \leq_m^p B$, B is intractable too. So hard and complete sets for classes containing intractable problems are intractable themselves.

In order to generalize this approach for demonstrating intractability via hardness proofs, one can generalize the polynomial-time reducibility underlying the hardness (hence completeness) notions. There is a great variety of polynomial-time reducibilities which are more general then *p*-*m*-reducibility where the polynomial-time bounded version of Turing reducibility (*p*-T-reducibility for short), which formalizes the notion of a relativized polynomial-time bounded computation, is the most general polynomial-time reducibility (see Ladner et al. (1975) for a comparison of the various types of p-reducibilities). In fact, when Cook (1971) introduced NP-completeness first, he based this notion on p-T-reducibility and only Karp (1972) later refined this notion by basing it on p-m-reducibility.

It should be noted that thus obtained generalizations of NP- or E(XP)-completeness are of minor interest for applications, since natural problems which are p-T-complete for any of theses classes usually turn out to be in fact p-m-complete. So the main interest and importance of these generalizations is in the role they play in the structural analysis of complexity classes in the setting of structural complexity theory. Hence the study of generalized hardness and completeness notions should be viewed as foundational work in the investigation of complexity classes and their structures.

The idea underlying the above generalizations of hardness and completeness is to replace the underlying reducibility by a more general one, i.e., to allow more flexible codings of the members of a complexity class C into the hard sets A. Lutz (1995) proposed an alternative way for generalizing hardness and completeness. While, in the classical sense, a set A is hard for a class C if *all* problems in C can be reduced to A, Lutz proposed to call a set A weakly hard if a *nonnegligible* part of C can be reduced to A (and to call A weakly complete if in addition $A \in$ C). Lutz also proposed to determine, what the negligible parts of a complexity class are, by applying (Lebesgue) measure. Since any complexity class is countable and since any countable class has measure 0, however, this requires the introduction of a resource-bounded measure theory (see Lutz (1992)). Then, by choosing appropriate time-bounds, Lutz introduced measures for the exponential-time classes E and EXP and called a set A weakly E-hard if the part of E which is p-m-reducible to A does not have measure 0 in E (and similarly for EXP). Lutz (1995) showed that his weak hardness concept for E (and EXP) is a proper generalization of the classical hardness concept for E (and EXP) and still guarantees intractability. In fact, Ambos-Spies et al. (1997) have shown that the weakly E-complete sets have measure 1 in E whereas the E-complete sets have measure 0 in E. So a typical set in E is weakly E-hard but not E-hard in the classical sense. Moreover, some structural differences between hard sets and weakly hard sets have been revealed. So any E-complete set contains infinite easy parts (Berman (1976)) whereas there are weakly E-complete sets which are P-bi-immune, i.e., a.e. p-complex (Mayordomo (1994)).

A variant of Lutz's weak hardness notions, based on resource bounded Baire category in place of measure was introduced by Ambos-Spies (1996) where now a class is declared to be negligible if it is meager in the corresponding resource bounded sense. In the following we will refer to the weak hardness concepts of Lutz and Ambos-Spies as measure-hardness and category-hardness, respectively.

A short coming of measure-hardness and category-hardness is that these concepts are based on the quite technical and quite involved concepts of resource-bounded measure and resource-bounded category. In this thesis we will introduce and study some new hardness concepts which are not only more general than the concepts of Lutz and Ambos-Spies but are also conceptually much simpler by being based only on very fundamental concepts from complexity theory.

The first of these new concepts proposed by Ambos-Spies, called nontriviality, is intended to give the most general meaningful weak hardness notions for the exponential-time classes. We discuss this here for the case of E. Since the notion of weak hardness is based on the concept of (non)negligibility, we have to make precise what is the minimum requirement for a subclass of E to be negligible. Since (by the time hierarchy theorem) E can be viewed as the union of the classes of the linear exponential hierarchy $E_1 \subset E_2 \subset E_3 \subset \dots$ where E_k denotes the class $DTIME(2^{kn})$, it is natural to say that a class which is contained in a fixed level of this hierarchy is negligible. So, by taking this as a definition of nonneglibiliy, we may argue that this is the most narrow negligibility concept for E whence if we call a set A E-nontrivial if the part of E p-m-reducible to A is not negligible in this sense then nontriviality is the most general weak hardness notion for E. Note that P is contained in the first level E_1 of the linear-exponential hierarchy, hence is negligible. So E-nontrivial sets are intractable. Moreover, by results in the literature, E-measure and E-category hard sets are E-nontrivial.

Note that a set A is E-nontrivial if, for any $k \geq 1$, there is a 2^{kn}-complex set in E which can be p-m-reduced to A. Correspondingly, we say that A is EXP-nontrivial if, for any $k \geq 1$, there is a 2^{n^k}-complex set in EXP which can be p-m-reduced to A. The second new weak hardness concept we consider, called strong nontriviality, is obtained from nontriviality by replacing infinitely-often complexity by almost-everywhere complexity. So a set A is strongly E-nontrivial if, for any $k \geq 1$, there is an a.e.-2^{kn}-complex set in E which can be p-m-reduced to A (and similarly for EXP).

In the following we give an outline of our thesis mentioning the main results.

In Chapter 2 we present some material from complexity theory to be needed while in Chapter 3 we review the weak hardness notions of Lutz and Ambos-Spies.

In Chapter 4 we introduce nontriviality for E and EXP. There, as in this thesis in general, our focus will be on the concept for E and on sets in E, i.e., we focus on E-nontriviality as a weak E-*completeness* concept. We show that sets of low hyperpolynomial complexity are E-trivial. So, in particular, by applying some results from the literature on hyperpolynomial shifts, we get some first examples of E-trivial intractable problems. We also show, however, that there are E-trivial sets at arbitrarily high levels $E_{k+1} \setminus E_k$ of the linear-exponential hierarchy, thertherebyby showing that high deterministic time complexity within E alone does not guarantee E-nontriviality. Moreover, by extending a result of Buhrman and Mayordomo (1997), we show that (for appropriate time bounds) the set of random strings in the setting of time-bounded Kolmogorov complexity is E-trivial. Moreover we reveal some interesting relations between density of a set and (non)triviality. For instance, we show that any exptally set in $E \setminus E_1$ is E-nontrivial, i.e., very sparse but complex sets are nontrivial.

In Chapter 5 we introduce strong nontriviality together with a third new weak hardness concept, called compression hardness, which may be viewed as a link between strong nontriviality and the stronger category- hardness (and the still stronger measure-hardness). We give some alternative characterization of strong nontriviality for E in terms of E_1-bi-immunity, and, by distinguishing the possible densities of nontrivial, strongly-nontrivial, compression-hard, category-hard, and measure hard sets, we obtain a (strict) hierarchy for these weak hardness and completeness notions for both E and EXP.

In Chapter 6 we compare weak hardness for E and EXP. While, by a simple padding argument, E-hardness and EXP-hardness coincide, Juedes and Lutz (1995b) have shown that any E-measure hard set is EXP-measure hard but that the converse in general fails, and Ambos-Spies (1996) has shown the corresponding phenomenon for category-hardness. Here we duplicate these results for compression-hardness and strong nontriviality, and show that there is an EXP-nontrivial set which is E-trivial. In fact, by giving an EXP-measure complete set which is E-trivial, we show that none of the weak hardness concepts for EXP implies any of the weak hardness concepts for E. We also show that there is an E-nontrivial set which is EXP-trivial which contrasts the above mentioned results for the other weak hardness notions.

In Chapter 7 we raise the question of whether it is typical for a set to be weakly hard for E where we take typicalness in the sense of Lebesgue measure and Baire category. We show that among all sets E-nontrivial sets (hence weakly hard sets for E w.r.t. all other concepts) are rare, i.e., the class of E-nontrivial sets has measure 0 and is meager. This is contrasted by the situation where we only consider sets in E (and work with the corresponding resource-bounded measure and category concepts). Here all the weak hardness notions are typical in the sense of measure and all - with the exception of measure-hardness - are typical in the sense of category. If we look at the universe of the computable sets (and take computable measure and category) the picture becomes still another one. Here strong nontriviality (hence all stronger concepts) is untypical, i.e., the class of strongly E-nontrivial sets has computable measure 0 and is computably meager, whereas E-nontriviality is neither typical nor untypical.

In Chapter 8 we look at the degrees of the E-nontrivial and strongly E-nontrivial sets in E, i.e., look at the distribution of these sets among the sets in E with respect to *p-m*-reducibility. Besides some density type results we obtain a number of splitting theorems. For instance, we show that no E-complete set can be split into two E-nontrivial sets whereas there is such a splitting into two weakly E-trivial sets (i.e., not strongly E-nontrivial) sets.

Finally, in Chapter 9 we look at our new nontriviality notions for E and EXP under the other standard polynomial-time reducibilities. For strong nontriviality we obtain the expected hierarchy theorems showing that, for multi-query reducibilities, more general reducibilities yield more strongly nontrivial sets. For nontriviality, however, we get a corresponding hierarchy theorem only in the case of E whereas in case of EXP this hierarchy collapses.

Finally in Section 10 we conclude with a short discussion of our results.

Acknowledgments

I am deeply grateful to my advisor, Klaus Ambos-Spies, for his intensive and committed supervision. A large part of the results in this thesis emerged from numerous discussions with him, and the concepts treated in this thesis were suggested by him. Moreover, he patiently helped to improve the presentation of the material.

I thank my bachelor and master advisor Professor Serikzhan Badaev for introducing me to mathematical logic and theoretical computer science and for his continuous support during the work on this thesis.

I am also grateful to the other members of the Heidelberg Logic Group, that is, Felicitas Hirsch, Rupert Hölzl, Thorsten Kräling and Wolfgang Merkle, for creating a friendly atmosphere.

And, of course, I am very grateful to my parents, my brother Nurzhan and my sister Ainur who were providing me with both moral and financial support during my stay in Germany.

CHAPTER 2

The Exponential Time Classes

In this chapter we review the fundamental concepts and results from computational complexity theory which we will need. We first shortly review the deterministic time complexity classes and polynomial time reducibilities. Then we have a closer look at the exponential time classes which will be central for our thesis. Finally we shortly discuss almost-everywhere complexity and the related bi-immunity notions.

2.1 Notation

Before we start with our survey of the required concepts of computational complexity theory, we introduce some notations.

2.1.1 Growth of Functions

Let $\mathbb{N} = \{0,1,2,\dots\}$ be the set of natural numbers and let f and g be functions on $\mathbb{N}$, i.e., $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$.

We say that f is *linearly bounded* in g and write $f \in O(g)$ if there are constants $c,d \geq 0$ such that

$$\forall\, n\ (f(n) \leq cg(n) + d).$$

The function g *majorizes* the function f ($f \leq g$) if $f(n) \leq g(n)$ for all $n \geq 0$, and g *dominates* f ($f \leq_{a.e.} g$) if $f(n) \leq g(n)$ almost everywhere (a.e.) i.e., if $f(n) \leq g(n)$ for almost all (i.e., all but finitely many) $n \geq 0$.

f is *polynomially bounded* ($f(n) \in poly(n)$) if f is majorized by some polynomial p. Note that f is polynomially bounded iff f is dominated by some polynomial iff $f \in O(n^k)$ for some $k \geq 0$. f is *polynomially bounded in g* ($f(n) \in poly(g(n))$) if there is a polynomial p such that f is dominated by $p(g)$. f and g are *polynomially related* if $f \in poly(g)$ and $g \in poly(f)$. f is *polynomially honest* if $f(n)$ and n are polynomially related.

2.1.2 Words, Languages, Classes

Let $\Sigma = \{0,1\}$ be the binary alphabet, and let Σ^* be the set of finite binary strings. We call a binary string also a *word* or simply a *string*. A set of words, i.e., a subset of Σ^*, is called a *(binary) language* or a *(decision) problem* or simply a *set*. A set of languages - i.e., a subset of $\mathcal{P}(\Sigma^*)$, the power set of Σ^*, is called a *class*. In the following we let lower case letters from the end of the alphabet $(u,v,w,x,y,z,u_i,\dots)$ denote words, italic capital letters $(A,B,C,\dots)$ denote sets (i.e., languages), and straight capital letters $(\mathrm{A},\mathrm{B},\mathrm{C},\dots)$ denote classes.

The empty word is denoted by λ; $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$. The length of a word x is denoted by $|x|$. $\Sigma^{=n}$ (or shortly Σ^n), $\Sigma^{\leq n}$, $\Sigma^{<n}$ are the sets of words of length n, of

length $\leq n$, and of length less than n, respectively. Similarly, $A^{=n}$, $A^{\leq n}$, $A^{<n}$ are the sets of words in A which are of length n, of length $\leq n$, and of length less than n, respectively. Note that $|\Sigma^n| = 2^n$ and $|\Sigma^{<n}| = 2^n - 1$.

The *length-lexicographical (canonical) ordering* on Σ^* is denoted by $\leq$:

$$x < y \Leftrightarrow |x| < |y| \text{ or } |x| = |y| \ \& \ \exists u, v, w \ (x = u0v \ \& \ y = u1w)$$

The $(n+1)$th word w.r.t. $\leq$ is denoted by z_n. Note that $|z_n| \approx log(n)$.

Frequently we identify Σ^* with the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of (natural) numbers by identifying z_n and n. In particular, for $x \in \Sigma^*$ and $k \geq 0$, $x + k$ is defined by $z_n + k = z_{n+k}$.

We write $x \sqsubseteq y$ if x is a prefix (or initial segment) of y and $x \sqsubset y$ if x is a proper prefix of y. The initial segment of x of length n is denoted by $x \upharpoonright n$; i.e., $x \upharpoonright n = x(0) \dots x(n-1)$.

For a set A and a string x, $A \upharpoonright x$ is the restriction of A to the strings less than x, i.e.,

$$A \upharpoonright x = A \cap \{y : y < x\}.$$

(Note that, by our convention above, $A \upharpoonright n = A \upharpoonright z_n$.)

2.1.3 Density of Languages

The *density* of a set A is measured by its *census function*

$$\sharp_A(n) = |A^{\leq n}|.$$

A set A is *(polynomially) sparse* if the census function of A is polynomially bounded. A is *exponentially dense* if there is a real $\varepsilon > 0$ such that $2^{\varepsilon n}$ is dominated by $\sharp_A(n)$.

A set A is *tally* (or *unary*) if A is a subset of $\{0\}^* = \{0^n : n \geq 0\}$. Note that, for a tally set A, $\sharp_A(n) \leq n + 1$. (So, in particular, any tally set is sparse.) A set A is *exptally* if

$$A \subseteq \{0^{\delta(n)} : n \geq 0\}$$

where $\delta : \mathbb{N} \to \mathbb{N}$ is the *iterated exponential function* inductively defined by $\delta(0) = 0$ and $\delta(n+1) = 2^{\delta(n)}$. Note that the census function of an exptally set is logarithmically bounded, $\sharp_A(n) \in O(log(n))$.

2.1.4 Characteristic Functions and Sequences

The *characteristic function* $c_A : \Sigma^* \to \Sigma$ of a set A is defined by

$$c_A(x) = 1 \Leftrightarrow x \in A.$$

In our notation we will not distinguish between a set and its characteristic function. I.e., we write $A(x) = 1$ if $x \in A$ and $A(x) = 0$ if $x \notin A$.

The *characteristic sequence* χ_A of a set A is the infinite binary sequence defined by

$$\chi_A(n) = 1 \Leftrightarrow z_n \in A.$$

Again, in our notation we will not distinguish between a set and its characteristic sequence. (So, for instance, $A(n)(=\chi_A(n)) = 1$ and $A(z_n)(=c_A(z_n)) = 1$ both say that $z_n \in A$. Moreover, we may identify $A \upharpoonright z_n$ with the string $A(0)\dots A(n-1)$ of length n.)

The set of all infinite binary sequences is denoted by Σ^ω and is called the *Cantor space*. In the following, infinite binary sequences will be denoted by lower case Greek letters $(\alpha, \beta, \gamma, \dots)$.

Note that Σ^ω may be viewed as the set of the infinite paths of the infinite full binary tree, while Σ^* may be viewed as the nodes (or the finite paths) of this tree.

2.1.5 Closure Under Finite Variants

For functions f and f' we call f' a *finite variant* of f if $f(n) = f'(n)$ for almost all n. If f is a finite variant of f' we write $f =_{a.e.} f'$ or shortly $f =^* f'$. By identifying numbers with strings and sets with their characteristic functions, this notion carries over to word functions and sets. We say that a class C is *closed under finite variants (cfv)* if

$$\forall A, A' \ (A \in \mathrm{C} \ \& \ A =_{a.e} A' \ \Rightarrow A' \in \mathrm{C}).$$

2.2 Time Complexity Classes

Here we shortly review some basic facts about the time complexity of deterministic Turing machines. We assume that the reader is familiar with the fundamentals of computability theory and complexity theory. In particular, we assume familiarity with the basic concepts related to Turing machines. For unexplained notation see e.g. Hopcroft and Ullman (1979).

Our model of computation is the deterministic multi-tape Turing machine. We consider both Turing *transducers* computing functions $f : \Sigma^* \to \Sigma^*$ (or, more generally, n-ary functions $f : (\Sigma^*)^n \to \Sigma^*$) and Turing *acceptors* accepting languages $A \subseteq \Sigma^*$ (or, more generally, n-dimensional languages $A \subseteq (\Sigma^*)^n$).

A Turing machine M is *total* if M converges on any input x. Note that the language accepted by a total Turing acceptor is computable (in the formal sense, i.e., recursive) and, similarly, the function computed by a total Turing transducer is total and computable (i.e., (total) recursive). The language accepted by machine M is denoted by $L(M)$. In our notation, however, we usually identify a machine M with its accepted language and write $M(x) = 1$ or $x \in M$ in place of $x \in L(M)$.

For a machine M and a string x, the *run time* of M on input x, $time_M(x)$, is the length of the computation of M on input x, i.e., the number of steps (more formally: the number of instantaneous descriptions) of the computation (if M does not stop on input x, $time_M(x)$ is undefined). Note that, for a total machine M, the run time $time_M$ is computable (total recursive).

A Turing machine M is $t(n)$*-time-bounded* for the computable function $t : \mathbb{N} \to \mathbb{N}$ if M is total and

$$\forall^\infty x \ (time_M(x) \leq t(|x|))$$

(where $\forall^\infty x$ has to be read as *for almost all (i.e., for all but finitely many) strings* x). We will only consider nondecreasing computable time bounds $t(n)$ where $t(n) \geq n$.

Definition 2.1 Let $t : \mathbb{N} \to \mathbb{N}$ be a total computable function. The *deterministic time class* with *bound* t, $\mathrm{DTIME}(t(n))$, consists of all languages A which are accepted by some $t(n)$-time bounded Turing machine.

Similarly, the functional deterministic time class consisting of the functions $f : \Sigma^* \to \Sigma^*$ computable in time $t(n)$ is defined correspondingly and denoted by $\mathrm{FDTIME}(t(n))$. (In fact, in our notation usually we will not distinguish between the complexity class $\mathrm{DTIME}(t(n))$ of sets and the complexity class $\mathrm{FDTIME}(t(n))$ of functions and will write $\mathrm{DTIME}(t(n))$ in both cases.)

Note that the deterministic time classes $\mathrm{DTIME}(t(n))$ are closed under finite variants. Moreover, for computable time bounds $t(n)$ and $t'(n)$ such that $t(n) \leq_{a.e.} t'(n)$,

$$\mathrm{DTIME}(t(n)) \subseteq \mathrm{DTIME}(t'(n)).$$

A sufficient criterion for getting some proper superclass is given by the time-hierarchy theorem.

Theorem 2.2 (Deterministic Time Hierarchy Theorem) *Let $t(n)$ and $t'(n)$ be computable functions such that*

(i) $t(n) \geq n$,

(ii) $t'(n)$ *is (fully) time constructible, and*

(iii) $t'(n) \notin O(t(n) \cdot \log(t(n)))$.

Then

$$\mathrm{DTIME}(t'(n)) \not\subseteq \mathrm{DTIME}(t(n)).$$

Here a computable function $f(n)$ is *(fully) time constructible* if there is a total Turing machine M such that $time_M(x) = f(|x|)$ for all strings x. In the following we will tacitly use that the common time bounds like polynomials or the exponential functions $f(n) = 2^{k \cdot n}$ or $f(n) = 2^{n^k}$ ($k \geq 1$) are time constructible. Moreover, for any computable function $f(n)$ there is a strictly increasing time constructible function f' dominating f.

A class $\mathrm{F} = \{f_k : k \geq 0\}$ (or sequence $(f_k)_{k \geq 0}$) of computable functions f_k is *uniformly computable* if the function $f(k,x) = f_k(x)$ is computable. We call a computable function f a *universal function* for a (uniformly computable) class F if $\mathrm{F} = \{f_k : k \geq 0\}$ where f_k is the kth branch of f (i.e., $f_k(x) = f(k,x)$). A class C of languages is *uniformly computable* if the class of the characteristic functions of the sets in C is uniformly computable, and a computable set A is *universal* for a class C if its characteristic function is universal for the class of the characteristic functions of the members of C.

For uniformly computable F, we call

$$\mathrm{DTIME}(F) = \bigcup_{k \geq 0} \mathrm{DTIME}(f_k(n))$$

a *generalized (deterministic) time class*. The exponential time classes we will consider here (see Section 2.4 below) are examples of generalized time classes. The probably most important generalized time class is the polynomial-time class

$$\mathrm{P} = \mathrm{PTIME} = \bigcup_{p \text{ a polynomial}} \mathrm{DTIME}(p(n)) = \bigcup_{k \geq 1} \mathrm{DTIME}(n^k).$$

By Cook's Thesis, the sets in P, called *polynomial time computable*, are just the sets which or *feasibly computable* or *tractable*, i.e., the sets which are not only computable in theory but also computable in practice. Correspondingly sets $A \notin \mathrm{P}$ are considered to be computable in theory only but not in practice and are called *intractable*.

Note that any generalized time class $\mathrm{DTIME}(F)$ is contained in a time class $\mathrm{DTIME}(f)$. (Namely, for the uniformly computable class $F = \{f_k : k \geq 0\}$, the computable function $f(n) = \max\{f_k(m) : k,m \leq n\}$ will do.)

Moreover, any deterministic time class $\mathrm{DTIME}(t)$ (and any generalized time class $\mathrm{DTIME}(F)$) is itself uniformly computable. I.e., there is a computable set $A \subseteq \mathbb{N} \times \Sigma^*$ such that, for $A_n = \{x \in \Sigma^* : (n,x) \in A\}$, $\mathrm{DTIME}(t(n)) = \{A_n : n \geq 0\}$.

Universal sets for the time classes are used for diagonalization over the classes. So it is of interest to get some time bounds on the complexity of the (least complex) universal sets for a given time class. Such time bounds are provided by the Universal Machine Theorem (which is also used in the proof of the hierarchy theorem above).

Theorem 2.3 (Universal Machine Theorem) *(Hennie and Stearns (1966)) There is a universal Turing machine U such that if $M_e(x) = U(e,x)$ halts within $t(x)$ steps then $U(e,x)$ halts within $c \cdot t(|x|)\log(t(|x|))$ steps, where constant c is independent of the length of x and depends only on alphabet size, number of tapes, and number of states of M_e, and can be computed from these parameters.*

2.3 Polynomial Time Reducibilities

By Cook's Thesis, the polynomial time computable sets and functions are the feasibly computable sets and functions. So the polynomial time bounded reducibilities are a natural tool for comparing intractable problems according to their degree of intractability.

The most common, and at the same time most simple, polynomial time reducibility is the polynomial time bounded variant of the many-one reducibility, also called *Karp-reducibility*, which was independently introduced by Karp (1972) and Levin (1973).

2.3.1 *p-m*-Reducibility

Definition 2.4 A set A is *many-one reducible* to a set B *in polynomial time* (*p-m-reducible*, for short; $A \leq_m^p B$) if there is a function $f \in \mathrm{P}$ such that $A = f^{-1}(B)$, i.e., such that $A(x) = B(f(x))$ for all strings x.

Note that $\leq_m^p$ is a *preordering*, i.e., reflexive (i.e., $A \leq_m^p A$) and transitive (i.e., $A \leq_m^p B$ and $B \leq_m^p C$ implies $A \leq_m^p C$). Moreover, for any sets A and B,

$$A \leq_m^p B \,\&\, A \notin \mathrm{P} \;\Rightarrow\; B \notin \mathrm{P}. \tag{2.1}$$

This property makes *p-m*-reducibility a useful tool for proving intractability of a problem B since it suffices to show that a known intractable problem A can be reduced to B. The same idea can be used to get hyperpolynomial lower bounds on the time complexity.

Definition 2.5 A set A is *p-m-hard* for a class C (or C-*p-m-hard* or C-*hard* for short) if

$$\forall\, C \in \mathrm{C}\ (C \leq_m^p A).$$

And A is *p-m-complete* for a class C (or C-*p-m-complete* or C-*complete* for short) if $A \in \mathrm{C}$ and A is C-*p-m*-hard.

Note that, by transitivity of $\leq_m^p$, a set A is C-hard if $B \leq_m^p A$ for some C-hard set B.

Lemma 2.6 (Reduction Lemma) *Let* C *be a class such that* C $\not\subseteq$ P. *Then any computable* C*-hard set is intractable.*

Since most of our concepts work with $\leq_m^p$ as the underlying reducibility we introduce some more notations and give some more elementary facts here.

For a set A we let

$$\mathrm{P}_m(A) = \{B : B \leq_m^p A\}$$

be the *p-m-lower cone* of A and, similarly, for a class C,

$$\mathrm{P}_m(\mathrm{C}) = \bigcup_{A \in \mathrm{C}} \mathrm{P}_m(A)$$

is the *p-m-lower cone* of C.

2.3.2 *p-m*-Degrees

Two sets A and B are *p-m-equivalent* ($A =_m^p B$) if $A \leq_m^p B$ and $B \leq_m^p A$. Note that $=_m^p$ is an equivalence relation. The *p-m*-equivalence class of A is called the *p-m*-degree of A:

$$deg_m^p(A) = \{B : B =_m^p A\}.$$

We denote degrees by boldface lower case letters ($\mathbf{a}, \mathbf{b}, \mathbf{c}, \dots$). For a class C, we let

$$\mathbf{C} = \mathbf{C}_m^p = \{deg_m^p(A) : A \in \mathrm{C}\}$$

be the class of *p-m*-degrees of the sets in C. In particular we let **REC** (or $\mathbf{REC}_m^p$) denote the class of the *p-m*-degrees of the computable (recursive) sets.

p-m-reducibility induces a partial ordering on the *p-m*-degrees by

$$deg_m^p(A) \leq deg_m^p(B) \Leftrightarrow A \leq_m^p B$$

(i.e., $\leq$ is reflexive, transitive, and anti-symmetric). The partial ordering of the *p-m*-degrees of computable sets, $(\mathbf{REC}_m^p, \leq)$, has a least element, namely $\mathbf{0} =$ P. (Strictly speaking, the empty set $\emptyset$ and the set of all strings Σ^* are not *p-m*-equivalent to the other polynomial-time computable sets. But, by convention, we assume $\emptyset =_m^p \Sigma^* =_m^p A$ for any $A \in$ P.)

The partial ordering of *p-m*-degrees is an upper semi-lattice (u.s.l.), i.e., any pair of *p-m*-degrees, **a** and **b** possesses a least upper bound, called the *join* of **a** and **b** and denoted by $\mathbf{a} \vee \mathbf{b}$. Note that

$$deg_m^p(A) \vee deg_m^p(B) = deg_m^p(A \oplus B)$$

where

$$A \oplus B = 0A \cup 1B = \{0x : x \in A\} \cup \{1y : y \in B\}$$

is the effective disjoint union of A and B. In general, however, a pair of *p-m*-degrees, $\mathbf{a}$ and $\mathbf{b}$ may not possess a greatest lower bound. So $(\mathbf{REC}^p_m, \leq)$ is not a lattice. If $\mathbf{a}$ and $\mathbf{b}$ have a greatest lower bound then it is called the *meet* of $\mathbf{a}$ and $\mathbf{b}$ and is denoted by $\mathbf{a} \wedge \mathbf{b}$. $(\mathbf{a}, \mathbf{b})$ is a *minimal pair* if $\mathbf{a}, \mathbf{b} > \mathbf{0}$ and $\mathbf{a} \wedge \mathbf{b} = \mathbf{0}$.

Ladner has shown that the partial ordering $(\mathbf{REC}^p_m, \leq)$ of the computable *p-m*-degrees is *dense*, i.e., for $\mathbf{a}$ and $\mathbf{b}$ such that $\mathbf{a} < \mathbf{b}$ there is a degree $\mathbf{c}$ such that $\mathbf{a} < \mathbf{c} < \mathbf{b}$. Moreover any computable *p-m*-degree $> \mathbf{0}$ *splits* (or is *join reducible*), i.e., is the join of two lesser degrees, and every computable *p-m*-degree is *branching* (or *meet reducible*), i.e., the meet of two greater degrees.

Another interesting structural property of the upper semi-lattice of the *p-m*-degrees of computable sets is distributivity. Here a u.s.l. $\mathcal{U} = (U, \leq, \vee)$ is *distributive* if

$$\forall\, x_0, x_1, y \in U \ ([y \leq x_0 \vee x_1] \ \Rightarrow \exists\, y_0 \leq x_0, y_1 \leq x_1 \ [y = y_0 \vee y_1]).$$

Theorem 2.7 *The u.s.l.* $(\mathbf{REC}^p_m, \leq, \vee)$ *is distributive.*

Theorem 2.7 easily follows from the following *Distributivity Lemma*.

Lemma 2.8 (Distributivity Lemma) *Let A, B, C be sets such that $C \leq^p_m A \oplus B$. There is a set $D \in$* P *such that $C \cap D \leq^p_m A$ and $C \cap \overline{D} \leq^p_m B$*

PROOF (IDEA). Fix f such that $C \leq^p_m A \oplus B$ via f. Then $D = \{x : i \sqsubseteq f(x)\}$ will have the desired properties. □

For a more detailed outline of the basic results on the polynomial-time degrees, see the survey Ambos-Spies (1999).

2.3.3 Other Polynomial-Time Reducibilities

The most general polynomial-time reducibility is the polynomial-time-bounded variant of *Turing reducibility*, called *p-T-reducibility* for short. A set A is *p-T*-reducible to a set B ($A \leq^p_T B$) if there is a polynomial-time bounded oracle Turing machine M which accepts A if provided with an oracle for B ($A = M^B$). Note that in the computation of $M^B(x)$, a query to the oracle has to be written on the distinguished oracle tape of M. So number and sizes of the oracle queries are bounded by $p(|x|)$ if p is a polynomial bounding the run time of M. Otherwise, there are no restrictions on the oracle queries. In particular the queries may be adaptive, i.e., a query may be chosen depending on the answers of the oracle to the previous queries.

If in a polynomial-time bounded oracle Turing machine, the oracle queries of M on any input x do not depend on the oracle then M is called *nonadaptive*, and we say that A is *truth-table* reducible to B in *polynomial time* (*p-tt-reducible* for short; $A \leq^p_{tt} B$) if $A = M^B$ for a nonadaptive polynomial-time-bounded oracle machine.

If in a *p-tt*-reduction of A to B the number of queries in a computation does not depend on the input, then A is *p-btt-reducible* (*bounded-truth-table*) to B and we write $a \leq^p_{btt}$. If k is bound for the oracle queries in $M^B(x)$ for each x then k is called the *norm* of the *p-btt*-reduction M and we say that A is *p-k-tt*-reducible to B ($A \leq^p_{k\text{-}tt} B$).

A *p-k-tt*-reduction of A to B can be alternatively described by k *selection functions* $g_i : \Sigma^* \to \Sigma^*$ ($i < k$) and an *evaluation function* $h : \Sigma^* \times \Sigma^k \to \Sigma$ where the functions g_i and h are polynomial-time-computable and

$$\forall\, x\, [A(x) = h(x, B(g_0(x)), \ldots, B(g_{k-1}(x)))].$$

Note that a *p-m*-reduction is a special case of a *p*-1-*tt*-reduction where the queries are evaluated *positively*, i.e., where the evaluation function h is given by $h(x,i) = i$.

Refinements of the polynomial-time bounded many-one reducibility are obtained by imposing some restraints on the reduction f in Definition 2.4. If A is *p-m*-reducible to B via f then we say that

- A is *p*-1-*reducible* to B (*polynomial-time one-one reducible*, $A \leq^p_1 B$) if f is one-to-one,
- A is *p-m-li-reducible* to B (*length increasing polynomial-time many-one reducible*, $A \leq^p_{m\text{-}li} B$) if f is length increasing, i.e., $|x| < |f(x)|$ for all x, and
- A is *p*-1-*li-reducible* to B (*length increasing polynomial-time one-one reducible*, $A \leq^p_{1\text{-}li} B$) if f is one-to-one and length increasing.

We call reducibility $\leq_{r'}$ *weaker* than reducibility $\leq_r$ if, for all sets A and B,

$$A \leq_r B \Rightarrow A \leq_{r'} B,$$

and $\leq_{r'}$ is *strictly weaker* than $\leq_r$ if $\leq_{r'}$ is weaker than $\leq_r$ but $\leq_r$ is not weaker than $\leq_{r'}$.

By definition, $\leq^p_T$ is weaker than $\leq^p_{tt}$, $\leq^p_{tt}$ is weaker than $\leq^p_{btt}$, $\leq^p_{btt}$ is weaker than $\leq^p_{k\text{-}tt}$, $\leq^p_{(k+1)\text{-}tt}$ is weaker than $\leq^p_{k\text{-}tt}$, $\leq^p_{1\text{-}tt}$ is weaker than $\leq^p_m$, $\leq^p_m$ is weaker than $\leq^p_1$ and $\leq^p_{m\text{-}li}$, and $\leq^p_1$ and $\leq^p_{m\text{-}li}$ are weaker than $\leq^p_{1\text{-}li}$ (for any $k \geq 1$). In fact, all of these implications are strict (see Ambos-Spies (1999) for references and details).

In the following we call a polynomial-time bounded reducibility $\leq^p_r$ a *standard polynomial-time reducibility* if $\leq^p_r$ is among the above reducibilites and we call $\leq^p_r$ a *normal polynomial-time reducibility* if $r = T, tt, btt, 1 - tt, m, 1$.

The notions and results of Section 2.3.1 on *p-m*-reducibility can be carried over to all standard reducibilities $\leq^p_r$.

The normal polynomial-time reducibilities are reflexive and transitive. (For $r = k - tt$ with $k \geq 2$, $\leq^p_r$ is not transitive, and for $r = 1 - li, m - li$, $\leq^p_r$ is not reflexive.) So, for such r, *p-r*-degrees can be defined as the *p-m*-degrees as in Section 2.3.1. Again we obtain the same results for the *p-r*-degrees as for the *p-m*-degrees with the exception of the distributivity theorem (Theorem 2.7) which only holds for the 1-query reducibilities but fails for *btt*, *tt* and T (see Ambos-Spies (1999)).

2.4 The Exponential Time Classes E and EXP

2.4.1 Linear and Polynomial Exponential Time

We now introduce the exponential time classes we will deal with. We will focus on the following two classes.

$$\mathrm{E} = \bigcup_{k\geq 1} \mathrm{DTIME}(2^{kn}) \quad (\mathit{Linear\ Exponential\ Time}) \tag{2.2}$$

$$\mathrm{EXP} = \bigcup_{k\geq 1} \mathrm{DTIME}(2^{n^k}) \quad (\mathit{Polynomial\ Exponential\ Time}) \tag{2.3}$$

We will use the following abbreviations for the individual levels of these classes.

$$\mathrm{E}_k = \mathrm{DTIME}(2^{kn})$$

$$\mathrm{EXP}_k = \mathrm{DTIME}(2^{n^k})$$

Note that, by the time-hierarchy theorem, the hierarchies of the linear exponential time classes and of the polynomial exponential time classes are proper, i.e.,

$$\mathrm{E}_1 \subset \mathrm{E}_2 \subset \mathrm{E}_3 \subset \ldots \subset \mathrm{E} \tag{2.4}$$

and

$$\mathrm{EXP}_1 \subset \mathrm{EXP}_2 \subset \mathrm{EXP}_3 \subset \ldots \subset \mathrm{EXP}. \tag{2.5}$$

Moreover,

$$\mathrm{E} \subset \mathrm{EXP}_2 \tag{2.6}$$

and

$$\mathrm{P} \subset \mathrm{E}_1. \tag{2.7}$$

(Also note that $\mathrm{E}_1 = \mathrm{EXP}_1$.) The fact that the classes E and EXP may be viewed as hierarchies will be fundamental for the weak completeness notions we will discuss.

Note that the classes E and EXP are generalized time classes. So E and EXP as well as the individual levels E_k and EXP_k of these classes are uniformly computable. By Theorem 2.3 we may fix computable enumerations of these classes as follows.

- $\{E_e^k : e \geq 0\} = \mathrm{E}_k$ where $E_e^k(x)$ can be uniformly computed in $O(2^{(k+1)\cdot max(e,|x|)})$ steps ($k \geq 1$).
- $\{E_e : e \geq 0\} = \mathrm{E}$ where $E_e(x)$ can be uniformly computed in $O(2^{e\cdot max(e,|x|)})$ steps.
- $\{EXP_e^k : e \geq 0\} = \mathrm{EXP}_k$ where $EXP_e^k(x)$ can be uniformly computed in $O(2^{max(e,|x|)^{k+1}})$ steps ($k \geq 1$).
- $\{EXP_e : e \geq 0\} = \mathrm{EXP}$ where $EXP_e(x)$ can be uniformly computed in $O(2^{max(e,|x|)^e})$ steps.

In the following we will tacitly use the fact that enumerations as above exist.

2.4.2 Exponential Time and Polynomial Reducibilities

The polynomial exponential time class EXP is downward closed under p-T-reducibility (hence under all polynomial-time reducibilities).

Lemma 2.9 *Let A and B be sets such that $A \leq^p_T B$ and $B \in \mathrm{EXP}$. Then $A \in \mathrm{EXP}$.*

PROOF (IDEA). Fix k such that $B \in \mathrm{EXP}_k$, fix a polynomial time bounded oracle Turing machine M such that $A = M^B$, and fix k' such that the run time of M is dominated by the polynomial $n^{k'}$. Then, in order to compute $A(x) = M^B(x)$ for a string x of length n, we have to simulate the $\leq n^{k'}$ steps of the machine M on input x where each of the at most $n^{k'}$ oracle queries, all of size $\leq n^{k'}$ have to be answered using a given 2^{n^k} time bounded algorithm for computing B. All this can be done in

$$O(n^k + n^{k'} \cdot 2^{(n^{k'})^k}) \leq O(2^{n^{kk'+1}})$$

steps. So $A \in \mathrm{EXP}_{kk'+1} \subseteq \mathrm{EXP}$. □

By straightforward modifications of the above proof we obtain the following lemma (where we only consider p-m-reducibility).

Lemma 2.10 *Let A and B be sets and let f be a polynomial-time-computable function such that $A \leq^p_m B$ via f.*

(i) If $B \in \mathrm{E}_k$ and $|f(x)| \leq_{a.e.} k' \cdot |x|$ then $A \in \mathrm{E}_{kk'}$.

(i) If $B \in \mathrm{EXP}_k$ and $|f(x)| \leq_{a.e.} |x|^{k'}$ then $A \in \mathrm{EXP}_{kk'}$.

In general the above bounds cannot be improved. In fact, by some simple padding argument, EXP is the closure of the first level E_1 of the E-hierarchy under p-m-equivalence.

Theorem 2.11 (First Padding Lemma) *For any set $A \in \mathrm{EXP}$ there is a set $A' \in \mathrm{E}_1$ such that $A \leq^p_{1\text{-}li} A' \leq^p_m A$. So, in particular, $A =^p_m A'$.*

PROOF (IDEA). Given $A \in \mathrm{EXP}$, fix k such that $A \in \mathrm{EXP}_k$ and let $A' = \{0^{|x|^k}1x : x \in A\}$. □

Corollary 2.12 *For any p-r-reducibility weaker than $\leq^p_m$, the classes E_k ($k \geq 1$), E, and EXP_k ($k \geq 1$) are not closed under p-r-equivalence, hence not downward closed under $\leq^p_r$.*

Corollary 2.13 *For any standard polynomial-time reducibility $\leq^p_r$,*

$$\mathrm{P}_r(\mathrm{E}_1) = \mathrm{P}_r(\mathrm{E}) = \mathrm{P}_r(\mathrm{EXP}) = \mathrm{EXP}.$$

2.4.3 Complete Sets

An example of an E complete set is the *bounded halting problem* for deterministic time Turing machines. More formally, given a standard universal k-tape Turing machine U (see Theorem 2.3), let

$$K_{bd} = \{\langle e, x, z_n \rangle : U \text{ on input } (e,x) \text{ stops in at most } n \text{ steps}\}.$$

(Note that $O(n) = O(2^{|z_n|})$. So simulating the computation of U on input (e,x) for n steps takes $O(2^{|\langle e,x,z_n\rangle|})$ steps.)

Lemma 2.14 *The bounded halting problem K_{bd} is* E*-complete, in fact p-*1*-li-complete for* E*.*

By the padding lemma above (Theorem 2.11), the hardnes notions for all of the exponential time classes coincide.

Theorem 2.15 *For any standard polynomial-time reducibility $\leq_r^p$ and any set A the following are equivalent.*

(i) A is p-r-hard for E_1.

(ii) A is p-r-hard for E.

(iii) A is p-r-hard for EXP.

PROOF. This is immediate by Corollary 2.13. □

Corollary 2.16 *For any standard polynomial-time reducibility $\leq_r^p$ and any set $A \in$* E *the following are equivalent.*

(i) A is p-r-complete for E.

(ii) A is p-r-complete for EXP.

PROOF. This is immediate by Theorem 2.15. □

2.4.4 Comparing Completeness Notions for E

The relations among the completeness (and hardness) notions for the exponential time classes under the different polynomial-time reducibilities have been studied in the literature. By Theorem 2.15 it suffices to consider the case of completeness for the linear exponential time class E.

Let

$$\mathrm{EC}_r = \{A : A \ p\text{-}r\text{-complete for E}\}.$$

Watanabe has given a complete separation of the completenes notions for E under the multi-query reducibilities.

Theorem 2.17 *(Watanabe (1987)) For $k \geq 2$,*

$$\mathrm{EC}_m \subset \mathrm{EC}_{k-tt} \subset \mathrm{EC}_{(k+1)-tt} \subset \mathrm{EC}_{btt} \subset \mathrm{EC}_{tt} \subset \mathrm{EC}_T. \tag{2.8}$$

In contrast to Watanabe's results, however, the completeness notions for E under the 1-query reducibilities coincide.

Theorem 2.18 *(Berman (1976) and Homer et al. (1993))*

$$\mathrm{EC}_{1\text{-}li} = \mathrm{EC}_{1} = \mathrm{EC}_{m\text{-}li} = \mathrm{EC}_{m} = \mathrm{EC}_{1\text{-}tt}. \tag{2.9}$$

2.5 Almost-Everywhere Complexity and Bi-Immunity

If a set A is not a member of the deterministic time class $\mathrm{DTIME}(t(n))$ then any Turing machine computing A will run for more than $t(|x|)$ steps on *infinitely many* inputs x. So A is *infinitely often* $t(n)$-complex. In this section we will introduce the basic notions and facts on *almost everywhere* complexity. For more details see e.g. the second volume of the monograph by Balcázar et al. (1990).

For any time bound $t(n)$, call a set A *a.e.* $t(n)$*-complex* if for any Turing machine M computing A, $time_M(x) > t(|x|)$ for almost all strings x. Almost-everywhere complexity can be described in terms of bi-immunity.

Definition 2.19 A set A is *immune* against a class C (or C-*immune* for short) if A is infinite and A does not contain any infinite subset B where $B \in \mathrm{C}$. A set A is *bi-immune* against C (or C-*bi-immune* for short) if A and the complement of A, $\overline{A}$, are immune against C.

Note that A is bi-immune against a c.f.v. C if and only if, for any infinite set $B \in \mathrm{C}$, $A \cap B$ and $\overline{A} \cap B$ are infinite. The relations between bi-immunity, a.e.-complexity, and i.o.-complexity can be summarized as follows.

Lemma 2.20 *For any computable time bound $t(n)$ and any set A the following are equivalent.*

(i) A is a.e. $t(n)$-complex.

(ii) A is $\mathrm{DTIME}(t(n))$-bi-immune.

(iii) For any infinite set $B \in \mathrm{DTIME}(t(n))$, $A \cap B \notin \mathrm{DTIME}(t(n))$.

The time-hierarchy theorem can be extended to bi-immunity (hence a.e.-complexity). The following hierarchy theorem for bi-immune sets has been shown by Geske, Huynh, Selman.

Theorem 2.21 *(Geske et al. (1987)). Let $t_1(n)$ and $t_2(n)$ be computable nondecreasing functions such that* *(i)* $t_2(n)$ *is (fully) time-constructible,*

(ii)

$$\liminf_{n\to\infty} \frac{t_1(n)\log t_1(n)}{t_2(n)} = 0,$$

and

(iii) there exists a (fully) time-constructible nondecreasing and unbounded function $f(n)$ *such that*

$$\liminf_{n\to\infty} \frac{f(n)t_1(n)\log t_1(n)}{t_2(n)} = 0.$$

Then there exists a $\mathrm{DTIME}(t_1(n))$*-bi-immune set in* $\mathrm{DTIME}(t_2(n))$*.*

So, in particular, we obtain the following existence results for bi-immune sets for the exponential time classes.

Corollary 2.22 *For any* $k \geq 1$ *there is an* E_k*-bi-immune set in* E_{k+1} *and an* EXP_k*-bi-immune set in* EXP_{k+1}.

PROOF. Let $f(n) = n$. Then the hypothesis of Theorem 2.21 holds for $t_1(n) = 2^{kn}$ and $t_2(n) = 2^{(k+1)n}$ (and $t_1(n) = 2^{n^k}$ and $t_2(n) = 2^{n^{k+1}}$). □

It is interesting to note that, for the 1-query reducibilities, almost-everywhere complexity and hardness for E are not compatible as Berman (1976) has shown.

Theorem 2.23 *(Berman (1976)) Let A be* E*-hard (under p-m-reducibility). Then A is not* P*-immune.*

2.5.1 Bi-Immunity and Incompressibility

We close our short discussion of bi-immunity with introducing a stronger incompressibility poperty which we will use in the following too.

Definition 2.24 A set A is *many-one reducible* to a set B *in time* $t(n)$ ($t(n)$*-m-reducible*, for short; $A \leq_m^{t(n)} B$) if there is a function $f \in \mathrm{DTIME}(t(n))$ such that $A = f^{-1}(B)$, i.e. $A(x) = B(f(x))$ for all strings x.

Definition 2.25 (Ko and Moore (1981)) A set A is $t(n)$*-incompressible* if, for any set B and any function g such that $A \leq_m^{t(n)} B$ via g, g is almost one-to-one (i.e., for some string x, $g(y) \neq g(z)$ for all strings $x < y < z$).

We also say, that a set A is C*-incompressible* for some class C if, for any set B and any function $g \in$ C such that $A \leq_m B$ via g, g is almost one-to-one. In particular sometimes we write $\mathrm{DTIME}(t(n))$-incompressible in place of $t(n)$-incompressible. Moreover we write p-incompressible in place of P-incompressible. In the literature, $t(n)$-incompressibility is also called *strong* $\mathrm{DTIME}(t(n))$*-bi-immunity*.

Lemma 2.26 *(Ko and Moore (1981)) Let A be $t(n)$-incompressible. Then A is* $\mathrm{DTIME}(t(n))$*-bi-immune.*

Note that the converse of Lemma 2.26 is not true. For instance, for any P-bi-immune set A, $A \oplus A$ is P-bi-immune too but, for any set A, $A \oplus A$ is not p-incompressible.

CHAPTER 3

Weak Completeness Notions in the Literature

In this chapter we review the weak hardness notions in the literature. Weak hardness was proposed in Lutz (1995) as a generalization of hardness. The idea underlying this concept is as follows. While, for a C-hard set A, all sets from C are reducible to A, in case of a weakly hard set A for C, only a nonnegligible part of the sets in C must be reducible to A. For the exponential time classes E and EXP Lutz formalized the notion of negligibility by first introducing some resource-bounded measures for these classes and by then declaring a class to be negligible if it has measure 0 in E and EXP, respectively. Later, Ambos-Spies (1996) gave some alternative interpretation of negligibility in terms of resource-bounded Baire category thereby giving some alternative weak hardness notions.

In the following we first introduce Lutz's resource bounded measure theory and then introduce the corresponding weak hardness notions which we call measure-hardness here. Then we describe Ambos-Spies' alternative weak hardness concepts, called category-hardness here, where we again start with a short survey of the underlying resource-bounded Baire category concept.

In case of resource-bounded measure and resource-bounded Baire category we describe these concepts in terms of typical sets, namely random sets and generic sets, respectively, which will yield useful characterizations of the corresponding weak hardness concepts. For more details on this approach see Ambos-Spies and Mayordomo (1997) and Ambos-Spies (1996), respectively.

3.1 Computable and Time-Bounded Measure

In this section we shortly review the basic concepts and facts from the theory of computable and time-bounded measure which will be the basis of Lutz's weak completeness concept.

Using the characterization of the classical Lebesgue measure on the Cantor space in terms of martingales, Schnorr (1971) introduced a computable measure based on *computable* martingales. This measure can be used for a quantitative analysis of the class REC of computable sets since the class REC does not have computable measure 0 whereas, for instance, any time complexity class DTIME$(t(n))$ has measure 0.

By considering resource-bounded martingales, Lutz (1992) refined Schnorr's theory, and developped measure theories for sufficiently closed complexity classes. In particular he introduced such measures for the exponential time classes E and EXP.

The following overview is based on the survey article Ambos-Spies and Mayordomo (1997). For proofs missing here and, in general, for a more complete treatment of the material, we refer to this survey.

3.1.1 Martingales and Measure

The classical (Lebesgue) measure μ on the Cantor space Σ^ω is the product measure on the space of the infinite binary sequences induced by the uniform measure $\mu(\{0\}) = \mu(\{1\}) = \frac{1}{2}$ on $\mathcal{P}(\{0,1\})$. By identifying a set (language) $A \subseteq \{0,1\}^*$ with its characteristic sequence $A(z_0)A(z_1)A(z_2)\dots$, a complexity class C becomes a subset of the Cantor space whence $\mu(\mathrm{C})$ is well defined and assigns a size to the class C. Since any complexity class C is countable, however, $\mu(\mathrm{C}) = 0$. So, in order to be able to distinguish between the sizes of complexity classes, we will need some effective or even resource-bounded variants of the Lebesgue measure. The definition of these variants is based on the following alternative characterization of Lebesgue measure in terms of betting games.

Definition 3.1 (a) A *martingale* is a function $d : \{0,1\}^* \to [0,\infty)$ such that $d(\lambda) > 0$ and, for every $x \in \{0,1\}^*$, the following equality (called *fairness condition*) holds.

$$\frac{d(x0)+d(x1)}{2} = d(x) \tag{3.1}$$

$d(\lambda)$ is called the *norm* of d. d is *normed* if $d(\lambda) = 1$.

(b) A martingale *d succeeds* on a set A if

$$\limsup_{n\geq 0} d(A \upharpoonright n) = \infty.$$

$S^\infty[d]$ denotes the class of sets on which the martingale d succeeds. A martingale *d succeeds* on a class C if $\mathrm{C} \subseteq S^\infty[d]$.

Definition 3.2 (a) A *(betting) strategy s* is a function $s : \{0,1\}^* \to [0,1]$.

(b) The *strategy s_d underlying the martingale d* is the function

$$s_d(x) = \begin{cases} \frac{d(x0)}{2d(x)} & \text{if } d(x) \neq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

(c) Conversely, for every strategy s and every real $\alpha > 0$, the *martingale $d[s,\alpha]$* of norm α *induced* by s is defined by $d(\lambda) = \alpha$ and, for any string $X \upharpoonright (n+1)$ where $n \geq 0$,

$$d(X \upharpoonright (n+1)) = \begin{cases} 2 \cdot s(X \upharpoonright n) \cdot d(X \upharpoonright n) & \text{if } \; X(n) = 0 \\ 2 \cdot (1 - s(X \upharpoonright n)) \cdot d(X \upharpoonright n) & \text{if } \; X(n) = 1. \end{cases} \tag{3.3}$$

The intuition behind the above definitions is as follows.

In a betting game, a player bets on the successive bits of a hidden sequence X in Σ^ω using a strategy s. The player's initial capital is $\alpha > 0$, and the martingale $d = d[s,\alpha]$ describes the capital of the palyer in the course of the game.

In round n, after the first $n-1$ bits, $X \upharpoonright n$, have been revealed to the player, the player bets on the value of $X(n)$. According to his strategy s, the player splits his current capital $d(X \upharpoonright n)$ into two parts where $s(X \upharpoonright n) \cdot d(X \upharpoonright n)$ is the stake on outcome 0 while the remaining capital $(1 - s(X \upharpoonright n)) \cdot d(X \upharpoonright n)$ is bet on outcome

1. Then $X(n)$ is revealed, and the stake on the correct outcome is doubled while the stake on the wrong outcome is lost. So $d(X \upharpoonright (n+1))$ will be the capital of the player after round n.

The player succeeds on the sequence X if his capital is unbounded in the infinitely many rounds of this game.

Theorem 3.3 *A class* C *has Lebesgue measure* 0 *if and only if there is a martingale which succeeds on* C.

Based on this observation, Schnorr (1971) introduced an effective measure by considering only computable martingales. As one can easily show (see e.g. Ambos-Spies and Mayordomo (1997)) it suffices to consider (normed) rational valued martingales.

3.1.2 Computable and Time-Bounded Martingales

Definition 3.4 (Schnorr (1971), Lutz (1992)) (a) A rational valued strategy $s : \{0,1\}^* \to [0,1] \cap \mathbb{Q}$ is a *computable strategy* if s is computable, and s is a $t(n)$-*strategy* if $s \in \mathrm{DTIME}(t(n))$.

(b) A *computable martingale* is a martingale $d = d[s,\alpha]$ induced by a $t(n)$-strategy s and a rational number $\alpha > 0$, and d is a $t(n)$-*martingale* if $d = d[s,\alpha]$ for some $t(n)$-strategy s and some rational number $\alpha > 0$.

In the following we tacitly assume that, for any time bound $t(n)$, $t(n)$ is computable and nondecreasing. In defining the complexity of a martingale, we follow Ambos-Spies and Mayordomo (1997) and consider the complexity of the underlying strategy not the complexity of the martingale itself. (As shown there, the two possible approaches for defining the complexity of martinagales lead to the same measures on the classes REC, E and EXP which we will consider in this thesis.) The complexity of a martingale and the complexity of its underlying strategy are related to each other as follows.

Lemma 3.5 *(see Ambos-Spies and Mayordomo (1997)) (a) For any $t(n)$-martingale d, $d \in \mathrm{DTIME}(n \cdot t(n) \cdot log(t(n))^2)$.*

(b) Any martingale $d \in \mathrm{DTIME}(t(n))$ is a $(t(n) \cdot log(t(n))^2)$-martingale.

Moreover, we obtain the following upper bound on the deterministic time classes containig sets on which a given $t(n)$-martingale does not succeed.

Lemma 3.6 *Let $t(n) \geq n$ and $t'(n)$ be computable nondecreasing functions such that*

$$t'(n) \geq_{a.e.} 2^n \cdot t(2^{n+1}) \tag{3.4}$$

holds, and let d be a $t(n)$-martingale. There is a set $A \in \mathrm{DTIME}(t'(n))$ such that d does not succeed on A.

PROOF. Fix a $t(n)$-strategy s and a rational number $\alpha > 0$ such that $d = d[s,\alpha]$. Inductively define A by letting

$$A(z_n) = \begin{cases} 0 & \text{if } s(A \upharpoonright n) \leq \frac{1}{2} \\ 1 & \text{otherwise.} \end{cases} \tag{3.5}$$

Then, by definition of $d = d[s,\alpha]$,

$$d(A \upharpoonright (n+1)) \leq d(A \upharpoonright n)$$

for all $n \geq 0$. So

$$\limsup_{n\to\infty} d(A \upharpoonright n) = \inf_{n\to\infty} d(A \upharpoonright n) \leq d(\lambda) = \alpha < \infty$$

whence d does not succeed on A.

It remains to show that $A \in \mathrm{DTIME}(t'(n))$. This is established by analysing the complexity of the following procedure for computing A.

Given x, in order to compute $A(x)$ it suffices

- to compute m such that $x = z_m$ and
- to compute $i_0, \ldots, i_m$ where, for $k \leq m$,

$$i_k = \begin{cases} 0 & \text{if } s(i_0 \ldots i_{k-1}) \leq \frac{1}{2} \\ 1 & \text{otherwise.} \end{cases}$$

Then, by (3.5), $A(x) = i_m$. Now, the time for computing m can be neglected. On the other hand, since s is a $t(n)$-strategy, since t is nondecreasing, and since $m+1 \leq 2^{|z_m|+1} = 2^{|x|+1}$, $i_0, \ldots, i_m$ can be computed in

$$O(\sum_{k=0}^{m} t(k)) \leq O((m+1)\cdot t(m)) \leq O(2^{|x|+1} \cdot t(2^{|x|+1})) = O(2^{|x|} \cdot t(2^{|x|+1}))$$

steps. So, by (3.4), $A(x)$ can be computed in $O(t'(|x|))$ steps. □

3.1.3 Computable and Time-Bounded Measure

Now, inspired by Theorem 3.3, the computable or time-bounded measure of a class is defined as follows.

Definition 3.7 (Schnorr (1971), Lutz (1992)) (a) A class C has *computable (or effective) measure* 0 ($\mu_{\mathrm{rec}}(\mathrm{C}) = 0$) if there is a computable martingale d that succeeds on C; and C has $t(n)$*-measure* 0 ($\mu_t(\mathrm{C}) = 0$) if there is a $t(n)$-martingale d that succeeds on C.

(b) A class C has *computable (or effective) measure* 1 ($\mu_{\mathrm{rec}}(\mathrm{C}) = 1$) if $\overline{\mathrm{C}}$ has computable measure 0; and C has $t(n)$*-measure* 1 ($\mu_t(\mathrm{C}) = 1$) if $\overline{\mathrm{C}}$ has $t(n)$-measure 0.

Note that classical measure μ, computable measure μ_{rec} and $t(n)$-time-bounded measure μ_t are related as follows. For any class C and for any computable function $t(n)$,

$$\mu_t(\mathrm{C}) = 0 \Rightarrow \mu_{\mathrm{rec}}(\mathrm{C}) = 0 \Rightarrow \mu(\mathrm{C}) = 0 \tag{3.6}$$

and

$$\mu_t(\mathrm{C}) = 1 \Rightarrow \mu_{\mathrm{rec}}(\mathrm{C}) = 1 \Rightarrow \mu(\mathrm{C}) = 1 \tag{3.7}$$

(but, in general, none of these implications can be reversed). Moreover, the following relations among the time-bounded measures are immediate by definition.

Proposition 3.8 *(a) Let t, t' be computable functions such that $t(n) \leq t'(n)$ almost everywhere. Then, for any class* C *and for $i \in \{0,1\}$,*

$$\mu_t(\mathrm{C}) = i \Rightarrow \mu_{t'}(\mathrm{C}) = i \Rightarrow \mu_{\mathrm{rec}}(\mathrm{C}) = i \Rightarrow \mu(\mathrm{C}) = i.$$

(b) For any class C *and for $i \in \{0,1\}$, $\mu_{\mathrm{rec}}(\mathrm{C}) = i$ if and only if there is a computable function $t(n)$ such that $\mu_t(\mathrm{C}) = i$.*

Computable measure and $t(n)$-time bounded measure are not measures in the classical sense since they are not σ-additive. These algorithmic measures, however, are finitely additive, and the following union theorem holds (see Ambos-Spies and Mayordomo (1997)) which is a very useful tool for the investigation of the time-bounded measures.

Theorem 3.9 (Union Theorem for Time-Bounded Martingales) *Let $t(n)$ and $t'(n)$ be nondecreasing computable functions such that $t(n)$ is time constructible and $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ almost everywhere. There is a $t'(n)$-martingale d which succeeds on all $t(n)$-measure-0 classes, i.e.,*

$$\mu_{t'}(\bigcup\{\mathrm{C} : \mu_t(\mathrm{C}) = 0\}) = 0.$$

The ideas underlying the proof of the Union Theorem are as follows. First, given a sequence of martingales d_m ($m \geq 0$), by taking the weighted sum of the sequence, we obtain a martingale d which succeeds on all sets on which at least one of the given martingales succeeds. Second, for any time bound $t(n)$ there are only countably many functions f_m ($m \geq 0$), which can be computed in time $t(n)$ and, for time constructible $t(n)$, by using a universal machine, these function can be combined into one computable (binary) function f of time complexity $t'(n)$, where the time bound $t'(n)$ reflects the overhead required by the universal machine (compare with the time-hierarchy theorem).

There is another difference between classical and algorithmic measure. The size assigned to a class by computable or resource-bounded measure also depends on the algorithmic structure of its membes. In fact, there are sets A, called *random* sets, such that the singleton classes $\{A\}$ do not have resource-bounded or computable measure 0.

Since randomness is a useful tool for describing computable and time-bounded measure, next we look at this concept in some more detail before we will introduce measures on the classes of the computable and exponential time computable sets.

3.1.4 Time-Bounded Randomness

Definition 3.10 (a) Let $\mathrm{F} = \{f_n : n \geq 0\}$ be a countable class of martingales. A set A is F-*random* if no martingale in F succeeds on A.

(b) A set A is *computably random* (or *rec-random* for short) if no computable martingale succeeds on A (i.e., if A is F-random for the class F of computable martingales), and A is $t(n)$-*random* if no $t(n)$-martingale succeeds on A (i.e., if A is F-random for the class F of $t(n)$-martingales).

The classes of *rec*-random and $t(n)$-random sets are denoted by $\mathrm{RAND}(rec)$ and $\mathrm{RAND}(t(n))$, respectively.

The following two facts are immediate by definition and by Proposition 3.8, respectively.

Proposition 3.11 *For any set A, the following are equivalent.*

(i) A is $t(n)$-random.

(ii) $\mu_t(\{A\}) \neq 0$.

(iii) For every $t(n)$-measure-1 class C, $A \in \mathrm{C}$.

Proposition 3.12 *(a) Let t, t' be computable functions such that $t(n) \leq t'(n)$ almost everywhere. Then any $t'(n)$-random set is $t(n)$-random, i.e.,*

$$\mathrm{RAND}(t'(n)) \subseteq \mathrm{RAND}(t(n)).$$

(b) A set A is rec-random if and only if A is $t(n)$-random for all computable functions $t(n)$. I.e.,

$$\mathrm{RAND}(rec) = \bigcap_{t \in \mathrm{REC}} \mathrm{RAND}(t(n)).$$

Moreover, since the dual strategy $\overline{s}(x) = 1 - s(x)$ of a $t(n)$-strategy is a $t(n)$-strategy too, the classes of time-bounded random sets are closed under complements.

Proposition 3.13 *A set A is $t(n)$-random (rec-random) if and only if $\overline{A}$ is $t(n)$-random (rec-random).*

Since, for any martingale d, the class of sets on which the martingale d does not succeed has measure 1, for any countable class F of martingales, the class of F-random sets has (classical) measure 1.

Lemma 3.14 *For any countable class* F *of martingales, the class of* F*-random sets has measure 1. So, in particular, $\mu(\mathrm{RAND}(rec)) = 1$.*

By the Union Theorem for Time-Bounded Martingales, we get the following effectivization of the previous fact for the class of the $t(n)$-random sets.

Theorem 3.15 (Time-Bounded-Randomness Theorem) *Let $t(n)$ and $t'(n)$ be nondecreasing computable functions such that $t(n)$ is time constructible and $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ almost everywhere. Then $\mu_{t'}(\mathrm{RAND}(t(n))) = 1$ and there is a $t(n)$-random set $A \in \mathrm{DTIME}(2^n \cdot t'(2^{n+1}))$.*

PROOF. By definition,

$$\overline{\mathrm{RAND}(t(n))} = \bigcup_{d\ t(n)\text{-martingale}} S^\infty[d]. \tag{3.8}$$

Moreover, for any $t(n)$-martingale d, $\mu_t(S^\infty[d]) = 0$. Since there are only countably many $t(n)$-martingales, it follows with the Union Theorem for Time-Bounded Martingales, that there is a $t'(n)$-martingale d' such that

$$\bigcup_{d\ t(n)\text{-martingale}} S^\infty[d] \subseteq S^\infty[d']. \tag{3.9}$$

whence, in particular,

$$\mu_{t'}(\bigcup_{d\ t(n)\text{-martingale}} S^\infty[d]) = 0.$$

So, by (3.8), $\mu_{t'}(\mathrm{RAND}(t(n))) = 1$.

Moreover, by (3.9), any set A on which the $t'(n)$-martingale d' does not succeed is $t(n)$-random. So there is a $t(n)$-random set A in $\mathrm{DTIME}(2^n \cdot t'(2^{n+1}))$ by Lemma 3.6. □

3.1.5 Some Properties of Time-Bounded Random Sets

Intuitively, $t(n)$-random sets do not show any infinite redundancies or patterns which can be recovered in time corresponding to $t(n)$. One also says that in a $t(n)$-random set there are built in diagonalizations of complexity corresponding to $t(n)$. We conclude our discussion of time-bounded randomness by listing some of these properties of $t(n)$-random sets which we will use later. (See Ambos-Spies and Mayordomo (1997) for more details.)

Theorem 3.16 *Let A be $t(n)$-random. Then $A \notin \mathrm{DTIME}(t(2^n - 1))$. In fact, A is $\mathrm{DTIME}(t(2^n - 1))$-bi-immune.*

Theorem 3.17 *Let A be $n \cdot t(n)$-random. Then A is $t(2^n - 1)$-incompressible.*

For the next theorem recall that a set A *has gaps* if, for infinitely many numbers n, $A \cap \{0,1\}^n = \emptyset$.

Theorem 3.18 *Let A be $t(n)$-random where $t(n) \geq n^2$. Then A is exponentially dense (hence not sparse) and A does not have gaps.*

3.1.6 Randomness and Measure

By the Time-Bounded-Randomness Theorem we obtain the following relations between time-bounded randomness and time-bounded measure which we will exploit below.

Lemma 3.19 *Let $t(n)$ and $t'(n)$ be nondecreasing computable functions such that $t(n)$ is time constructible and $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ almost everywhere, and let* C *be any class.*

(i) $\mu_t(\mathrm{C}) = 0 \Rightarrow \mathrm{RAND}(t(n)) \cap \mathrm{C} = \emptyset \ \Rightarrow \mu_{t'}(\mathrm{C}) = 0$

(ii) $\mu_t(\mathrm{C}) = 1 \ \Rightarrow \mathrm{RAND}(t(n)) \subseteq \mathrm{C} \ \Rightarrow \mu_{t'}(\mathrm{C}) = 1$

PROOF. The first implication in (i) (and in (ii)) is immediate by definition while the second implication follows from Theorem 3.15. □

By Proposition 3.8, Lemma 3.19 implies the following characterization of the computable measure in terms of time-bounded randomness.

Lemma 3.20 *For any class* C *the following hold.*

$$\mu_{\mathrm{rec}}(\mathrm{C}) = 0 \Leftrightarrow \exists\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \cap \mathrm{C} = \emptyset)$$

$$\mu_{\mathrm{rec}}(\mathrm{C}) \neq 0 \Leftrightarrow \forall\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \cap \mathrm{C} \neq \emptyset)$$

$$\mu_{\mathrm{rec}}(\mathrm{C}) = 1 \Leftrightarrow \exists\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \subseteq \mathrm{C})$$

3.1.7 A Measure on the Class REC of Computable Sets

As we will discuss now, Schnorr's computable measure serves as an adequate measure on the space REC of the computable sets. While REC itself does not have computable measure 0, it is an easy consequence of the Union Theorem for Time-Bounded Martingales that any class of *uniformly* computable sets has computable measure 0. So, in particular, any time complexity class DTIME$(t(n))$ has computable measure 0.

Theorem 3.21 $\mu_{\mathrm{rec}}(\mathrm{REC}) \neq 0$.

Theorem 3.22 (Union Theorem for REC**)** *Let d_n, $n \geq 0$, be uniformly computable martingales. There is a computable martingale d such that, for $n \geq 0$, $S^\infty[d_n] \subset S^\infty[d]$. I.e.,*

$$\mu_{\mathrm{rec}}(\bigcup_{n\geq 0} S^\infty[d_n]) = 0.$$

Corollary 3.23 *Let* C *be uniformly computable. Then* $\mu_{\mathrm{rec}}(\mathrm{C}) = 0$.

Corollary 3.24 *For any computable function $t(n)$,* $\mu_{\mathrm{rec}}(\mathrm{DTIME}(t(n))) = 0$.

Following Lutz (1992) we define a measure on REC based on μ_{rec} as follows.

Definition 3.25 (Measure on REC**)** (Lutz (1992)) A class C has *measure* 0 *in* REC ($\mu(\mathrm{C}|\mathrm{REC}) = 0$ for short) if

$$\mu_{\mathrm{rec}}(\mathrm{C} \cap \mathrm{REC}) = 0,$$

and C has *measure* 1 *in* REC ($\mu(\mathrm{C}|\mathrm{REC}) = 1$ for short) if the complement $\overline{\mathrm{C}}$ of C has measure 0 in REC.

Intuitively, the computable part of a class C is *small* if C has measure 0 in REC (i.e., if $\mu(\mathrm{C}|\mathrm{REC}) = 0$), the computable part of class C is *nonsmall* if C does not have measure 0 in REC (i.e., if $\mu(\mathrm{C}|\mathrm{REC}) \neq 0$), and the computable part of a class C is *large* if C has measure 1 in REC (i.e., if $\mu(\mathrm{C}|\mathrm{REC}) = 1$). The validity of this intuition follows from the following observations which are easy consequences of the above given facts of the computable measure.

Theorem 3.26 *1.* REC *has measure 1 in* REC *(i.e., the class of computable sets is large).*

2. *For any computable time bound $t(n)$,* DTIME$(t(n))$ *has measure 0 in* REC *(i.e., any deterministic time class is small).*

3. *If a class* C *has measure 1 in* REC *then* C *does not have measure 0 in* REC *(i.e., large classes are not small).*

4. *If a class* C *has measure 0 (1) in* REC *then* $\overline{\mathrm{C}}$ *has measure 1 (0) in* REC *(i.e., the complement of a small (large) class is large (small)).*

5. *If a class* C *has measure 0 in* REC *then any subclass of* C *has has measure 0 in* REC *(i.e., subclasses of small classes are small again).*

6. *If a class* C *has measure 1 in* REC *then any superclass of* C *has has measure 1 in* REC *(i.e., superclasses of large classes are large again).*

Also note that, by Lemma 3.20, the measure in REC can be characterized in terms of time-bounded randomness as follows.

Corollary 3.27 *For any class* C *the following hold.*

$$\mu(\mathrm{C}|\mathrm{REC}) = 0 \Leftrightarrow \exists\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \cap \mathrm{REC} \cap \mathrm{C} = \emptyset)$$

$$\mu(\mathrm{C}|\mathrm{REC}) \neq 0 \Leftrightarrow \forall\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \cap \mathrm{REC} \cap \mathrm{C} \neq \emptyset)$$

$$\mu(\mathrm{C}|\mathrm{REC}) = 1 \Leftrightarrow \exists\, t(n) \in \mathrm{REC}\ (\mathrm{RAND}(t(n)) \cap \mathrm{REC} \subseteq \mathrm{C})$$

3.1.8 Lutz's Measures on the Exponential Time Classes E and EXP

Lutz (1992) has shown that the above idea of defining a measure on the class of the computable sets can be adapted to define measures on sufficiently closed complexity classes by considering some corresponding time-bounded measures. In particular, Lutz (1992) has shown that the p-measure given by the polynomial time computable martingales leads to a measure on the exponential time class E and, similarly, the p_2-measure given by the $2^{(\log n)^k}$-time bounded martingales ($k \geq 1$) gives an adequate measure on EXP.

Definition 3.28 (Lutz (1992)) Let C be any class.

1. For $i \in \{0,1\}$, C has *p-measure i* ($\mu_p(\mathrm{C}) = i$ for short) if there is a $k \geq 1$ such that $\mu_{n^k}(\mathrm{C}) = i$.

2. C has *measure* 0 *in* E ($\mu(\mathrm{C}|\mathrm{E}) = 0$ for short) if $\mathrm{C} \cap \mathrm{E}$ has p-measure 0; and C has *measure* 1 *in* E ($\mu(\mathrm{C}|\mathrm{E}) = 1$ for short) if $\overline{\mathrm{C}}$ has measure 0 in E.

Definition 3.29 (Lutz (1992)) Let C be any class.

1. For $i \in \{0,1\}$, C has *p_2-measure i* ($\mu_{p_2}(\mathrm{C}) = i$ for short) if there is a $k \geq 1$ such that $\mu_{2^{(\log n)^k}}(\mathrm{C}) = i$.

2. C has *measure* 0 *in* EXP ($\mu(\mathrm{C}|\mathrm{EXP}) = 0$ for short) if $\mathrm{C} \cap \mathrm{EXP}$ has p_2-measure 0; and C has *measure* 1 *in* EXP ($\mu(\mathrm{C}|\mathrm{EXP}) = 1$ for short) if $\overline{\mathrm{C}}$ has measure 0 in EXP.

Note that, by definition, the following relations hold among these measure concepts ($i \in \{0,1\}, \mathrm{C}$ any class):

$$\begin{tikzcd}
\mu_p(\mathrm{C}) = i \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mu_{p_2}(\mathrm{C}) = i \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mu(\mathrm{C}) = i \\
\mu(\mathrm{C}|\mathrm{E}) = i & \mu(\mathrm{C}|\mathrm{EXP}) = i &
\end{tikzcd} \tag{3.10}$$

(It will follow from results below that, in general, no other implications hold.)

The following theorem shows that the measure on E and the measure on EXP are sound.

Theorem 3.30 *(Lutz (1992))*

(a) For any k, $\mu_p(\mathrm{DTIME}(2^{kn})) = 0$ *and* $\mu_{p_2}(\mathrm{DTIME}(2^{n^k})) = 0$*, whence* $\mu(\mathrm{DTIME}(2^{kn})|\mathrm{E}) = 0$ *and* $\mu(\mathrm{DTIME}(2^{n^k})|\mathrm{EXP}) = 0$.

(b) For any class C *such that* $\mu(\mathrm{C}|\mathrm{E}) = 1$ ($\mu(\mathrm{C}|\mathrm{EXP}) = 1$), $\mu(\mathrm{C}|\mathrm{E}) \neq 0$ ($\mu(\mathrm{C}|\mathrm{EXP}) \neq 0$). *In particular,* $\mu(\mathrm{E}|\mathrm{E}) \neq 0$ *and* $\mu(\mathrm{EXP}|\mathrm{EXP}) \neq 0$ *(whence* $\mu_p(\mathrm{E}) \neq 0$ *and* $\mu_{p_2}(\mathrm{EXP}) \neq 0$*).*

The following theorem is a special case of the Union Theorem for Time-Bounded Martingales (Theorem 3.9).

Theorem 3.31 (Union Theorem for p and p_2) *(Lutz (1992)) Let* $\mathrm{C}_m, m \geq 0$, *be classes such that* $\mu_{n^k}(\mathrm{C}_m) = 0$ $(\mu_{2^{log(n)^k}}(\mathrm{C}_m) = 0)$ *for some k and all m. Then* $\mu_p(\mathrm{C}) = 0$ $(\mu_{p_2}(\mathrm{C}) = 0)$ *for* $\mathrm{C} = \bigcup_{m \geq 0} \mathrm{C}_m$. *In particular, the finite union of p-(p_2-) measure-*0 *classes has p-(p_2-)measure* 0 *again.*

From the Time-Bounded Randomness Theorem (Theorem 3.15 and Lemma 3.19) together with Theorem 3.16 we get the following characterization of p- and p_2-measures as well as of the corresponding measures on E and EXP together with some existence results for random sets in the exponential time classes.

Theorem 3.32 *(Ambos-Spies et al. (1997)) For any class* C *the following hold:*

$$\begin{array}{rcl}\mu_p(\mathrm{C}) = 0 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(n^k) \cap \mathrm{C} = \emptyset) \\ \mu_{p_2}(\mathrm{C}) = 0 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \cap \mathrm{C} = \emptyset) \\ \mu(\mathrm{C}|\mathrm{E}) = 0 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(n^k) \cap \mathrm{E} \cap \mathrm{C} = \emptyset) \\ \mu(\mathrm{C}|\mathrm{EXP}) = 0 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \cap \mathrm{EXP} \cap \mathrm{C} = \emptyset)\end{array} \tag{3.11}$$

$$\begin{array}{rcl}\mu_p(\mathrm{C}) \neq 0 & \Leftrightarrow & \forall k \geq 1\ (\mathrm{RAND}(n^k) \cap \mathrm{C} \neq \emptyset) \\ \mu_{p_2}(\mathrm{C}) \neq 0 & \Leftrightarrow & \forall k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \cap \mathrm{C} \neq \emptyset) \\ \mu(\mathrm{C}|\mathrm{E}) \neq 0 & \Leftrightarrow & \forall k \geq 1\ (\mathrm{RAND}(n^k) \cap \mathrm{E} \cap \mathrm{C} \neq \emptyset) \\ \mu(\mathrm{C}|\mathrm{EXP}) \neq 0 & \Leftrightarrow & \forall k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \cap \mathrm{EXP} \cap \mathrm{C} \neq \emptyset)\end{array} \tag{3.12}$$

$$\begin{array}{rcl}\mu_p(\mathrm{C}) = 1 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(n^k) \subseteq \mathrm{C}) \\ \mu_{p_2}(\mathrm{C}) = 1 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \subseteq \mathrm{C}) \\ \mu(\mathrm{C}|\mathrm{E}) = 1 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(n^k) \cap \mathrm{E} \subseteq \mathrm{C}) \\ \mu(\mathrm{C}|\mathrm{EXP}) = 1 & \Leftrightarrow & \exists k \geq 1\ (\mathrm{RAND}(2^{(\log n)^k}) \cap \mathrm{EXP} \subseteq \mathrm{C})\end{array} \tag{3.13}$$

Theorem 3.33 *(Ambos-Spies et al. (1997)) (a) For* $k \geq 1$, *the class* $\mathrm{RAND}(n^k)$ *of the n^k-random sets has p-measure* 1, *and* $\mathrm{RAND}(2^{(\log n)^k})$ *has p_2-measure* 1.

(b) For $k \geq 1$, *there is an n^k-random set A in* $\mathrm{DTIME}(2^{(k+5)n})$ *but there is no such set in* $\mathrm{DTIME}(2^{kn})$. *Similarly, there is a* $2^{(log\,n)^k}$*-random set A in* $\mathrm{DTIME}(2^{n^{k+1}})$ *but there is no such set in* $\mathrm{DTIME}(2^{n^k})$.

We conclude this short discussion of the measures on E and EXP by listing some properties which are abundant in E.

Theorem 3.34 *The following classes have p-measure* 1 *hence measure* 1 *in* E*:*

(i) The class of the $\mathrm{DTIME}(2^{kn})$*-bi-immune sets (for any fixed* $k \geq 1$*; Mayordomo (1994)).*

(ii) The class of the 2^{kn}*-incompressible sets (for any fixed* $k \geq 1$*; Juedes and Lutz (1995a)).*

(iii) The class of the p-btt-incomplete sets for E *(Ambos-Spies et al. (1996b)).*

(iv) The class of the exponentially dense sets (Lutz).

Using the characterization of p-measure in terms of randomness, the observations in the preceding theorem can be expressed (and refined) as follows.

Theorem 3.35 *(i) Any n^k-random set is* DTIME(2^{kn})*-bi-immune.*

(ii) Any n^{k+1}-random set is 2^{kn}-incompressible.

(iii) No n^3-random set is p-btt-hard for E.

(iv) Any n^2-random set is exponentially dense.

Note that some of the above results are immediate by the more general observations on $t(n)$-random sets made in Section 3.1.5. Moreover, there are results corresponding to Theorems 3.34 and 3.35 for the class EXP in place of E.

The final result in this subsection is a very useful tool for analysing the p- (or p_2-) measure of classes closed downwards under $\leq_m^p$.

Theorem 3.36 *(Ambos-Spies et al. (1997)) Let A be an n^2-random set. For any $k \geq 1$ there is an n^k-random set $A_k \leq_m^p A$. In fact, there is a p-random set A_∞ with $A_\infty \leq_m^p A$ and, for any $k \geq 1$, there is a $2^{(log\, n)^k}$-random set B_k with $B_k \leq_m^p A$. If, moreover, $A \in$ E then A_k and A_∞ can be chosen so that $A_k \in$ E and $A_\infty \in$* DTIME(2^{n^2}).

PROOF. Since we will need some similar observations on generic sets, incompressible sets and bi-immune sets, we shortly give the idea of the proof. The sets A_k, A_∞ and B_k are chosen as follows.

$$A_k = \{x : 0^{k\cdot|x|}x \in A\}$$

$$A_\infty = \{x :\ 0^{(|x|+1)(log(|x|+1))}x \in A\}$$

$$B_k = \{x :\ 0^{|x|^{k+1}}x \in A\}$$

Then, obviously, $A_k \leq_m^p A$ via $g(x) = 0^{k\cdot|x|}x$ and, for $A \in \mathrm{E}_c$, $A_k \in \mathrm{E}_{(k+1)c}$. The proof that A_k is n^k-random is indirect. Assume that the normed n^k-martingale d succeeds on A_k. We convert d into an n^2-martingale $\hat{d}$ such that $\hat{d}$ will succeed on A. Since A is n^2-random, this gives the desired contradiction. For the definition of $\hat{d}$, use the following notation: For a string $X \upharpoonright 0^{k\cdot|x|}x$ let $\tilde{X} \upharpoonright x$ be defined by $\tilde{X}(y) = X(0^{k\cdot|y|}y)$ for $y < x$. Then, for the strategy s underlying d, let $\hat{s}(X \upharpoonright 0^{k\cdot|x|}x) = s(\tilde{X} \upharpoonright x)$ and, for any string $X \upharpoonright y$ not of this form let $\hat{s}(X \upharpoonright y) = \frac{1}{2}$. As one can easily check, $\hat{s}$ is a 2^n-strategy and, for $\hat{d} = d[\hat{s}, 1]$, $\hat{d}(A \upharpoonright 0^{k\cdot|x|}x) = d(A_k \upharpoonright x)$ for all strings x. So, by assumption on d, $\hat{d}$ succeeds on A.

The proof that the sets A_∞ and B_k have the required properties is similar. □

3.2 Lutz's Measure Completeness

The weak hardness notions for the exponential time classes E and EXP proposed by Lutz are based on the measures defined on this classes. Recall that Lutz proposed to call a set A *weakly hard* for a complexity class C if a nonnegligible part of C can be reduced to A, i.e., if $\mathrm{P}_m(A) \cap \mathrm{C}$ is nonnegligible. Now having a measure defined on C it is quite natural to say that a subclass is negligible if and only if it has measure 0 in C.

Definition 3.37 (Lutz (1995)) (a) A set A is *measure hard* for E (or E-*measure hard* for short) if

$$\mu(\mathrm{P}_m(A)|\mathrm{E}) \neq 0 \tag{3.14}$$

and A is *measure complete* for E (or E-*measure complete* for short) if $A \in \mathrm{E}$ and A is measure hard for E.

(b) A set A is *measure hard* for EXP (or EXP-*measure hard* for short) if

$$\mu(\mathrm{P}_m(A)|\mathrm{EXP}) \neq 0 \tag{3.15}$$

and A is *measure complete* for EXP if $A \in \mathrm{EXP}$ and A is measure hard for EXP.

Note that (3.14) and (3.15) are equivalent to

$$\mu_p(\mathrm{P}_m(A) \cap \mathrm{E}) \neq 0 \tag{3.16}$$

and

$$\mu_{p_2}(\mathrm{P}_m(A) \cap \mathrm{EXP}) \neq 0, \tag{3.17}$$

respectively. Since EXP is closed downwards under $\leq_m^p$, the latter implies that a set A is EXP-measure complete if and only if $A \in \mathrm{EXP}$ and

$$\mu_{p_2}(\mathrm{P}_m(A)) \neq 0, \tag{3.18}$$

holds.

By exploiting the relations between resource bounded measure and resource bounded randomness stated in Theorem 3.32, we obtain the following equivalent characterization of the measure hardness and completeness notions.

Lemma 3.38 *(a) A set A is measure hard for* E *if and only if, for any $k \geq 1$ there is an n^k-random set $R \in \mathrm{E}$ such that $R \leq_m^p A$.*

(b) A set A is measure hard for EXP *if and only if, for any $k \geq 1$ there is an $2^{(\log n)^k}$-random set $R \in \mathrm{EXP}$ such that $R \leq_m^p A$.*

The above weak hardness notions for E and EXP are sound in the following sense.

Lemma 3.39 *For* $\mathrm{C} = \mathrm{E}, \mathrm{EXP}$ *the following hold.*

(i) If A is C*-hard then A is* C*-measure hard.*

(ii) If A is C*-measure hard then A is intractable, i.e., $A \notin \mathrm{P}$.*

PROOF. We consider the case of $\mathrm{C} = \mathrm{E}$. For a proof of (i) note that, for an E-hard set A, $\mathrm{P}_m(A) \cap \mathrm{E} = \mathrm{E}$ and $\mu_p(\mathrm{E}) \neq 0$ by Theorem 3.30 (b). For a proof of (ii) note that $\mu_p(\mathrm{P}) = 0$ (since $\mathrm{P} \subseteq \mathrm{E}_1$ this follows from Theorem 3.30 (a)). So any E-measure hard set A has a predecessor B under $\leq_m^p$ such that $B \notin \mathrm{P}$. Obviously this implies $A \notin \mathrm{P}$. □

So measure hardness is a generalization of hardness and the crucial property of hard sets, namely to be intractable, is inherited by the measure hard sets:

$$\begin{array}{c} A \text{ E-hard} \\ \Downarrow \\ A \text{ E-measure hard} \\ \Downarrow \\ A \text{ intractable} \end{array} \tag{3.19}$$

(And similarly, for EXP in place of E.)

As Lutz (1995) has shown, the implications in (3.19) are strict even if we consider only sets $A \in \mathrm{E}$. In particular, there are E(EXP)-measure complete sets which are not E(EXP)-complete. This result and some stronger results are immediate by the following characterization of measure hardness.

Theorem 3.40 (Characterization Theorem for Measure Hardness) *(Ambos-Spies et al. (1997)) A set A is* $\mathrm{E}(\mathrm{EXP})$*-measure hard if there is an n^2-random set $B \in \mathrm{E}(\mathrm{EXP})$ such that $B \leq_m^p A$.*

PROOF. This easily follows from Theorem 3.36 and the characterization of the measures in E and EXP in terms of time-bounded random sets (Lemma 3.38). □

The following corollaries are stated for the exponential time class E. (The corresponding statements for EXP also hold.)

Theorem 3.41 *While the class of* E*-hard sets has measure 0 in* E *(Mayordomo (1994)), the class of* E*-measure hard sets has measure 1 in* E *(Ambos-Spies et al. (1997)).*

PROOF. The first part follows from Theorem 3.34 (iii). The second part follows from Theorem 3.40 since, by Theorem 3.33, the class of n^2-random sets has measure 1 in E. □

Corollary 3.42 *(Lutz (1995)) There is an* E*-measure complete set which is not* E*-complete.*

PROOF. This is immediate by Theorem 3.41. □

In fact, as shown in Ambos-Spies et al. (1997), there are E-measure complete sets which are not *p-btt*-complete. (Note that this is immediate by Theorem 3.34 (iii) and Theorem 3.41). The question whether there are E-measure complete sets which are not *p-tt*-complete for E or even not *p-T*-complete for E is open.

As the next theorem shows, there are E-measure complete sets which are P-bi-immune (in fact, E_k-bi-immune for any given k. On the other hand, by Theorem 2.23, all E-complete sets possess infinite polynomial-time computable sets. So while no E-complete set is almost everywhere intractable there are E-measure complete sets with this property.

Theorem 3.43 *While no* E*-complete set is* P*-bi-immune (Berman (1976)), there are* E*-measure complete sets which are* P*-bi-immune. In fact, for any $k \geq 1$, there is an* E*-measure complete set which is* E_k*-bi-immune (Ambos-Spies et al. (1997)).*

PROOF. By Theorem 2.23 and by Theorems 3.41 and 3.35 (i), respectively. □

Though, by Theorem 3.43, E-completeness and E-measure completeness can be distinguished by structural properties, some of the structural properties of E-complete sets are shared by all E-measure complete sets. For example, all E-measure complete sets have high density.

Theorem 3.44 *(Ambos-Spies et al. (1997)) Let A be* E*-measure hard (*EXP*-measure hard). Then A is exponentially dense hence, in particular, not sparse.*

PROOF (IDEA). By Theorem 3.41 there is an n^2-random set B such that $B \leq_m^p A$. Moreover, by Theorem 3.35, B is p-incompressible and exponentially dense. So it suffices to observe that any set A to which a p-incompressible exponentially dense set B can be p-m-reduced is exponentially dense too. □

Theorem 3.40 also clarifies the relation between measure hardness for E and EXP. While, by a simple padding argument, E-hardness and EXP-hardness coincide (see Theorem 2.15), in case of measure hardness the relations are as follows.

Theorem 3.45 *(Juedes and Lutz (1995b)) Every* E*-measure hard set is* EXP*-measure hard. But there is an* EXP*-measure complete set $A \in$* E *which is not* E*-measure hard.*

PROOF (IDEA). The first part is immediate by Theorem 3.41. For a proof of the second part let $\hat{A}$ be any p-random set in EXP and, by the First Padding Lemma, let A be a set in E such that $A =_m^p \hat{A}$. Then, by Theorem 3.41, A is EXP-measure complete. Moreover, in order to show that $\hat{A}$ (hence A) is not E-measure hard it suffices to show that there is no n^2-random set $B \in$ E such that $B \leq_m^p \hat{A}$. Since any

n^2-random set is p-incompressible and any p-random set is E-bi-immune, this follows from the observation that, for p-incompressible $B \in \mathrm{E}$ and $B \leq^p_m C$, C cannot be E-bi-immune. □

3.3 Computable and Time-Bounded Baire Category

The topological concept of Baire category is an alternative to Lebesgue measure for classifying the size of (uncountable) subclasses of the Cantor space. Here the meager classes are the small classes (corresponding to measure 0) and the comeager classes are the large classes (corresponding to measure 1). The concept of Baire category and Lebesgue measure are in part incompatible, however, i.e., there are comeager measure-0 classes and meager measure-1 classes. So a class might be large in one sense and small in the other sense.

Just as in case of measure, effective and resource-bounded variants of Baire category have been introduced in computability and computational complexity theory. And just as the random sets, as typical sets in the sense of measure, can be used for describing the algorithmic measure notions, algorithmic Baire category can be developed in terms of generic sets, i.e., sets typical in the sense of category.

There are various effectivizations of Baire category based on different characterizations of the classical category concept which are equivalent in the general setting but lead to concepts of quite different strengths if resource bounds are attached. Here we consider only one concept which is based on *partial* extension functions and which was introduced by Ambos-Spies, Fleischhack and Huwig (Ambos-Spies et al. (1988)). In fact, this concept is based on *bounded* extension functions which makes the concept compatible with measure. So the corresponding weak completeness concept will be compatible with and more general than Lutz's measure completeness.

For a more detailed and systematic presentation of the material of this section see Ambos-Spies (1996) and Ambos-Spies and Mayordomo (1997). Ambos-Spies (1996) compares various resource-bounded genericity notions. The genericity concept of Ambos-Spies, Fleischack and Huwig which we will use here is described in Chapter 6 there. The relations between randomness and genericity needed here are described in the survey Ambos-Spies and Mayordomo (1997).

3.3.1 Classical Baire Category on the Cantor Space

We start with shortly introducing the classical Baire category concept on the Cantor space which is based on the canonical topology on Σ^ω.

Definition 3.46 (a) For any string x, the class $\mathrm{B}_x = \{A : x \sqsubset \chi(A)\}$ is *basic open*.

(b) A class C is *open* if it is the union of basic open classes or empty.

Definition 3.47 (Baire Category) (a) A class C is *dense* if it intersects all open classes.

(b) A class C is *nowhere dense* if C is contained in the complement of an open and dense class.

(c) A class C is *meager* if C is the countable union of nowhere dense classes.

(d) A class C is *comeager* if C is the complement of a meager class.

Intuitively, meager classes are small and comeager classes large. The following observations are easy consequences of Definition 3.47.

Proposition 3.48 *A class* C *is comeager if and only if there are countably many open and dense classes* C_n*,* $n \geq 0$*, such that*

$$\bigcap_{n\geq 0} \mathrm{C}_n \subseteq \mathrm{C}.$$

Proposition 3.49 *(i) Any countable class is meager.*

(ii) The countable union of meager classes is meager.

(iii) Any subclass of a meager class is meager.

Proposition 3.50 *(i) The countable intersection of comeager classes is comeager.*

(ii) Any superclass of a comeager class is comeager.

(iii) Any class C *with countable complement is comeager.*

In particular, Σ^ω is comeager. The non-triviality of the Baire category concept, i.e., the fact that there is no class which is both meager and comeager follows from Baire's Theorem.

Theorem 3.51 (Baire) Σ^ω *is not meager.*

Corollary 3.52 *If* C *is comeager then* C *is not meager.*

3.3.2 Extension Functions and Baire Category

We now give the alternative characterization of classical Baire category in terms of partial extension functions which will lead to the time-bounded versions of Baire category we are interested in.

Intuitively, an extension function f maps a string x to a string y extending x. If we let $f(x)$ denote only the part added to x, i.e., let $y = xf(x)$, then any word function $f : \Sigma^* \to \Sigma^*$ can be viewed as an extension function. In order to define Baire category in terms of partial extension functions we will need the following notions. (In the following we write $f(x) \downarrow$ if $f(x)$ is defined and $f(x) \uparrow$ otherwise.)

Definition 3.53 An *(partial) extension function* f is a (partial) function $f : \Sigma^* \to \Sigma^*$. A partial extension function f is *dense along* a set (i.e., infinite binary sequence) A if there are infinitely many numbers n such that $f(A \upharpoonright n)$ (i.e., $f(\chi_A \upharpoonright n)$) is defined. A set A *meets* an extension function f if there is a number n such that $f(A \upharpoonright n)$ is defined and $(A \upharpoonright n)f(A \upharpoonright n) \sqsubset A$ (i.e., $(\chi_A \upharpoonright n)f(\chi_A \upharpoonright n) \sqsubset \chi_A$).

Since in the following we will always consider partial extension functions, we simply write extension function in place of partial extension function and write total extension function if we want to stress that a partial extension function is total.

For an extension function f we let

$$\mathrm{M}_f = \{A : f \text{ is not dense along } A \text{ or } A \text{ meets } f\}.$$

Then comeagerness can be defined in terms of extension functions as follows

Lemma 3.54 *A class* C *is comeager if and only if there is a countable family* $\mathrm{F} = \{f_n : n \geq 0\}$ *of extension functions such that*

$$\bigcap_{n \geq 0} \mathrm{M}_{f_n} \subseteq \mathrm{C}.$$

The genericity notions we will consider are special instances of the following abstract genericity notion.

Definition 3.55 Let $\mathrm{F} = \{f_n : n \geq 0\}$ be a countable family of extension functions. A set G is F-*generic* if G meets all extension functions in F which are dense along G, i.e., if

$$G \in \bigcap_{n \geq 0} \mathrm{M}_{f_n}.$$

Note that, by Lemma 3.54, for any countable F, there are F-generic sets, in fact the class of F-generic sets is comeager (hence, in particular, nonempty).

Lemma 3.56 *For any countable class* F *of extension functions, the class of* F-*generic sets is comeager.*

As mentioned before, in general Baire category and Lebesgue measure are not compatible. If we consider comeager classes, however, which are defined by *bounded* extension functions then these classes have measure 1 too.

Definition 3.57 An extension function f is *k-bounded* $(k \geq 1)$, if for any string x such that $f(x)\downarrow$, $|f(x)| \leq k$. f is *bounded* if f is k-bounded for some $k \geq 1$, and f is *simple* if f is 1-bounded.

Lemma 3.58 *Let f be a bounded extension function. Then* M_f *has Lebesgue measure 1.*

Lemma 3.59 *Let* F *be a countable class of bounded extension functions. Then the class of* F*-generic sets is comeager and has measure 1.*

3.3.3 Time-Bounded Genericity

Since extension functions are word functions we immediately get time-bounded variants of this concept by confinig us to extension functions in a given (generalized) time class. Since we will also consider partial extension functions, however, we have to say what it means that a partial function can be computed in time $t(n)$.

Definition 3.60 A partial function $f : \Sigma^* \rightarrow \Sigma^*$ is computable in time $t(n)$ if there is a $t(n)$-time-bounded Turing machine which on input x computes $f(x)$ if x is in the domain of f and which outputs $\uparrow$ otherwise.

If a partial function f is $t(n)$-time-computable we also write $f \in \mathrm{DTIME}(t(n))$.

Definition 3.61 Let $t(n)$ be a computable function. A $t(n)$*-extension function* is an extension function f such that $f \in \mathrm{DTIME}(t(n))$.

We now have all the concepts needed for defining the time-bounded genericity concept of Ambos-Spies, Fleischhack and Huwig.

Definition 3.62 (Ambos-Spies et al. (1988)) Let $t(n)$ be a computable function. A set A is $t(n)$*-generic* if A is F-generic for the (countable) class F of the simple $t(n)$-extension functions.

Note that, by Lemma 3.59, for any computable function $t(n)$, the class of $t(n)$-generic sets is not only comeager but also has measure 1. The latter can be strengthened in terms of time-bounded measure.

Theorem 3.63 *(Ambos-Spies et al. (1996b), Ambos-Spies et al. (1997)) Every $t(n)$-random set is $t(n)$-generic.*

By Theorem 3.63, from the existence results for random sets we obtain the corresponding results for generic sets.

Corollary 3.64 *Let $t(n)$ and $t'(n)$ be nondecreasing computable functions such that $t(n)$ is time constructible and $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ almost everywhere. Then there is a $t(n)$-generic set $A \in \mathrm{DTIME}(2^n \cdot t'(2^{n+1}))$.*

In particular, for $k \geq 1$, there is an n^k-generic set in $\mathrm{E}_{k+5} = \mathrm{DTIME}(2^{(k+5)n})$ and a $2^{(\log n)^k}$-generic set in $\mathrm{EXP}_{k+1} = \mathrm{DTIME}(2^{n^{k+1}})$.

PROOF. By Theorems 3.63 and 3.15. □

It should be noted that, by some more direct arguments, we can get some better upper bounds. But the bounds given in Corollary 3.64 will be sufficient for our purposes.

3.3.4 Properties of Generic Sets

We next list some properties of the $t(n)$-generic sets together with some simple facts we will need later. For proofs and more details, see Ambos-Spies and Mayordomo (1997).

From the properties of random sets given in Theorem 3.35 the following are shared by the generic sets.

Theorem 3.65 *(Ambos-Spies et al. (1996b))*

(i) There is no $t(n)$-generic set in $\mathrm{DTIME}(t(2^n - 1))$. So, in particular, there is no n^k-generic set in $\mathrm{E}_k = \mathrm{DTIME}(2^{kn})$ and no $2^{(\log n)^k}$-generic set in $\mathrm{EXP}_k = \mathrm{DTIME}(2^{n^k})$.

In fact, any $t(n)$-generic set is $\mathrm{DTIME}(t(2^n - 1))$-bi-immune. So, in particular, any n^k-generic set is E_k-bi-immune and any $2^{(\log n)^k}$-generic set is EXP_k-bi-immune.

(ii) Any $n \cdot t(n)$-generic set is $t(2^n - 1)$-incompressible. So, in particular, any n^{k+1}-generic set is 2^{kn}-incompressible and any $2^{(\log n)^{k+1}}$-generic set is 2^{n^k}-incompressible.

(iii) No n^3-generic set is p-btt-hard for E.

In contrast to random sets, however, generic sets might be sparse.

Theorem 3.66 *(Ambos-Spies et al. (1996b)) Let $s(n)$ and $t(n)$ be any computable nondecreasing and unbounded functions. There is a computable $t(n)$-generic set A such that $|A^{\leq n}| \leq s(n)$. So, in particular, for any time bound $t(n)$, there are computable sparse $t(n)$-generic sets. Moreover, for $k \geq 1$, there is a sparse n^k-generic set in E.*

We close this subsection with a technical fact which we will need later and which illustrates the diagonalization strength of $t(n)$-generic sets.

Call a partial function $f : \Sigma^* \rightarrow (\Sigma^*, \Sigma)^k$ $(k \geq 1)$ a *generalized k-bounded extension function* if, for any string $X \upharpoonright x$ such that $f(X \upharpoonright x)$ is defined,

$$f(X \upharpoonright x) = (x_0, i_0), \ldots (x_{k-1}, i_{k-1})$$

where $x \leq x_0 < x_2 < \cdots < x_{k-1}$. Then, as before, f is dense along a set A if $f(A \upharpoonright x) \downarrow$ for infinitely many x. *A meets f at x* if $f(A \upharpoonright x) \downarrow$, say $f(A \upharpoonright x) = (x_0, i_0), \ldots (x_{k-1}, i_{k-1})$, and $A(x_j) = i_j$ for $j < k$.

Lemma 3.67 *(see Ambos-Spies and Mayordomo (1997)) Let $k \geq 1$, let A be $n \cdot t(n)$-generic, and let f be a generalized k-bounded $t(n)$-extension function which is dense along A. Then A meets f at infinitely many x.*

3.3.5 Time-Bounded Baire Category

Above we did not introduce time-bounded Baire category but only the corresponding genericity notions. From these genericity notions we now derive the examples of algorithmic and resource-bounded Baire category which are of interest for our investigations.

Definition 3.68 (Ambos-Spies (1996)) (a) A class C is *computably meager* (or *rec-meager* for short) if there is a computable function t such that no $t(n)$-generic set is in C; and C is *computably comeager* (or *rec-comeager* for short) if $\overline{\mathrm{C}}$ is computably meager.

(b) A class C is *p-meager* if there is a number $k \geq 1$ such that no n^k-generic set is in C; and C is *p-comeager* if $\overline{\mathrm{C}}$ is p-meager.

(c) A class C is *p_2-meager* if there is a number $k \geq 1$ such that no $2^{(\log n)^k}$-generic set is in C; and C is *p_2-comeager* if $\overline{\mathrm{C}}$ is p_2-meager.

From the first part of Definition 3.68 we get a category concept for the class REC of the computable sets as follows.

Definition 3.69 A class C is *meager in* REC if $\mathrm{C} \cap \mathrm{REC}$ is computably meager; and C is *comeager in* REC if $\overline{\mathrm{C}}$ is meager in REC.

If we let $\mathrm{GEN}(t(n))$ denote the class of $t(n)$-generic sets then the Baire category on REC can be described as follows:

$$\begin{array}{rcl} \text{C is meager in REC} & \Leftrightarrow & \exists\, t \in \mathrm{REC}\ (\mathrm{GEN}(t(n)) \cap \mathrm{REC} \cap \mathrm{C} = \emptyset) \\ \text{C is not meager in REC} & \Leftrightarrow & \forall\, t \in \mathrm{REC}\ (\mathrm{GEN}(t(n)) \cap \mathrm{REC} \cap \mathrm{C} \neq \emptyset) \\ \text{C is comeager in REC} & \Leftrightarrow & \exists\, t \in \mathrm{REC}\ (\mathrm{GEN}(t(n)) \cap \mathrm{REC} \subseteq \mathrm{C}). \end{array} \quad (3.20)$$

3.3.6 Baire Category on E and EXP

Similarly, from the second and third parts of Definition 3.68 we obtain Baire category concepts for the exponential-time classes E and EXP.

Definition 3.70 (Ambos-Spies (1996)) (a) A class C is *meager in* E if $\mathrm{C} \cap \mathrm{E}$ is p-meager; and C is *comeager in* E if $\overline{\mathrm{C}}$ is meager in E.

(b) A class C is *meager in* EXP if $\mathrm{C} \cap \mathrm{EXP}$ is p_2-meager; and C is *comeager in* EXP if $\overline{\mathrm{C}}$ is meager in EXP.

The Baire category concepts for E and EXP can be described in terms of genericity as follows (immediate by Definitions 3.68 and 3.70):

$$\begin{array}{rcl} \text{C is meager in E} & \Leftrightarrow & \exists\, k\, (\mathrm{GEN}(n^k) \cap \mathrm{E} \cap \mathrm{C} = \emptyset) \\ \text{C is not meager in E} & \Leftrightarrow & \forall\, k\, (\mathrm{GEN}(n^k) \cap \mathrm{E} \cap \mathrm{C} \neq \emptyset) \\ \text{C is comeager in E} & \Leftrightarrow & \exists\, k\, (\mathrm{GEN}(n^k) \cap \mathrm{E} \subseteq \mathrm{C}) \end{array} \tag{3.21}$$

$$\begin{array}{rcl} \text{C is meager in EXP} & \Leftrightarrow & \exists\, k\, (\mathrm{GEN}(2^{(\log n)^k}) \cap \mathrm{E} \cap \mathrm{C} = \emptyset) \\ \text{C is not meager in EXP} & \Leftrightarrow & \forall\, k\, (\mathrm{GEN}(2^{(\log n)^k}) \cap \mathrm{E} \cap \mathrm{C} \neq \emptyset) \\ \text{C is comeager in EXP} & \Leftrightarrow & \exists\, k\, (\mathrm{GEN}(2^{(\log n)^k}) \cap \mathrm{E} \subseteq \mathrm{C}) \end{array} \tag{3.22}$$

The consistency of the Baire category concepts on E and EXP easily follows from Corollary 3.64 and Theorem 3.65 (i):

Theorem 3.71 *(Ambos-Spies (1996)) (a) For any $k \geq 1$, E_k is p-meager, hence meager in* E*. Similarly, for any $k \geq 1$, EXP_k is p_2-meager, hence meager in* EXP.

(b) E *is not p-meager, hence not meager in* E*. Similarly,* EXP *is not p_2-meager, hence not meager in* EXP.

3.3.7 Measure vs. Category on E and EXP

There are the following relations between the measure and category conceps on the exponential-time classes and the underlying time-bounded measure and category notions.

Theorem 3.72 *(a) Any p-meager class* C *has p-measure 0 and any p-comeager class* C *has p-measure 1. Similarly, any p_2-meager class* C *has p_2-measure 0 and any p_2-comeager class* C *has p_2-measure 1.*

(b) Any class C *which is meager in* E *has measure 0 in* E *and any class* C *which is comeager in* E *has measure 1 in* E*. Similarly, any class* C *which is meager in* EXP *has measure 0 in* EXP *and any class* C *which is comeager in* EXP *has measure 1 in* EXP.

PROOF. Since any $t(n)$-random set is $t(n)$-generic (Theorem 3.63), this follows from the characterizations of p-measure, p_2-measure, and measure on E and EXP in terms of randomness given in Theorem 3.32 and the corresponding characterizations of p-category, p_2-category, and category on E and EXP in terms of genericity given in Definition 3.68 and in the equations (3.21) and (3.22) above. □

By a similar argument, we obtain the following relations between computable category and computable measure.

Theorem 3.73 *(a) Any computably-meager class* C *has computable-measure 0 and any computably-comeager class* C *has computable-measure 1.*

(b) Any class C *which is meager in* REC *has measure 0 in* REC *and any class* C *which is comeager in* REC *has measure 1 in* REC.

3.4 Ambos-Spies' Category Completeness

While Lutz's weak completeness notions for the exponential-time classes are based on corresponding time-bounded measure concepts taylored for these complexity classes, Ambos-Spies (Ambos-Spies (1996)) introduced weak completeness notions based on corresponding Baire category concepts. I.e., intuitively, a set A is weakly complete for E in the sense of Ambos-Spies (1996) if the class of sets in E which can be reduced to A is nonnegligible in the sense of Baire category, i.e., is not meager in E. While in Ambos-Spies (1996) this concept is formalized for various alternative effectivizations of Baire category, here we will only consider the concept based on the bounded category concept of Ambos-Spies, Fleischhack and Huwig for which we have introduced the corresponding category concepts for the exponential time classes in Section 3.3.6 already.

Definition 3.74 (Ambos-Spies (1996)) (a) A set A is *category hard* for E (or E-*category hard* for short) if $\mathrm{P}_m(A)$ is not meager in E, and A is *category complete* for E (or E-*category complete* for short) if $A \in \mathrm{E}$ and A is category hard for E.

(b) A set A is *category hard* for EXP (or EXP-*category hard* for short) if $\mathrm{P}_m(A)$ is not meager in EXP, and A is *category complete* for EXP (or EXP-*category complete* for short) if $A \in \mathrm{EXP}$ and A is category hard for EXP.

By (3.21) and (3.22), category hardness for E and EXP can be described in terms of genericity as follows.

$$A \text{ category hard for E} \Leftrightarrow \forall\, k \geq 1\ \exists\, G \in \mathrm{E}\ (G\ n^k\text{-generic } \&\ G \leq^p_m A) \tag{3.23}$$

$$A \text{ category hard for EXP} \Leftrightarrow \forall\, k \geq 1\ \exists\, G \in \mathrm{EXP}\ (G\ 2^{(\log n)^k}\text{-generic } \&\ G \leq^p_m A) \tag{3.24}$$

Moreover, by Theorem 3.72, category hardness generalizes measure hardness.

Lemma 3.75 *Let A be measure hard (complete) for* E. *Then A is category hard (complete) for* E. *Similarly, any measure hard (complete) set for* EXP *is category hard (complete) for* EXP.

Strictness of the implications in Lemma 3.75 and some other basic facts on category hardness have been established by using a characterization of category hardness in the style of the Characterization Theorem for Measure Hardness (Theorem 3.40) based on the following observation (compare with Theorem 3.36).

Theorem 3.76 *(Ambos-Spies (1996)) Let A be an n^2-generic set. For any $k \geq 1$ there is an n^k-generic set $A_k \leq^p_m A$. In fact, there is a p-generic set A_∞ with $A_\infty \leq^p_m A$ and, for any $k \geq 1$, there is a $2^{(\log n)^k}$-generic set B_k with $B_k \leq^p_m A$. If, moreover, $A \in \mathrm{E}$ then A_k and A_∞ can be chosen so that $A_k \in \mathrm{E}$ and $A_\infty \in \mathrm{DTIME}(2^{n^2})$.*

Here a set A is *p-generic* if A is n^k-generic for all $k \geq 1$. The proof of Theorem 3.76 is a straightforward variant of the proof of Theorem 3.36.

Theorem 3.77 (Characterization Theorem for Category Hardness) *(Ambos-Spies (1996)) A set A is* E*-category hard if and only if there is an n^2-generic set $B \in \mathrm{E}$ such that $B \leq^p_m A$. And, similarly, A set A is* EXP*-category hard if and only if there is an n^2-generic set $B \in \mathrm{EXP}$ such that $B \leq^p_m A$.*

PROOF. By Theorem 3.76 and (3.23) and (3.24). □

Corollary 3.78 *The class of* E*-category hard sets is comeager in* E *and the class of* EXP*-category hard sets is comeager in* EXP.

PROOF. By (3.21) and (3.22), the class of n^2-generic sets is comeager in E and EXP, respectively. Since, by Theorem 3.77, any n^2-generic set in E is E-category hard and any n^2-generic set in EXP is EXP-category hard, this implies the claim. □

Corollary 3.79 *Any category hard set for* E *is category hard for* EXP.

PROOF. Immediate by Theorem 3.77. □

Corollary 3.80 *There is a sparse set $A \in \mathrm{E}$ which is category complete for* E.

PROOF. By Theorem 3.77 any n^2-generic set in E is category complete for E and, by Theorem 3.66, there is a sparse n^2-generic set in E. □

Corollary 3.81 *There is a category complete set for* E *which is not measure hard for* EXP *(hence not measure hard for* E*).*

PROOF. This follows from Corollary 3.80 since, by Theorem 3.44, any EXP-measure hard set is exponentially dense. □

Finally, we note that the proof of Theorem 3.45 showing that there are EXP-measure hard sets which are not E-measure hard actually proves the following stronger result. (It suffices to note that n^2-generic sets are p-incompressible.)

Theorem 3.82 *(Ambos-Spies (1996)) There is an* EXP*-measure complete (hence* EXP*-category complete) set $A \in \mathrm{E}$ which is not* E*-category hard.*

3.4.1 Summary of Relations

We can summarize the relations among the hardness notions for E and EXP and the weak completeness for these classes in the literature as follows.

Theorem 3.83 *For any set A the following hold.*

$$\begin{tikzcd}
A\ \mathrm{E}\text{-}\mathit{hard} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{hard} \arrow[d, Rightarrow] \\
A\ \mathrm{E}\text{-}\mathit{measure\text{-}hard} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{measure\text{-}hard} \arrow[d, Rightarrow] \\
A\ \mathrm{E}\text{-}\mathit{category\text{-}hard} \arrow[r, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{category\text{-}hard}
\end{tikzcd} \tag{3.25}$$

Moreover, (up to transitive closure) no other implications hold and sets witnessing the failure of the other relations can be found in E.

Proof. The positive relations are established as follows. The equivalence in line 1 has been shown in Theorem 2.15 while the implications from left to right in lines 2 and 3 hold by Theorem 3.45 and Corollary 3.79, respectively. For the downwards implications see Lemmas 3.39 and 3.75.

Completeness of the diagram follows from the following facts (all witnessed by sets $A \in \mathrm{E}$). By Corollaries 3.42 and 3.81 there cannot be any upwards arrows, and, by Theorem 3.82, the only arrow leading from the right column to the left column is the one given in line 1. □

Corollary 3.84 *For any set $A \in \mathrm{E}$ the following hold.*

$$\begin{tikzcd}
A\ \mathrm{E}\text{-}\mathit{complete} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{complete} \arrow[d, Rightarrow] \\
A\ \mathrm{E}\text{-}\mathit{measure\text{-}complete} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{measure\text{-}complete} \arrow[d, Rightarrow] \\
A\ \mathrm{E}\text{-}\mathit{category\text{-}complete} \arrow[r, Rightarrow] & A\ \mathrm{EXP}\text{-}\mathit{category\text{-}complete}
\end{tikzcd} \tag{3.26}$$

Moreover, (up to transitive closure) no other implications hold.

CHAPTER 4

Nontriviality for E and EXP

Having reviewed the weak completeness notions in the literature, we now introduce a new weak hardness concept for E which can be considered to be the *weakest* weak hardness notion for E (and, similarly, for EXP).

By Lutz's proposal, a set A is weakly hard for E if a nonnegligible part of E can be reduced to A, and Lutz (1995) interpreted negligible subclasses of E as classes which have p-measure 0, i.e., measure 0 in E. Ambos-Spies (1996) took up Lutz's idea but interpreted the size of subclasses of E in terms of (polynomial-time bounded) Baire category, and defined a class to be negligible if it is p-meager, i.e., meager in E. Both approaches are quite natural since Lebesgue measure and Baire category are the traditional tools for measuring the size of sets in mathematical analysis. Still we might ask whether there are some more restrictive or even whether there is some most restrictive notion of negligibility of a subclass in E. Since the linear time class E is actually a hierarchy

$$\mathrm{E}_1 \subset \mathrm{E}_2 \subset \mathrm{E}_3 \subset \bigcup_{k \geq 1} \mathrm{E}_k = \mathrm{E}$$

one would hardly consider a subclass C of E to be nonnegligible if it is contained in a finite level of this hierarchy. If one agrees with this thesis and declares a class $\mathrm{C} \subseteq \mathrm{E}$ to be negligible if *and only if* $\mathrm{C} \subseteq \mathrm{E}_k$ for some $k \geq 1$, then this will be the most restrictive interpretation of negligibility whence the corresponding weak hardness concept will be the most general one. We call this corresponding weak hardness concept E-*nontriviality*, and, similarly, we call a set A EXP-*nontrivial* if, for any level EXP_k of the hierarchy EXP, there is a set $B \in \mathrm{EXP} \setminus \mathrm{EXP}_k$ which is p-m-reducible to A.

It follows from the results in the previous chapter that the individual levels of the E-hierarchy have p-measure 0 and are p-meager whence E-nontriviality generalizes E-measure hardness and E-category hardness. Moreover, since P is contained in the first level E_1 of the E-hierarchy, P is negligible whence E-nontrivial sets are intractable. So E-nontriviality achieves the goals of weak E-hardness notions and generalizes the weak E-hardness notions in the literature.

In this chapter we introduce nontriviality and begin with the analysis of this property. For instance, we show that sets of low complexity in E are E-trivial but we also show that there are E-trivial sets in arbitrarily high classes $\mathrm{E}_{k+1} \setminus \mathrm{E}_k$ ($k \geq 1$) whence high complexity alone does not imply E-nontriviality. By analyzing the possible densities of the E-nontrivial sets, however, we also show that for very sparse sets (namely, for exptally sets) sufficiently high complexity implies E-nontriviality.

4.1 E-Nontriviality: Definitions and Basic Facts

Definition 4.1 A set A is *trivial for* E (or E-*trivial* for short) if

$$\exists\, k \geq 1\ [\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{E}_k] \tag{4.1}$$

holds, and A is *nontrivial for* E (or E-*nontrivial* for short) otherwise.

Note that, by transitivity of $\leq_m^p$, any predecessor of an E-trivial set is E-trivial too. Hence any successor of an E-nontrivial set is E-nontrivial too. So, in particular, E-triviality and E-nontriviality are invariant under p-m-equivalence.

Proposition 4.2 *(i) Let A and B be sets such that B is* E*-trivial and $A \leq_m^p B$. Then A is* E*-trivial too.*

(ii) Let A and B be sets such that A is E*-nontrivial and $A \leq_m^p B$. Then B is* E*-nontrivial too.*

(iii) Let A and B be sets such that A is E*-(non)trivial and $A =_m^p B$. Then B is* E*-(non)trivial too.*

E-nontriviality is related to the previously introduced weak hardness notions for E as follows.

Lemma 4.3 *For any set A the following hold.*

$$\begin{array}{c} A\ \mathrm{E}\text{-}\textit{hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{measure hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{category hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \textit{intractable} \end{array} \tag{4.2}$$

PROOF. For the first two implications (from top) see Theorem 3.83. For a proof of the third implication let A be E-category hard. Then, given $k \geq 1$, by (3.23) there is an n^k-generic set G in $\mathrm{P}_m(A) \cap \mathrm{E}$. Since, by Theorem 3.65, $G \notin \mathrm{E}_k$, it follows that A is E-nontrivial. Finally, the fourth implication is immediate by definition of E-nontriviality. □

In Chapter 3 we have already seen that the first two implications in Lemma 4.3 are strict, even if we consider only sets in E, i.e., if we consider the corresponding weak completeness notions. The strictness of the other two implications will be established below (see Corollary 4.34 and Corollary 4.10).

In the remainder of this section we give an alternative characterization of E-nontriviality and introduce a strengthening of E-triviality, *strict triviality*.

By definition, a set A is E-nontrivial if the part of E which can be reduced to A is not contained in finitely many levels of the E-hierarchy. As we will show next, in fact any E-nontrivial set has predecessors at all levels of the E-hierarchy.

Theorem 4.4 *The following are equivalent.*

1. *A is* E*-nontrivial.*
2. *For any $k \geq 1$ there is a set $B \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$ such that $B \leq^p_m A$.*

The nontrivial implication in this theorem is immediate by the following refinement of the First Padding Lemma (Theorem 2.11).

Lemma 4.5 (Second Padding Lemma) *Let A and $k \geq 1$ be given such that $A \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$. Then, for any $k' \leq k$ (with $k' \geq 1$), there is a set $A' \in \mathrm{E}_{k'+1} \setminus \mathrm{E}_{k'}$ such that $A' =^p_m A$ (in fact, $A \leq^p_{1\text{-}li} A' \leq^p_m A$).*

PROOF. It suffices to show that, for given $k \geq 2$ and $A \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$, there is a set A' such that $A \leq^p_{1\text{-}li} A' \leq^p_m A$ and $A' \in \mathrm{E}_k \setminus \mathrm{E}_{k-1}$. Then the claim follows by induction (using transitivity of $\leq^p_m$ and $\leq^p_{1-li}$).

The idea is as follows. Just as in the padding lemma, for any string x we define a padded version x' and we let A' consist of the padded versions of the strings in A, i.e., $A' = \{x' : x \in A\}$. In order to make sure that A' has the right complexity, we ensure that

$$2^{k|x'|} \approx 2^{(k+1)|x|},$$

i.e.,

$$k|x'| \approx (k+1)|x|$$

or

$$|x'| \approx \frac{k+1}{k}|x| = \frac{|x|}{k} + |x|.$$

This is achieved by letting

$$x' = 0^{f(|x|)}1x \quad \text{where} \quad f(n) = \lfloor \frac{n}{k} \rfloor.$$

Then, clearly, $A' \leq^p_{1-li} A \leq^p_m A'$. It remains to show that $A' \in \mathrm{E}_k$ and $A' \notin \mathrm{E}_{k-1}$.

$\underline{A' \in \mathrm{E}_k.}$ Given y, $y \in A'$ if and only if there is a string x such that $y = 0^{f(|x|)}1x$ and $x \in A$. Now, whether there is such an x, can be determined in polynomial time, and if there is such an x then it is unique and it can be found in polynomial time too. Moreover, by $A \in \mathrm{E}_{k+1}$, the question whether x is an element of A can be decided in $2^{(k+1)|x|}$ steps. Since, by definition, $|y| = \lfloor \frac{|x|}{k} \rfloor + 1 + |x|$ it follows that

$$(k+1)|x| = |x| + k|x| = k(\frac{|x|}{k} + |x|) \leq k(\lfloor \frac{|x|}{k} \rfloor + 1 + |x|) = k|y|.$$

So $x \in A$ can be decided in $O(2^{k|y|})$ steps. It follows that $A' \in \mathrm{E}_k$.

$\underline{A' \notin \mathrm{E}_{k-1}}$. For a contradiction assume that $A' \in \mathrm{E}_{k-1}$. Since $x \in A$ iff $y = 0^{f(|x|)}1x \in A'$ this implies that $x \in A$ can be decided in $O(2^{(k-1)|y|})$ steps. Since

$$|y| = \lfloor \frac{|x|}{k} \rfloor + 1 + |x| \leq \frac{k+1}{k}|x| + 1$$

hence

$$(k-1)|y| \leq (k-1)(\frac{k+1}{k}|x| + 1) = \frac{k^2-1}{k}|x| + k \leq k|x| + k$$

it follows that $x \in A$ can be decided in $O(2^{k|x|+k}) = O(2^{k|x|})$ steps. But this contradicts the assumption that $A \notin \mathrm{E}_k$.

This completes the proof. □

Note that in the definition of an E-trivial set A we only require that *the sets from* E which can be reduced to A are contained in some level E_k of the hierarchy $\mathrm{E} = \cup_{k \geq 1}\mathrm{E}_k$, i.e., that $\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{E}_k$ (see (4.1)). In general, however, this does not imply that *all sets* which can be reduced to A are contained in some level E_k of E, i.e., that $\mathrm{P}_m(A) \subseteq \mathrm{E}_k$ holds. We call sets with this stronger property *strictly trivial*.

Definition 4.6 A set A is *strictly trivial* if

$$\exists\, k \geq 1\, [\mathrm{P}_m(A) \subseteq \mathrm{E}_k] \tag{4.3}$$

holds.

Proposition 4.7 *Let A be strictly trivial. Then $A \in$* E *and A is trivial for* E*.*

PROOF. The latter is immediate by definition. For a proof of the former, it suffices to note that, by reflexivity of $\leq^p_m$, $A \in \mathrm{P}_m(A)$. So, for $A \notin \mathrm{E}$, $\mathrm{P}_m(A) \not\subseteq \mathrm{E}$ whence A is not strictly trivial. □

Proposition 4.8 *Let A and B be sets such that A is strictly trivial and $B \leq^p_m A$. Then B is strictly trivial too.*

PROOF. This is immediate by definition and by transitivity of $\leq^p_m$. □

In Chapters 6 and 7 we will give examples of E-trivial sets outside of E. So strict triviality and E-triviality do not coincide. In Chapter 6 we will also show that there are sets in E which are E-trivial but not strictly trivial.

4.2 E-Trivial Sets in E

In this section we describe two approaches for obtaining trivial sets in E.

- First, we show that sets of low time-complexity are strictly trivial (hence E-trivial). In particular, we show that any hyperpolynomial shift of any set in EXP is strictly trivial.
- Second, we give a diagonal argument which allows us to construct strictly trivial sets at arbitrarily high levels of the E-hierarchy.

Moreover, by refining some argument by Buhrman and Mayordomo (1997), we give some natural examples of intractable strictly trivial sets in E.

4.2.1 Sets of Low Complexity Are Trivial

We first observe that sets of low hyperpolynomial time-complexity are strictly trivial, hence E-trivial. By the time hierarchy theorem this gives some first examples of sets which are intractable but E-trivial thereby showing that our triviality concept is meaningful.

Theorem 4.9 *Let t be a nondecreasing, time constructible function such that, for some number $k \geq 1$,*

$$t(p(n)) \leq_{a.e.} 2^{kn} \tag{4.4}$$

for all polynomials p. Then any set $A \in \mathrm{DTIME}(t(n))$ is strictly trivial (hence E*-trivial).*

PROOF. Given $A \in \mathrm{DTIME}(t(n))$ it suffices to show that $\mathrm{P}_m(A) \subseteq \mathrm{E}_k$. So let $B \in \mathrm{P}_m(A)$, and fix f and a polynomial p such that $B \leq_m^p A$ via f and p is a time bound for f. Now,

$$B(x) = A(f(x))$$

and, by p being a time bound for f, $|f(x)| \leq p(|x|)$. So, $B(x)$ can be computed in

$$p(|x|) + O(t(p(|x|)))$$

steps where $p(|x|)$ steps are required for computing $f(x)$ and

$$O(t(|f(x)|)) \leq O(t(p(|x|)))$$

steps for computing $A(f(x))$. Since, by (4.4),

$$O(t(p(|x|))) \leq 2^{k|x|}$$

for all sufficiently large x, this implies $B \in \mathrm{E}_k$. □

Corollary 4.10 *There is a strictly trivial (hence* E*-trivial) set in* $\mathrm{E} \setminus \mathrm{P}$.

PROOF. Note that, for any polynomial p, $p(n) \leq_{a.e.} 2^{(\log n)^2}$ whence

$$\mathrm{P} \subseteq \mathrm{DTIME}(2^{(\log n)^2}).$$

Moreover, as one can easily check, $2^{(\log n)^4} \not\in O(2^{(\log n)^2} \cdot \log(2^{(logn)^2}))$ whence, by the time hierarchy theorem,

$$\mathrm{DTIME}(2^{(\log n)^2}) \subset \mathrm{DTIME}(2^{(\log n)^4}).$$

So

$$\mathrm{P} \subset \mathrm{DTIME}(2^{(\log n)^4}).$$

Moreover, as one can easily show, $2^{(\log\, p(n))^4} \leq_{a.e.} 2^n$ for all polynomials p. So the claim follows from Theorem 4.9. □

4.2.2 Hyperpolynomial Shifts Are Trivial

We obtain some further examples of strictly trivial sets along these lines by considering hyperpolynomial shifts of intractable sets in EXP. Hyperpolynomial shifts have been introduced in Ambos-Spies (1989) for analyzing the structure of the polynomial-time reducibilities.

Definition 4.11 (a) A *hyperpolynomial shift h* is a time constructible, nondecreasing function $h : \mathbb{N} \to \mathbb{N}$ such that h dominates all polynomials.

(b) For any set A and any hyperpolynomial shift h,

$$A_h = \{1^{h(|x|)}0x : x \in A\}$$

is the *h-shift* of A. B is a *hyperpolynomial shift* of A if $B = A_h$ for some hyperpolynomial shift h.

Note that in the Padding Lemma we used *linear* shifts. While for a linear or polynomial shift p, $A_p =^p_m A$, for a hyperpolynomial shift h, A_h is strictly less than A w.r.t. $\leq^p_m$.

Lemma 4.12 *(see Ambos-Spies (1989)) For any set $A \not\in \mathrm{P}$ and any hyperpolynomial shift h, $A_h <^p_m A$.*

In the following we will use the following result on the existence of intractable hyperpolynomial shifts of intractable computable problems.

Theorem 4.13 *(Ambos-Spies (1989)) For any computable set $A \not\in \mathrm{P}$ there is a hyperpolynomial shift A_h of A such that $A_h \not\in \mathrm{P}$. If, moreover, B is a computable set such that $A \not\leq^p_m B$ then A_h can be chosen so that $A_h \not\leq^p_m B$.*

Our next theorem shows that hyperpolynomial shifts of exponential time computable sets are strictly trivial (hence E-trivial).

Theorem 4.14 *Let $A \in \mathrm{EXP}$ and let h be a hyperpolynomial shift. Then A_h is strictly trivial (hence* E*-trivial).*

Proof. By Theorem 4.9 it suffices to show that there is a nondecreasing time constructible function t such that $A_h \in \mathrm{DTIME}(t(n))$ and such that

$$t(p(n)) \leq_{a.e.} 2^n \tag{4.5}$$

for all polynomials p.

Fix k such that $A \in \mathrm{EXP}_k = \mathrm{DTIME}(2^{n^k})$, let

$$g(n) = \mu m(h(m) \geq n),$$

and

$$t(n) = max\{n^2, 2^{g(n)^k}\}.$$

Since $h(m)$ is nondecreasing, time constructible, and $h(m) >_{a.e.} m$, the functions $g(n)$ and $t(n)$ are nondecreasing, and $t(n)$ is time constructible.

Moreover, given a string y of length n, the question whether $y \in A_h$ can be decided as follows.

- First decide whether $y = 1^{h(|x|)}0x$ for some string x and, if so, compute the unique such x. By time constructibility of h, this can be done in $O(n^2)$ steps. If there is no such x then $y \notin A_h$. Otherwise, fix x such that $y = 1^{h(|x|)}0x$ and proceed as follows.
- Decide whether $x \in A$. Since $A \in \mathrm{DTIME}(2^{n^k})$, this can be done in $O(2^{|x|^k}) \leq O(2^{g(n)^k})$ steps, and $y \in A_h$ if and only if $x \in A$.

So $A_h \in \mathrm{DTIME}(t(n))$.

It remains to show that, given $k' \geq 1$, (4.5) holds for the polynomial $p(n) = n^{k'}$. Since $(n^{k'})^2 = n^{k' \cdot 2} <_{a.e.} 2^n$, it suffices to show that

$$2^{g(n^{k'})^k} \leq_{a.e.} 2^n,$$

i.e., that

$$g(n^{k'})^k \leq_{a.e.} n. \tag{4.6}$$

Now, since h is hyperpolynomial,

$$h(n) >_{a.e.} n^{k \cdot k'} = (n^k)^{k'}$$

whence

$$h(\sqrt[k]{n}) >_{a.e.} n^{k'}.$$

So, by definition of g,

$$g(n^{k'}) = \mu m(h(m) \geq n^{k'}) \leq \sqrt[k]{n}$$

whence (4.6) holds. □

Theorem 4.14 together with Theorem 4.13 implies that any intractable set in E has an intractable strictly trivial set among its predecessors and that the class of the strictly trivial sets (hence the E-trivial sets) in E is bounded from above only by the E-complete sets.

Corollary 4.15 *For any set $B \in \mathrm{E} \setminus \mathrm{P}$ there is an intractable strictly trivial set A such that $A <^p_m B$.*

PROOF. Given a set $B \in \mathrm{E} \setminus \mathrm{P}$, by Theorem 4.13, fix a hyperpolynomial shift h such that $B_h \notin \mathrm{P}$ and let $A = B_h$. Then, by Theorem 4.14, A is strictly trivial and, by Lemma 4.12, $A <^p_m B$. □

Corollary 4.16 *For any set $B \in \mathrm{E}$ which is not E-complete there is a strictly trivial set A such that $A \not\leq^p_m B$.*

PROOF. Given an E-incomplete set $B \in \mathrm{E}$, fix an E-complete set C, and, by Theorem 4.13, fix a hyperpolynomial shift h such that $C_h \not\leq^p_m B$. Then, by Theorem 4.14, $A = C_h$ has the required properties. □

4.2.3 Strictly Trivial Sets in E of High Complexity

The above results yield E-trivial sets of low complexity. In particular, all the E-trivial sets obtained by Theorem 4.9 are in the lowest level E_1 of the E-hierarchy. Next we will show that there are E-trivial sets (in fact, strictly trivial sets) at arbitrarily high levels $\mathrm{E} \setminus \mathrm{E}_k$ of the E - hierarchy. So, by the Second Padding Lemma (Lemma 4.5), there are E-trivial sets (and strictly trivial sets) at all levels of the E-hierarchy.

Theorem 4.17 *For any $k \geq 1$ there is a strictly trivial (hence E-trivial) set A in $\mathrm{E} \setminus \mathrm{E}_k$.*

The proof of Theorem 4.17 is based on the following observation.

Lemma 4.18 (Boundedness Lemma) *Let A and B be sets and let f be a p-m-reduction function such that $A \in \mathrm{E}_k$, $B \leq^p_m A$ via f, and*

$$\forall^\infty x\ (|f(x)| \leq k' \cdot |x| + k'' \ \text{ or } \ f(x) \notin A) \tag{4.7}$$

(for some $k, k', k'' \geq 1$). Then $B \in \mathrm{E}_{k' \cdot k}$.

PROOF. Given x, in order to compute $B(x)$ it suffices to first compute $y = f(x)$ (requiring $poly(|x|)$ steps) and second compute $A(y)$. Now, if

$$|y| = |f(x)| \leq k' \cdot |x| + k''$$

then, by $A \in \mathrm{E}_k$, $A(y)$ can be computed in $2^{k|y|} \leq 2^{k\cdot(k'|x|+k'')} \leq O(2^{(k\cdot k')|x|})$ steps. Otherwise, by (4.7), w.l.o.g. we may assume that $A(y) = 0$.

Obviously, this implies $B \in \mathrm{E}_{k'\cdot k}$. □

PROOF OF THEOREM 4.17. Fix $k \geq 1$, and let $\{E^k_e : e \geq 0\}$ and $\{f_e : e \geq 0\}$ be enumerations of E_k and of the class of the *p*-*m*-reduction functions, respectively, such that $E^k_e(x)$ can be computed in time $O(2^{(k+1)max(e,|x|)})$ and $f_e(x)$ can be computed in time $O(2^{max(e,|x|)})$ (uniformly in e and x).

By a diagonal argument we define a set $A \in \mathrm{E}$ which meets the requirements

$$\mathfrak{R}_{2e} : A \neq E^k_e$$

and

$$\mathfrak{R}_{2e+1} : \forall x \in \Sigma^* \ (|f_e(x)| > |x| + e + 1 \Rightarrow f_e(x) \notin A)$$

for $e \geq 0$.

Obviously, the requirements with even indices ensure that $A \notin \mathrm{E}_k$. Similarly, assuming that $A \in \mathrm{E}$, say $A \in \mathrm{E}_{\hat{k}}$, the requirements with odd indices ensure that A is strictly trivial since, by Lemma 4.18, $\mathrm{P}_m(A) \subseteq \mathrm{E}_{\hat{k}}$.

For the definition of A, call a string y *forbidden* if $y = f_e(x)$ for some number e and some string x such that $|x| + e + 1 < |y|$. Note that the requirements $\mathfrak{R}_{2e+1}$ are met if we do not put any forbidden string into A. Moreover, the question whether a string y is forbidden can be decided in $O(2^{2|y|})$ steps. Finally, by a simple counting argument, for any $n \geq 0$ there is a string of length n which is not forbidden.

Now, define A by letting $A = \{y_e : y_e \notin E^k_e\}$ where y_e is the least string of length e which is not forbidden. Then all requirements are met and, as one can easily check, $A \in \mathrm{E}_{k+2}$.

This completes the proof. □

Corollary 4.19 *For any $k \geq 1$ there is a strictly trivial (hence* E*-trivial) set A in* $\mathrm{E}_{k+1} \setminus \mathrm{E}_k$.

PROOF. Since the class of the strictly trivial sets is closed downwards under $\leq^p_m$ (Proposition 4.8), this follows from Theorem 4.17 and Lemma 4.5. □

4.2.4 Some Natural Examples of Intractable Strictly Trivial Sets

Next we will show that there are ”natural” examples of intractable problems which are strictly trivial, hence E-trivial. These examples are found in the theory of time-bounded Kolmogorov complexity. Buhrman and Mayordomo (1997) have shown that for some appropriate time bounds $t(n)$ the sets R^t of strings which are random (i.e. incompressible) with respect to $t(n)$-time-bounded Kolmogorov complexity are intractable but not measure complete for E. We extend this observation by showing that the sets R^t are actually strictly trivial.

We first shortly review the basic notions of time-bounded Kolmogorov complexity to be needed (see Li and Vitányi (1997) for more details).

Let M be a (multi-tape) Turing machine and let $t : \mathbb{N} \to \mathbb{N}$ be computable. Then, for any string x,

$$C_M(x) = \min\{|y| : M(y) = x\}$$

and

$$C^t_M(x) = \min\{|y| : M(y) = x \text{ and } time_M(y) = t(|x|)\}$$

are the *Kolmogorov complexity of x with respect to M* and the *$t(n)$-time-bounded Kolmogorov complexity of x with respect to M*, respectively (where $\min\emptyset = \infty$).

Note that, for t and t' such that $t(n) \leq t'(n)$ for $n \geq 0$,

$$C_M(x) \leq C^{t'}_M(x) \leq C^t_M(x).$$

We will tacitly use this fact below. Moreover, in the following, we will identify the number n with the n-th string z_n. So, in particular, $|n| = |z_n| \leq \log(n) + 1$.

Though the (time-bounded) Kolmogorov complexity depends on the chosen Turing machine, we can choose a Turing machine U (e.g. the universal Turing machine of Hennie and Stearns (1966)) such that the Kolmogorov complexity of strings with respect to U is minimal up to an additive constant. The corresponding fact for the time-bounded case holds up to some moderate increase of the time bound (due to tape reduction) too.

Theorem 4.20 (Time-Bounded Invariance Theorem) *There is a universal Turing machine U such that for any Turing machine M there is a constant c such that, for any computable function $t : \mathbb{N} \to \mathbb{N}$*

$$\forall x \in \Sigma^*(C_U^{c\cdot t\cdot log(t)}(x) \leq C^t_M(x) + c) \tag{4.8}$$

holds. So, in particular,

$$\forall x \in \Sigma^*(C_U(x) \leq C_M(x) + c). \tag{4.9}$$

For a proof of Theorem 4.20 see Li and Vitányi (1997), Theorem 7.1.

In the following we let

$$C(x) = C_U(x) \text{ and } C^t(x) = C^t_U(x)$$

and call $C(x)$ and $C^t(x)$ the *Kolmogorov complexity* of x and $t(n)$*-time-bounded Kolmogorov complexity* of x, respectively.

Definition 4.21 A string x is K*-incompressible* or K*-random* if $C(x) \geq |x|$ and x is $t(n)$-K*-incompressible* or $t(n)$-K*-random* if $C^t(x) \geq |x|$.

We let

$$R = \{x : x \text{ is } K\text{-random}\}$$

and

$$R^t = \{x : x \text{ is } t(n)\text{-}K\text{-random}\}.$$

It is a well-known result of computability theory that the complement $\bar{R}$ of the set R of the non-K-random strings is computably enumerable (c.e.) but neither computable nor m-complete (though it is T-complete).

Buhrman and Mayordomo (1997) have shown, that, for $t(n) = 2^{kn}$ $(k \geq 2)$, R^t is in E, intractable (i.e. not in P) but not E-complete, in fact not even measure complete for E. Here we extend this result by showing that R^t is strictly trivial, hence E-trivial. (For simplicity we consider only the case of $t(n) = 2^{2n}$ but our argument can be easily generalized to $t(n) = 2^{kn}$ for $k \geq 2$.)

We first review the observation that $R^{2^{2n}}$ is in E but intractable.

Lemma 4.22 *For* $t(n) = 2^{2n}$, R^t *is in* E_3 *but not in* P.

Proof. We first show that $R^t \in \mathrm{E}_3$. Given x and $n = |x|$,

$$x \in R^t \Leftrightarrow \forall y \in \Sigma^{<n}(time_U(y) \leq 2^{2n} \Rightarrow U(y) \neq x).$$

So, in order to decide whether x is in R^t, it suffices to compute $U(y)$ for any of the $2^n - 1$ strings y of length less than n for up to 2^{2n} steps. Hence $R^t(x)$ can be computed in $O(2^n \cdot 2^{2n}) = O(2^{3n})$ steps. So $R^t \in \mathrm{E}_3$.

Next we show that R^t is not in P. For a contradiction assume that R^t is in P, and fix a polynomial p such that $R^t \in \mathrm{DTIME}(p(n))$.

Note that for any n there is a string of length n in R^t since there are 2^n strings of length n but only $2^n - 1$ strings of length less than n (whence at least one string of length n cannot be compressed). Let x_n be the least string of length n in R^t. By assumption, x_n can be computed in $O(2^n \cdot p(n))$ steps. So we may fix a Turing machine M and a number $c \geq 0$ such that, for all $n \geq 0$,

$$M(n) = x_n$$

and

$$time_M(n) \leq c \cdot p(n) \cdot 2^n.$$

Then, for $t'(n) = c \cdot p(n) \cdot 2^n$,

$$C_M^{t'}(x_n) = |n| \leq \log(n) + 1.$$

Since, for any constant c',

$$c' \cdot t'(n) \cdot \log(t'(n)) <_{a.e.} 2^{2n} = t(n)$$

it follows by Theorem 4.20 that there is a constant c', such that

$$C^t(x_n) \leq C_M^{t'}(x_n) + c' \leq log(n) + 1 + c' <_{\text{a.e.}} n = |x_n|.$$

So, for sufficiently large n, $x_n \notin R^t$ contrary to choice of x_n.

This completes the proof. □

Theorem 4.23 *For $t(n) = 2^{2n}$, R^t is strictly trivial hence* E*-trivial.*

For the proof we need the following lemma.

Lemma 4.24 *Let $t(n) = 2^{2n}$ and let $f : \Sigma^* \to \Sigma^*$ be polynomial-time computable. There is a constant c such that*

$$\forall^\infty x(C^t(f(x)) \leq |x| + c). \tag{4.10}$$

PROOF. Let M be a polynomial-time bounded Turing machine such that $M(x) = f(x)$ and let p be a polynomial such that $time_M(x) \leq p(|x|)$ for all x. Then

$$C_M^p(f(x)) \leq |x|.$$

Since, for any constant c,

$$\forall^\infty n(c \cdot p(n) \cdot \log(p(n)) \leq 2^{2n}),$$

it follows by Theorem 4.20 that there is a constant c such that

$$C^t(f(x)) \leq C_M^p(f(x)) + c \leq |x| + c$$

for almost all x. □

PROOF OF THEOREM 4.23. It suffices to show that $\mathrm{P}_m(R^t) \subseteq \mathrm{E}_6$.

So fix A such that $A \leq_m^p R^t$ and let f be a polynomial-time computable function such that $A \leq_m^p R^t$ via f, i.e.,

$$x \in A \Leftrightarrow f(x) \in R^t. \tag{4.11}$$

Note that, by Lemma 4.22, $R^t \in \mathrm{E}_3$. So, in order to show that $A \in \mathrm{E}_6$, by the Boundedness Lemma (Lemma 4.18), it suffices to show that there is a number $c \geq 0$ such that

$$|x| > c \;\&\; x \in A \Rightarrow |f(x)| < 2 \cdot |x| \tag{4.12}$$

holds.

For a proof of (4.12), by Lemma 4.24 we may fix c such that, for any string x,

$$|x| > c \Rightarrow C^t(f(x)) \leq |x| + c \tag{4.13}$$

holds. Now fix x such that $|x| > c$ and $x \in A$. By the latter and by (4.11), $f(x) \in R^t$ whence $C^t(f(x)) \geq |f(x)|$. So, by $|x| > c$ and by (4.13),

$$2 \cdot |x| > |x| + c \geq C^t(f(x)) \geq |f(x)|$$

whence $|f(x)| < 2 \cdot |x|$.

This completes the proof. □

4.3 E-Nontrivial Sets in E

We now give some existence results for E-nontrivial sets in E. By Lemma 4.3 any E-complete or E-measure complete or E-category complete set is E-nontrivial. So existence results for sets with those properties give existence results for E-nontrivial sets. In particular, the following observation on E-complete sets shows that there are E-nontrivial sets at all levels of E.

Proposition 4.25 *There is an* E*-complete set $A_1 \in \mathrm{E}_1$ and, for any $k \geq 1$, there is an* E*-complete set $A_{k+1} \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$.*

(Hence, in particular, there is an E*-nontrivial set $A_1 \in \mathrm{E}_1$ and, for any $k \geq 1$, there is an* E*-nontrivial set $A_{k+1} \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$.)*

PROOF. Let A be E-complete and, by the time hierarchy theorem, fix $B_{k+1} \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$. By the First Padding Lemma (Theorem 2.11) there is a set A_1 in E_1 such that $A_1 =^p_m A$. So, for $A_{k+1} = A_1 \oplus B_{k+1}$, $A_1 \in \mathrm{E}_1$, $A_{k+1} \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$, and

$$\forall\, k \geq 1 \; (A \leq^p_m A_1 \leq^p_m A_{k+1}). \tag{4.14}$$

Since A is E-complete, it follows that the sets A_k are E-complete too. □

4.3.1 Splitting E-Nontrivial Sets

We obtain more examples of E-nontrivial sets by observing that, for any p-splitting of an E-nontrivial set, at least one of the parts is E-nontrivial again.

Definition 4.26 A splitting of a set A into two disjoint sets A_0 and A_1 is a *p-splitting* if there is a set $B \in \mathrm{P}$ such that $A_0 = A \cap B$ and $A_1 = A \cap \overline{B}$.

The properties of p-splittings to be needed are summarized in the following lemma.

Lemma 4.27 *Let A and B be sets such that $B \in \mathrm{P}$ and let (A_0, A_1) be the p-splitting of A by B (i.e., $A_0 = A \cap B$ and $A_1 = A \cap \overline{B}$).*

(i) $A_0, A_1 \leq^p_m A$. In fact, $A =^p_m A_0 \oplus A_1$.

(ii) If $A \in \mathrm{E}_k$ then $A_0, A_1 \in \mathrm{E}_k$ $(k \geq 1)$.

(iii) If $A \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$ then $A_0 \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$ or $A_1 \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$ $(k \geq 1)$.

PROOF. The proof is straightforward. We only give the proof of claim (iii). For a contradiction assume that $A \in \mathrm{E}_{k+1} \setminus \mathrm{E}_k$ but $A_0, A_1 \in \mathrm{E}_k$. Then, given x, $A(x)$ can be computed by first checking whether $x \in B$ ($poly(|x|)$ steps), and, if so, by computing $A_0(x)$; and by computing $A_1(x)$ otherwise (either can be done in $2^{k|x|}$ steps). So $A \in \mathrm{E}_k$. Contradiction! □

Theorem 4.28 *Let A be E-nontrivial and let (A_0, A_1) be a p-splitting of A. Then A_0 is E-nontrivial or A_1 is E-nontrivial (or both).*

PROOF. For a contradiction assume that A_0 and A_1 are E-trivial. Fix k_i such that

$$\mathrm{P}_m(A_i) \cap \mathrm{E} \subseteq \mathrm{E}_{k_i}$$

$(i = 0, 1)$ and let $k = \max(k_0, k_1)$. Moreover, fix $B \in \mathrm{P}$ such that $A_0 = A \cap B$ and $A_1 = A \cap \overline{B}$. Finally, by E-nontriviality of A, fix a set $C \in \mathrm{E} \setminus \mathrm{E}_k$ such that $C \leq^p_m A$ and let f be a polynomial-time computable function such that $C \leq^p_m A$ via f. Then, for $D = \{x : f(x) \in B\}$, $D \in \mathrm{P}$ whence $C_0 = C \cap D$ and $C_1 = C \cap \overline{D}$ is a p-splitting of C. So, by Lemma 4.27 (ii) and (iii), we may fix $i \leq 1$ such that $C_i \in \mathrm{E} \setminus \mathrm{E}_k$. On the other hand, however, $C_i \leq^p_m A_i$ via the p-m-reduction g_i defined by

$$g_0(x) = \begin{cases} f(x) & \text{if } x \in D \\ y_0 & \text{otherwise} \end{cases} \quad \text{and} \quad g_1(x) = \begin{cases} f(x) & \text{if } x \notin D \\ y_1 & \text{otherwise} \end{cases}$$

where y_0 and y_1 are fixed strings such that $y_0 \notin A_0$ and $y_1 \notin A_1$. (W.l.o.g. we may assume that A_0 and A_1 are not empty since otherwise the claim is trivial.) But this contradicts the choice of k_0 and k_1. □

By applying some result of Ladner on p-splittings, Theorem 4.28 yields the dual of Corollary 4.16, namely that no intractable set is a lower bound of the E-nontrivial sets in E (w.r.t. $\leq^p_m$).

Corollary 4.29 *For any set $B \in \mathrm{E}$ which is not polynomial-time computable there is an* E*-nontrivial set $A \in \mathrm{E}$ such that $B \not\leq^p_m A$.*

PROOF. Ladner (1975) has shown that, for any computable sets B and C such that $B \notin \mathrm{P}$, there is a p-splitting (C_0,C_1) of C such that $B \not\leq^p_m C_0,C_1$. Now, given $B \in \mathrm{E} \setminus \mathrm{P}$, apply Ladner's result to B and any E-complete set C. Then $C_0,C_1 \in \mathrm{E}$, $B \not\leq^p_m C_0,C_1$ and, by Theorem 4.28, at least one of the sets C_0 and C_1 is E-nontrivial. □

More results on the distribution of the E-nontrivial sets under p-m-reducibility will be given in Chapter 8.

4.3.2 E-Nontrivial Sets of Low Density

Next we show that there are tally E-nontrivial sets of very low density. This will distinguish nontriviality from the previously introduced weak completeness concepts. We first observe that the tally part of any E_1-bi-immune set in E is E-nontrivial. In fact, we obtain the following somewhat stronger result.

Theorem 4.30 *Let $A \in \mathrm{E}$ be E_1-bi-immune and let D be an infinite tally set such that $D \in \mathrm{P}$. Then $A \cap D$ is* E*-nontrivial. In particular, $A \cap \{0\}^*$ is* E*-nontrivial.*

PROOF. Fix $k \geq 1$. We will show that there is a set $B \leq^p_m A \cap D$ such that $B \in \mathrm{E} \setminus \mathrm{E}_k$.

For $n \geq 0$, let

$$m_n = \mu\, m\ ((k+1)n \leq m < (k+1)(n+1)\ \&\ 0^m \in D)$$

(if there is such an m) and let

$$B = \{0^n : m_n \downarrow\ \&\ 0^{m_n} \in A\}.$$

Note that, given n, we can compute m_n (if exists) in polynomial time, and $B \leq^p_m A$ via the function f defined by

$$f(x) = \begin{cases} 0^{m_n} & \text{if } x = 0^n \ \&\ m_n \downarrow \\ y & \text{otherwise} \end{cases}$$

where y is any fixed string such that $y \notin A$. Moreover, for almost all x, $|f(x)| < (k+1)(|x|+1)$. By $A \in \mathrm{E}$ and by Lemma 4.18 this implies that $B \in \mathrm{E}$.

It remains to shows that $B \notin \mathrm{E}_k$. For a contradiction assume that $B \in \mathrm{E}_k$. Let $B' = \{0^{m_n} : 0^n \in B\}$. Then, by infinity of B, B' is infinite and, by definition of B, $B' \subseteq A$.

Moreover, $B' \in \mathrm{E}_1$. Namely, given a string y, we can decide whether $y \in B'$ by first checking (in polynomial time) whether there is a number n such that $y = 0^{m_n}$ and, if so, by computing $B(0^n)$. Since $B \in \mathrm{E}_k$ and $n < \frac{m_n}{k+1}$, the latter can be done in

$$O(2^{kn}) \leq O(2^{\frac{k}{k+1}m_n}) \leq O(2^{|y|})$$

steps.

So A contains the infinite set $B' \in \mathrm{E}_1$. But this contradicts E_1-bi-immunity of A.

□

Corollary 4.31 *For any infinite tally set $D \in \mathrm{P}$ there is an* E*-nontrivial set A in* E *such that $A \subseteq D$. In particular, there is a tally* E*-nontrivial set A in* E*.*

PROOF. By the existence of E_1-bi-immune sets in E and by Theorem 4.30. □

In contrast to Corollary 4.31, category complete sets cannot be tally. This is an easy consequence of the following observation.

Lemma 4.32 *Let A, B be sets such that A is 2^n-incompressible and $A \leq_m^p B$. Then B is not tally.*

PROOF. For a contradiction assume that B is tally. Fix a function f such that $A \leq_m^p B$ via f. Let

$$f'(x) = \begin{cases} f(x) & \text{if } f(x) \in \{0\}^* \\ 1 & \text{otherwise.} \end{cases}$$

Then $f' \in \mathrm{P}$ and $A \leq_m^p B$ via f'. By $f' \in \mathrm{P}$ fix a polynomial p such that $|f'(x)| \leq p(|x|)$ for all x and fix n_0 such that $p(n+2) < 2^n$ for all $n \geq n_0$. Then, for any $n \geq n_0$, there are strings $x \neq x'$ of length n such that $f'(x) = f'(x')$ since $f'(\Sigma^n) \subseteq \{0^0, ..., 0^{p(n)}, 1\}$, whence $|f'(\Sigma^n)| \leq p(n) + 2 < 2^n = |\Sigma^n|$. So f' is not almost one-to-one. But that contradicts the assumption that A is 2^n-incompressible. □

Theorem 4.33 *No tally set is* E*-category hard.*

PROOF. The proof is by contraposition. Let A be E-category hard. By (3.23), there is an n^2-generic set $G \leq_m^p A$. Since, by Theorem 3.65, any n^2-generic set is 2^n-incompressible, it follows with Lemma 4.32 that A is not tally. □

Corollary 4.34 *There is an* E*-nontrivial set A in* E *which is not* E*-category complete, hence not* E*-measure complete.*

PROOF. By Corollary 4.31 there is a tally E-nontrivial set A in E whereas, by Theorem 4.33, no E-category complete set is tally. □

Theorem 4.30 also implies that, though there are arbitrarily complex E-trivial sets in E (see Theorem 4.17), no E-trivial set in E is almost-everywhere complex for the first level E_1 of the E-hierarchy.

Corollary 4.35 *Let $A \in \mathrm{E}$ be E_1-bi-immune. Then A is* E*-nontrivial.*

PROOF. By Theorem 4.30, $A \cap \{0\}^*$ is nontrivial. Since $A \cap \{0\}^* \leq_m^p A$, the claim follows by upward closure of E-nontriviality under $\leq_m^p$. □

By Corollary 4.31 there are arbitrarily sparse E-nontrivial sets A in E. In fact, as we will show next, *all* exponential-time computable subsets of very sparse polynomial-time computable sets are E-nontrivial unless they are contained in the first level E_1 of E. In order to make this more precise we need the following notion.

Definition 4.36 Let δ be the iterated exponential function inductively defined by $\delta(0) = 0$ and $\delta(n+1) = 2^{\delta(n)}$. A set A is *exptally* if $A \subseteq \{0^{\delta(n)} : n \geq 0\}$.

Note that the iterated exponential function is time constructible and strictly increasing whence $\{0^{\delta(n)} : n \geq 0\} \in \mathrm{P}$ and, for any number n, we can check in $poly(n)$ steps whether or not $n = \delta(m)$ for some number m and, if so, determine the unique such number m.

Theorem 4.37 *Let $A \in \mathrm{E} \setminus \mathrm{E}_1$ be exptally. Then A is* E*-nontrivial.*

PROOF. Given $k \geq 0$, we have to show that there is a set $B \leq_m^p A$ such that $B \in \mathrm{E} \setminus \mathrm{E}_k$.

Fix n_0 such that, for $n > n_0$, $(k+1)\delta(n-1) < \delta(n)$ and, for $n > n_0$, let

$$\delta_k(n) = \mu m\,((k+1)m \geq \delta(n).$$

Finally, let

$$B = \{0^{\delta_k(n)} : n > n_0 \;\&\; 0^{\delta(n)} \in A\}.$$

Note that, given m, in $poly(m)$ steps we can decide whether $m = \delta_k(n)$ for some $n > n_0$ and if so compute the corresponding, uniquely determined n. So $B \leq_m^p A$ via the function f defined by

$$f(x) = \begin{cases} 0^{\delta(n)} & \text{if } x = 0^{\delta_k(n)} \text{ for some } n > n_0 \\ y & \text{otherwise} \end{cases}$$

where y is any fixed string such that $y \notin A$.

It remains to show that $B \in \mathrm{E} \setminus \mathrm{E}_k$. In order to show this, first observe that, by definition of δ_k and f,

$$\forall^\infty x\,(k|x| \leq |f(x)| \leq (k+1)|x|). \tag{4.15}$$

So $B \in \mathrm{E}$ is immediate by $A \in \mathrm{E}$ and by Lemma 4.18.

Finally, for a proof of $B \notin \mathrm{E}_k$, for a contradiction assume that $B \in \mathrm{E}_k$.

Then, given x, $A(x)$ can be computed in $O(2^{|x|})$ steps as follows. First, in $poly(|x|)$ steps, decide whether $x = 0^{\delta(n)}$ for some n and, if so, compute the unique corresponding n. Now if such an n does not exist then $A(x) = 0$ and if $n \leq n_0$ then $A(x)$ can be computed by looking up a finite table. Finally, if $x = 0^{\delta(n)}$ for some

$n > n_0$ then $A(x) = B(0^{\delta_k(n)})$. But then, since, by assumption, $B \in \mathrm{E}_k$ and since, by (4.15), w.l.o.g. $k \cdot \delta_k(n) \leq |x|$, $B(0^{\delta_k(n)})$ (hence $A(x)$) can be computed in $O(2^{|x|})$ steps.

So $A \in \mathrm{E}_1$ contrary to choice of A. □

In order to make the previous theorem meaningful we observe that, for any $k \geq 1$, there are exptally sets in $\mathrm{E} \setminus \mathrm{E}_k$.

Lemma 4.38 *For any $k \geq 1$, there is an exptally set A in* $\mathrm{E}_{k+1} \setminus \mathrm{E}_k$.

PROOF. Fix $k \geq 1$ and let $\{E_e^k : e \geq 0\}$ be an enumeration of E_k such that $E_e^k(x)$ can be uniformly computed in $O(2^{(k+1)\cdot max(e,|x|)})$ steps. Define $A \subseteq \{0^{\delta(n)} : n \geq 0\}$ by

$$0^{\delta(n)} \in A \Leftrightarrow 0^{\delta(n)} \notin E_n^k.$$

Then, as one can easily check, A has the required properties. □

We close this section with an application of Theorem 4.37. Recall that, for any polynomial-time reducibility $\leq_r^p$, a pair of sets $A, B \notin \mathrm{P}$ is a *p-r-minimal pair* if

$$\forall\, C\, (C \leq_r^p A \,\&\, C \leq_r^p B \;\Rightarrow\; C \in \mathrm{P}).$$

Corollary 4.39 *There is a p-m-minimal pair (A_0, A_1) of* E*-nontrivial sets $A_0, A_1 \in$* E.

PROOF. By a straightforward variant of the proof of Lemma 4.38 there are exptally sets $A_i \in \mathrm{E}_2 \setminus \mathrm{E}_1$ such that $A_i \subseteq \{0^{\delta(4n+2i)} : n \geq 0\}$ $(i = 0, 1)$. Then, by Theorem 4.37, A_0 and A_1 are strongly E-nontrivial. So it suffices to show that A_0 and A_1 form a *p*-*m*-minimal pair.

This is shown as in the proof of Corollary 3.2 in Ambos-Spies (1999). So we only sketch the proof. Assume that $B \leq_m^p A_i$ via f_i $(i = 0, 1)$ and let the polynomial p be a time bound for f_0 and f_1. Then $B(x)$ can be computed in polynomial time as follows. Compute $f_0(x)$ and $f_1(x)$. If, for some $i \leq 1$, $f_i(x) \notin \{0^{\delta(4n+2i)} : n \geq 0\}$ then $x \notin B$. So we may assume that $f_i(x) = 0^{\delta(4n_i+2i)}$ and we may fix $i_0 \leq 1$ such that $4n_{i_0} + 2i_0 < 4n_{1-i_0} + 2(1 - i_0)$. Then, by definition of δ and by p being a time of f_{1-i_0},

$$2^{2\cdot\delta(4n_{i_0}+2i_0)} \leq \delta(4n_{1-i_0} + 2(1 - i_0)) \leq p(|x|).$$

So, by $A_{i_0} \in \mathrm{E}_2$,

$$B(x) = A(f_{i_0}(x)) = A(0^{\delta(4n_{i_0}+2i_0)})$$

can be computed in $p(|x|)$ steps. □

Intuitively, Corollary 4.39 says that there are E-nontrivial sets $A_0, A_1 \in \mathrm{E}$ without any common nontrivial (in the sense of complexity) information content.

In Chapter 8 we will present some more results on the distribution of the E-nontrivial sets among the sets in E with respect to $\leq_m^p$.

4.4 EXP-Nontriviality

The nontriviality notion for E (Definition 4.1) can be easily adapted to EXP.

Definition 4.40 A set A is *trivial for* EXP (or EXP-*trivial* for short) if

$$\exists\, k \geq 1\ [\mathrm{P}_m(A) \cap \mathrm{EXP} \subseteq \mathrm{EXP}_k] \tag{4.16}$$

holds, and A is *nontrivial for* EXP (or EXP-*nontrivial* for short) otherwise.

Obviously, EXP-triviality is closed downwards under $\leq^p_m$ and EXP- nontriviality is closed upwards under $\leq^p_m$. Moreover, the analog of Lemma 4.3 with EXP in place of E can be easily established (by straightforward modifications of the proof of Lemma 4.3).

Lemma 4.41 *For any set A the following hold.*

$$\begin{array}{c} A\ \mathrm{EXP}\text{-}\textit{hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{measure hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{category hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \textit{intractable} \end{array} \tag{4.17}$$

Since, in contrast to E, EXP is closed downwards under $\leq^p_m$, for a set $A \in \mathrm{EXP}$, $\mathrm{P}_m(A) \subseteq \mathrm{EXP}$. So, for $A \in \mathrm{EXP}$, (4.16) is equivalent to

$$\exists\, k \geq 1\ [\mathrm{P}_m(A) \subseteq \mathrm{EXP}_k]. \tag{4.18}$$

Lemma 4.42 *For $A \in \mathrm{EXP}$, A is* EXP-*trivial if and only if* (4.18) *holds.*

Note that the assumption that $A \in \mathrm{EXP}$ in Lemma 4.42 is necessary. For any set $A \not\in \mathrm{EXP}$, (4.18) fails since $A \in \mathrm{P}_m(A)$. On the other hand, there are EXP-trivial sets outside of EXP (see below).

Just as any E-nontrivial set has predecessors at all levels of the E-hierarchy (Theorem 4.4), any EXP-nontrivial set has predecessors at all levels of the EXP-hierarchy.

Theorem 4.43 *The following are equivalent.*

1. *A is* EXP-*nontrivial.*

2. *For any $k \geq 1$ there is a set $B \in \mathrm{EXP}_{k+1} \setminus \mathrm{EXP}_k$ such that $B \leq^p_m A$.*

The nontrivial implication in Theorem 4.43 is immediate by the following variant of the padding lemma which is obtained from the Second Padding Lemma (Lemma 4.5) by replacing E and E_k by EXP and EXP_k, respectively.

Lemma 4.44 (Third Padding Lemma) *Let A and $k \geq 1$ be given such that $A \in \mathrm{EXP}_{k+1} \setminus \mathrm{EXP}_k$. Then, for any $k' \leq k$ (with $k' \geq 1$), there is a set $A' \in \mathrm{EXP}_{k'+1} \setminus \mathrm{EXP}_{k'}$ such that $A' =^p_m A$ (in fact, $A \leq^p_{1\text{-}li} A' \leq^p_m A$).*

PROOF. Since the proof follows the same lines as the proof of the Second Padding Lemma, we only sketch the proof.

Given $k \geq 2$ and $A \in \mathrm{EXP}_{k+1} \setminus \mathrm{EXP}_k$, it suffices to give a set A' such that $A \leq^p_{1\text{-}li} A' \leq^p_m A$ and $A' \in \mathrm{EXP}_k \setminus \mathrm{EXP}_{k-1}$. Then the claim follows by induction.

Let

$$A' = \{0^{f(|x|)}1x : x \in A\} \quad \text{where} \quad f(n) = \lfloor n^{\frac{k+1}{k}} - n \rfloor.$$

Then, clearly, $A' \leq^p_{1-li} A \leq^p_m A'$. Moreover, $A' \in \mathrm{EXP}_k$ and $A' \notin \mathrm{EXP}_{k-1}$ easily follow from the fact that (up to some additive constant), for $y = 0^{f(|x|)}1x$,

$$|x|^{(k+1)} = (|x|^{\frac{k+1}{k}})^k \leq (|x|^{\frac{k+1}{k}} + 1)^k = |y|^k$$

and

$$|y|^{(k-1)} = (|x|^{\frac{k+1}{k}} + 1)^{(k-1)} \leq (|x|^{\frac{k+1}{k}})^{(k-1)} = |x|^{\frac{k^2-1}{k}} \leq |x|^k,$$

respectively. □

We will discuss the relations between the nontriviality notions for E and EXP in Chapter 6 below. Here we only want to point out that the results on E-triviality and E-nontriviality easily carry over to corresponding results on EXP-triviality and EXP-nontriviality, repectively. For this sake we first observe that any strictly trivial set is not only E-trivial but also EXP-trivial.

Proposition 4.45 *Every strictly trivial set is* EXP*-trivial.*

PROOF. Immediate by definition. □

So, since all the existence results for E-trivial sets in E presented in Section 4.2 actually yielded strictly trivial sets, all the results from this section remain correct for EXP-triviality in place of E-triviality. Moreover, the proof of Theorem 4.17, showing that there are E-trivial sets at arbitrarily high levels of the E-hierarchy, can be easily modified to get the following corresponding result for the class EXP.

Theorem 4.46 *For any $k \geq 1$ there is an* EXP*-trivial set A in* $\mathrm{EXP} \setminus \mathrm{EXP}_k$.

Similarly, the proofs in Subsection 4.2.4 that, for $t(n) = 2^{kn}$ $(k \geq 2)$, the set R^t of the $t(n)$-time bounded Kolmogorov random strings is strictly trivial, hence E-trivial (and EXP-trivial) can be easily modified to show that, for $t(n) = 2^{n^k}$ $(k \geq 2)$, R^t is in EXP_{k+1}, R^t is not in P and R^t is EXP-trivial.

The proofs of the results on E-nontrivial sets in E in Section 4.3 also can be easily modified to yield corresponding results on EXP-nontrivial sets in EXP (and, by padding, in E). In particular, by straightforward modifications of the proofs of the corresponding facts for E-nontriviality one can show the following.

Theorem 4.47 *Let A be* EXP*-nontrivial and let (A_0, A_1) be a p-splitting of A. Then A_0 is* EXP*-nontrivial or A_1 is* EXP*-nontrivial (or both).*

Corollary 4.48 *For any set $B \in$* EXP *which is not polynomial-time computable there is an* EXP*-nontrivial set A such that $B \not\leq^p_m A$.*

Theorem 4.49 *Let $A \in$* EXP *be* E_1*-bi-immune and let D be an infinite tally set such that $D \in$* P*. Then $A \cap D$ is* EXP*-nontrivial. In particular, $A \cap \{0\}^*$ is* EXP*-nontrivial.*

Corollary 4.50 *For any infinite tally set $D \in$* P *there is an* EXP*-nontrivial set A in* E *such that $A \subseteq D$. In particular, there is a tally* EXP*-nontrivial set A in* E.

Theorem 4.51 *No tally set is* EXP*-category hard.*

Corollary 4.52 *There is an* EXP*-nontrivial set A in* E *which is not* EXP*-category complete, hence not* EXP*-measure complete.*

Corollary 4.53 *Let $A \in$* EXP *be* E_1*-bi-immune. Then A is* EXP*-nontrivial.*

Theorem 4.54 *Let $A \in \mathrm{EXP} \setminus \mathrm{E}_1$ be exptally. Then A is* EXP*-nontrivial.*

Corollary 4.55 *There is a p-m-minimal pair (A_0, A_1) of* EXP*-nontrivial sets $A_0, A_1 \in$* E.

CHAPTER 5

Intermediate Weak Completeness Notions

In this chapter we introduce another two weak hardness notions for the exponential time classes which are more strict than nontriviality but more general than category hardness.

The first concept, *strong nontriviality*, is a strengthening of nontriviality where infinitely-often complexity is replaced by almost-everywhere complexity. To be more precise, if a set A is nontrivial for E then, for any $k \geq 1$, there is a set $B_k \in \mathrm{E}$ which can be *p-m*-reduced to A such that $B_k \notin \mathrm{E}_k$, i.e., B_k is *infinitely-often* 2^{kn}-complex. Now, if we can choose B_k so that B_k is *almost-everywhere* 2^{kn}-complex, i.e., E_k-bi-immune, then we call A *strongly* nontrivial for E.

In the second new concept, *compressibility hardness*, the above requirement is further strengthened by requiring that the sets B_k are not only E_k-bi-immune but even *strongly* E_k-bi-immune, i.e., 2^{kn}-incompressible (see Definition 2.25).

More formally, the new weak hardness notions for E and EXP are defined as follows.

Definition 5.1 A set A is *strongly nontrivial for* E (or *strongly* E-*nontrivial* or E-*snt* for short) if

$$\forall\, k \geq 1\; \exists\, B\; (B \in \mathrm{P}_m(A) \cap \mathrm{E}\; \&\; B\; \mathrm{E}_k\text{-bi-immune}) \tag{5.1}$$

holds; and A is *weakly trivial for* E (or *weakly* E-*trivial* for short) otherwise.

Similarly, A is *strongly nontrivial for* EXP (or *strongly* EXP-*nontrivial* or EXP-*snt* for short) if

$$\forall\, k \geq 1\; \exists\, B\; (B \in \mathrm{P}_m(A) \cap \mathrm{EXP}\; \&\; B\; \mathrm{EXP}_k\text{-bi-immune}) \tag{5.2}$$

holds; and A is *weakly trivial for* EXP (or *weakly* EXP-*trivial* for short) otherwise.

Definition 5.2 A set A is *compression hard for* E (or E-*compression hard* for short) if

$$\forall\, k \geq 1\; \exists\, B\; (B \in \mathrm{P}_m(A) \cap \mathrm{E}\; \&\; B\; 2^{kn}\text{-incompressible}) \tag{5.3}$$

holds. A is *compression complete for* E (or E-*compression complete* for short) if $A \in \mathrm{E}$ and A is E-compression hard.

Similarly, A is *compression hard for* EXP (or EXP-*compression hard* for short) if

$$\forall\, k \geq 1\; \exists\, B\; (B \in \mathrm{P}_m(A) \cap \mathrm{EXP}\; \&\; B\; 2^{n^k}\text{-incompressible}) \tag{5.4}$$

holds. A is *compression complete for* EXP (or EXP-*compression complete* for short) if $A \in \mathrm{EXP}$ and A is EXP-compression hard.

Note that strong E-nontriviality and E-compression hardness are preserved upwards under $\leq^p_m$ (hence weak E-triviality is preserved downwards).

Before we study these new concepts individually and in more detail in the next two sections, we state the obvious relations among strong nontriviality and compression hardness and the previously introduced weak hardness notions.

Lemma 5.3 *For any set A the following hold.*

$$\begin{array}{c} A\ \mathrm{E}\text{-}\textit{hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{measure hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{category hard} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{compression hard} \\ \Downarrow \\ A\ \textit{strongly}\ \mathrm{E}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \mathrm{E}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \textit{intractable} \end{array} \tag{5.5}$$

PROOF. By Lemma 4.3, it suffices to prove the third, fourth and fifth implications (from top). These implications follow from the definitions of E-category hardness, E-compression hardness, strong E-nontriviality and E-nontriviality by observing that any n^{k+1}-generic set is 2^{kn}-incompressible (Theorem 3.65), any 2^{kn}-incompressible set is E_k-bi-immune (Lemma 2.26), and no E_k-bi-immune set is a member of E_k (Lemma 2.20). □

By some similar arguments, we obtain the corresponding relations for the weak hardness notions for the polynomial exponential-time class EXP.

Lemma 5.4 *For any set A the following hold.*

$$\begin{array}{c} A\ \mathrm{EXP}\text{-}\textit{hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{measure hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{category hard} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{compression hard} \\ \Downarrow \\ A\ \textit{strongly}\ \mathrm{EXP}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \mathrm{EXP}\text{-}\textit{nontrivial} \\ \Downarrow \\ A\ \textit{intractable} \end{array} \tag{5.6}$$

5.1 Strong Nontriviality

In the following we have a closer look at strong nontriviality for E. We give some alternative characterizations of strong nontriviality, analyse the density of strongly nontrivial sets, and give some results on the distribution of the strongly nontrivial sets among the exponential-time computable sets.

5.1.1 Alternative Characterizations of Strong E-Nontriviality

In Section 4.1 we have shown, that any E-nontrivial set has predecessors B_k (under $\leq^p_m$) from all levels $\mathrm{E}_{k+1} \setminus \mathrm{E}_k$ of the E-hierarchy ($k \geq 1$), i.e., sets which are infinitely-often 2^{kn}-complex but not infinitely-often $2^{(k+1)n}$-complex (see Theorem 4.4). Here we prove the corresponding result for strongly E-nontrivial sets with almost-everywhere complexity (i.e., bi-immunity) in place of infinitely-often complexity.

Theorem 5.5 *Let $A \in \mathrm{E}$. The following are equivalent.*

(i) A is strongly E*-nontrivial.*

(ii) For any $k \geq 1$ there is an E_k*-bi-immune set $B \in \mathrm{E}$ such that B is not* E_{k+1}*-bi-immune and such that $B \leq^p_m A$.*

Proof. For the proof of the nontrivial implication "$(i) \Rightarrow (ii)$" assume that A is strongly E-nontrivial.

Given $k \geq 1$, fix $k' > k$ minimal, such that

$$\exists B \in \mathrm{E}\ (B \leq^p_m A \text{ and } B \text{ is } \mathrm{E}_k\text{-bi-immune and } B \text{ is not } \mathrm{E}_{k'}\text{-bi-immune}). \tag{5.7}$$

Note that, by choice of A, k' must exist. So it suffices to show that $k' = k+1$.

For a contradiction assume that $k' > k+1$. Fix B as in (5.7) and g sucht that $B \leq^p_m A$ via g, and define B' by

$$B' = (B \setminus \{0^{f(|x|)}1x : x \in \Sigma^*\}) \cup \{0^{f(|x|)}1x : x \in B\},$$

where $f(n) = \lfloor \frac{k'-(k+1)}{k} n \rfloor$. Obviously $B' \in \mathrm{E}$ and $B' \leq^p_m A$ via

$$h(y) = \begin{cases} g(y) & \text{if } y \notin \{0^{f(|x|)}1x : x \in \Sigma^*\} \\ g(x) & \text{if } y = 0^{f(|x|)}1x. \end{cases}$$

So in order to get the desired contradiction, it suffices to show that

$$B' \text{ is } \mathrm{E}_k\text{-bi-immune} \tag{5.8}$$

and

$$B' \text{ is not } \mathrm{E}_{k+1}\text{-bi-immune} \tag{5.9}$$

contrary to minimality of k'.

For a proof of (5.8), for a contradiction assume that B' is not E_k-bi-immune. Then, by symmetry, w.l.o.g. there is an infinite subset C' of B' such that $C' \in \mathrm{E}_k$. Let

$$C_0 = \{x : 0^{f(|x|)}1x \in C'\} \text{ and } C_1 = \{x : x \in C' \text{ and } x \notin \{0^{f(|y|)}1y : y \in \Sigma^*\}\}.$$

Note that C_0 and C_1 are subsets of B, and by infinity of C', at least one of these sets is infinite. So it suffices to show that $C_0, C_1 \in \mathrm{E}_{k'-1}$ whence B is not $\mathrm{E}_{k'-1}$-bi-immune contrary to choice of B and minimality of k'.

To show that $C_1 \in \mathrm{E}_{k'-1}$, note that C_1 is the intersection of C' with the polynomial-time computable set $\{0^{f(|y|)}1y : y \in \Sigma^*\}$. So, by $C' \in \mathrm{E}_k$, $C_1 \in \mathrm{E}_k$ whence, by $k \leq k'-1$, $C_1 \in \mathrm{E}_{k'-1}$.

$C_0 \in \mathrm{E}_{k'-1}$ is shown as follows. Given x, in order to compute $C_0(x)$ we need to compute $C'(0^{f(|x|)}1x)$ and that can be done in

$$O(2^{k \cdot \frac{k'-1}{k}|x|}) \leq O(2^{(k'-1)|x|})$$

steps. This completes the proof of (5.8).

It remains to prove (5.9). Since B is not $\mathrm{E}_{k'}$-bi-immune, by symmetry w.l.o.g. there is an infinite set $C \subseteq B$ such that $C \in \mathrm{E}_{k'}$.

Let

$$C' = \{0^{f|x|}1x : x \in C\}.$$

Then C' is an infinite subset of B' and to compute $C'(y)$ we first in polynomial time check whether $y \in \{0^{f(|x|)}1x : x \in \Sigma^*\}$ and, if so, find the corresponding x. Then it suffices to compute $C(x)$, and since $|x| = \frac{k}{k'-1}|y|$ that can be done in

$$O(2^{k' \cdot \frac{k}{k'-1}|y|}) \leq O(2^{\frac{k'}{k'-1} \cdot k \cdot |y|}) \leq O(2^{(k+1)|y|})$$

steps. So $C' \in \mathrm{E}_{k+1}$ whence B' is not E_{k+1}-bi-immune. □

While we will not work with the above characterization of strong E- nontriviality, the following alternative characterization will be very useful for analysing the strong nontriviality concept. Recall that in Chapter 3 we have seen that the characterizations of the weak hardness notions for E from the literature in terms of polynomial randomness and polynomial genericity can be simplified, by observing that any n^2-random (n^2-generic) set in E has predecessors in E which are n^k-random (n^k-generic) for any $k \geq 1$ (see Theorems 3.40 and 3.77). Here, by establishing the corresponding expansion result for bi-immunity, we get a similar simplification of the definition of strong nontriviality.

Theorem 5.6 *Let A be E_1-bi-immune. Then, for any $k \geq 1$, there is an E_k-bi-immune set A_k and an EXP_k-bi-immune set A'_k such that $A_k, A'_k \in \mathrm{P}_m(A)$. If moreover $A \in \mathrm{E}$ then the set A_k can be chosen such that $A_k \in \mathrm{P}_m(A) \cap \mathrm{E}$.*

PROOF. The proof follows the proofs of the corresponding Theorems 3.36 and 3.76 for randomness and genericity, respectively.

Let $A_k = \{x : 0^{k|x|}1x \in A\}$ and $A'_k = \{x : 0^{|x|^k}1x \in A\}$. Then $A_k \leq^p_m A$ via $f(x) = 0^{k|x|}1x$ and $A'_k \leq^p_m A$ via $g(x) = 0^{|x|^k}1x$. Moreover, if $A \in \mathrm{E}$, say $A \in \mathrm{E}_m$ then $A_k \in \mathrm{E}_{(k+1)m}$, hence $A_k \in \mathrm{E}$ too.

It remains to show that A_k is E_k-bi-immune and A'_k is EXP_k-bi-immune. We will prove the former, the proof of the latter is similar.

For a contradiction assume that A_k is not E_k-bi-immune. By symmetry, we may assume that there is an infinite set $B' \subseteq A_k$ such that $B' \in \mathrm{E}_k$.

Now let $B = \{0^{k|x|}1x : x \in B'\}$. Then, by infinity of B', B is infinite, and, by $B' \subseteq A_k$ and by definition of A_k, $B \subseteq A$. Moreover $B \in \mathrm{E}_1$, since, for a string y we can decide whether $y \in B$ by first checking (in polynomial time) whether there is a string x such that $y = 0^{k|x|}1x$ and, if so, by checking in $O(2^{k|x|}) \leq O(2^{|y|})$ steps whether $x \in B'$. So A is not E_1-bi-immune contrary to assumption. □

Theorem 5.7 (Characterization Theorem for Strong Nontriviality) *A set A is strongly* $\mathrm{E(EXP)}$*-nontrivial if and only if there is an* E_1*-bi-immune set $B \in \mathrm{E(EXP)}$ such that $B \leq^p_m A$.*

PROOF. Immediate by Theorem 5.6. □

This characterization theorem immediately implies that strong nontriviality for E implies strong nontriviality for EXP.

Corollary 5.8 *Any strongly* E*-nontrivial set is strongly* EXP*-nontrivial.*

5.1.2 Density of Strongly E-Nontrivial Sets

We now turn to the question of how sparse a strongly E-nontrivial set can be. We first show that there are tally strongly E-nontrivial sets in E. This will follow from the existence of bi-immune length languages which we will establish next. A set A is a *length language* if, for any n, $\Sigma^n \subseteq A$ or $\Sigma^n \cap A = \emptyset$.

Lemma 5.9 *Let A in* E *be* E_{k+1}*-bi-immune ($k \geq 1$) . Then the length language $\hat{A} = \{x : 0^{|x|} \in A\}$ is* E_k*-bi-immune, and $\hat{A} \in \mathrm{E}$ and $\hat{A} \leq^p_m A$.*

PROOF. Obviously, $\hat{A} \in \mathrm{E}$ and $\hat{A} \leq^p_m A$. It remains to show that $\hat{A}$ is E_k-bi-immune. For a contradiction assume that $\hat{A}$ is not E_k-bi-immune. Then, w.l.o.g, there is an infinite set $B \in \mathrm{E}_k$ such that $B \subseteq \hat{A}$. Then, for $B' = \{0^{|x|} : x \in B\}$, B' is infinite (by infinity of B), $B \in \mathrm{E}_{k+1}$ (by $B \in \mathrm{E}_k$; namely, in order to check whether $0^n \in B'$ it suffices to check whether one of the 2^n strings of length n is in B), and $B' \subseteq A$ (by $B \subseteq \hat{A}$ and by definition of $\hat{A}$) whence A is not E_{k+1}-bi-immune contrary to assumption. □

By combining Lemma 5.9 with Theorem 5.6, we obtain the following existence result for bi-immune length languages in E.

Theorem 5.10 *Let $A \in \mathrm{E}$ be E_1-bi-immune. For any $k \geq 1$ there is an E_k-bi-immune length language $\hat{A} \in \mathrm{E}$ such that $\hat{A} \leq^p_m A$.*

So, in particular, for any $k \geq 1$ there is an E_k-bi-immune length language A_k in E.

Corollary 5.11 *There is a tally set $A \in \mathrm{E}$ which is strongly* E*-nontrivial.*

PROOF. By Theorem 5.10 there is a length language $A_1 \in \mathrm{E}$ which is E_1-bi-immune. Moreover, by Theorem 5.7, A_1 is strongly E-nontrivial. So (by closure of the class of strongly E-nontrivial sets under $=^p_m$) it suffices to give a tally set $A \in \mathrm{E}$ such that $A_1 =^p_m A$. Obviously, $A = A_1 \cap \{0\}^*$ has the desired properties. □

The above can be easily modified in order to prove the following strengthening of Corollary 5.11 which is partial analog of Theorem 4.30 for strong nontriviality.

Theorem 5.12 *Let $A \in \mathrm{E}$ be E_1-bi-immune. Then $A \cap \{0\}^*$ is strongly* E*-nontrivial.*

PROOF. For E_2-bi-immune $A \in \mathrm{E}$, as above we can argue that $\hat{A} = \{x : 0^{|x|} \in A\}$ is E_1-bi-immune and $\hat{A} =^p_m A \cap \{0\}^*$ whence $A \cap \{0\}^*$ is strongly E-nontrivial.

So given an E_1-bi-immune set $A \in \mathrm{E}$, it suffices to argue that there is an E_2-bi-immune set $A' \in \mathrm{E}$ such that $A' \cap \{0\}^* \leq^p_m A \cap \{0\}^*$. Let $A' = \{x : 0^{|x|}x \in A\}$. Then one can easily show (as in the proof of Theorem 5.6) that $A' \in \mathrm{E}$ and that A' is E_2-bi-immune. Finally, $A' \cap \{0\}^* \leq^p_m A \cap \{0\}^*$ since $0^n \in A'$ iff $0^{2n} \in A$. □

By the above, strongly E-nontrivial sets can be tally. In contrast to the E-nontrivial sets, however, no strongly E-nontrivial set in E is exptally. This follows from the following observation on exptally sets in E.

Lemma 5.13 *Let A and B be sets such that $A \in \mathrm{E}$, A is exptally, and $B \leq^p_m A$. Then B is not* P*-bi-immune (hence not E_1-bi-immune).*

PROOF. Fix a polynomial-time computable function f such that $B \leq^p_m A$ via f. In order to show that B is not P-bi-immune we will define an infinite set $D \in \mathrm{P}$ such that, for $x \in D$, $B(x)$ can be decided in polynomial time.

For the definition of D we first have to introduce some notation. Fix k such that $A \in \mathrm{E}_k$ and a polynomial p such that p is a time bound for f (where w.l.o.g. $p(n) \geq n$ for all n). Moreover, let $q(n)$ be the greatest number m such that

$$\delta(n) \leq m \leq p(m) < 2^{\delta(n)} = \delta(n+1) \tag{5.10}$$

and let $q(n) = 0$ if no such m exists. Note that a number m satisfying (5.10) exists for all sufficiently large n. Hence we may fix n_0 such that, for all $n \geq n_0$,

$$\delta(n) \leq q(n) \leq p(q(n)) < 2^{\delta(n)} = \delta(n+1) \leq p(q(n)+1) \tag{5.11}$$

holds. (Note that $\delta(n+1) \leq p(q(n)+1)$ follows from maximality of m.)

Now the set D is defined by

$$D = \{0^{q(n)} : n \geq 0\}.$$

By time-constructibility of q, D is polynomial time computable and, given $x \in D$, in polynomial time we can compute the unique number n such that $x = 0^{q(n)}$.

In order to decide whether such a string $x = 0^{q(n)}$ with $n \geq n_0$ is in B, first (in polynomial time) compute $f(x) = f(0^{q(n)})$. Next decide whether $f(x)$ is a string $0^{\delta(s)}$ for some s, and if so, fix the corresponding s. (Note that this can be done in polynomial time). Now, if $f(x)$ does not have this form, then $f(x)$ is not an element of the exptally set A, hence $B(x) = 0$. Otherwise, fix m such that $f(x) = 0^{\delta(m)}$. Since $|f(x)| < p(|x|) = p(q(n))$, it follows by (5.11) that $s \leq n$ and therefore

$$\delta(s) \leq \delta(n) \leq p(q(n)+1).$$

So, by $A \in \mathrm{E}_k$, $A(f(x))$ can be computed in time

$$2^{k|f(x)|} = 2^{k\delta(s)} = (2^{\delta(s)})^k \leq p(q(n)+1)^k = p(|x|+1)^k.$$

It follows that $B(x) = A(f(x))$ can be computetd in polynomial time (namely, the polynomial p' defined by $p'(n) = p(n+1)^k$ is a time bound). □

Theorem 5.14 *Let $A \in \mathrm{E}$ be exptally. Then A is not strongly* EXP*-nontrivial and not strongly* E*-nontrivial.*

PROOF. By Lemma 5.13, no set $B \leq^p_m A$ is E_1-bi-immune. So, by Theorem 5.7 , A is neither strongly EXP-nontrivial nor strongly E-nontrivial. □

Corollary 5.15 *There is a set $A \in \mathrm{E}$ which is* E*-nontrivial and* EXP*-nontrivial but not strongly* EXP*-nontrivial (hence not strongly* E*-nontrivial).*

PROOF. By Lemma 4.38 there is an exptally set $A \in \mathrm{E} \setminus \mathrm{E}_1$. By Theorems 4.37 and 4.54, A is E-nontrivial and EXP-nontrivial whereas, by Theorem 5.14, A is neither strongly EXP-nontrivial nor strongly E-nontrivial. □

The above observation that exptally sets in E are weakly E-trivial can be generalized as follows.

Theorem 5.16 *Let $A \in \mathrm{E}$ and assume that there is an infinite polynomial-time computable set $B \subseteq \{0\}^*$ such that, for any number n with $0^n \in B$,*

$$A \cap \{x : n \leq |x| < 2^n\} = \emptyset. \tag{5.12}$$

Then A is not strongly E*-nontrivial.*

We omit the proof which is based on a straigthforward generalization of Lemma 5.13. Theorem 5.16 implies that many constructions (of sets in E) in the theory of the polynomial-time degrees which are based on so-called gap languages (see e.g. Section 3 Ambos-Spies (1999)) yield sets which are weakly E-trivial.

5.2 Compression Completeness

Compression hardness narrows the gap between strong nontriviality and category hardness. Since the motivation for this weak hardness is not as trong as for the other weak hardness notions discussed here, we have only a short look at this concept. In particular, we provide some results which will separate compression hardness from strong nontriviality and category hardness. The key to these results is a characterization of compression hardness in terms of 2^n-incompressibility which is in the spirit of the previous characterization theorems for strong nontriviality, category hardness, and measure hardness (see Theorems 3.40, 3.77 and 5.7).

5.2.1 An Alternative Characterization of Compression Hardness

We first observe that - just as for randomness, genericity, and bi-immunity - there is an expansion theorem for incompressibility.

Theorem 5.17 *Let A be* E_1*-incompressible. Then for any $k \geq 1$ there is an* E_k*-incompressible set A_k and an* EXP_k*-incompressible set A'_k such that $A_k, A'_k \in P_m(A)$. If moreover $A \in \mathrm{E}$ then the set A_k can be chosen such that $A_k \in P_m(A) \cap \mathrm{E}$.*

PROOF. The proof follows the proofs of the corresponding Theorems 3.36, 3.76 and 5.6 for randomness, genericity and bi-immunity, respectively.

Let $A_k = \{x : 0^{k|x|}1x \in A\}$ and $A'_k = \{x : 0^{|x|^k}1x \in A\}$. Then, as observed before, $A_k \leq^p_m A$ and $A'_k \leq^p_m A$ and, for $A \in \mathrm{E}$, $A_k \in \mathrm{E}$.

So it suffices to show that A_k is E_k-incompressible and A'_k is EXP_k-incompressible. We show the former. (The proof of the latter is similar.)

For a contradiction assume that $A_k \leq_m C$ via $f \in \mathrm{E}_k$, where f is not almost one-to-one, i.e.,

$$\exists^\infty x, y \ (x \neq y \text{ and } f(x) = f(y))$$

In order to get the desired contradiction we define a function $g \in \mathrm{E}_1$ such that $A \leq_m A \oplus C$ via g and g is not almost one-to-one (So A is not E_2-incompressible contrary to assumption).

Define g by

$$g(x) = \begin{cases} 1f(x') & \text{if } x = 0^{k|x'|}1x' \text{ (some } x'\text{)} \\ 0x & \text{otherwise} \end{cases}$$

Then g is not almost one-to-one since f is not almost one-to-one, and, by $A_k \leq_m C$ via f, $A \leq_m A \oplus C$ via g. Namely, for $x = 0^{k|x'|}1x'$,

$$x \in A \Leftrightarrow x' \in A_k \Leftrightarrow f(x') \in C \Leftrightarrow 1f(x') \in A \oplus C \Leftrightarrow g(x) \in A \oplus C$$

It remains to show that $g \in \mathrm{E}_1$. Given x of length n, in $poly(n)$ steps we can decide whether or not $x = 0^{k|x'|}1x'$ and if so, find the corresponding x'. If x is not of this form, $g(x) = 0x$ can be computed in $O(n)$ steps. If $x = 0^{k|x'|}1x'$ then $g(x) = 1f(x')$ can be computed in $O(2^{k|x'|})$ steps (since $f \in \mathrm{E}_k$), hence, by $n \geq k \cdot |x'|$, in $O(2^n)$ steps. □

Theorem 5.18 (Characterization Theorem for Compression Hardness) *A set A is* E(EXP)*-compression hard if and only if there is an 2^n-incompressible (i.e.,* E_1*-incompressible) set $B \in$* E(EXP) *such that $B \leq_m^p A$.*

PROOF. Immediate by Theorem 5.17. □

An immediate consequence of the characterization theorem is the following relation between compression hardness for E and EXP.

Corollary 5.19 *Any* E*-compression hard set is* EXP*-compression hard.*

5.2.2 Density of Compression Hard Sets

In contrast to Corollary 5.11, by which there are tally strongly E-nontrivial sets in E, no E-compression hard set is tally.

Theorem 5.20 *Let A be* EXP- *or* EXP*-compression hard. Then A is not tally.*

PROOF. By Lemma 4.32, no 2^n-incompressible set can be *p*-*m*-reduced to any tally set. So the claim follows from Theorem 5.18. □

Corollary 5.21 *There is a set $A \in$* E *which is strongly* E*-nontrivial (hence strongly* EXP*-nontrivial) but not* EXP*-compression hard (hence not* E*-compression hard).*

PROOF. By Corollary 5.11 and Theorem 5.20. □

Compression hardness and category hardness can be separated by some density argument too, but here the proof is more involved. We will show that compression hard sets can be *almost* tally whereas no category hard set has this property.

Definition 5.22 A set A is *almost tally* if

$$\forall\, n \geq 0\; (|A \cap \Sigma^n| \leq 1) \tag{5.13}$$

Lemma 5.23 *There is an 2^n-incompressible set $A \in$* E *which is almost tally.*

PROOF. Let $\{f_e, e \geq 0\}$ be an enumeration of the functions in E_1 such that, for x with $|x| \geq e$, $f_e(x)$ can be computed in time $O(2^{2|x|})$. A set A with the desired properties is constructed in stages.

To make A 2^n-incompressible we need to satisfy the following requirements:

$$\mathfrak{R}_e : \exists^\infty x, y (x \neq y \text{ and } f_e(x) = f_e(y)) \Rightarrow \exists x, y (A(x) \neq A(y) \text{ and } f_e(x) = f_e(y))$$

Stage s of the construction, at which we define $A \cap \Sigma^s$, is as follows.

We say that $\mathfrak{R}_e$ requires attention, if

(i) $e \leq s$

(ii) $\mathfrak{R}_e$ has not been active at any stage $s' < s$

(iii) $\exists x, y(y < x$ and $|x| = s$ and $f_e(x) = f_e(y))$

Fix the highest priority requirement $\mathfrak{R}_m$ which requires attention at stage s (If no requirement requires attention, let $A(x) = 0$ for all $x \in \Sigma^s$ and end stage s). We say that $\mathfrak{R}_m$ is active at stage s. Fix x and y minimal as in (iii). If $|y| < s$ then let $A(x) = 1 - A(y)$ and let $A(x) = 1$ otherwise. In either case let $A(x') = 0$ for all $x' \in \Sigma^s \setminus \{x\}$.

This completes the construction.

Obviously, (5.13) holds. So the correctness of A follows from the following claims.

Claim 1. $A \in \mathrm{E}_5$

Proof. Given $s, A \upharpoonright 0^s, ACTIVE(s-1)$, where

$$ACTIVE(s-1) = \{n : \mathfrak{R}_n \text{ is active at a stage } \leq s-1\}$$

we can compute $A \cap \Sigma^s$ and $ACTIVE(s)$ as follows.

Given $e \leq s$, to check whether $\mathfrak{R}_e$ requires attention at stage s we do the following:

1. Check whether $e \in ACTIVE(s-1)$. If so, $\mathfrak{R}_e$ does not require attention. Otherwise,

2. in 2^{3s} steps compute $\{f_e(x) : |x| \leq s\}$ and check whether there are x and y such that $y < x, |x| = s$ and $f_e(x) = f_e(y)$. $\mathfrak{R}_e$ requires attention iff such x and y exist.

Since we have to do this for all $e \leq s$, in

$$s \cdot 2^{3s} \leq O(2^{4s})$$

steps we can find the least e such that $\mathfrak{R}_e$ requires attention at stage s (if any) and the corresponding numbers x and y. Since $ACTIVE(s) = ACTIVE(s-1) \cup \{e\}$ and $A(x) = 1 - A(y)$ if $|y| < s$, $A(x) = 1$ if $|y| = s$, and $A(x') = 0$ for all $x' \in \Sigma^s \setminus \{x\}$, this shows that $A \cap \Sigma^s$ and $ACTIVE(s)$ can be computed from $ACTIVE(s-1)$ and $A \upharpoonright 0^s$ in $O(2^{4s})$ steps.

So, by induction, $A \cap \Sigma^s$ and $ACTIVE(s)$ can be computed in time $s \cdot O(2^{4s}) \leq O(2^{5s})$.

Claim 2. Every requirement $\mathfrak{R}_e$ is active at most once.

Proof. This follows from the fact that if requirement $\mathfrak{R}_e$ is active then it will never require attention again and hence will never be active again.

Claim 3. Every requirement $\mathfrak{R}_e$ requires attention at most finitely often.

Proof. The proof is by induction on e. By inductive hypothesis, fix a stage s_0 such that no requirement $\mathfrak{R}_{e'}$ with $e' < e$ requires attention after stage s_0. Then at the first stage $s > s_0$ at which $\mathfrak{R}_e$ requires attention (if any) $\mathfrak{R}_e$ will become active, hence will not require attention after stage s. So $\mathfrak{R}_e$ will require attention after stage s_0 at most once.

Claim 4. Every requirement $\mathfrak{R}_e$ is met.

Proof. For a contradiction assume that requirement $\mathfrak{R}_e$ is not met. Then there are infinitely many x and y such that $f_e(x) = f_e(y)$ and requirement $\mathfrak{R}_e$ has never been active. But that means that requirement $\mathfrak{R}_e$ requires attention infinitely many times and that contradicts Claim 3.

This completes the proof of Lemma 5.23.

□

Theorem 5.24 *There is an almost tally* E*-compression complete set A.*

PROOF. This is immediate by Lemma 5.23 and Theorem 5.18. □

Lemma 5.25 *Let A and G be sets such that G is n^3-generic and $G \leq_m^p A$. Then*

$$\sup_{n\to\infty} |A \cap \Sigma^n| = \infty. \tag{5.14}$$

For the proof of Lemma 5.25 we need Lemma 3.67 which guarantees that the n^3-generic set G will meet any generalized k-bounded extension functions which are computable in time n^2 and dense along G (for any $k \geq 1$).

PROOF OF LEMMA 5.25. For a contradiction assume that there is some q such that

$$\forall n (|A \cap \Sigma^n| \leq q).$$

Fix g such that $G \leq_m^p A$ via g and fix a polynomial bound p for this function. Since G is n^3-generic, hence p-incompressible (see Theorem 3.65), there is some n_0 such that g is 1-to-1 on all strings of length $n \geq n_0$.

So if we fix $n_1 \geq n_0$ such that, for all $n \geq n_1$, $2^n \geq (q+1)p(n)$ holds then

$$\forall n \geq n_1\ \exists m\ \exists x_0 < x_1 < \ldots < x_q \in \Sigma^n\ (|g(x_i)| = m) \tag{5.15}$$

holds. Note that there is some $i \leq q$ such that $x_i \notin G$ since, by assumption, there are only q elements of length m in A. Moreover, given $n \geq n_1$, the least $x_0 < x_1 < \ldots < x_q$ satisfying (5.15) for some m can be found in $O(2^{2n})$ steps. Hence the $(q+1)$-bounded extension function f defined by

$$f(X \restriction 0^n) = (x_0, 1), \ldots, (x_q, 1)$$

for $n \geq n_1$ (and $f(X \restriction x) \uparrow$ otherwise) is an n^2-extension function.

It follows, by n^3-genericity of G and by Lemma 3.67, that G meets f at some 0^n. So $G(x_0) = \ldots = G(x_q) = 1$ contrary to our observation above. □

Theorem 5.26 *Let A be* EXP*-category hard. Then* (5.14) *holds. So, in particular, A is not almost tally.*

PROOF. This is immediate by Lemma 5.25 since, by definition, any EXP-category hard set has an n^3-generic predecessor (under $\leq_m^p$). □

Corollary 5.27 *There is a set $A \in$* E *which is* E*-compression hard (hence* EXP*-compression hard) but not* EXP*-category hard (hence not* E*-coategory hard).*

PROOF. By Theorems 5.24 and 5.26. □

5.3 The Hierarchy of Weak Completeness Notions

By combining results on the various weak hardness notions for the exponential time classes we obtain the following (strict) hierarchy theorems for E and EXP.

Theorem 5.28 *(a) (Hierarchy Theorem for* E*) For any set A,* (5.5) *holds. Moreover, all implications in* (5.5) *are strict, and, for any of the implications, there is a set A in* E *witnessing that the implication cannot be reversed.*

(b) (Hierarchy Theorem for EXP*) For any set A,* (5.6) *holds. Moreover, all implications in* (5.6) *are strict, and, for any of the implications, there is a set A in* E *witnessing that the implication cannot be reversed.*

(c) In fact, there are sets $A_1, A_2, A_3, A_4, A_5, A_6 \in$ E *such that*

(i) *A_1 is intractable but but A is neither* E*-nontrivial nor* EXP*-nontrivial,*

(ii) *A_2 is* E*-nontrivial and* EXP*-nontrivial but neither strongly* E*-nontrivial nor strongly* EXP*-nontrivial,*

(iii) *A_3 is strongly* E*-nontrivial and strongly* EXP*-nontrivial but neither* E*- compression hard nor* EXP*-compression hard,*

(iv) *A_4 is* E*-compression hard and* EXP*-compression hard but neither* E*-category hard nor* EXP*-category hard, and*

(v) *A_5 is* E*-category hard and* EXP*-category hard but neither* E*-measure hard nor* EXP*-measure hard.*

(vi) *A_6 is* E*-measure hard and* EXP*-measure hard but neither* E*-hard nor* EXP*-hard.*

PROOF. By Lemmas 5.3 and 5.4 it suffices to prove part (c).

Part (i) of (c) follows from the existence of intractable strictly trivial sets in E (see e.g. Theorem 4.17) together with the observation that strictly trivial sets are E-trivial and EXP-trivial (Propositions 4.7 and 4.45). Part (vi) follows from Corollary 3.84. The other parts follow from the differences in the possible densities of the weakly hard sets for the different concepts:

(ii) holds since, by Lemma 4.38, there is an exptally set $A \in \mathrm{E} \setminus \mathrm{E}_1$; and, by Theorems 4.37 and 4.54, all exptally sets in $\mathrm{E} \setminus \mathrm{E}_1$ are E-nontrivial and EXP-nontrivial; but, by Theorem 5.14, no exptally set in E is strongly E-nontrivial or strongly EXP-nontrivial.

(iii) holds since, by Corollary 5.11, there is a tally set $A \in \mathrm{E}$ which is strongly E-nontrivial hence, by Corollary 5.8, strongly EXP-nontrivial; but, by Theorem 5.20, no tally set is E-category hard or EXP-category hard.

(iv) holds since, by Theorem 5.24, there is an almost tally set $A \in \mathrm{E}$ which is E-compression hard hence, by Corollary 5.19, EXP-compression hard; but, by Theorem 5.26 and Corollary 3.79, no almost tally set is E-category hard or EXP-category hard.

(v) holds since, by Corollary 3.80, there is a sparse set $A \in \mathrm{E}$ which is E-category hard hence, by Corollary 3.79, EXP-category hard; but, by Theorem 3.44, no sparse set is E-measure hard or EXP-measure hard. □

In the next chapter we will compare weak hardness for E with weak hardness for EXP. Recall that in Theorem 3.83 we have already summarized all the relations among the weak hardness notions for E and EXP in the literature, whereas in Theorem 5.28 above, we have only looked at the old and new weak hardness for E and EXP separately.

CHAPTER 6

Comparing Weak Completeness for E and EXP

While hardness for E and EXP coincide, for the weak hardness notions in the literature - Lutz's measure hardness and Ambos-Spies's category hardness - weak hardness for E is (strictly) stronger than weak hardness for EXP. Moreover, witnesses for strictness can be found in E so that, for sets in E, weak completenes for E implies weak completeness for EXP but, in general, not vice versa (see Theorem 3.83 and Corollary 3.84).

Here we compare our new weak hardness notions for E and EXP. As we have shown already, for the two new intermediate notions - compression hardness and strong nontriviality - weak hardness for E implies weak hardness for EXP (see Corollary 5.19 and Corollary 5.8, respectively), and, as we will show here, again these implications are strict.

For the weakest weak hardness notion - nontriviality -, however, the situation is different. As we will show, here, as for the other weak hardness notions, nontriviality for EXP does not imply nontriviality for E, but the converse fails too, i.e., there are E-nontrivial sets in E which are not nontrivial for EXP. So nontriviality for E and EXP are incomparable.

6.1 An E-Trivial EXP-Measure Complete Set

In order to prove that, for our new concepts, the weak hardness notions for EXP in general do not imply the corresponding weak hardness notions for E, we prove a stronger result. We construct a set $A \in$ E which is measure complete for EXP (i.e., has the strongest weak hardness property for EXP) but E-trivial (i.e., fails to have the weakest weak hardness property for E).

Theorem 6.1 *There is an* EXP*-measure complete set in* E *which is* E*-trivial.*

This theorem is an easy consequence of the following lemma on the existence of E-trivial n^2-random sets in EXP.

Lemma 6.2 *There is a set A such that*

$$A \in DTIME(2^{n^2}) \tag{6.1}$$

$$A \text{ is } n^2\text{-random} \tag{6.2}$$

and

$$\forall B \in \mathrm{E}(B \leq^p_m A \Rightarrow B \in DTIME(2^n)) \tag{6.3}$$

Before we prove Lemma 6.2 we show how Theorem 6.1 is obtained from this lemma.

PROOF OF THEOREM 6.1. Fix A as in Lemma 6.2. By (6.1) and by the Padding Lemma (Theorem 2.11) we may fix $A' \in \mathrm{E}$ such that $A' =_m^p A$. It suffices to show that A' is EXP-measure complete and E-trivial. But the former follows from (6.2) by the characterization theorem for measure hardness (Theorem 3.40) and by $A' =_m^p A$. For the latter it suffices to note that, by $A' =_m^p A$ and by (6.3), $P_m(A') \cap \mathrm{E} \subseteq \mathrm{E}_1$. □

PROOF OF LEMMA 6.2. By a slow diagonalization we inductively construct a set A with the desired properties. I.e., at stage s of the construction we determine the value $A(z_s)$ of A on the sth string z_s and, at the same time, we satisfy the highest priority requirement $\mathfrak{R}_e$ (to be defined below) which has not yet been satisfied before and which can be satisfied by appropriately choosing the value of $A(z_s)$.

Before we give the formal construction, we first explain the two main goals of the construction, point out the conflicts between the strategies for achieving these goals, and explain how these conflicts are resolved.

In order to make A n^2-random (i.e., to satisfy (6.2)), we have to ensure that $\mu_{n^2}(\{A\}) \neq 0$, i.e., that no n^2-martingale succeeds on A. Since, by the Union Theorem for Time-Bounded Martingales (Theorem 3.9), there is a normed n^6-martingale d which succeeds on all n^2-measure-0 classes, it suffices to fix such a universal martingale d and to guarantee that d does not succeed on A. We will do this by ensuring

$$\forall s\, (d(A \upharpoonright z_s) \leq 1). \tag{6.4}$$

The second major goal, namely to make A E-trivial, i.e., to be more precise, to satisfy (6.3), is achieved by guaranteeing that any p-m-reduction f of a set $B \in \mathrm{E}$ to A sufficiently compresses B so that, by ensuring (6.1), we can argue that $B(x)$ will be computable in $O(2^{|x|})$ steps by using the identity $B(x) = A(f(x))$.

To achieve this, we have to destroy the p-m-reductions from sets in E to A which are not sufficiently compressing by diagonalization. In order to ensure that the time required for these diagonalizations is compatible with making A obey the time bound (6.1) we have to use a somewhat tricky strategy which is reminiscent of the diagonalization technique in the proof of Blum's speed-up theorem.

Let $\{f_e : e \geq 0\}$ be a computable enumeration of the class of the polynomial time computable functions such that, for uniformly given polynomial time bounds p_e for f_e $(e \geq 0)$, $p_e(|x|^2) \leq 2^{|x|}$ for all $|x| > e$, and let $\{E_e : e \geq 0\}$ be a computable enumeration of the class E such that, for x with $|x| > e$, $E_e(x)$ can be uniformly computed in time $2^{e \cdot |x|}$. Then (6.3) is split up into the finitary requirements

$$\mathfrak{R}_e : E_{e_0} \leq_m^p A \; via \; f_{e_1} \Rightarrow \forall^\infty x (|x| > 2^{-e} \cdot |f_{e_1}(x)|^2)$$

where $e \geq 0$ and $e = \langle e_0, e_1 \rangle$. In addition, we ensure

$$\forall \alpha > 0\, (A \in \mathrm{DTIME}(2^{\alpha \cdot n^2})) \tag{6.5}$$

where α is a real number. (This will a fortiori ensure that A meets the time bound (6.1).)

To show that the above will guarantee that A satisfies (6.3), fix a set $B \in \mathrm{E}$ such that $B \leq_m^p A$. It suffices to show that $B \in \mathrm{DTIME}(2^n)$. Fix e_0 and e_1 such that $B = E_{e_0}$ and $B \leq_m^p A$ via f_{e_1}, and let $e = \langle e_0, e_1 \rangle$. Then, by requirement $\mathfrak{R}_e$, we may fix n_0 such that, for $\alpha = 2^{-e}$,

$$\forall\, x\ (|x| \geq n_0 \Rightarrow |x| > \alpha \cdot |f_{e_1}(x)|^2). \tag{6.6}$$

Now, given a string x with $|x| \geq \max(e, n_0)$, $B(x)$ can be computed in time $O(2^n)$ (for $n = |x|$) as follows. Since $B(x) = A(f_{e_1}(x))$, it suffices to compute $y = f_{e_1}(x)$ and $A(y)$. The former can be done in $poly(n)$, hence in $O(2^n)$, steps. The latter can be done in 2^n steps as follows. By (6.6), $\alpha \cdot |y|^2 < n$. So, by (6.5), $A(y)$ can be computed in $2^{\alpha \cdot |y|^2} \leq 2^n$ steps.

Having isolated the properties of A to be guaranteed by the construction, namely to statisfy condition (6.4) and the requirements $\mathfrak{R}_e$ ($e \geq 0$) and at the same time ensure the time bounds given in (6.5), we next look at the strategies for satisfying (6.4) and the requirements $\mathfrak{R}_e$, respectively, and show how this strategies can be made to be compatible with each other.

The basic strategy for meeting the martingale equation (6.4) is quite simple. Note that, by the fairness property of martingales,

$$\frac{d((A \restriction z_s)0) + d((A \restriction z_s)1)}{2} = d(A \restriction z_s). \tag{6.7}$$

So, for any $s \geq 0$, there is an $i \leq 1$ such that

$$d((A \restriction z_s)i) \leq d(A \restriction z_s). \tag{6.8}$$

Since d is normed, i.e., $d(\lambda) = 1$, it follows that (6.4) can be trivially satisfied by letting

$$A(z_s) = i \text{ for some (say the least) } i \text{ such that } d((A \restriction z_s)i) \leq d(A \restriction z_s). \tag{6.9}$$

In the following we say that $A(z_s)$ is defined according to the *basic randomness strategy* if (6.9) holds.

The basic strategy for meeting a requirement $\mathfrak{R}_e$ ($e = \langle e_0, e_1 \rangle$) (in the following called the *basic $\mathfrak{R}_e$-strategy*) is as follows. Wait for a stage s such that there is a string x with $|x| \leq 2^{-e}|z_s|^2$ and $f_{e_1}(x) = z_s$. Then meet the requirement by letting

$$A(z_s) = 1 - E_{e_0}(x) \tag{6.10}$$

thereby ensuring that the hypothesis $E_{e_0} \leq_m^p A$ via f_{e_1} of $\mathfrak{R}_e$ fails.

Of course it may happen that defining $A(z_s)$ according to (6.10) is not compatible with the basic randomness strategy since

$$d((A \restriction z_s)(1 - E_{e_0}(x))) > d(A \restriction z_s).$$

So, how can we ensure that requirement $\mathfrak{R}_e$ will be eventually met? First note that we can relax the basic randomness strategy as follows. If $\mathfrak{R}_e$ wants to act at stage s and wants to define $A(z_s)$ according to (6.10), this does not do any harm to ensuring (6.4) as long as

$$d((A \upharpoonright z_s)(1 - E_{e_0}(x))) \leq 1. \tag{6.11}$$

So, since there will be infinitely many stages s such that $\mathfrak{R}_e$ can be met at stage s by letting the basic $\mathfrak{R}_e$-strategy act as described above (unless $\mathfrak{R}_e$ is trivially met and no action becomes necessary), it suffices to ensure that, for one of these stages, (6.11) will hold. But this can be achieved by the following observation. Whenever we cannot meet $\mathfrak{R}_e$ at a stage s since (6.11) fails then, by letting $d(A \upharpoonright z_{s+1}) = d(A \upharpoonright z_s)E_{e_0}(x)$, the value of d is strictly decreased (by the fairness property of martingales). So, assuming that no other requirement is interfering with the definition of d, eventually the value of $d(A \upharpoonright z_s)$ will be so small that (6.11) will hold. In order to make sure that the decreases in values of the martingale d on the initial segments of A occuring at stages at which requirement $\mathfrak{R}_e$ is blocked from acting are not compensated by increases of d caused by actions of some other requirements thereby blocking $\mathfrak{R}_e$ forever, we endow requirement $\mathfrak{R}_e$ with an account in which the amounts are accumulated by which d is dropping at stages at which requirement is eligible to act but blocked. Then it is safe to relax the basic randomness strategy by letting $\mathfrak{R}_e$ act at stage s according to (6.10) as long as

$$d((A \upharpoonright z_s)(1 - E_{e_0}(x))) \leq d(A \upharpoonright z_s) + b_e(s-1) \tag{6.12}$$

where $b_e(s-1)$ is the balance of the account of $\mathfrak{R}_e$ at the end of stage $s-1$. Moreover, as one can easily check, whenever $\mathfrak{R}_e$ is blocked (after the first time) the balance of $\mathfrak{R}_e$'s account is doubled. So, eventually, the balance of the account of $\mathfrak{R}_e$ will be high enough to allow $\mathfrak{R}_e$ to pay the prize for its action.

The above strategy for combining the construction of a random set with the satisfaction of finitary diagonalization requirements which can be met by fixing the constructed set on a single string is taken from Ambos-Spies and Kräling (2009).

We conclude our discussion of the basic strategies underlying the construction of A by explaining the reason why our strategy for meeting the requirements $\mathfrak{R}_e$ is compatible with satisfying (6.5). Here it is crucial to note that the bound for the search of a diagonalization witness is decreasing in e. So, since the requirements are finitary, we may speed-up the algorithm for computing A given by the actual construction as follows. Use a finite table summarizing the impact of the first e requirements on the construction and ignore these requirements in the construction otherwise. As we will show in the verification part of the proof following the formal construction, this sped-up versions of the construction will witness (6.5).

We now turn to the formal construction. Simultaneously with A we define the balances $b_e(s)$ of the accounts of the requirements $\mathfrak{R}_e$. Moreover, we will determine which requirements $\mathfrak{R}_e$ require attention (if any) and which of these requiremenets will be eligible to act and, possibly, become active or satisfied.

Stage 0. Let $A(z_0)$ be the least $i \leq 1$ such that $d(i) \leq 1$. For $e \geq 0$, let $b_e(0) = 0$. Moreover, no requirement $\mathfrak{R}_e$ requires attention at stage 0, no requirement is eligible to act, and no requirement becomes active or satisfied.

Stage $s > 0$. Let r_s be the least $i \leq 1$ such that (6.8) holds, and say that requirement $\mathfrak{R}_e$ *requires attention* at stage s if $e < |z_s|$, $\mathfrak{R}_e$ has not been satisfied at any previous stage, and the following holds:

$$\exists x(|x| \leq 2^{-e} \cdot |z_s|^2 \ \& \ f_{e_1}(x) = z_s). \tag{6.13}$$

Now, if no requirement requires attention then let $A(z_s) = r_s$ and $b_e(s) = b_e(s-1)$ for all $e \geq 0$. Otherwise, fix e minimal such that $\mathfrak{R}_e$ requires attention, declare that $\mathfrak{R}_e$ is *eligible to act* at stage s, fix e_0, e_1 such that $e = \langle e_0, e_1 \rangle$, fix the least number x as in (6.13), let

$$i = 1 - E_{e_0}(x), \tag{6.14}$$

let $b_{e'}(s) = b_{e'}(s-1)$ for $e' \neq e$, and distinguish the following cases.

If

$$d((A \upharpoonright z_s)i) > d(A \upharpoonright z_s) + b_e(s-1) \tag{6.15}$$

then say that $\mathfrak{R}_e$ is *blocked* at stage s, and let $A(z_s) = r_s$ and

$$b_e(s) = b_e(s-1) + (d(A \upharpoonright z_s) - d(A \upharpoonright z_{s+1})). \tag{6.16}$$

Otherwise, let $A(z_s) = i$ and $b_e(s) = 0$, and say that $\mathfrak{R}_e$ is *active* and *satisfied* at stage s.

This completes the construction.

In order to show that the thus defined set A has the required properties, we prove a series of claims.

Claim 1. For $s \geq 0$, $b_e(s) \geq 0$ (for all $e \geq 0$) and

$$d(A \upharpoonright z_{s+1}) + \sum_{e \geq 0} b_e(s) \leq 1. \tag{6.17}$$

Proof. The proof is by induction on s.

For $s = 0$, $b_e(0) = 0$ for all $e \geq 0$ and, by choice of $A(z_0)$, $d(A \upharpoonright z_{s+1}) = d(A(z_0)) \leq d(\lambda) = 1$.

For $s > 0$, distinguish the following cases.

If no requirement requires attention then $b_e(s) = b_e(s-1)$ for all $e \geq 0$ and $A(z_s)$ is chosen so that $d(A \upharpoonright z_{s+1}) \leq d(A \upharpoonright z_s)$. So the claims are immediate by inductive hypothesis.

If requirement $\mathfrak{R}_e$ is eligible to act at stage s but blocked, then, by construction, $d(A \upharpoonright z_{s+1}) < d(A \upharpoonright z_s)$ and (by (6.16))

$$d(A \upharpoonright z_{s+1}) + b_e(s) = d(A \upharpoonright z_s) + b_e(s-1)$$

while $b_{e'}(s) = b_{e'}(s-1)$ for $e' \neq e$. So, in particular, $b_e(s) > b_e(s-1)$ and

$$d(A \upharpoonright z_{s+1}) + \sum_{e \geq 0} b_e(s) = d(A \upharpoonright z_s) + \sum_{e \geq 0} b_e(s-1)$$

whence the claims follow by inductive hypothesis.

Finally, if requirement $\mathfrak{R}_e$ becomes active at stage s then, by construction,

$$d(A \upharpoonright z_{s+1}) \leq d(A \upharpoonright z_s) + b_e(s-1)$$

and $b_e(s) = 0$ while $b_{e'}(s) = b_{e'}(s-1)$ for $e' \neq e$. So, again, the claims are immediate by inductive hypothesis.

Claim 2. A satisfies (6.4).

Proof. This is immediate by Claim 1.

Claim 3. Every requirement $\mathfrak{R}_e$ requires attention at most finitely often.

Proof. For a contradiction, pick e minimal such that requirement $\mathfrak{R}_e$ requires attention infinitely many times. By minimality of e, we may fix s^* such that no requirements $\mathfrak{R}_{e'}$ with $e' < e$ will require attention after stage s^*. Then, whenever $\mathfrak{R}_e$ requires attention after stage s^*, $\mathfrak{R}_e$ will be eligible to act. On the other hand, $\mathfrak{R}_e$ will never become active since once a requirement became active it stops to require attention.

So there are infinitely many stages at which $\mathfrak{R}_e$ is eligible to act and $\mathfrak{R}_e$ becomes blocked at all of these stages. Let $s_0 < s_1 < s_2 < \dots$ be these stages. Now, by a straightforward induction on s, $0 \leq b_e(s) \leq b_e(s+1)$ (since $\mathfrak{R}_e$ is never active). Moreover, for any stage s_n ($n \geq 0$), $A(z_s) = 1 - i$ for some $i \leq 0$ satisfying (6.15) whence, by the fairness condition (6.7),

$$d(A \upharpoonright z_{s+1}) < d(A \upharpoonright z_s) - b_e(s-1).$$

So, by (6.16), $b_e(s_n) > 2 \cdot b_e(s_n - 1)$. It follows that

$$\lim_{s \to \infty} b_e(s) = \lim_{n \to \infty} b_e(s_n) = \infty.$$

Since d is a martingale, hence nonnegative, this contradicts (6.17) in Claim 1.

Claim 4. Every requirement $\mathfrak{R}_e$ is met.

Proof. For a contradiction assume that requirement $\mathfrak{R}_e$ is not met. Fix e_0, e_1 such that $e = \langle e_0, e_1 \rangle$. Then $E_{e_0} \leq_m^p A$ via f_{e_1} and

$$\exists^\infty x \, (|x| < 2^{-e} \cdot |f_{e_1}(x)|^2). \tag{6.18}$$

Moreover, $\mathfrak{R}_e$ is never satisfied. (Obviously, if $\mathfrak{R}_e$ becomes satisfied at a stage s then the hypothesis of $\mathfrak{R}_e$ fails whence $\mathfrak{R}_e$ is met.) So $\mathfrak{R}_e$ requires attention at any stage s such that $e < |z_s|$ and (6.13) holds. But, as one can easily show, by (6.18) there will be infinitely many such stages s. So, contrary to Claim 3, $\mathfrak{R}_e$ requires attention infinitely often.

It remains to analyse the complexity of A. Recall that d is an n^6-martingale whence, by Lemma 3.5, $d \in \mathrm{DTIME}(n^8)$. So, given $A \upharpoonright z_s$, $d(A \upharpoonright z_s)$ can be computed in $O(2^{8 \cdot |z_s|})$ steps.

Claim 5. Given $e, e_0, e_1, s \geq 0$ such that $e = \langle e_0, e_1 \rangle$ and $6 < e < |z_s|$, the following can be done in $O(2^{\frac{1}{e+1}|z_s|^2})$ steps: decide whether (6.13) *holds and, if so, compute the least witness x for* (6.13) *and decide whether $x \in E_{e_0}$.*

Proof. It suffices to look at all strings x with

$$|x| \leq 2^{-e} \cdot |z_s|^2, \tag{6.19}$$

and to compute $f_{e_1}(x)$ and $E_{e_0}(x)$ for each such x. Now, by (6.19) and by choice of $\{f_m : m \geq 0\}$, $f_{e_1}(x)$ can be computed in $O(2^{|z_s|})$ steps, while, by (6.19) and by choice of $\{E_m : m \geq 0\}$, $E_{e_0}(x)$ can be computed in

$$O(2^{e_0|x|}) \leq O(2^{e_0(2^{-e} \cdot |z_s|^2)})$$

steps.

Since there are $O(2^{2^{-e} \cdot |z_s|^2})$ strings x as in (6.13), the above procedure can be completed in

$$\begin{aligned} O(2^{2^{-e} \cdot |z_s|^2}) \cdot (O(2^{|z_s|}) + O(2^{e_0(2^{-e} \cdot |z_s|^2)})) &\leq O(2^{2^{-e} \cdot |z_s|^2} \cdot 2^{e_0(2^{-e} \cdot |z_s|^2)}) \\ &\leq O(2^{(e_0+1)2^{-e} \cdot |z_s|^2}) \\ &\leq O(2^{\frac{1}{e+1}|z_s|^2}) \end{aligned}$$

steps.

Claim 6. Let

$$SAT(s) = \{e' : \exists t \leq s \ (\mathfrak{R}_{e'} \textit{ is satisfied at stage } t)\}.$$

For any $k \geq 1$ there is a procedure which computes $A(z_s)$, $SAT(s)$ and $b_{e'}(s)$ for $k < e' \leq s$ in $O(2^{\frac{1}{k}|z_s|^2})$ steps.

Proof. Fix $k \geq 1$ and, by Claim 3, fix s_0 such that no requirement $\mathfrak{R}_{e'}$ with $e' \leq k$ is active after stage s_0. It suffices to give a procedure which, for $s > s_0$, computes $A(z_s)$, $SAT(s)$ and $b_{e'}(s)$ (for $k < e' \leq s$) from $A \upharpoonright z_s$, $SAT(s-1)$ and $b_{e'}(s-1)$ (for $k < e' \leq s-1$) in $O(2^{\frac{1}{k+1}|z_s|^2})$ steps (where $SAT(-1) = \emptyset$). (Then, given $s > s_0$, we can inductively compute

- $SAT(0) \subseteq SAT(1) \subseteq \ldots \subseteq SAT(s)$
- $A(z_0), \ldots, A(z_s)$
- $b_{e'}(0), \ldots, b_{e'}(s)$ for $k < e' \leq s$

  (Note that $b_s(0) = \ldots = b_s(s) = 0$.)

in a total of

$$O(s \cdot 2^{\frac{1}{k+1}|z_s|^2}) = O(2^{|z_s|} \cdot 2^{\frac{1}{k+1}|z_s|^2}) \leq O(2^{\frac{1}{k}|z_s|^2})$$

steps, where for $s \leq s_0$ we obtain the required parameters by looking up a finite table.)

Now, given $s > s_0$, $A \upharpoonright z_s$, $SAT(s-1)$ and $b_e(s-1)$ (for $k < e' \leq s-1$), we proceed as follows.

- Compute r_s.

  This can be done in $O(2^{8 \cdot |z_s|})$ *steps.*

- Decide whether there is a requirement $\mathfrak{R}_e$, $e < |z_s|$ which is eligible to act at stage s and, if so, compute e, the least x as in (6.13), and $i = 1 - E_{e_0}(x)$.

  To do so, for any $e < |z_s|$, such that $k < e$ and $e \notin SAT(s-1)$, it suffices to check whether (6.13) *holds and, if so, to compute the least witness x for* (6.13) *and to decide whether $x \in E_{e_0}$. By Claim 5 this can be done in* $O(s \cdot 2^{\frac{1}{k+2}|z_s|^2}) = O(2^{\frac{1}{k+2}|z_s|^2 + |z_s|})$ *steps.*

- If no requirement is eligible to act at stage s then $A(z_s) = r_s$, $SAT(s) = SAT(s-1)$ and $b_e(s) = b_e(s-1)$ for all $e \leq s$.

- If $\mathfrak{R}_e$ is eligible to act at stage s then check whether (6.15) holds. If so, $A(z_s) = r_s$, $SAT(s) = SAT(s-1)$ and $b_e(s)$ can be computed from (6.16); otherwise, $A(z_s) = i$, $SAT(s) = SAT(s-1) \cup \{e\}$, and $b_e(s) = 0$. In either case, $b_{e'}(s) = b_{e'}(s-1)$ for $e' \neq e$.

  This can be done in $O(2^{8 \cdot |z_s|})$ *steps.*

This completes the procedure. By the analysis of the time required for performing the individual steps, the procedure runs in time $O(2^{\frac{1}{k+1}|z_s|^2})$.

Claim 7. A satisfies (6.5).

Proof. This is immediate by Claim 6.

Note that, by Claims 2, 4 and 7, the constructed set A has the required properties. This completes the proof of Lemma 6.2. □

We end this subsection with observing some consequence of Lemma 6.2 on relation between E-nontriviality and E-bi-immunity.

In Section 4.3.2 we have shown that any E_1-bi-immune set $A \in \mathrm{E}$ is E-nontrivial (Corollary 4.35). Since any n^2-random set is E_1-bi-immune, Lemma 6.2 shows that the assumption that $A \in \mathrm{E}$ is necessary: By Lemma 6.2 there is an E_1-bi-immune set $A \in \mathrm{EXP}$ which is E-trivial. Similarly, the assumption that $A \in \mathrm{E}$ cannot be dropped in Theorems 4.30 and 4.37.

6.2 An EXP-Trivial E-Nontrivial Set

Theorem 6.3 *There is a set $A \in \mathrm{E}$ such that A is* E*-nontrivial and* EXP*-trivial.*

PROOF. We construct a set $A \in \mathrm{E}$ with the required properties. It suffices to ensure that A satisfies the following two conditions.

$$\forall\, k \geq 1\; (\{0^{k|x|-1}1x : x \in \Sigma^*\} \cap A \notin \mathrm{E}_1) \tag{6.20}$$

$$\forall\, f \in \mathrm{FP}\, \forall^\infty x\, (|f(x)| \geq |x|^2 \Rightarrow f(x) \notin A) \tag{6.21}$$

Note that (6.20) and (6.21) imply that A is E-nontrivial and A is not EXP-nontrivial, respectively. Namely, (6.20) implies that, for any number $k \geq 1$, the set $A_k = \{x : 0^{k|x|-1}1x \in A\}$ is not in E_{k+1}. On the other hand, since $A \in \mathrm{E}$ the set A_k is in E too. Since $A_k \leq^p_m A$ it follows that A is not E-trivial. To show that A is EXP-trivial, it suffices to show that $\mathrm{P}_m(A) \subseteq \mathrm{EXP}_3$. Given B such that $B \leq^p_m A$, fix $f \in \mathrm{FP}$ such that $B \leq^p_m A$ via f. Then $B(x) = A(f(x))$. So it suffices to show that $A(f(x))$ can be computed in $O(2^{|x|^3})$ steps for almost all strings x. For x such that $|f(x)| \geq |x|^2$ this is true by (6.21) since, for almost all such x, $A(f(x)) = 0$. For analysing the case of x with $|f(x)| < |x|^2$, by $A \in \mathrm{E}$, fix $k \geq 1$ such that $A \in \mathrm{E}_k$. Then $A(f(x))$ can be computed in at most $2^{k|f(x)|} < 2^{k|x|^2}$ steps and the latter is less than $2^{|x|^3}$ for almost all strings x.

For breaking (6.20) and (6.21) down into requirements, fix recursive enumerations $\{E^1_n : n \geq 0\}$ and $\{f_n : n \geq 0\}$ of E_1 and FP, respectively, such that, for x with $|x| \geq n$, $E^1_n(x)$ and $f_n(x)$ can be uniformly computed in $2^{3|x|}$ and $2^{|x|}$ steps, respectively. Then, in order to satisfy (6.20) and (6.21), it suffices to meet the requirements

$$\mathcal{P}_{\langle k,m\rangle} : \exists x\, (A(0^{k|x|-1}1x) \neq E^1_m(0^{k|x|-1}1x))$$

$$\mathcal{N}_e : \exists n\, \forall x\, (|x| \geq n\ \&\ |f_e(x)| \geq |x|^2 \Rightarrow f_e(x) \notin A)$$

for all numbers k, m, e.

Before we describe the construction of A we will inductively define a sequence of numbers l_s ($s \geq 0$) as follows. We let $l_0 = 0$ and, given l_s and k, m such that $s = \langle k,m\rangle$, we let l_{s+1} be the least number l such that $l_s < l$, $k+1$ devides l, and $s \cdot 2^{l+1} < 2^{\frac{l^2}{k+1}}$. As one can easily check, such numbers $l_0 < l_1 < l_2$ ... exist and, given a string x, in polynomial time we can decide whether $|x| = (l_s)^2$ and, if so, compute the corresponding number s.

Now the set A will consist only of strings of length $(l_s)^2$ for $s \geq 1$. At stage s we will determine which strings x of length $(l_{s+1})^2$ are put into A, i.e., define $A \cap \Sigma^{(l_{s+1})^2}$. This is done in such a way that requirement $\mathcal{P}_s$ will be met and that this definition will be consistent with all requirements $\mathcal{N}_e$ with $e < s$.

Now $A \cap \Sigma^{(l_{s+1})^2}$ is defined as follows. Fix k, m such that $s = \langle k,m\rangle$ and fix the least string y of length $(l_{s+1})^2$ such that y is of the form $y = 0^{k|x|-1}1x$ and such that, for all numbers $e < s$ and strings z with $|z| \leq l_{s+1}$, $f_e(z) \neq y$. Note that such a string y exists by choice of l_{s+1}. Namely, for y of the form $y = 0^{k|x|-1}1x$, $|y| = (k+1)|x|$. So, by $k+1$ deviding l_{s+1}, there are exactly $2^{\frac{(l_{s+1})^2}{k+1}}$ such strings of length $(l_{s+1})^2$. On the other hand, there are at most $s \cdot 2^{l_{s+1}+1}$ numbers $e < s$ and strings z with $|z| \leq l_{s+1}$ such that $|f_e(z)| = (l_{s+1})^2$. Since, by definition of l_{s+1}, $s \cdot 2^{l_{s+1}+1} < 2^{\frac{(l_{s+1})^2}{k+1}}$ the desired string y exists. Now, if for the least such string y, $E^1_m(y) = 0$ then let $A \cap \Sigma^{(l_{s+1})^2} = \{y\}$. Otherwise, let $A \cap \Sigma^{(l_{s+1})^2} = \emptyset$.

Obviously this ensures that requirement $\mathcal{P}_s$ is met. Moreover, by construction,

$$\forall x(|x| \geq (l_{e+1})^2 \ \& \ |f_e(x)| \geq |x|^2 \Rightarrow f_e(x) \notin A)$$

holds whence the requirements $\mathcal{N}_e$ are met too. It remains to show that $A \in \mathrm{E}$. But, by a straightforward analysis of the construction, $A \in \mathrm{E}_5$.

This completes the proof. □

6.3 Main Theorem on Comparing Weak Completeness for E and EXP

By combining the theorems in the preceding sections with some previous results we obtain our main theorem of this chapter which completely describes the relations among all of the weak hardness (and completeness) notions for E and EXP.

Theorem 6.4 *For any set A the following hold.*

$$\begin{tikzcd}
A\ \mathrm{E}\text{-}\textit{hard} \arrow[rr, leftrightarrow] \arrow[d] & & A\ \mathrm{EXP}\text{-}\textit{hard} \arrow[d] \\
A\ \mathrm{E}\text{-}\textit{measure hard} \arrow[rr] \arrow[d] & & A\ \mathrm{EXP}\text{-}\textit{measure hard} \arrow[d] \\
A\ \mathrm{E}\text{-}\textit{category hard} \arrow[rr] \arrow[d] & & A\ \mathrm{EXP}\text{-}\textit{category hard} \arrow[d] \\
A\ \mathrm{E}\text{-}\textit{compression hard} \arrow[rr] \arrow[d] & & A\ \mathrm{EXP}\text{-}\textit{compression hard} \arrow[d] \\
A\ \textit{strongly}\ \mathrm{E}\text{-}\textit{nontrivial} \arrow[rr] \arrow[d] & & A\ \textit{strongly}\ \mathrm{EXP}\text{-}\textit{nontrivial} \arrow[d] \\
A\ \mathrm{E}\text{-}\textit{nontrivial} \arrow[dr] & & A\ \mathrm{EXP}\text{-}\textit{nontrivial} \arrow[dl] \\
& A\ \textit{intractable} &
\end{tikzcd} \tag{6.22}$$

Moreover, (up to transitive closure) no other implications hold and sets witnessing the failure of the other relations can be found in E.

PROOF. We first establish the positive relations in (6.22). The downward arrows ($\downarrow$, $\searrow$, $\swarrow$) are justified by Theorem 5.28. The equivalence ($\leftrightarrow$) in line 1 and the implications from left to right ($\rightarrow$) in lines 2 - 5 are jusitified by Theorem 2.15, Theorem 3.45, Corollary 3.79, Corollary 5.19, and Corollary 5.8, respectively.

It remains to show that no other implications hold and that the failure is witnessed by sets in E. By part (c) of Theorem 5.28, no concept in line $n+1$ implies either of the concepts in line n ($n = 1, \ldots, 6$). So no upward arrows ($\uparrow$, $\nwarrow$, $\nearrow$) can be added. By Theorem 6.1, the only valid implication from the right column to the left column is the implication in line 1. So no arrows $\leftarrow$ or $\swarrow$ may be added. Finally, by Theorem 6.3, E-triviality does not imply EXP-triviality. So, up to transitive closure, only the implications in (6.22) are valid in general. Moreover, all of the counter examples given in the theorems referred to were in E.

This completes the proof of Theorem 6.4. □

CHAPTER 7

Nontrivial Sets Outside of E and EXP

Though we are mainly interested in E-nontriviality as a weak *completeness* notion, i.e., in E-nontrival sets *in* E, it is natural to also look at the corresponding weak *hardness* notion, i.e., at E-nontrivial sets *outside of* E. So in this section we give some results on E-trivial and E-nontrival sets which are not in E. We will focus on the question whether *typical* sets are E-trivial or E-nontrivial where we will look at typical sets in the sense of measure (random sets) and category (generic sets). The answer to this question will depend on whether we look at the universe of all (not necessarily computable) sets or whether we will consider computable sets only. We will show that, among all sets, the E-trivial sets are the typical ones, i.e., the E-nontrivial sets are rare. In the class of the computable sets, however, neither the E-trivial sets nor the E-nontrivial sets are rare though, as we will also show, the strongly E-nontrivial sets (hence the weakly E-hard sets in the sense of measure, category, and compression) are rare among the computable sets.

7.1 Are Typical Sets E-Nontrivial?

Are typical sets E-nontrivial? From a global point of view (i.e., if we consider any, not necessarily computable, sets) this question can be made more precise by asking:

- Does the class of all (not necessarily computable) E-nontrivial sets have measure 1 (*or* measure 0 *or* neither measure 1 nor measure 0)?

- Is the class of all (not necessarily computable) E-nontrivial sets comeager (*or* meager *or* neither comeager nor meager)?

If we consider only computable sets - or sets in some given complexity classes - then, in the above questions, we have to replace the classical measure and classical Baire category concepts by their computable - or resource bounded - counterparts.

So, if we consider only sets in E then we have to work with the measure and category concepts in E introduced in Chapter 3. In this setting, i.e., in the case of weak *completeness*, it has been shown that

- $\mu(\{A : A \text{ E-measure complete}\}|\mathrm{E}) = 1$ and

- $\{A : A \text{ E-category complete}\}$ is comeager in E

(see Theorem 3.41 and Corollary 3.78). Since E-measure complete sets and E-category complete sets are E-nontrivial, it follows that the class of E-nontrivial sets has measure 1 in E and is comeager in E. So, both in the sense of measure and in the sense of category, typical sets in E are E-nontrivial.

In the following we will consider the question how common are the E-nontrivial sets among all sets and among the computable sets. Since a typical computable set is not exponential-time computable and since a typical set is not computable, we cannot necessarily expect that the above result on typicalness of the E-nontrivial sets among the members of the exponential time class E carries over to the classes of all sets and all computable sets, respectively.

In fact, next we will show that among all sets the typical sets are E-trivial, not E-nontrivial.

7.2 Noncomputable E-Trivial and E-Nontrivial Sets

If we consider arbitrary sets, not only sets in E, i.e., if we move from weak completeness to weak hardness then the typical sets are not E-nontrivial but E-trivial. In order to show this we prove that computably random sets and computably generic sets are E-trivial. We first recall these notions.

Definition 7.1 A set A is *computably random* (or *rec-random*, for short) if A is $t(n)$-random for all computable functions t. And A is *computably generic* (or *rec-generic*, for short) if A is $t(n)$-generic for all computable functions t.

Proposition 7.2 *(i) Every rec-random set is rec-generic.*

(ii) The class of rec-random sets has measure 1.

(iii) The class of rec-generic sets is comeager and has measure 1.

PROOF. (i) is immediate by Theorem 3.63 and (ii) has been shown in Lemma 3.14 already. The first part of (iii) is immediate by Lemma 3.59 while the second part follows from (i) and (ii). □

Theorem 7.3 *Let A and B be sets such that A is rec-generic, B is computable and $B \leq_m^p A$. Then $B \in \mathrm{P}$.*

PROOF. For a contradiction assume that $B \notin \mathrm{P}$ and fix f such that $B \leq_m^p A$ via f. Then $f(B)$ is infinite. Moreover, since f and B are computable, $f(B)$ is computably enumerable whence $f(B)$ contains an infinite computable set D. Fix a computable function t such that $D \in \mathrm{DTIME}(t(n))$. Now, by $B \leq_m^p A$ via f, D is contained in A whence A is not $\mathrm{DTIME}(t(n))$-immune. It follows by Theorem 3.65 that A is not $t(n)$-generic. So A is not rec-generic contrary to choice of A. □

Corollary 7.4 *Any rec-generic set is* E*-trivial.*

PROOF. Let A be *rec*-generic. Since all sets in E are computable it follows from Theorem 7.3 that

$$\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{P} \subseteq \mathrm{E}_1$$

whence A is E-trivial. □

Corollary 7.5 *The class of* E*-nontrivial sets has measure 0 and is meager.*

PROOF. By Corollary 7.4 and by Proposition 7.2 (iii), the class of E-trivial sets has measure 1 and is comeager. □

Since E-nontriviality is the weakest hardness notion for E, Corollary 7.5 implies that the sets with the stronger weak hardness properties are rare in the sense of measure and Baire category too. (In some cases this has been shown in the literature before.)

Corollary 7.6 *The following classes have measure 0 and are meager:*

(i) The class of the E*-hard sets.*

(ii) The class of the E*-measure hard sets.*

(iii) The class of the E*-category hard sets.*

(iv) The class of the E*-compression hard sets.*

(iv) The class of the strongly E*-nontrivial sets.*

PROOF. By Lemma 5.3 and by Corollary 7.5. □

7.3 Computable Strongly E-Nontrivial Sets

We now come to the case of computable sets which turns out to be the most interesting one. We first consider the question of abundance for the weak hardness notions which are stronger than nontriviality. We show that, both in the sense of computable measure and in the sense of computable Baire category, a typical set is weakly E-trivial. So strongly E-nontrivial sets (hence weakly E-hard sets in the sense of measure, category, and compression) are rare among the computable sets.

By the characterization of computable measure and computable Baire category in terms of time bounded randomness and time bounded genericity, respectively, it suffices to prove the following theorem.

Theorem 7.7 *There is a computable function $t(n)$ such that any $t(n)$-generic set is weakly* E*-trivial.*

Before we turn to the proof of Theorem 7.7 we give the desired consequences.

Corollary 7.8 *The class of the weakly* E*-trivial sets is computably comeager and has computable measure 1.*

PROOF. The first part is immediate by Theorem 7.7 and Definition 3.68. For the second part, note that by Theorem 7.7 and Theorem 3.63 for some computable $t(n)$, any $t(n)$-random set is weakly E-trivial. So the claim follows from Lemma 3.20. □

Corollary 7.9 *The following classes have computable measure 0 and are computably meager (hence have measure 0 and are meager in the class of computable sets):*

(i) The class of the E*-hard sets.*

(ii) The class of the E*-measure hard sets.*

(iii) The class of the E*-category hard sets.*

(iv) The class of the E*-compression hard sets.*

(v) The class of the strongly E*-nontrivial sets.*

PROOF. Part (v) is immediate by Corollary 7.8. The other claims follow with Lemma 5.3. □

We now turn to the proof of Theorem 7.7. The core of the proof is the following Lemma.

Lemma 7.10 *Let*

$$h(n) = 2^{2^{2^{2^{2^n}}}}$$

and let A and B be sets, such that A is $\mathrm{DTIME}(h(n))$*-bi-immune, $B \in \mathrm{E}$ and $B \leq_m^p A$. Then B is not* E_2*-bi-immune.*

For the proof of Lemma 7.10 we need the following observation.

Proposition 7.11 *Let $f : \Sigma^* \to \Sigma^*$ be a function such that, for almost all strings x,*

$$2^{2^{2^{|f(x)|}}} < |x|. \tag{7.1}$$

Then, for any $k \geq 1$,

$$\exists^\infty x \, \exists y \, (f(x) = f(y) \,\&\, k \cdot |y| \leq |x|)$$

holds.

PROOF. Fix $k \geq 1$. Since, for almost all numbers m,

$$k^{2^m} \cdot m < 2^{2^{2^m}}, \tag{7.2}$$

by choice of f we may fix m_0 such that, for all numbers $m \geq m_0$, (7.2) holds and, for all strings x of length $\geq m_0$, (7.1) holds. It suffices to show that, for given $m \geq m_0$, there are strings x and y such that

$$|x| \geq m \;\&\; f(x) = f(y) \;\&\; k \cdot |y| \leq |x| \tag{7.3}$$

holds.

Define D by $D = \{0^{k^n \cdot m} : 0 \leq n \leq 2^m\}$. Then it is easy to see that, for any $x, y \in D$ such that $y < x$, $|x| \geq m$ and $k \cdot |y| < |x|$ holds. So, for establishing (7.3), it suffices to show that there are strings $y < x$ in D such that $f(x) = f(y)$. Since $|D| = 2^m + 1 > 2^m - 1 = |\Sigma^{<m}|$, the latter can be shown by demonstrating that, for any $x \in D$, $|f(x)| < m$.

So fix $x \in D$. By definition of D, $m \leq |x| \leq k^{2^m} m$. So, by $m \geq m_0$, (7.1) and (7.2) hold whence

$$2^{2^{2^{|f(x)|}}} < |x| \leq k^{2^m} m < 2^{2^{2^m}}.$$

Obviously this implies $|f(x)| < m$. □

PROOF OF LEMMA 7.10. Since $B \in \mathrm{E}$ and $B \leq^p_m A$ we may fix $k \geq 1$ such that $B \in \mathrm{E}_k$ and a polynomial time computable function f such that $B \leq^p_m A$ via f, i.e., such that $A(x) = B(f(x))$ for all strings x. We have to show that B is not E_2-bi-immune.

The outline of the argument is as follows. First, since A is DTIME($h(n)$)-bi-immune, we can argue that the reduction function f will dramatically compress the exponential time computable set B. This will imply that the reduction function f is not one-to-one and that there are infinitely many x such that, for some y with $k|y| < |x|$, $f(x) = f(y)$ whence $B(x) = B(y)$. By $B \in \mathrm{E}_k$, it follows that, for x and y as above, $B(x)$ can be computed in $O(2^{k|y|}) = O(2^{|x|})$ steps whence B will not be E_2-bi-immune.

Having given the idea of the proof, we now turn to the details. For notational convenience, let $\exp_k(n)$ be the the k-ply iterated exponential function, i.e., $\exp_0(n) = n$ and $\exp_{k+1}(n) = 2^{\exp_k(n)}$. So, in particular, $h(n) = \exp(5, n)$.

First we show that, for almost all x, (7.1) holds, i.e., $\exp(3, |f(x)|) < |x|$. For a contradiction assume that there are infinitely many strings x for which (7.1) fails. Then, for

$$C = \{y : \exists x\, [|x| < \exp(3, |y|) \;\&\; y = f(x)]\},$$

C is infinite and (since there are $\exp(4, |y|)$ strings x with $|x| < \exp(3, |y|)$ and since, for any such x, $f(x)$ can be computed in $poly(|x|) \leq poly(\exp(3, |y|)) \leq O(\exp(4, |y|))$ steps, $C \in \mathrm{DTIME}(\exp(4, n)) \subseteq \mathrm{DTIME}(h(n))$. So, in order to get the desired contradiction, it suffices to show that, for $y \in C$, $A(y)$ can be computed in $h(|y|)$ steps thereby contradicting the assumption that A is DTIME$(h(n))$-bi-immune.

So fix $y \in C$ and compute $A(y)$ as follows. By definition of C, in $O(\exp(4,|y|))$ steps find a string x of length $< \exp(3,|y|)$ such that $f(x) = y$. Then $A(y) = B(x)$ and, by $B \in \mathrm{E}_k$, the latter can be computed in $O(2^{k\cdot|x|}) \leq O(2^{k\cdot\exp(3,|y|)}) \leq O(\exp(5,|y|)) = O(h(|y|)$ steps.

Now, since (7.1) holds almost everywhere, by Proposition 7.11, the set

$$D = \{x : \exists y\ (f(x) = f(y)\ \&\ k\cdot|y| \leq |x|)\}$$

is infinite. Moreover, as one can easily check, $D \in \mathrm{E}_2$. So, in order to show that B is not E_2-bi-immune, it suffices to show that, for given $x \in D$, $B(x)$ can be computed in $O(2^{2|x|})$ steps. But this can be done as follows. Search for the least y such that $f(y) = f(x)$. Obviously, this can be done in $O(2^{2|x|})$ steps. Moreover, since $B \leq^p_m A$ via f, $B(x) = B(y)$ whence it suffices to compute $B(y)$. Finally, by definition of D, $k|y| \leq |x|$ whence, by $B \in \mathrm{E}_k$, $B(y)$ can be computed in $O(2^{k|y|}) \leq O(2^{|x|})$ steps.

This completes the proof of Lemma 7.10. □

PROOF OF THEOREM 7.7. Fix $h(n)$ as in Lemma 7.10, let $t(n) = h(n)$, and let A be any $t(n)$-generic set. Then, by Theorem 3.68, A is DTIME$(h(n))$-bi-immune. So, by Lemma 7.10, A does not have any predecessor (under $\leq^p_m$) in E which is E_2-bi-immune. By definition, this implies that A is weakly E-trivial. □

Though the above results show that a typical computable set (in the sense of computable measure or computable Baire category) is weakly E-trivial, they leave open the question whether a typical computable set is E-trivial or not. Before we answer this question we first give some examples of computable E-trivial sets outside of the exponential time classes E and EXP in the next section.

7.4 Some Examples of Computable E-Trivial Sets

By the following observation, we can get some existence results for computable E-trivial sets from some theorem on minimal pairs in the literature.

Proposition 7.12 *Let A and B be sets such that B is* E*-hard and (A,B) is a p-m-minimal pair. Then A is* E*-trivial.*

PROOF. Since B is E-hard,

$$\mathrm{E} \subseteq \mathrm{P}_m(B) \tag{7.4}$$

and, since (A,B) is a *p*-*m*-minimal pair,

$$\mathrm{P}_m(A) \cap \mathrm{P}_m(B) = \mathrm{P}. \tag{7.5}$$

So

$$\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{P}_m(A) \cap \mathrm{P}_m(B) = \mathrm{P} \subset \mathrm{E}_1.$$

□

Note that Theorem 7.3 can be rephrased as follows. If A is rec-generic and B is a computable set such that $B \notin \mathrm{P}$ then (A,B) is a *p*-*m*-minimal pair. So, in particular, any rec-generic set A and any E-complete set B form a *p*-*m*-minimal pair whence, by Proposition 7.12, any rec-generic set is E-trivial (as observed before; see Corollary 7.4 above). Since rec-generic sets are not computable, this does not give us any new insight in the distribution of the E-trivial sets among the computable sets. The following minimal pair theorem, however, gives some first examples of computable E-trivial sets $A \notin \mathrm{EXP}$ (hence of computable E-trivial sets which are not strictly trivial). In fact, it implies that there are computable E-trivial sets of arbitrarily high time complexity.

Theorem 7.13 *(Ambos-Spies (1987)) For any computable set $B \notin \mathrm{P}$ there is a computable set A such that (A,B) is a p-m-minimal pair. So, in particular, there is a minimal pair (A,B) where B is* E*-complete and A is computable.*

Corollary 7.14 *There is a computable set $A \notin \mathrm{EXP}$ such that A is* E*-trivial.*

PROOF. By Theorem 7.13 let (A,B) be a minimal pair such that B is E-complete and A is computable. Then, since any E-complete set is EXP-complete and since $A \not\leq^p_m B$, $A \notin \mathrm{EXP}$. Finally, by Proposition 7.12, A is E-trivial. □

Corollary 7.15 *Let t be any computable function. There is a computable set $A \notin \mathrm{DTIME}(t(n))$ such that A is* E*-trivial.*

PROOF. Fix computable sets B_0 and B_1 such that B_0 is *p*-*m*-hard for $\mathrm{DTIME}(t(n))$ and B_1 is E-complete, and apply Theorem 7.13 to the computable set $B = B_0 \oplus B_1$.

□

7.5 Computable E-Trivial Sets Are Not Rare

By a refinement of Ambos-Spies's minimal pair theorem stated in the preceding section (Theorem 7.13) we will now show that the class of the computable E-trivial sets does not have computable measure 0, hence is not computably meager.

So intuitively, in the sense of computable measure and computable Baire category, the E-trivial sets are not rare among the computable sets.

Theorem 7.16 *Let $B \notin \mathrm{P}$ be computable and let $t : \mathbb{N} \to \mathbb{N}$ be a computable function. There is a computable set A such that*

$$A \text{ is } t(n)\text{-random} \tag{7.6}$$

and A and B are a p-m-minimal pair, i.e.,

$$\forall C(C \leq_m^p A, B \Rightarrow C \in \mathrm{P}). \tag{7.7}$$

Before we give the proof, we state the corollaries we are interested in.

Corollary 7.17 *For any computable function $t(n)$ there is a computable $t(n)$- random set which is* E*-trivial.*

PROOF. By Proposition 7.12, it suffices to apply Theorem 7.16 to an E-complete set B. □

Corollary 7.18 *The class of the computable* E*-trivial sets does not have computable measure 0 hence does not have measure 0 in* REC.

PROOF. This is immediate by Lemma 3.20 and Corollary 7.17. □

Corollary 7.19 *The class of the computable* E*-trivial sets is not computably meager hence is not meager in* REC.

PROOF. This is immediate by Definition 3.68, by (3.20) and by Corollary 7.18. □

PROOF OF THEOREM 7.16. The proof combines the iterated look-ahead technique introduced in Ambos-Spies (1987) for extending a given intractable computable set B to a minimal pair of computable sets A and B with the technique for constructing random sets described in the proof of Lemma 6.2.

We construct a computable set A with desired properties by a slow diagonalization where at stage s of the construction we determine the value $A(z_s)$ of A on the sth string z_s.

In order to make A $t(n)$-random, by Theorem 3.9, fix a computable normed martingale d which succeeds on all $t(n)$-measure-0 classes. Then it suffices to guarantee that

$$\forall s\ (d(A \upharpoonright z_s) \leq 1) \tag{7.8}$$

thereby ensuring that d does not succeed on A.

In order to satisfy (7.7) we guarantee that A meets the requirements

$$\mathfrak{R}_e : \forall x(A(f_{e_0}(x)) = B(f_{e_1}(x))) \Rightarrow \{x : f_{e_0}(x) \in A\} \in \mathrm{P} \tag{7.9}$$

(for $e \geq 0$, $e = \langle e_0, e_1 \rangle$) where $\{f_e : e \geq 0\}$ is a computable enumeration of the polynomial time computable functions. To show that this suffices to ensure (7.7), given $C \leq^p_m A, B$, fix $e = \langle e_0, e_1 \rangle$ such that $C \leq^p_m A$ via f_{e_0} and $C \leq^p_m B$ via f_{e_1}. Then $C(x) = A(f_{e_0}(x)) = B(f_{e_1}(x))$ for all x, whence requirement $\mathfrak{R}_e$ ensures that $C = \{x : f_{e_0}(x) \in A\} \in \mathrm{P}$.

Requirement $\mathfrak{R}_e$ will be met by diagonalization. There will be at most one stage s_e at which $\mathfrak{R}_e$ acts and if $\mathfrak{R}_e$ acts it will choose the value i of $A(z_s)$ in such a way that the hypothesis of the requirement $\mathfrak{R}_e$ will fail. For the success of the strategy it will be crucial to assign appropriate bounds to the individual requirements which will serve as bounds for the search for diagonalization candidates. So, simultaneously with A, we define infinitely many time bounds t_e, $e \geq 0$, for A. Roughly speaking, time bound $t_e(z_s)$ for computing $A(z_s)$ is based on the assumption that the first $e+1$ requirements $\mathfrak{R}_0, ..., \mathfrak{R}_e$ will not require attention at stage s. Time bound t_{e+1} will then be used by the strategy for meeting requirement $\mathfrak{R}_e$ as bound for the search for a diagonalization witness. Namely, given a stage $s \geq e$, by which $\mathfrak{R}_e$ is not yet satisfied, we check whether there is some string x such that

$$|x| \leq t_{e+1}(z_s) \;\&\; f_{e_0}(x) = z_s.$$

If so, then in order to meet $\mathfrak{R}_e$, it suffices to fix the least such x and let $A(z_s) = 1 - B(f_{e_1}(x))$ thereby ensuring that $A(f_{e_0}(x)) \neq B(f_{e_1}(x))$.

The success of this strategy is based on the following observation.

Claim 1. Let $e = \langle e_0, e_1 \rangle$, let $t_{e+1} : \Sigma^* \to \mathbb{N}$ be a computable function such that $A(z_s)$ can be computed in $t_{e+1}(z_s)$ steps for almost all $s \geq 0$, and assume that, for almost all s,

$$\nexists x(|x| \leq t_{e+1}(z_s) \;\&\; f_{e_0}(x) = z_s). \tag{7.10}$$

Then $\mathfrak{R}_e$ is met.

Proof. Let $C = \{x : f_{e_0}(x) \in A\}$ and fix s_0 such that, for $s \geq s_0$, $A(z_s)$ can be computed in $t_{e+1}(z_s)$ steps and (7.10) holds. Then $C \in \mathrm{P}$ by the following procedure.

Given x, compute s such that $f_{e_0}(x) = z_s$ ($poly(|x|)$ steps, by $f_{e_0} \in \mathrm{P}$). Then $C(x) = A(z_s)$ whence it suffices to compute $A(z_s)$. If $s < s_0$, use a finite table in order to compute $A(z_s)$. If $s \geq s_0$, compute $A(z_s)$ in $t_{e+1}(z_s)$ steps by the given algorithm for A. By (7.10), $|x| > t_{e+1}(z_s)$ whence the latter can be done in $O(|x|)$ steps.

This completes the proof of Claim 1.

As in the proof of Lemma 6.2 the potential action of a diagonalization requirement $\mathfrak{R}_e$ might be blocked if the intended action does not go along with (7.8). In order to make sure that this does not happen forever, each requirement $\mathfrak{R}_e$ is supplied with an account in which the decreases of d at stages s at which $\mathfrak{R}_e$ becomes blocked are accumulated, and $\mathfrak{R}_e$ is allowed to act if the increase of d caused by this action is bounded by the current balance of the account of $\mathfrak{R}_e$. As in the proof of Lemma 6.2, the balance of the account of $\mathfrak{R}_e$ at the end of stage s is denoted by $b_e(s)$.

Having explained the ideas underlying the proof we now turn to the formal construction. Simultaneously with A we define the balances $b_e(s)$ of the accounts of the requirements $\mathfrak{R}_e$, finite variants A_e of A, corresponding time bounds t_e, and the actual time bound t of A corresponding to the construction ($e \geq 0$). At stage s of the construction we specify $A(z_s)$, $A_e(z_s)$, $t_e(z_s)$, $t(z_s)$, and $b_e(s)$. Moreover, we will determine which requirements $\mathfrak{R}_e$ require attention (if any) and which of these requirements will be eligible to act and, possibly, may become active and satisfied. In order to ensure that stage s is finite, we let $A_e(z_s) = A_{s+1}(z_s)$, $t_e(z_s) = t_{s+1}(z_s)$, and $b_e(s) = b_{s+1}(s)$ for all $e > s$, and we let only requirements $\mathfrak{R}_e$ with $e < s$ require attention.

<u>Stage 0.</u> Let $A(z_0) = i$ for the least $i \leq 1$ such that $d(i) \leq 1$ and let $A_e(z_0) = t_e(z_0) = b_e(0) = 0$ for all $e \geq 0$. Moreover, no requirement $\mathfrak{R}_e$ requires attention at stage 0, no requirement is eligible to act, and no requirement becomes active or satisfied. Finally, let $t(z_0)$ be the number of steps taken by the construction up to this point.

<u>Stage $s > 0$.</u> The stage consists of $s+2$ substages $s, \dots, -1$ which are performed in decreasing order.

<u>Substage s.</u> For $e > s$ let $A_e(z_s) = 0$ and $t_e(z_s) = t(z_{s-1})$. Let

$$r_s = \mu\, i \leq 1\ [d((A \upharpoonright z_s)i) \leq d(A \upharpoonright z_s)], \tag{7.11}$$

set $A_s(z_s) = r_s$, and let $t_s(z_s)$ be equal to the number of steps taken by the construction up to this point.

<u>Substage e $(0 \leq e < s)$.</u> If requirement $\mathfrak{R}_e$ is not satisfied at any stage s', $s' < s$, then check whether

$$\exists x\ (|x| \leq t_{e+1}(z_s)\ \&\ f_{e_0}(x) = z_s) \tag{7.12}$$

holds. If (7.12) does not hold or if requirement $\mathfrak{R}_e$ is already satisfied at some stage s', $s' < s$, then let $A_e(z_s) = A_{e+1}(z_s)$ and let $t_e(z_s)$ be equal to the number of steps taken by the construction up to this point.

Otherwise, let $x_{e,s}$ be the least string x as in (7.12), and do the following. Say that requirement $\mathfrak{R}_e$ *requires attention* at stage s. Compute

$$i = 1 - B(f_{e_1}(x_{e,s})) \tag{7.13}$$

and say that $\mathfrak{R}_e$ is *blocked* at stage s if

$$d((A \upharpoonright z_s)i) > d(A \upharpoonright z_s) + b_e(s-1) \tag{7.14}$$

holds. If $\mathfrak{R}_e$ is not blocked then let $A_e(z_s) = i$, and let $A_e(z_s) = A_{e+1}(z_s)$ otherwise. In either case let $t_e(z_s)$ be equal to the number of steps taken by the construction up to this point.

Substage -1. If no requirement requires attention at stage s then let $A(z_s) = r_s$, let $b_e(s) = b_e(s-1)$ for $e \geq 0$, and let $t(z_s)$ be equal to the number of steps taken by the construction up to this point.

Otherwise, let e_s be the least e such that requirement $\mathfrak{R}_e$ requires attention. Say that $\mathfrak{R}_{e_s}$ is *eligible to act* at stage s. Moreover, if $\mathfrak{R}_{e_s}$ is not blocked, let $A(z_s) = A_{e_s}(z_s)$ and $b_{e_s}(s) = 0$ and say that $\mathfrak{R}_{e_s}$ is *active* and *satisfied* at stage s. If $\mathfrak{R}_{e_s}$ is blocked, let $A(z_s) = r_s$ and

$$b_{e_s}(s) = b_{e_s}(s-1) + (d(A \upharpoonright z_s) - d(A \upharpoonright z_{s+1})). \tag{7.15}$$

In either case let $b_e(s) = b_e(s-1)$ for $e \geq 0$ such that $e \neq e_s$, and let $t(z_s)$ be equal to the number of steps taken by the construction up to this point.

This completes the construction.

Note that, for given s and all $e > s$, all parameters are trivial, i.e., $b_e(s) = 0$, $A_e(z_s) = 0$ and $t_e(z_s) = t(z_{s-1})$. So at any stage we have to compute only finitely many parameters and any stage will eventually be completed.

In order to show that A has the required properties, we prove a sequence of claims.

Claim 2. A is computable.

Proof. Since, as pointed out above, all stages are completed, this is immediate by effectivity of the construction.

Claim 3. For $s \geq 0$, $b_e(s) \geq 0$ (for all $e \geq 0$) and

$$d(A \upharpoonright z_{s+1}) + \sum_{e \geq 0} b_e(s) \leq 1. \tag{7.16}$$

Proof. This is shown as the corresponding claim in the proof of Lemma 6.2.

Claim 4. Condition (7.8) *is satisfied.*

Proof. This is immediate by Claim 3.

Claim 5. Every requirement requires attention at most finitely often.

Proof. This is shown as the corresponding claim in the proof of Lemma 6.2. (Note that any requirement will be active at most once.)

Claim 6. Let $e \geq 0$. For almost all $s \geq 0$, $A(z_s)$ can be computed in $t_e(z_s)$ steps.

Proof. By construction, $A_e(z_s)$ can be computed in $t_e(z_s)$ steps. Moreover, for any stage s at which no requirement $\mathfrak{R}_{e'}$ with $e' < e$ requires attention, $A(z_s) = A_e(z_s)$. So, by Claim 5, A and A_e differ only on finitely many strings. Obviously, this implies the claim.

Claim 8. Every requirement $\mathfrak{R}_e$ is met. (Hence (7.7) *holds.)*

Proof. Note that if $\mathfrak{R}_e$ is satisfied at some stage then $\mathfrak{R}_e$ is met. So, w.l.o.g., we may assume that $\mathfrak{R}_e$ is never satisfied. By Claim 5 fix $s_0 > e$ such that $\mathfrak{R}_e$ does not require attention after stage s_0. Then (7.10) holds for all $s \geq s_0$. Since, by Claim 6, $A(z_s)$ can be computed in $t_{e+1}(z_s)$ steps for almost all $s \geq 0$, it follows by Claim 1 that $\mathfrak{R}_e$ is met.

This completes the proof of Theorem 7.16. □

7.6 Computable E-Nontrivial Sets Are Not Rare

Here we will complement the result of the previous section by showing that the class of the computable E-nontrivial sets does not have computable measure 0 (hence is not computably meager) too. So intuitively, in the sense of computable measure and computable Baire category, not only the E-trivial sets are not rare among the computable sets but also the E-nontrivial sets are not rare. So, a typical computable set may either be E-trivial or E-nontrivial.

Theorem 7.20 *For any computable function $t(n)$ there is a computable $t(n)$- random set which is* E*-nontrivial.*

PROOF. Let $t(n)$ be computable. We have to give a computable $t(n)$-random set A_t which is E-nontrivial.

Since any computable function is dominated by a strictly increasing time constructible function and since, for computable functions t and t' such that $t(n) \leq_{a.e.} t'(n)$, any $t'(n)$-random set is $t(n)$-random, w.l.o.g. we may assume that $t(n)$ is strictly increasing, $t(n) > n$, and $t(n)$ is time constructible.

Then the required set A_t is defined as follows. By Theorem 3.15, fix an n^2-random set $A \in \mathrm{E}$ and let

$$A_t = \{z_n : 0^{t(n)} \in A\}.$$

Obviously, A_t is computable.

$t(n)$-randomness of A_t is shown as follows. For a contradiction assume that s is a strategy in DTIME$(t(n))$ such that the corresponding normed martingale $d = d[s,1]$ succeeds on A_t. We convert s into an $O(n)$-strategy s' such that the corresponding normed martingale $d' = d[s',1]$ succeeds on A. So A is not n^2-random contrary to assumption.

The strategy s' is defined by

$$s'(X \restriction n) = \begin{cases} s(X' \restriction m) & z_n = 0^{t(m)} \text{ for some } m \geq 0 \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

where $X' \restriction m = X(0^{t(0)})...X(0^{t(m-1)})$.

Then $s' \in \text{DTIME}(O(n))$. Namely, given a string $X \restriction n$ of length n, by $t(m) \geq m$ and by time constructibility of t, in $O(|z_n|^2) = O((\log n)^2) \leq O(n)$ steps, first, we can decide whether $z_n = 0^{t(m)}$ and, second, if so find the corresponding m together with the values $t(0), \ldots, t(m-1)$. So, in a total of $O(n)$ steps, we can decide whether the first case in the definition of $s'(X \restriction n)$ holds and if so compute the string $X' \restriction m = X(0^{t(0)})...X(0^{t(m-1)})$. Since, in the nontrivial (i.e., first) case, $s'(X \restriction n) = s(X' \restriction m)$ and, since $s \in \text{DTIME}(t(n))$, it follows that $s'(X \restriction n)$ can be computed in

$$O(t(|X' \restriction m|)) = O(t(m)) = O(|z_n|) \leq O(n)$$

steps.

In order to show that the martingale d' induced by s' succeeds on A, we first observe (by a straightforward induction on n) that, for $n \geq 0$,

$$d'(A \restriction 0^{t(n)}) = d(A_t \restriction n)(= d(A_t \restriction z_n)).$$

Since d succeeds on A_t this implies

$$\begin{array}{rcl} \limsup_{n\to\infty} d'(A \restriction n) & \geq & \limsup_{n\to\infty} d'(A \restriction 0^{t(n)}) \\ & = & \limsup_{n\to\infty} d(A_t \restriction n) \\ & = & \infty \end{array}$$

whence d' succeeds on A.

It remains to show that A_t is E-nontrivial. By choice of $t(n)$, the tally set

$$D = \{0^{t(n)} : n \geq 0\}$$

is infinite and $D \in \text{P}$. Since A is n^2-random hence, by Theorem 3.16, E_1-bi-immune and since $A \in \text{E}$ it follows by Theorem 4.30 that $A \cap D$ is E-nontrivial. Moreover,

$$A \cap D \leq^p_m A_t$$

via f where $f(0^{t(n)}) = z_n$ and, for $x \notin D$, $f(x) = y_0$ for some fixed string $y_0 \notin A_t$. (By $t(n)$-randomness of A_t, A_t is co-infinite whence such a string y_0 exists.) Since the class of E-nontirival sets is closed upwards under $\leq^p_m$, it follows that A_t is E-nontrivial.

This completes the proof. □

Corollary 7.21 *The class of the computable* E*-nontrivial sets does not have computable measure 0 hence not measure 0 in* REC.

Proof. This is immediate by Lemma 3.20 and Theorem 7.20. □

Corollary 7.22 *The class of the computable* E*-nontrivial sets is not computably meager hence not meager in* REC.

Proof. This is immediate by Theorem 3.73 and Corollary 7.21. □

7.7 Summary of Results

The main results of this chapter can be summarized as follows. Let C be one of the classes E, REC and ALL $= \mathcal{P}(\Sigma^*)$, and let $\mathcal{H}$ be one of the weak hardness notions we are considering. Then we say that property $\mathcal{H}$ is *typical* with respect to measure for C if the class of sets with property $\mathcal{H}$ has measure 1 in C, and property $\mathcal{H}$ is *untypical* with respect to measure for C if the class of sets with property $\mathcal{H}$ has measure 0 in C. Similarly, we say that property $\mathcal{H}$ is *typical* with respect to Baire category for C if the class of sets with property $\mathcal{H}$ is comeager in C, and property $\mathcal{H}$ is *untypical* with respect to Baire category for C if the class of sets with property $\mathcal{H}$ is meager in C.

Then, for measure, we obtain the following typicalness results:

	E	REC	ALL
E-hard	untypical	untypical	untypical
E-measure hard	typical	untypical	untypical
E-category hard	typical	untypical	untypical
E-compression hard	typical	untypical	untypical
strongly E-nontrivial	typical	untypical	untypical
E-nontrivial	typical	neither typical nor untypical	untypical

Typicalness of the weak hardness notions w.r.t. measure

The results on E (in the first column) follow from Theorem 3.41. The results on REC (in the second column) follow from Corollary 7.9, Corollary 7.18, and Corollary 7.21. Finally, the results on ALL (in the third column) follow from Corollary 7.5.

For category the typicalness results are as follows.

	E	REC	ALL
E-hard	untypical	untypical	untypical
E-measure hard	neither typical nor untypical	untypical	untypical
E-category hard	typical	untypical	untypical
E-compression hard	typical	untypical	untypical
strongly E-nontrivial	typical	untypical	untypical
E-nontrivial	typical	neither typical nor untypical	untypical

Typicalness of the weak hardness notions w.r.t. category

The results on REC (in the second column) follow from Corollary 7.9, Corollary 7.19, and Corollary 7.22. The results on ALL (in the third column) follow from Corollary 7.5.

From the typicalness results in the first column on weak hardness in E, typicalness of E-category hardness (hence of the weaker concepts) has been shown in Corollary 3.78. Untypicalness of E-hardness follows from the fact that E-hard sets are not P-bi-immune (Theorem 2.23) and the fact that the class of P-bi-immune sets is p-comeager (by Theorem 3.65 and Definition 3.68).

Finally, the following theorem shows that, in the sense of Baire category, E-measure hardness is neither typical nor untypical for sets in E.

Theorem 7.23 *Let* $\mathrm{C} = \{A : A$ E-*measure complete*$\}$. *Then neither* C *nor* $\mathrm{E} \setminus \mathrm{C}$ *is p-meager. (So, by* $\mathrm{C} \subseteq \mathrm{E}$, C *is neither meager nor comeager in* E.*)*

PROOF. By (3.21), it suffices to show that, for any $k \geq 2$, there are n^k-generic sets A_k and $\hat{A}_k$ in E such that A_k is E-measure complete whereas $\hat{A}_k$ is not E-measure complete.

A set A_k with the required properties is obtained as follows. By Theorem 3.15 let A_k be an n^k-random set in E. Then, by Theorem 3.63, A_k is n^k-generic and, by Theorem 3.40, A_k is E-measure complete.

A set $\hat{A}_k$ with the required properties is obtained as follows. By Theorem 3.66 let $\hat{A}_k$ be an n^k-generic set in E which is sparse. By Theorem 3.44, $\hat{A}_k$ is not E-measure complete. □

The reader should keep in mind that here we work with a weak Baire category concept based on simple extension functions, i.e., on extensions of bounded length. As pointed out before, this concept is compatible with measure whereas, in general, Baire category and measure are incompatible. So our results on typicalness w.r.t. category have to be interpreted as results in this particular settings. By considering algorithmic versions of Baire category based on unbounded extension functions, the corresponding typicalness results may not completely coincide with the results obtained here.

CHAPTER 8

Nontriviality and Degrees

In this chapter we look at the distribution of the nontrivial and strongly nontrivial sets w.r.t. *p-m*-reducibility. We will only look at (strong) E-nontriviality, not at (strong) EXP-nontriviality, and we will look at these notions only as weak completeness notions, not as weak hardness notions. In other words, we look at (strongly) E-nontrivial sets in E. (In general, our results should directly carry over to (strongly) EXP-nontrivial sets in EXP, but some results may not be extendible to (strongly) E-nontrivial sets outside of E.)

It will be convenient to phrase our result in terms of degrees. So we first introduce some notation and state some general facts on the *p-m*-degrees to be used later. Then we will look at the distribution of the E-trivial sets and E-nontrivial sets among the sets in E, and finally we will look at strong E-nontriviality and relations among E-nontriviality and strong E-nontriviality.

For the basic notion of a *p-m*-degree and some more basic notation, see Section 2.3.2. In particular, recall that we denote *p-m*-degrees by lower case boldface letters $\mathbf{a},\mathbf{b},\mathbf{c},\ldots$ and let $\leq$ be the partial ordering on the *p-m*-degrees induced by *p-m*-reducibility. For *p-m*-degrees $\mathbf{a}$ and $\mathbf{b}$ such that $\mathbf{a} < \mathbf{b}$, we let $(\mathbf{a},\mathbf{b})$ and $[\mathbf{a},\mathbf{b}]$ denote the open and closed intervals

$$(\mathbf{a},\mathbf{b}) = \{\mathbf{c} : \mathbf{a} < \mathbf{c} < \mathbf{b}\} \ \& \ [\mathbf{a},\mathbf{b}] = \{\mathbf{c} : \mathbf{a} \leq \mathbf{c} \leq \mathbf{b}\},$$

respectively.

For $A \in \mathrm{E}$ we call $deg^p_m(A)$ an E-*degree* and, similarly, for $A \in \mathrm{EXP}$ we call $deg^p_m(A)$ an EXP-*degree*. We let $\mathbf{E}$ and $\mathbf{EXP}$ denote the classes of the E-degrees and EXP-degrees, respectively. Note that, by the padding lemma, any EXP-degree contains a set from E whence

$$\mathbf{E} = \mathbf{EXP}. \tag{8.1}$$

This also shows that, by definition, any E-degree $\mathbf{a}$ contains *some* set from E but not necessarily *all* sets in $\mathbf{a}$ are members of E, though, by closure of EXP under *p-m*-equivalence, all sets in $\mathbf{a}$ are in EXP, i.e., $\mathbf{a} \subseteq \mathrm{EXP}$. Moreover, by (8.1) and downward closure of EXP under $\leq^p_m$, $\mathbf{E}$ is an initial segment of the partial ordering of the computable (or all) *p-m*-degrees. In fact,

$$\mathbf{E} = [\mathbf{0},\mathbf{1}] \tag{8.2}$$

where $\mathbf{0}$ is the least *p-m*-degree, consisting of the polynomial-time computable sets and $\mathbf{1}$ is the degree of the E-complete sets. I.e, by the coincidence of E-hardness and EXP-hardness and the padding lemma,

$$\{A : A \text{ E-complete}\} \subset \mathbf{1} = \{A : A \text{ EXP-complete}\}.$$

(So $\mathbf{0}$ is an example of an E-degree which is entirely contained in E whereas $\mathbf{1}$ is an example of an E-degree which is not contained in E. Note that the *p-m*-degrees of strictly trivial sets are further examples of E-degrees which are entirely contained in E.)

Recall that the partial ordering of the *p*-*m*-degrees is an upper semi-lattice (usl), where the join (least upper bound) of two degrees **a** and **b** is represented by the disjoint union $A \oplus B$ of any sets $A \in \mathbf{a}$ and $B \in \mathbf{b}$. So, by (8.2), the partial ordering $(\mathbf{E}, \leq)$ is an upper semi-lattice too. Moreover, distributivity of the usl $(\mathbf{REC}, \leq, \vee)$ is inherited by the initial segment **E**. (See Section 2.3.2 for the definition of a distributive usl.)

Some basic structural properties of the *p*-*m*-degrees we will need are the following: Ladner has shown that the partial ordering of the computable *p*-*m*-degrees is dense and that every computable *p*-*m*-degree splits. There are several extensions of these results which can be summarized by the following embedding theorem due to Ambos-Spies (see Theorem 4.4 in the survey paper Ambos-Spies (1999) for a more general, infinitary version of this theorem).

Theorem 8.1 *(Ambos-Spies) Let $\mathcal{L}$ be a finite distributive lattice, let $\mathbf{a}, \mathbf{b}$ be computable p-m-degrees such that $\mathbf{a} < \mathbf{b}$, and let $\mathbf{c}_0, \ldots, \mathbf{c}_n$ $(n \geq 0)$ be p-m-degrees such that $\mathbf{c}_0, \ldots, \mathbf{c}_n \in (\mathbf{a}, \mathbf{b})$. There are lattice embeddings $f_i : \mathcal{L} \to [\mathbf{a}, \mathbf{b}]$ of the lattice $\mathcal{L}$ into the interval $[\mathbf{a}, \mathbf{b}]$, where f_0 maps the least element 0 of $\mathcal{L}$ to $\mathbf{a}$ and f_1 maps the greatest element 1 of $\mathcal{L}$ to $\mathbf{b}$. Moreover, for any $a \in \mathcal{L} \setminus \{0, 1\}$, $f_i(a)$ is incomparable with all of the degrees $\mathbf{c}_0, \ldots, \mathbf{c}_n$.*

Note that, by letting $\mathcal{L}$ be the 2-atom Boolean algebra, the embedding f_1 of $\mathcal{L}$ into $[\mathbf{a}, \mathbf{b}]$ shows that, for any given intermediate degrees $\mathbf{c}_0, \ldots, \mathbf{c}_n$, the top **b** of the interval can be split into two degrees $\mathbf{b}_0$ and $\mathbf{b}_1$ above the bottom **a** of the interval which are incomparable with $\mathbf{c}_0, \ldots, \mathbf{c}_n$.

Corollary 8.2 *Let $\mathbf{a}, \mathbf{b}, \mathbf{c}_0, \ldots, \mathbf{c}_n$ $(n \geq 0)$ be computable p-m-degrees such that, for $i \leq n$, $\mathbf{a} < \mathbf{c}_i < \mathbf{b}$. There are computable p-m-degrees $\mathbf{b}_0$ and $\mathbf{b}_1$ such that $\mathbf{b} = \mathbf{b}_0 \vee \mathbf{b}_1$, $\mathbf{a} < \mathbf{b}_j < \mathbf{b}$, and $\mathbf{b}_j | \mathbf{c}_i$ for $j \leq 1$ and $i \leq n$. (Here $\mathbf{d}|\mathbf{e}$ denotes that the degrees $\mathbf{d}$ and $\mathbf{e}$ are incomparable, i.e., $\mathbf{d} \not\leq \mathbf{e}$ and vice versa.)*

For more information on the *p*-*m*-degrees, see the survey Ambos-Spies (1999).

8.1 Trivial and Nontrivial E-Degrees

Call an E-degree **a** *trivial* if **a** contains a set $A \in \mathrm{E}$ such that A is E-trivial and call **a** *nontrivial* if **a** contains a set $A \in \mathrm{E}$ such that A is E-nontrivial; and let **T** and **NT** denote the classes of the trivial and nontrivial E-degrees, respectively:

$$\mathbf{T} = \{deg_m^p(A) : A \in \mathrm{E} \;\&\; A \text{ E-trivial}\}$$

$$\mathbf{NT} = \{deg_m^p(A) : A \in \mathrm{E} \;\&\; A \text{ E-nontrivial}\}$$

Note, that E-(non)triviality is closed under *p*-*m*-equivalence. So any trivial degree entirely consists of E-trivial sets (though, as pointed out above, not necessarily all of them are members of E) and, similarly, any nontrivial degree entirely consists of E-nontrivial sets. So the classes **T** and **NT** split the class of the E-degrees:

$$\mathbf{T} \cup \mathbf{NT} = \mathbf{E} \text{ and } \mathbf{T} \cap \mathbf{NT} = \emptyset \tag{8.3}$$

Moreover, since E-triviality is closed downward under $\leq_m^p$, hence E-nontriviality closed upward under $\leq_m^p$,

$$\mathbf{0} \in \mathbf{T} \,\&\, \forall\, \mathbf{a},\mathbf{b}\ (\mathbf{a} \leq \mathbf{b} \,\&\, \mathbf{b} \in \mathbf{T} \Rightarrow \mathbf{a} \in \mathbf{T}) \tag{8.4}$$

and

$$\mathbf{1} \in \mathbf{NT} \,\&\, \forall\, \mathbf{a},\mathbf{b}\ (\mathbf{a} \leq \mathbf{b} \,\&\, \mathbf{a} \in \mathbf{NT} \Rightarrow \mathbf{b} \in \mathbf{NT}), \tag{8.5}$$

i.e., **T** is an initial segment of $(\mathbf{E}, \leq)$ while **NT** is a final segment of $(\mathbf{E}, \leq)$. So, intuitively, the classes **T** and **NT** partition **E** into a lower and an upper part.

8.1.1 The Initial Segment T of the Trivial Degrees is an Ideal

Having seen that **T** is an initial segment of **E** it is natural to ask whether **T** is an *ideal*, i.e., whether **T** is closed under joins. By applying some of our previous results on *p*-splittings of nontrivial sets we get an affirmative answer.

Theorem 8.3 *The class* **T** *of the trivial degrees is an ideal of* $(\mathbf{E}, \leq)$*, i.e., closed downwards under* $\leq$ *and closed under join.*

PROOF. By (8.4), given degrees $\mathbf{a}, \mathbf{b} \in \mathbf{T}$ it suffices to show that $\mathbf{a} \vee \mathbf{b} \in \mathbf{T}$. So fix E-trivial sets $A, B \in \mathrm{E}$ such that $A \in \mathbf{a}$ and $B \in \mathbf{b}$. Then $\mathbf{a} \vee \mathbf{b} = deg_m^p(A \oplus B)$ and, obviously, $A \oplus B \in \mathrm{E}$. So it suffices to show that $A \oplus B$ is E-trivial. For a contradiction assume that $A \oplus B$ is E-nontrivial. Since $(0A, 1B)$ is a *p*-splitting of $A \oplus B$, it follows by Theorem 4.28 that $0A$ or $1B$ is E-nontrivial. But, since $0A =_m^p a$ and $1B =_m^p B$, this implies that A or B is E-nontrivial contrary to choice of A and B.
□

Corollary 8.4 *Let* $\mathbf{a}, \mathbf{b}, \mathbf{c}$ *be* E*-degrees such that* $\mathbf{a} \in \mathbf{NT}$ *and* $\mathbf{a} = \mathbf{b} \vee \mathbf{c}$*. Then* $\mathbf{b} \in \mathbf{NT}$ *or* $\mathbf{c} \in \mathbf{NT}$.

Intuitively, Corollary 8.4 says that if we split an E-nontrivial set into two parts then one of the parts is E-nontrivial again. As we will show later, for the stronger weak completeness notions for E this observation is not true anymore.

8.1.2 The Final Segment NT of the Nontrivial Degrees is not a Filter

Since **NT** may be viewed as the dual of **T** in **E**, it is natural to ask whether the dual of Theorem 8.3 is true too, i.e., whether **NT** is a filter. As we will show here, this is not the case. In fact, this is an immediate consequence of the existence of minimal pairs of E-nontrivial sets in E.

Since the usl $(\mathbf{E},\leq)$ is not a lattice, there are two ways for defining filters of $(\mathbf{E},\leq)$. A class of degrees $\mathbf{F}\subseteq\mathbf{E}$ which is closed upwards in **F** is called a *strong filter* if

$$\forall \mathbf{a},\mathbf{b}\in\mathbf{F}\;\exists\,\mathbf{c}\in\mathbf{F}\;(\mathbf{c}\leq\mathbf{a},\mathbf{b})$$

and **F** is called a *weak filter* if

$$\forall \mathbf{a},\mathbf{b}\in\mathbf{F}\;(\mathbf{a}\wedge\mathbf{b}\text{ exists }\Rightarrow\mathbf{a}\wedge\mathbf{b}\in\mathbf{F}).$$

Theorem 8.5 *The class* **NT** *of the nontrivial degrees is not a weak filter, hence not a strong filter.*

PROOF. By Corollary 4.39 there is a pair of degrees $\mathbf{a},\mathbf{b}\in\mathbf{NT}$ such that $\mathbf{a}\wedge\mathbf{b}=\mathbf{0}$. Since $\mathbf{0}\in\mathbf{T}$, this implies the claim. □

Theorem 8.5 can be extended as follows. While **T** is closed under $\vee$ and $\wedge$, the closure of **NT** under $\wedge$ is the class of all E-degrees.

Theorem 8.6 **NT** *generates* **E** *under meet. I.e., for any* $\mathbf{a}\in\mathbf{E}$ *there are* $\mathbf{b},\mathbf{c}\in\mathbf{NT}$ *such that* $\mathbf{a}=\mathbf{b}\wedge\mathbf{c}$.

PROOF (IDEA). Fix $\mathbf{a}\in\mathbf{E}$. If $\mathbf{a}\in\mathbf{NT}$ then the claim is trivial (just let $\mathbf{b}=\mathbf{c}=\mathbf{a}$). So w.l.o.g. $\mathbf{a}\notin\mathbf{NT}$. So we may fix $A\in\mathbf{a}\cap\mathrm{E}$ and $k\geq 1$ such that

$$\mathrm{P}_m(A)\cap\mathrm{E}\subseteq\mathrm{E}_k.$$

Now (by a straightforward variant of the proof of Corollary 4.39) construct exptally sets B and C such that $B,C\in\mathrm{E}\setminus\mathrm{E}_k$ and such that B and C form a *p*-*m*-minimal pair. Then, as one can easily check,

$$\mathbf{a}=deg_m^p(A\oplus B)\wedge deg_m^p(A\oplus C)$$

(this follows from distributivity of $\leq$) and $deg_m^p(A\oplus B),deg_m^p(A\oplus C)\in\mathbf{NT}$ (by Theorem 4.37 and upward closure of **NT**). □

8.1.3 Bounds on T and NT and Density Properties

Having analyzed the basic algebraic closure properties of the classes **T** and **NT**, here we address some more basic structural questions. In particular, we answer the following questions.

- Does **T** posses maximal elements and does **NT** possess minimal elements?
- Is there a degree $\mathbf{c} < \mathbf{1}$ which is an upper bound for **T** and is there a degree $\mathbf{d} > \mathbf{0}$ which is a lower bound for **NT**?

We will answer both questions negatively. The following *Sandwich Theorem* provides a negative answer to the first question.

Theorem 8.7 *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be* E*-degrees such that* $\mathbf{a} \in \mathbf{T}$*,* $\mathbf{b} \in \mathbf{NT}$ *and* $\mathbf{a} < \mathbf{b}$*. There are* E*-degrees* $\mathbf{c}$ *and* $\mathbf{d}$ *such that* $\mathbf{c} \in \mathbf{T}$*,* $\mathbf{d} \in \mathbf{NT}$ *and* $\mathbf{a} < \mathbf{c} < \mathbf{d} < \mathbf{b}$.

PROOF. By density of $(\mathbf{E}, \leq)$ and by Corollary 8.2, split $\mathbf{b}$ into degrees $\mathbf{b}_0$ and $\mathbf{b}_1$ such that $\mathbf{b} = \mathbf{b}_0 \vee \mathbf{b}_1$ and $\mathbf{a} < \mathbf{b}_0, \mathbf{b}_1 < \mathbf{b}$. By Corollary 8.4, fix $i \leq 1$ such that $\mathbf{b}_i \in \mathbf{NT}$ and let $\mathbf{d} = \mathbf{b}_i$.

For the definition of $\mathbf{c}$, fix sets $D \in \mathbf{d}$ and $A \in \mathbf{a} \cap \mathrm{E}$ and, by Theorem 4.13, fix a hyperpolynomial shift h such that $D_h \not\leq^p_m A$, and let $C = D_h \oplus A$. Then, by Theorem 4.14, $D_h \in \mathrm{E}$ and D_h is E-trivial. So, by Theorem 8.3, C is E-trivial too and, obviously, $C \in \mathrm{E}$. So, for $\mathbf{c} = deg^p_m(C)$, $\mathbf{c} \in \mathbf{T}$ and, by choice of C, $\mathbf{a} < \mathbf{c} \leq \mathbf{d}$. This completes the proof since, by $\mathbf{c} \in \mathbf{T}$ and $\mathbf{d} \in \mathbf{NT}$, $\mathbf{c} \leq \mathbf{d}$ implies that $\mathbf{c} < \mathbf{d}$, □

Corollary 8.8 *The class* **T** *does not posses any maximal elements (hence no greatest element). I.e., for any degree* $\mathbf{a} \in \mathbf{T}$ *there is a degree* $\hat{\mathbf{a}} \in \mathbf{T}$ *such that* $\mathbf{a} < \hat{\mathbf{a}}$.

Similarly, the class **NT** *does not posses any minimal elements (hence no least element). I.e., for any degree* $\mathbf{b} \in \mathbf{NT}$ *there is a degree* $\hat{\mathbf{b}} \in \mathbf{NT}$ *such that* $\hat{\mathbf{b}} < \mathbf{b}$.

PROOF. For a proof of the first part, fix $\mathbf{a} \in \mathbf{T}$ and apply Theorem 8.7 to $\mathbf{a}$ and $\mathbf{b} = \mathbf{1}$. Then $\hat{\mathbf{a}} = \mathbf{c}$ has the required properties. For a proof of the second part, fix $\mathbf{b} \in \mathbf{NT}$ and apply Theorem 8.7 to $\mathbf{a} = \mathbf{0}$ and $\mathbf{b}$. Then $\hat{\mathbf{b}} = \mathbf{d}$ has the required properties. □

A negative answer to our second question is provided by the following theorems.

Theorem 8.9 *For any computable p-m-degree* $\mathbf{a} \not\geq \mathbf{1}$ *there is a degree* $\mathbf{b} \in \mathbf{T}$ *such that* $\mathbf{b} \not\leq \mathbf{a}$.

PROOF. Given a E-complete set C and a set $A \in \mathbf{a}$, by Theorem 4.13, fix a hyperpolynomial shift C_h of C such that $C_h \not\leq^p_m A$. Then, by Theorem 4.14, $\mathbf{b} = deg^p_m(C_h)$ will have the required properties. □

Theorem 8.10 *For any* E*-degree* $\mathbf{a} > \mathbf{0}$ *there is a degree* $\mathbf{b} \in \mathbf{NT}$ *such that* $\mathbf{a} \not\leq \mathbf{b}$.

PROOF. For $\mathbf{a} = \mathbf{1}$ the claim is immediate by Corollary 8.8 whence we may assume $\mathbf{0} < \mathbf{a} < \mathbf{1}$. So, by Corollary 8.2, we may split $\mathbf{1}$ (over $\mathbf{0}$) into two degrees $\mathbf{b}_0$ and $\mathbf{b}_1$ which are incomparable with $\mathbf{a}$. Moreover, by Corollary 8.4, one of theses degrees will be in **NT**. □

8.1.4 E-trivial sets Don't Help

We say that a degree $\mathbf{a} \in \mathbf{E}$ is *noncuppable* if there is no degree $\mathbf{b} < \mathbf{1}$ such that $\mathbf{a} \vee \mathbf{b} = \mathbf{1}$. The property of sets corresponding to cuppability has also been called helping. A set $A \in \mathrm{E}$ *helps* if there is an incomplete set $B \in \mathrm{E}$ such that $A \oplus B$ is E-complete. Ambos-Spies (1989) has shown that hyperpolynomial shifts of sets in EXP do not help. Here we extend this result by showing that E-trivial sets in E do not help. So. intuitively, if we split a complete set in two incomplete parts then none of these parts can be E-trivial.

Theorem 8.11 *Let A and B be computable sets such that $A \in \mathrm{E}$ is* E*-trivial and B is not* E*-hard. Then $A \oplus B$ is not* E*-hard. So, in particular, if $A \in \mathrm{E}$ is* E*-trivial then A does not help.*

For the proof of Theorem 8.11 we need the following existence result for E_k-bi-immune sets.

Lemma 8.12 *Let $k \geq 1$ and let A be any computable set such that A is not* E*-hard. Then there is an* E_k*-bi-immune set B in* E *such that $B \not\leq^p_m A$ and $A \oplus B$ is not* E*-m-hard.*

Since the proof of Lemma 8.12 is quite lengthy we first show how Theorem 8.11 follows from Lemma 8.12.

PROOF OF THEOREM 8.11. Given an E-trivial set in E and a recursive set B which is not E-hard, it suffices to show that $A \oplus B$ is not E-hard too.

For a contradiction, assume that $A \oplus B$ is E-hard. By E-triviality of A, fix k such that

$$\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{E}_k$$

holds. Moreover, by Lemma 8.12, fix an E_k-bi-immune set C in E such that $C \not\leq^p_m B$. Now, since, by our assumption that $A \oplus B$ is E-hard, $C \leq^p_m A \oplus B$, it follows from the Distributivity Lemma that there is a set $D \in \mathrm{P}$ such that $C \cap D \leq^p_m A$ and $C \cap \overline{D} \leq^p_m B$. Now distinguish the following two cases. First assume that $C \cap D$ is infinite. Then, by E_k-bi-immunity of C, $C \cap D \notin \mathrm{E}_k$. By choice of A, however, this is impossible. This leaves the case that $C \cap D$ is finite. But then $C =^p_m C \cap \overline{D}$, hence $C \leq^p_m B$ contrary to choice of C. □

PROOF OF LEMMA 8.12. We will construct a set B with the required properties in stages. At stage s of the construction we determine the value $B(z_s)$.

Fix some E-m-complete set C in E_1.

To ensure that B is not P-m-reducible to A, we code sufficiently large parts of C into B so that B meets the following requirements for $e \geq 0$:

$$\mathfrak{R}_{4e} : B \text{ is not reducible to } A \text{ via } f_e$$

where $\{f_e : e \geq 0\}$ is an enumeration of all polynomial time computable functions with corresponding time-bounds p_e. To ensure $A \oplus B$ is not E-m-hard we make B look like the empty set on large intervals so that B meets the following requirements for $e \geq 0$:

$$\mathfrak{R}_{4e+1} : C \text{ is not reducible to } A \oplus B \text{ via } f_e.$$

In order to make B E_k-bi-immune it suffices to meet the following requirements for $(e \geq 0)$:

$$\mathfrak{R}_{4e+2} : \mathrm{E}_e^k \text{ is infinite } \Rightarrow B \cap \mathrm{E}_e^k \neq \emptyset$$

$$\mathfrak{R}_{4e+3} : \mathrm{E}_e^k \text{ is infinite } \Rightarrow \bar{B} \cap \mathrm{E}_e^k \neq \emptyset.$$

At stage s of the construction we look at requirements $\mathfrak{R}_n$ with $n \leq s$. For $i \leq 1$ we say that requirement $\mathfrak{R}_{4e+i}$ requires attention on stage s if

(i) $4e+i \leq s$

(ii) $\mathfrak{R}_{4e+i}$ is not yet satisfied.

And for $i > 1$ we say that requirement $\mathfrak{R}_{4e+i}$ requires attention on stage s if

(i) $4e+i \leq s$

(ii) $\mathfrak{R}_{4e+i}$ is not yet satisfied

(iii) $z_s \in \mathrm{E}_e^k$.

Fix $n = 4e+i$ $(i \leq 3)$ minimal such that $\mathfrak{R}_n$ requires attention. If there is no such n then let $B(z_s) = 0$ and finish stage s. We say that $\mathfrak{R}_n$ is active at stage s and let

$$B(z_s) = \begin{cases} C(z_s) & \text{if } i = 0 \\ 0 & \text{if } i = 1 \text{ or } i = 3 \\ 1 & \text{if } i = 2. \end{cases}$$

If $i > 1$ then we say that requirement $\mathfrak{R}_{4e+i}$ is satisfied at stage s. If $i = 0$ then we spend $|z_s|$ steps in order to find x with $B(x) \neq A(f_e(x))$ and $2^{|x|} < |z_s|$. If $i = 1$ then we spend $|z_s|$ steps in order to find x with $C(x) \neq A \oplus B(f_e(x))$, $2^{|x|} < |z_s|$ and $f_e(x) < z_s$.

In any case if there is such x then we say that requirement $\mathfrak{R}_{4e+i}$ is satisfied at stage s.

This completes the construction.

Claim 1. $B \in \mathrm{E}_{k+3}$

Proof. Given

$$SAT(s-1) = \{n : \mathfrak{R}_n \text{ is satisfied at a stage } \leq s-1\},$$

we can compute $A(z_s)$ and $SAT(s)$ as follows. Fix $n = 4e+i < s$ minimal such that $n \notin SAT(s-1)$.

For $i > 1$ $\mathfrak{R}_n$ will require attention at stage s if $z_s \in \mathrm{E}^k_e$. Since there are s such requirements, and, for given z_s, $\mathrm{E}^k_e(z_s)$ can be computed in $2^{|z_s|}$ steps, in

$$s \cdot 2^{k|z_s|} \leq O(2^{(k+1)|z_s|})$$

steps we can find the least $n = 4e+i < s$ such that $\mathfrak{R}_n$ requires attention at stage s (if any). For $i \leq 1$ $\mathfrak{R}_n = \mathfrak{R}_{4e+i}$ will require attention automatically.

Since $B(z_s) = C(z_s)$ for $i = 0$, $B(z_s) = 0$ for $i = 1$ or $i = 3$ and $B(z_s) = 1$ for $i = 2$ and whether requirement is satisfied at stage s or not we can decide in $|z_s|$ steps, this shows that $B(z_s)$ and $SAT(s)$ can be computed from $SAT(s-1)$ in $O(2^{(k+2)|z_s|})$. So, by induction, $B(z_s)$ can be computed in time $s \cdot O(2^{(k+2)|z_s|}) \leq O(2^{(k+3)|z_s|})$

Claim 2. $\mathfrak{R}_n$ requires attention at most finitely often

Proof. The proof is by inductiion on n. By inductive hypothesis, fix a stage s_0 such that no requirement $\mathfrak{R}_{n'}$ with $n' < n$ requires attention after stage s_0. Then at a stage $s > s_0$ at which requirement $\mathfrak{R}_n$ requires attention will become active. For $i > 1$ by construction requirement $\mathfrak{R}_n$ will be satisfied at stage s and will not require attention after stage s.

For $i \leq 1$ assume that requirement $\mathfrak{R}_n$ requires attention infinitely often. Let $n = 4e+i$.

For $i = 0$ that would mean that it is never satisfied and hence B is reducible to A via f_e and for all $s' > s$, $B(z_{s'}) = C(z_{s'})$. Since C is E-m-complete, that contradicts the assumtion that A is not E-m-hard.

For $i = 1$ that would mean that starting from stage s, B looks like the empty set and hence $A \oplus B =_m A$. Since $\mathfrak{R}_n$ recieves attention infinitely often, $C(x) = A \oplus B(f_e(x))$ and hence C is reducible to A. That again contradicts the assumption that A is not E-m-hard.

Claim 3. $\mathfrak{R}_n$ is met

Proof. Let $n = 4e+i$ $(i \leq 3)$, and, for contradiction, assume that $\mathfrak{R}_{4e+i}$ is not met. Then, by construction, requirement $\mathfrak{R}_n$ is never satisfied and requires attention infinitely often. But that contradicts Claim 2.

This completes the proof of Lemma 8.12.

□

8.2 Weakly Trivial and Strongly Nontrivial E-Degrees

We now turn to the distribution of the strongly E-nontrivial sets among the sets in E. We will focus on the question which of the results on the degrees of the E-trivial sets and E-nontrivial sets carry over to the degrees of the weakly E-trivial sets and strongly E-nontrivial sets, respectively.

Call an E-degree **a** *weakly trivial* if **a** contains a set $A \in \mathrm{E}$ such that A is weakly E-trivial and call **a** *strongly nontrivial* if **a** contains a set $A \in \mathrm{E}$ such that A is strongly E-nontrivial; and let **WT** and **SNT** denote the classes of the weakly trivial and strongly nontrivial E-degrees, respectively:

$$\mathbf{WT} = \{deg_m^p(A) : A \in \mathrm{E} \;\&\; A \text{ weakly E-trivial}\}$$

$$\mathbf{SNT} = \{deg_m^p(A) : A \in \mathrm{E} \;\&\; A \text{ strongly E-nontrivial}\}$$

Since weak E-triviality is closed downwards under $\leq_m^p$ and strong E-nontriviality is closed upwards under $\leq_m^p$ in E, as in case of **T** and **NT**, the classes **WT** and **SNT** split the class of the E-degrees:

$$\mathbf{WT} \cup \mathbf{SNT} = \mathbf{E} \text{ and } \mathbf{WT} \cap \mathbf{SNT} = \emptyset \tag{8.6}$$

and **WT** is closed downwards in **E**,

$$\mathbf{0} \in \mathbf{WT} \;\&\; \forall\, \mathbf{a}, \mathbf{b}\; (\mathbf{a} \leq \mathbf{b} \;\&\; \mathbf{b} \in \mathbf{WT} \Rightarrow \mathbf{a} \in \mathbf{WT}), \tag{8.7}$$

whereas **SNT** is closed upwards,

$$\mathbf{1} \in \mathbf{SNT} \;\&\; \forall\, \mathbf{a}, \mathbf{b}\; (\mathbf{a} \leq \mathbf{b} \;\&\; \mathbf{a} \in \mathbf{SNT} \Rightarrow \mathbf{b} \in \mathbf{SNT}). \tag{8.8}$$

Moreover,

$$\mathbf{T} \subseteq \mathbf{WT} \;\&\; \mathbf{SNT} \subseteq \mathbf{NT}. \tag{8.9}$$

So, for

$$\mathbf{I} = \mathbf{WT} \setminus \mathbf{T} = \mathbf{NT} \setminus \mathbf{SNT}, \tag{8.10}$$

we get a partition of **E** in three (disjoint) layers, the lower layer of **T**, the middle layer of **I** and the upper layer of **SNT**.

We begin our study of the initial segment **WT** and the final segment **SNT** by looking at the algebraic structure of these degree classes.

8.2.1 The Algebraic Structure of WT and SNT

First we show that - in contrast to **T** - the initial segment **WT** of the weakly trivial degrees is not an ideal. In fact, **WT** generates **E** under join.

Theorem 8.13 *The class* **WT** *of the weakly trivial degrees generates the class* **E** *of all* E*-degrees under join. So, in particular,* **WT** *is not an ideal.*

PROOF (IDEA). We only give the idea of the proof. Ladner's splitting theorem (or the more general Theorem 8.1) is proven by splitting a set C into two (or more) parts C_0 and C_1 by letting $C_0 = C \cap B$ and $C_1 = C \cap \overline{B}$ where B is a so called *gap language*. A gap language B is a set $B \in \mathrm{P}$ such that B and $\overline{B}$ are built up from alternating intervals of fast growing length. In particular this implies that, for a gap language B and a set $C \in \mathrm{E}$, the hypotheses of Theorem 5.16 are satisfied by $A = C \cap B$ and $A = C \cap \overline{B}$ whence $C \cap B$ and $C \cap \overline{B}$ are weakly E-trivial.

So, by Ladner splitting, any set $C \in \mathrm{E}$ can be p-split into weakly E-trivial sets C_0 and C_1. Since, for such a p-splitting, $deg^p_m(C) = deg^p_m(C_0) \vee deg^p_m(C_1)$, this implies the claim. □

Note that, by Theorem 8.13, the analog of Corollary 8.4 fails if we replace **NT** by **SNT**.

We now turn to the final segment **SNT**. In case of **NT** we could show that there are minimal pairs in **NT** whence **NT** is not a weak (hence not a strong) filter.

In case of **SNT** we leave the question whether there is a minimal pair of strongly nontrivial degrees as an open question. Even the weaker question whether or not **SNT** is a weak filter we have to leave open. In the following, however, we show that **SNT** is not a strong filter. In order to show this we need the following observation on E_1-bi-immune sets.

Theorem 8.14 *There are* E_1*-bi-immune sets* A_0 *and* A_1 *in* E *such that*

$$\forall\, B\ (B \leq^p_m A_0 \,\&\, B \leq^p_m A_1 \ \Rightarrow\ B \in \mathrm{E}_4) \tag{8.11}$$

Corollary 8.15 *The class* **SNT** *of the strongly nontrivial degrees in* **E** *is not a strong filter.*

PROOF OF COROLLARY 8.15. Fix A_0 and A_1 as in Theorem 8.14. By Theorem 5.7, A_0 and A_1 are strongly E-nontrivial whence, for $\mathbf{a}_i = deg^p_m(A_i)$, $\mathbf{a}_0, \mathbf{a}_1 \in$ **SNT**. Moreover, by (8.11), any set $B \leq^p_m A_0, A_1$ is strictly trivial (since, for any $C \leq^p_m B$, by transitivity of $\leq^p_m$, $C \leq^p_m A_0, A_1$ whence, by (8.11), $C \in \mathrm{E}_4$) hence E-trivial. So

$$\forall \mathbf{b} \in \mathbf{E}\ (\mathbf{b} \leq \mathbf{a}_0, \mathbf{a}_1 \Rightarrow \mathbf{b} \in \mathbf{T} \subseteq \mathbf{WT}).$$

□

PROOF OF THEOREM 8.14. By a slow diagonalization we construct sets $A_0, A_1 \in \mathrm{E}_4$ with the required properties. At stage s of the construction we determine the values of $A_0 \cap \Sigma^s$ and $A_1 \cap \Sigma^s$. At the same time we satisfy the highest priority requirement $\Re$ which has not yet been satisfied before and which can be satisfied.

Let $\{f_e : e \geq 0\}$ be an enumeration of the polynomial time computable functions with corresponding polynomial time-bounds p_e such that, for x with $|x| > e$, $f_e(x)$ can be uniformly computed in time $2^{|x|}$; and let $\{E^1_e : e \geq 0\}$ be an enumeration of E_1 such that, for x with $|x| > e$, $E_e(x)$ can be uniformly computed in time $2^{2|x|}$.

The requirements the set A has to meet are as follows (for $e = \langle e_0, e_1 \rangle$).

$$\begin{aligned}
\Re_{5e} = \Re^0_e :&\quad E^1_e \text{ infinite } \Rightarrow \exists\, x \in E^1_e\ (A_0(x) = 0)\\
\Re_{5e+1} = \Re^1_e :&\quad E^1_e \text{ infinite } \Rightarrow \exists\, x \in E^1_e\ (A_0(x) = 1)\\
\Re_{5e+2} = \Re^2_e :&\quad E^1_e \text{ infinite } \Rightarrow \exists\, x \in E^1_e\ (A_1(x) = 0)\\
\Re_{5e+3} = \Re^3_e :&\quad E^1_e \text{ infinite } \Rightarrow \exists\, x \in E^1_e\ (A_1(x) = 1)\\
\Re_{5e+4} = \Re^4_e :&\quad \exists^\infty x(|x| < |f_{e_0}(x)|\ \&\ |x| < |f_{e_1}(x)|) \Rightarrow\\
&\quad \exists x(A_0(f_{e_0}(x)) \neq A_1(f_{e_1}(x))).
\end{aligned}$$

We say that $\Re_m$ has *higher priority* than $\Re_{m'}$ if $m < m'$.

As one can easily check, requirements $\Re^0_e$ to $\Re^3_e$ guarantee E_1-bi-immunity of A_0 and A_1.

Assuming that $A_0, A_1 \in \mathrm{E}_4$, the requirements $\Re^4_e$, $(e \geq 0)$, imply (8.11) as follows. Given B such that $B \leq^p_m A_0, A_1$, fix e_0, e_1 such that $B \leq^p_m A_0$ via f_{e_0} and $B \leq^p_m A_1$ via f_{e_1}, i.e.

$$B = f^{-1}_{e_0}(A_0) = f^{-1}_{e_1}(A_1). \tag{8.12}$$

Then, for $e = \langle e_0, e_1 \rangle$, $\Re^4_e$ guarantees that

$$\exists^\infty x(|f_{e_0}| \leq |x| \text{ or } |f_{e_1}| \leq |x|) \tag{8.13}$$

since otherwise $f^{-1}_{e_0}(A_0) \neq f^{-1}_{e_1}(A_1)$ contrary to (8.12).

So, given x sufficiently large, in order to compute $B(x)$ it suffices to compute $f_{e_0}(x)$ and $f_{e_1}(x)$ (in polynomial time) and, for $i \leq 1$ minimal such that $|f_{e_i}| \leq |x|$, $A_i(f_{e_i})$. By $A_i \in \mathrm{E}_4$ and $|f_{e_i}| \leq |x|$ the latter can be done in $O(2^{4|x|})$ steps. So $B \in \mathrm{E}_4$.

We now turn to the construction. It suffices to describe stage $s \geq 0$ of the construction.

Stage s. We say that requirement $\Re^i_e$ *requires attention at stage s* if $e < |z_s|$, $\Re^i_e$ has not been active at any previous stage, and, depending on $i \leq 4$, the following hold:

If $i = 0, 1, 2, 3$ then

$$\exists x \in \Sigma^s\ (x \in E^1_e) \tag{8.14}$$

and if $i = 4$ then

$$\exists y \in \Sigma^{<s} \exists i \leq 1 (f_{e_i}(y) \in \Sigma^s\ \&\ f_{e_{1-i}}(y) \in \Sigma^{\leq s}) \tag{8.15}$$

where $e = \langle e_0, e_1 \rangle$.

Fix the highest priority requirement $\mathfrak{R}_m$ which requires attention at stage s. (If no requirement requires attention, let $A_0(x) = 0$, $A_1(x) = 0$ for all $x \in \Sigma^s$ and end stage s.) We say that $\mathfrak{R}_m$ is *active* at stage s and, depending on the type of $\mathfrak{R}_m$ we do the following

- If $\mathfrak{R}_m = \mathfrak{R}^0_e$ or $\mathfrak{R}_m = \mathfrak{R}^2_e$ then let $A_0(x) = A_1(x) = 0$ for all $x \in \Sigma^s$.
- If $\mathfrak{R}_m = \mathfrak{R}^1_e$ or $\mathfrak{R}_m = \mathfrak{R}^3_e$ then let $A_0(x) = A_1(x) = 1$ for all $x \in \Sigma^s$.
- If $\mathfrak{R}_m = \mathfrak{R}^4_e$ where $e = \langle e_0, e_1 \rangle$, fix $y \in \Sigma^{<s}$ minimal such that $f_{e_i}(y) \in \Sigma^s$ and $f_{e_{1-i}}(y) \in \Sigma^{\leq s}$.

  If $|f_{e_{1-i}}| < s$ then let

  $$A_0(x) = A_1(x) = 1 - A_{1-i}(f_{e_{1-i}}(y))$$

  for all $x \in \Sigma^s$ and if $|f_{e_{1-i}}| = s$ then let

  $$A_0(x) = 0 \text{ and } A_1(x) = 1$$

  for all $x \in \Sigma^s$.

This completes the construction.

The verification is standard. Note that if $\mathfrak{R}_m$ becomes active at some stage s then $\mathfrak{R}_m$ is met. Moreover, since any requirement acts at most once, any requirement with correct hypothesis will eventually become active. So all requirements are met.

Finally, knowing

- $A_0 \cap \Sigma^{<s}$ and $A_1 \cap \Sigma^{<s}$
- which requirement has been active prior to stage s

in $O(2^{3s})$ steps we can tell which requirements require attention at stage s, which requirement becomes active (if any), and how $A_0 \cap \Sigma^s$ and $A_1 \cap \Sigma^s$ are defined. So, by induction,

$$A_0, A_1 \in \mathrm{DTIME}(O(n \cdot 2^{3n})) \subseteq \mathrm{E}_4.$$

□

8.2.2 Further Properties of WT and SNT

We now look at the analogs of some of the questions discussed for **T** and **NT** in Section 8.1.3.

We first discuss the question of maximal and minimal elements. As in case of (non)triviality we show that the class **WT** does not posses maximal elements and the class **SNT** does not possess minimal elements. Here, however, the proofs are somewhat more sophisticated than in case of (non)triviality.

Theorem 8.16 *The class* **WT** *has no maximal elements. I.e., for any degree* $\mathbf{a} \in$ **WT** *there is a degree* $\mathbf{b} \in \mathbf{WT}$ *such that* $\mathbf{a} < \mathbf{b}$.

The corresponding result for **T** used the closure of this class under join. Since **WT** does not have this closure property, we first have to remedy this by observing the following mixed join lemma for **T** and **WT**.

Lemma 8.17 *Let* $A, B \in \mathrm{E}$ *be given such that* A *is* E*-trivial and* B *is weakly* E*-trivial. Then* $A \oplus B$ *is weakly* E*-trivial.*

PROOF (SKETCH). Fix k such that

$$\mathrm{P}_m(A) \cap \mathrm{E} \subseteq \mathrm{E}_k \tag{8.16}$$

and such that

$$\forall X \in \mathrm{P}_m(B) \cap \mathrm{E}\ (X \text{ not } \mathrm{E}_k\text{-bi-immune}) \tag{8.17}$$

hold. It suffices to show that there is no E_k-bi-immune set in E which can be *p-m*-reduced to $A \oplus B$.

For a contradiction assume that $C \in \mathrm{E}$ is E_k-bi-immune and $C \leq^p_m A \oplus B$. By the latter and by the Distributivity Lemma (Lemma 2.8) there is a set $D \in \mathrm{P}$ such that, for $C_1 = C \cap D$ and $C_2 = C \cap \overline{D}$, $C_1, C_2 \in \mathrm{E}$ and $C_1 \leq^p_m A$ and $C_2 \leq^p_m B$. It follows, by (8.16), that $C_1 \in \mathrm{E}_k$. Since $C_1 \subseteq C$, by E_k-bi-immunity of C this implies that C_1 is finite. So C_2 is a finite variant of C. Since the class of E_k-bi-immune sets is closed under finite variants, it follows that C_2 is E_k-bi-immune. But this contradicts (8.17). □

PROOF OF THEOREM 8.16. Given an incomplete weakly E-trivial set $A \in \mathrm{E}$, we have to find a weakly E-trivial set $B \in \mathrm{E}$ such that $A <^p_m B$. This is achieved as follows. By unboundedness of **T** there is an E-trivial set $\hat{B} \in \mathrm{E}$ such that $\hat{B} \not\leq^p_m A$. So, for $B = A \oplus \hat{B}$, $B \in \mathrm{E}$, $A <^p_m B$, and, by Lemma 8.17, B is weakly E-trivial. □

Having shown that there are no maximal weakly trival degrees we now prove the dual result for the strongly nontrivial degrees. This requires the following observation on E_1-bi-immune sets in E which is of interest by itself.

Theorem 8.18 *Let* $k, k' \geq 1$ *and let* $A \in \mathrm{E}$ *be* E_k*-bi-immune. There is an* $\mathrm{E}_{k'}$*-bi-immune set* $B \in \mathrm{E}$ *such that* $B <^p_m A$.

Corollary 8.19 *The class* **SNT** *of the strongly nontrivial degrees does not possess minimal elements. In fact, for any strongly nontrivial set A (not necessarily in* E*) there is a strongly nontrivial set $B \in \mathrm{E}$ such that $B <_m^p A$.*

PROOF OF COROLLARY 8.19. Let A be any strongly nontrivial set (not necessarily in E). By definition of strong nontriviality, there is an E_2-bi-immune set $A' \in \mathrm{E}$ such that $A' \leq_m^p A$. Moreover, by the Theorem 8.18, there is an E_1-bi-immune set $B \in \mathrm{E}$ such that $B <_m^p A'$, hence $B <_m^p A$. By the characterization theorem for strong nontriviality, B is strongly nontrivial. □

We now turn to the proof of Theorem 8.18. By the expansion theorem for bi-immunity (Theorem 5.6) it suffices to prove the following lemma.

Lemma 8.20 *Let $A \in \mathrm{E}_k$ be E_2-bi-immune ($k \geq 3$). There is an E_1-bi-immune set $B \in \mathrm{E}$ such that $B <_m^p A$.*

PROOF (SKETCH). Let

$$x_n = 0^{k^n}$$

and

$$I_n = \{y : k^{2n} \leq |y| < k^{2n+2}\}.$$

(Actually add λ to I_0 in order to make sure that the sets I_n give a partition of Σ^* into finite intervals.) The desired set B is defined by specifying B on I_n ($n \geq 0$) as follows.

$$\forall\, y \in I_n\ [B(y) = A(x_{2n+3})]$$

To show that B has the required properties, it suffices to establish the following claims.

Claim 1. $B \leq_m^p A$.

Proof (sketch). Define f by letting $f(y) = x_{2n+3}$ for $y \in I_n$. Then, as one can easily check, f is polynomial-time computable and $B \leq_m^p A$ via f.

Claim 2. $B \in \mathrm{E}$.

Proof (sketch). Note that, for f as in the proof of Claim 1, $|f(y)| \leq k^3|y|$. So, by $B \leq_m^p A$ via f and by $A \in \mathrm{E}_k$, $B \in \mathrm{E}_{k^4}$.

Claim 3. B is E_1-bi-immune.

Proof (sketch). For a contradiction assume that B is not E_1-bi-immune. By symmetry, w.l.o.g. we may fix an infinite subset S of B such that $S \in \mathrm{E}_1$. Let

$$\hat{S} = \{x_{2n+3} : S \cap I_n \neq \emptyset\}.$$

Then, by infinity of S, $\hat{S}$ is infinite too, and, by $S \subseteq B$ and by definition of B, $\hat{S}$ is a subset of A. Moreover, $\hat{S} \in \mathrm{E}_2$. (Namely, given x, in polynomial time we can check whether $x = x_{2n+3}$ for some n and if so compute the corresponding n. Now if x is not of this form then $x \notin \hat{S}$. If $x = x_{2n+3}$ then $x \in \hat{S}$ if and only if

$$\exists y \in I_n \ (y \in S).$$

Now, since $|I_n| \leq 2^{|x|}$, since any string $y \in I_n$ has length $< |x|$, and since $S \in \mathrm{E}_1$, the latter can be checked in $\leq 2^n \cdot 2^n = 2^{2n}$ steps.) It follows that A is not E_2-bi-immune contrary to assumption.

Claim 4. $A \not\leq^p_m B$.

Proof (sketch). For a contradiction assume that $A \leq^p_m B$ via g. We will show that A is not E_1-bi-immune contrary to assumption.

Define $\hat{g}$ by letting $\hat{g}(x)$ be the unique number n such that $g(x) \in I_n$. Note that $\hat{g}$ can be computed in polynomial time. Moreover, by definition of B,

$$A(x) = B(g(x)) = A(x_{2\hat{g}(x)+3})$$

whence, in particular,

$$B(g(x_{2n+2})) = A(x_{2n+2}) = A(x_{2\hat{g}(x_{2n+2})+3}) \tag{8.18}$$

for all $n \geq 1$. Distinguish the following two cases depending on whether

$$\exists^\infty n \ (\hat{g}(x_{2n+2}) < n) \tag{8.19}$$

holds or not.

Case 1: (8.19) *holds.* Then

$$D = \{x_{2n+2} : \hat{g}(x_{2n+2}) < n\}$$

is infinite.

By symmetry, w.l.o.g. we may assume that there are infinitely many strings x in D such that $g(x) \in B$, i.e., that

$$\hat{D} = \{x \in D : g(x) \in B\}$$

is infinite. Since, by $A \leq^p_m B$ via g, $\hat{D} \subseteq A$, we will get the desired contradiction by showing that $\hat{D} \in \mathrm{E}_1$.

Given x, $\hat{D}(x)$ can be computed in $O(2^{|x|})$ steps as follows. First decide whether $x \in D$ and, if so, compute the unique numbers n and $e < n$ such that $x = x_{2n+2}$ and $\hat{g}(x) = e$. Note that this can be done in polynomial time. Moreover, if $x \notin D$ then, obviously, $\hat{D}(x) = 0$. So, in the following, we may assume $x = x_{2n+2}$ and $\hat{g}(x) = e < n$. Then, by (8.18),

$$\hat{D}(x) = \hat{D}(x_{2n+2}) = B(g(x_{2n+2})) = A(x_{2e+3}).$$

So it suffices to compute $A(x_{2e+3})$. By $A \in \mathrm{E}_k$, this can be done in $O(2^{k|x_{2e+3}|})$ steps. But - since, by $e < n$, $2e+4 \leq 2n+2$ - it follows by definition of x_m that

$$k|x_{2e+3}| = |x_{2e+4}| \leq |x_{2n+2}| = |x|$$

whence $O(2^{k|x_{2e+3}|}) \leq O(2^{|x|})$.

Case 2: (8.19) *fails.* By failure of (8.19),

$$D' = \{x_{2n+2} : \hat{g}(x_{2n+2}) \geq n\}$$

is infinite. So

$$D'' = \{x_{2m+3} : \exists\, n \leq m\ (\hat{g}(x_{2n+2}) = m)\}$$

is infinite too. In fact, by symmetry, w.l.o.g. we may assume that $\tilde{D} = D'' \cap A$ is infinite. So, in order to get the desired contradiction, it suffices to show that $\tilde{D} \in \mathrm{E}_1$.

Now, given x, $\tilde{D}(x)$ can be computed in $O(2^{|x|})$ steps as follows. First decide whether $x \in D''$ and, if so, compute the unique number m such that $x = x_{2m+3}$ and the least $n \leq m$ such that $\hat{g}(x_{2n+2}) = m$. Then

$$\begin{array}{rcll} \tilde{D}(x) & = & \tilde{D}(x_{2m+3}) & \text{(by } x = x_{2m+3}\text{)} \\ & = & A(x_{2m+3}) & \text{(by Definition of } \tilde{D} \text{ and by } x_{2m+3} \in D''\text{)} \\ & = & A(x_{2n+2}) & \text{(by } \hat{g}(x_{2n+2}) = m \text{ and by (8.18))} \end{array}$$

So it only remains to compute $A(x_{2n+2})$. But this can be done in $O(2^{|x|})$ steps. (Namely, by $n \leq m$, $2n+2 < 2m+3$, whence, by definition, $k|x_{2n+2}| \leq |x_{2m+3}| = |x|$. So the claim follows from $A \in \mathrm{E}_k$.)

This completes the proof of Claim 4 and the proof of Lemma 8.20. □

Having shown that **WT** has no maximal elements and **SNT** has no minimal elements, we will now show that these classes do not have any nontrivial upper bounds and lower bounds, respectively, i.e., that

$$\forall\, \mathbf{a} < \mathbf{1}\ \exists\, \mathbf{b} \in \mathbf{WT}\ (\mathbf{b} \not\leq \mathbf{a}) \tag{8.20}$$

and

$$\forall\, \mathbf{a} > \mathbf{0}\ \exists\, \mathbf{b} \in \mathbf{SNT}\ (\mathbf{b} \not\geq \mathbf{a}) \tag{8.21}$$

hold.

In fact, since $\mathbf{T} \subseteq \mathbf{WT}$, the former is a direct consequence of our previous observation that $\mathbf{T}$ has no nontrivial upper bounds (Theorem 8.9). For a proof of the latter we will need the following observation on the distribution of the E_1-bi-immune sets in E.

Lemma 8.21 *For any computable set $A \notin \mathrm{P}$ there is an E_1-bi-immune set B in* E *such that $A \not\leq^p_m B$.*

Before we give a proof of Lemma 8.21 we show how this lemma implies (8.21) thereby refining Theorem 8.10.

Theorem 8.22 *For any* E*-degree* $\mathbf{a} > \mathbf{0}$ *there is a degree* $\mathbf{b} \in \mathbf{SNT}$ *such that* $\mathbf{a} \not\leq \mathbf{b}$.

PROOF. Fix an E-degree $\mathbf{a} > \mathbf{0}$ and let A be a set in $\mathbf{a}$. By Lemma 8.21 there is an E_1-bi-immune set B in E such that $A \not\leq^p_m B$. By the characterization theorem of strong E-nontriviality, B is strongly E-nontrivial. So $\mathbf{b} = deg^p_m(B)$ has the required properties. □

Lemma 8.21 can be proven by a delayed diagonalization argument. In fact, in the literature, there are various generic diagonalization lemmas capturing certain types of delayed diagonalizations. One on these lemmas given in Ambos-Spies (1988) can be used to simplify the proof of Lemma 8.21.

Lemma 8.23 *(Ambos-Spies (1988)) Let D be a computable set and let* C *be a uniformly computable class which is closed under finite variants such that $D \notin$* C*. There is a computable function $g_0 : \mathbb{N} \to \mathbb{N}$ such that, for any computable function g dominating g_0, the following holds. If B is a computable set such that B and D are g*-similar*, i.e.,*

$$\exists^\infty n \geq 0\,(B \cap [0^n, 0^{g(n)}) = D \cap [0^n, 0^{g(n)})), \tag{8.22}$$

then $B \notin$ C.

PROOF OF LEMMA 8.21. Fix a computable set $A \notin$ P. Then

$$\mathrm{C} = \mathrm{EXP} \cap \{B : A \leq^p_m B\} = \{B : A \leq^p_m B \leq^p_m C\}$$

(where C is any EXP-complete set) is uniformly computable and closed under finite variants (see e.g. Corollary 3.5 in Ambos-Spies (1988)) and $\emptyset \notin$ C. So, by Lemma 8.23, we may fix a strictly increasing time-constructible function g such that, for any set $B \in$ E satisfying

$$\exists^\infty n \geq 0\,(B \cap [0^n, 0^{g(n)}) = \emptyset), \tag{8.23}$$

$B \notin$ C, hence $A \not\leq^p_m B$. So it suffices to construct an E_1-bi-immune set B in E satisfying (8.23). This is done by a straightforward variant of the standard construction of an E_1-bi-immune set B by a slow diagonalization (where $B(z_s)$ is defined at stage s). It suffices to intertwine the bi-immunity requirements

$$\mathfrak{R}^1_e : E^1_e \text{ infinite } \Rightarrow B \cap E^1_e \neq \emptyset$$

$$\mathfrak{R}^2_e : E^1_e \text{ infinite } \Rightarrow \overline{B} \cap E^1_e \neq \emptyset$$

with requirements

$$\mathfrak{R}^3_e : \exists\, n \geq e\,(B \cap [0^n, 0^{g(n)}) = \emptyset).$$

Requirement $\mathfrak{R}^3_e$ is declared *satisfied* at stage s if, for some $n < s$, $n \geq e$ and $0^{g(n)} \leq z_s$ and $B \cap [0^n, 0^{g(n)}) = \emptyset$; and $\mathfrak{R}^3_e$ *requires attention* at stage s if $e \leq s$ and $\mathfrak{R}^3_e$ is not yet satisfied. Note that the action required for meeting $\mathfrak{R}^3_e$ is finitary, hence goes along with the basic strategy for meeting the bi-immunity requirements. Moreover, by choice of g, the question whether $\mathfrak{R}^3_e$ is satisfied at stage s or requires attention at stage s can be decided in $O(2^{c \cdot |z_s|})$ steps (where c does not depend on e).

We leave it to the reader to give the complete construction. □

We conclude this chapter with a Sandwich Theorem for the three layers **T**, **I** and **SNT** of **E**.

Theorem 8.24 *(i) Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be* E*-degrees such that* $\mathbf{a} \in \mathbf{T}$*,* $\mathbf{b} \in \mathbf{SNT}$ *and* $\mathbf{a} < \mathbf{b}$*. There is an* E*-degree* $\mathbf{c} \in \mathbf{I}$ *such that* $\mathbf{a} < \mathbf{c} < \mathbf{b}$*.*

(ii) Let $\mathbf{a} \in \mathbf{I}$*. There are p-m-degrees* $\mathbf{a}_{--} \in \mathbf{T}$*,* $\mathbf{a}_{-}, \mathbf{a}_{+} \in \mathbf{I}$*, and* $\mathbf{a}_{++} \in \mathbf{SNT}$ *such that*

$$\mathbf{0} < \mathbf{a}_{--} < \mathbf{a}_{-} < \mathbf{a} < \mathbf{a}_{+} < \mathbf{a}_{++} < \mathbf{1}.$$

PROOF. (i) Since the classes **T**, **I** and **SNT** are pairwise disjoint it suffices to give a degree $\mathbf{c} \in \mathbf{I}$ such that $\mathbf{a} \leq \mathbf{c} \leq \mathbf{b}$. By Theorem 8.13, split $\mathbf{b}$ into two degrees $\mathbf{b}_1, \mathbf{b}_2 \in \mathbf{WT}$. By Theorem 8.3, w.l.o.g., $\mathbf{b}_1$ is not trivial, hence in **I**. It follows with the mixed join lemma (Lemma 8.17) that $\mathbf{c} = \mathbf{a} \vee \mathbf{b}_1$ has the required properties.

(ii) Since $\mathbf{0} \in \mathbf{T}$ and $\mathbf{a} \in \mathbf{I} \subseteq \mathbf{NT}$, degrees $\mathbf{a}_{--}$ and $\mathbf{a}_{-}$ with the required properties are provided by Theorem 8.7. The existence of a strongly nontrivial degree $\mathbf{a}_{++}$ such that $\mathbf{a} < \mathbf{a}_{++} < \mathbf{1}$ follows from Lemma 8.12 and the characterization theorem for strong nontriviality. Finally, in order to get a degree $\mathbf{a}_{+}$ with the required properties it suffices to prove the following fact.

Let $\mathbf{b}$ and $\mathbf{c}$ be E-degrees such that $\mathbf{b} \in \mathbf{I}$, $\mathbf{c} \in \mathbf{SNT}$ and $\mathbf{b} < \mathbf{c}$. There is an E-degree $\mathbf{d} \in \mathbf{I}$ such that $\mathbf{b} < \mathbf{d} < \mathbf{c}$.

This fact is proven as follows. Since the classes **I** and **SNT** are disjoint it suffices to give a degree $\mathbf{d} \in \mathbf{I}$ such that $\mathbf{b} < \mathbf{d} \leq \mathbf{c}$. By Theorems 4.13 and 4.14 there is a trivial degree $\mathbf{e}$ such that $\mathbf{e} < \mathbf{c}$ and $\mathbf{e} \not\leq \mathbf{b}$. So, for $\mathbf{d} = \mathbf{b} \vee \mathbf{e}$, $\mathbf{b} < \mathbf{d} \leq \mathbf{c}$ and, by Lemma 8.17, $\mathbf{d} \in \mathbf{I}$.

□

CHAPTER 9

Nontriviality with Respect to Other Reducibilities

In this final chapter we look at our nontriviality notions under other polynomial-time reducibilities than p-m-reducibility. We will focus on nontriviality and strong nontriviality for E and we will consider these properties for sets in E, i.e., study these nontriviality notions as weak *completeness* (not hardness) notions. The reducibilities we will consider are the polynomial-time bounded versions of 1-li, 1, m-li, m, k-tt ($k \geq 1$), btt, tt, T (see Section 2.3.3).

The question we are interested is to find out whether the strength of r-E-nontriviality or strong r-E-nontriviality depends on the unerlying polynomial reducibility $\leq^p_r$. For instance, if we replace p-r-reducibility by the strictly weaker p-r'-reducibility, do we get more E-nontrivial sets (or more strongly E-nontrivial sets)?

Recall that for E-completeness the correponding questions have been solved by Berman, Homer et al., and Watanabe (see Theorems 2.17 and 2.18). Moreover, Ambos-Spies et al. (1996a) have compared measure-completeness for E under various polynomial-time reducibilities.

Our goal will be to complete the following diagram or, where we cannot do this, to isolate the relevant open problems.

$$\begin{tikzcd}
A\ 1\text{-}li\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Leftrightarrow] & A\ 1\text{-}li\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ 1\text{-}li\text{-E-nt} \arrow[d, Rightarrow] \\
A\ 1\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Leftrightarrow] & A\ 1\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ 1\text{-E-nt} \arrow[d, Rightarrow] \\
A\ m\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Leftrightarrow] & A\ m\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ m\text{-E-nt} \arrow[d, Rightarrow] \\
A\ 1\text{-}tt\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ 1\text{-}tt\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ 1\text{-}tt\text{-E-nt} \arrow[d, Rightarrow] \\
A\ k\text{-}tt\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-E-nt} \arrow[d, Rightarrow] \\
A\ (k+1)\text{-}tt\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-E-nt} \arrow[d, Rightarrow] \\
A\ btt\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ btt\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ btt\text{-E-nt} \arrow[d, Rightarrow] \\
A\ tt\text{-E-cpl} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-E-snt} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-E-nt} \arrow[d, Rightarrow] \\
A\ T\text{-E-cpl} \arrow[r, Rightarrow] & A\ T\text{-E-snt} \arrow[r, Rightarrow] & A\ T\text{-E-nt}
\end{tikzcd} \tag{9.1}$$

Here A is a set in the linear exponential time class E and k is a number ≥ 2. Moreover, r-E-cpl, r-E-snt, and r-E-nt abbreviate p-r-complete for E, strongly nontrivial for E under p-reducibility, and nontrivial for E under p-reducibility, respectively.

Then the left-right implications ($\Rightarrow$) and the top-down implications ($\Downarrow$) are immediate by definition while the upward implications in the first column reflect the collapse result for completeness under the 1-query reducibilities due to Berman and Homer et al. which are summarized in Theorem 2.18. Moreover, by Watanabe

(1987), none of the other downward arrows in the first column can be reversed (see Theorem 2.17).

After explaining some of our notations in more detail and giving some basic facts on the new notions (Section 9.1) we will proceed as follows.

- First we show that there are no implications from right to left (Section 9.2).
- Second we look at the 1-query reducibilities, i.e., at *m*, the strengthenings of *m* (*m*-*li*, 1 and 1-*li*), and at 1-*tt* (Sections 9.3 and 9.4)
- Third we look at the multi-query reducibilities (Section 9.5) and summarize the results for the various E-nontriviality and strong E-nontriviality notions (Section 9.6).
- Finally, we look at the corresponding questions for EXP and reveal a surprising difference in the strength of some concepts in the cases of E and EXP (Section 9.7).

9.1 *r*-E-Nontriviality and Strong *r*-E-Nontriviality

In the following let *r* stand for any reducibilities 1-*li*, 1, *m*-*li*, *m*, *k*-*tt* ($k \geq 1$), *btt*, *tt* or *T* and let *p*-*r* denote the corresponding polynomial-time reducibility (see Section 2.3.3).

Definition 9.1 (a) A set *A* is *p*-*r*-*trivial for* E (or *r*-E-*trivial* for short) if

$$\exists\, k \geq 1\ [\mathrm{P}_r(A) \cap \mathrm{E} \subseteq \mathrm{E}_k] \tag{9.2}$$

holds, and *A* is *p*-*r*-*nontrivial for* E (or *r*-E-*nontrivial* for short) otherwise.

(b) A set *A* is *strongly p*-*r*-*nontrivial for* E (or *strongly r*-E-*nontrivial* or *r*-E-*snt* for short) if

$$\forall\, k \geq 1\ \exists\, B\ (B \in \mathrm{P}_r(A) \cap \mathrm{E}\ \&\ B\ \mathrm{E}_k\text{-bi-immune}) \tag{9.3}$$

holds; and *A* is *weakly p*-*r*-*trivial for* E (or *weakly r*-E-*trivial* for short) otherwise.

Nontriviality and strong nontriviality for EXP under *p*-*r*-reducibility are defined correspondingly and are denoted and abbreviated correspondingly.

For the analysis of strong *r*-E-nontriviality it is useful to note that the characterization theorem of strong *m*-E-nontriviality (and strong *m*-EXP-nontriviality) can be extended to the other reducibilities. In order to show this, we first observe that the expansion theorem for bi-immunity (Theorem 5.6) actually holds for *p*-1-*li*-reducibility in place of *p*-*m*-reducibility.

Theorem 9.2 *Let A be E_1-bi-immune. Then, for any $k \geq 1$, there is an E_k-bi-immune set A_k and an EXP_k-bi-immune set A'_k such that $A_k, A'_k \in \mathrm{P}_{1\text{-}li}(A)$. If moreover $A \in \mathrm{E}$ then the sets A_k can be chosen such that $A_k \in \mathrm{P}_{1\text{-}li}(A) \cap \mathrm{E}$.*

PROOF. It suffices to note that the sets $A_k = \{x : 0^{k|x|}1x \in A\}$ and $A'_k = \{x : 0^{|x|^k}1x \in A\}$ introduced in the proof of Theorem 5.6 are p-1-li-reducible to A. □

Now, Theorem 9.2 easily implies the generalized characterization theorem.

Theorem 9.3 (Characterization Theorem for Strong r-E-Nontriviality and Strong r-EXP-Nontriviality)

The following are equivalent.

1. *A is strongly r-E(EXP)-nontrivial.*

2. *There is an E_1-bi-immune set $B \in \mathrm{E}$ ($B \in \mathrm{EXP}$) such that $B \leq^p_r A$.*

Corollary 9.4 *Let $A \in \mathrm{E}$ ($A \in \mathrm{EXP}$) be E_1-bi-immune. Then A is strongly r-E(EXP)-nontrivial.*

PROOF. We consider the case of E. Note that it suffices to consider $r = 1\text{-}li$. So, by Theorem 9.3, it suffices to show that there is an E_1-bi-immune set B in E such that $B \leq^p_{1\text{-}li} A$. But such a set exists by Theorem 9.2. (Note that $\leq^p_{1\text{-}li}$ is not reflexive. So we have to apply Theorem 9.2 here. We cannot argue that A is E_1-bi-immune and $A \leq^p_{1\text{-}li} A$.) □

9.2 Nontriviality vs. Strong Nontriviality and Strong Nontriviality vs. Completeness

Here we will show that in diagram (9.1) no implications from right to left can be added. It suffices to show

$$\exists\, A \in \mathrm{E}\ (A \text{ 1-}li\text{-E-nontrivial} \;\&\; A \text{ weakly } T\text{-E-trivial}) \tag{9.4}$$

$$\exists\, A \in \mathrm{E}\ (A \text{ strongly 1-}li\text{-E-nontrivial} \;\&\; A \text{ not } T\text{-E-complete}). \tag{9.5}$$

Theorem 9.5 *There is a set $A \in \mathrm{E}$ such that A is 1-li-E-nontrivial but A is not strongly T-E-nontrivial.*

The proof of Theorem 9.5 is immediate by the following two lemmas generalizing Theorems 4.37 and 5.14, respectively.

Lemma 9.6 *Any exptally set $A \in \mathrm{E} \setminus \mathrm{E}_1$ is 1-li-E-nontrivial.*

PROOF. Given $k \geq 0$, we have to show that there is a set $B \leq^p_{1-li} A$ such that $B \in \mathrm{E} \setminus \mathrm{E}_k$. Let $B = \{0^{\delta_k(n)} : 0^{\delta(n)} \in A \;\&\; n \geq n_0\}$ where $\delta_k(n)$ is the least number m such that $(k+1)m \geq \delta(n)$ and n_0 is chosen so that $\delta_k(n)$ is one-to-one for $n \geq n_0$. As one can easily check, $B \leq^p_m A$ and moreover, since $|0^{\delta_k(n)}| < |0^{\delta(n)}|$, $B \leq^p_{1-li} A$. □

Lemma 9.7 *No exptally set $A \in \mathrm{E} \setminus \mathrm{E}_1$ is strongly T-E-nontrivial.*

PROOF. Let $A \in \mathrm{E} \setminus \mathrm{E}_1$ be exptally. Then, given a set C and polynomial-time bounded oracle Turing Machine M such that $C \leq^p_T A$ via M, it suffices to show that C is not E_1-bi-immune. In fact, we will show that C is not P-bi-immune. For this sake we will define an infinite set $D \in \mathrm{P}$ such that, for $x \in D$, $C(x)$ can be decided in polynomial time.

Fix k such that $A \in \mathrm{E}_k$ and a polynomial p such that p is a time bound for M (where w.l.o.g. $p(n) \geq n$ for all n). Moreover, let $q(n)$ be the greatest number m such that

$$\delta(n) \leq m < 2^{\delta(n)} = \delta(n+1)$$

and let $q(n) = 0$ if no such m exists. Note that we may fix n_0 such that, for all $n \geq n_0$,

$$\delta(n) \leq q(n) \leq p(q(n)) < 2^{\delta(n)} = \delta(n+1) \leq p(q(n)+1) \tag{9.6}$$

holds. (Note that $\delta(n+1) \leq p(q(n)+1)$ follows from maximality of m.)

Now the set D is defined by

$$D = \{0^{q(n)} : n \geq 0\}.$$

By time-constructability of q, D is polynomial-time computable and, given $x \in D$, in polynomial time we can compute the unique number n such that $x = 0^{q(n)}$.

Now in order to decide whether such a string $x = 0^{q(n)}$ with $n \geq n_0$ is in C, we run the machine M with input $0^{q(n)}$ and emulate the oracle for this machine as follows. Given query y. We decide whether y is a string $0^{\delta(s)}$ for some s, and if so, fix the corresponding s. (Note that this can be done in polynomial time). Now, if y does not have this form, then y is not an element of the exptally set A, hence return 0. Otherwise, fix m such that $y = 0^{\delta(m)}$. Since $|y| < p(|x|) = p(q(n))$, it follows by (9.6) that $s \leq n$ and therefore

$$\delta(s) \leq \delta(n) \leq p(q(n)+1).$$

So, by $A \in \mathrm{E}_k$, $A(y)$ can be computed in time

$$2^{k|y|} = 2^{k\delta(s)} = (2^{\delta(s)})^k \leq p(q(n)+1)^k = p(|x|+1)^k.$$

Hence each query of the oracle machine M with input $0^{q(n)}$ can be computed in polynomial time. Since M is polynomial-time-bounded, the number of queries is also bounded by some polynomial. Hence $C(x)$ for $x \in D$ can be computed in polynomial time. □

Theorem 9.8 *There is a set $A \in \mathrm{E}$ such that A is strongly 1-li-E-nontrivial but A is not T-E-complete.*

PROOF (IDEA). By Corollary 9.4 it suffices to show that there is an E_1-bi-immune set in E which is not p-T-complete for E. Now, in Lemma 8.12 we have shown that there is an E_1-bi-immune set in E which is not p-m-complete, and the proof given there can be easily adapted to p-T-reducibility in place of p-m-reducibility. □

9.3 Nontriviality Under 1-Query Reducibilities

Now we will compare the nontriviality notions for E under the 1-query reducibilities. As we will show first, 1-tt-nontriviality, m-triviality and m-li-triviality coincide for E.

Lemma 9.9 *Let $A \in \mathrm{E}$ be 1-tt-nontrivial for E. Then A is m-nontrivial for E.*

PROOF. Given k, we have to show that there is a set $B \in \mathrm{E} \setminus \mathrm{E}_k$ such that $B \leq^p_m A$. By 1-tt-nontriviality of A we may pick $C \in \mathrm{E} \setminus \mathrm{E}_k$ such that $C \leq^p_{1\text{-}tt} A$, say $C \leq^p_{1\text{-}tt} A$ via the selector function g and the evaluator h. Then,

$$C(x) = \begin{cases} A(g(x)) & \text{if } h(x,0) < h(x,1) \\ 1 - A(g(x)) & \text{if } h(x,0) > h(x,1) \\ 0 & \text{if } h(x,0) = h(x,1) = 0 \\ 1 & \text{if } h(x,0) = h(x,1) = 1. \end{cases}$$

Now let

$$B(x) = \begin{cases} 1 - C(x) & \text{if } h(x,0) > h(x,1) \\ C(x) & \text{otherwise.} \end{cases}$$

Then, as one can easily check, $B \in \mathrm{E} \setminus \mathrm{E}_k$. Moreover, $B \leq^p_m A$ via the function f defined by

$$f(x) = \begin{cases} g(x) & \text{if } h(x,0) \neq h(x,1) \\ y_0 & \text{if } h(x,0) = h(x,1) = 0 \\ y_1 & \text{if } h(x,0) = h(x,1) = 1. \end{cases}$$

where y_0 and y_1 are fixed strings such that $y_0 \notin A$ and $y_1 \in A$. □

Lemma 9.10 *Let $A \in \mathrm{E}$ be m-nontrivial for E. Then A is m-li-nontrivial for E.*

PROOF. Given k, we have to show that there is a set $B \in \mathrm{E} \setminus \mathrm{E}_k$ such that $B \leq^p_{m\text{-}li} A$. Fix $k' \geq k$ such that $A \in \mathrm{E}_{k'}$ and, by m-nontriviality of A, pick $C \in \mathrm{E} \setminus \mathrm{E}_{k'}$ such that $C \leq^p_m A$, say $C \leq^p_m A$ via f.

Let
$$D = \{x : |f(x)| > |x|\}.$$

Note that $D \in \mathrm{P}$. Moreover, by $C(x) = A(f(x))$ and $A \in \mathrm{E}_{k'}$, for $x \notin D$, $C(x)$ can be computed in $O(2^{k'|x|})$ steps. So, by $C \notin \mathrm{E}_{k'}$, $C \cap D \notin \mathrm{E}_{k'}$.

Now define B by letting
$$B(x) = \begin{cases} C(x) & \text{if } x \in D \\ A(x0) & \text{otherwise.} \end{cases}$$

Then $B \leq^p_{m\text{-}li} A$ via
$$g(x) = \begin{cases} f(x) & \text{if } x \in D \\ x0 & \text{otherwise.} \end{cases}$$

Moreover, as one can easily check, $B \in \mathrm{E}$ but, by $B \cap D = C \cap D$, $B \notin \mathrm{E}_{k'}$. So $B \in \mathrm{E} \setminus \mathrm{E}_k$. □

Theorem 9.11 *For any set $A \in \mathrm{E}$ the following are equivalent.*

1. *A is m-li-nontrivial for* E.
2. *A is m-nontrivial for* E.
3. *A is* 1*-tt-nontrivial for* E.

PROOF. The nontrivial implications hold by Lemmas 9.10 and 9.9. □

The question whether m-E-nontriviality and 1-E-nontriviality coincide too seems to be more serious. As we we will show next, assuming P = PSPACE, we obtain the following collapse.

Lemma 9.12 *Assume* P = PSPACE. *Let $A \in \mathrm{E}$ be m-nontrivial for* E. *Then A is* 1*-li-nontrivial for* E.

PROOF. Given k, we have to show that there is a set $B \in \mathrm{E} \setminus \mathrm{E}_k$ such that $B \leq^p_{1\text{-}li} A$. Fix $k' \geq k$ such that $A \in \mathrm{E}_{k'}$ and, by m-nontriviality of A, pick $C \in \mathrm{E} \setminus \mathrm{E}_{2k'+1}$ such that $C \leq^p_m A$, say $C \leq^p_m A$ via f where w.l.o.g. $f(\lambda) \neq \lambda$.

Let
$$D = \{x : |f(x)| > 2|x| \;\&\; \forall\, y < x\, (f(y) \neq f(x))\}.$$

We will exploit the following properties of D.

- $D \in \mathrm{P}$.

  This is shown as follows. As one can easily check, $D \in \mathrm{PSPACE}$ hence, by assumption, $D \in \mathrm{P}$.

- $C \cap D \notin \mathrm{E}_{2k'+1}$.

  This is shown as follows. For a contradiction assume that $C \cap D \in \mathrm{E}_{2k'+1}$. We will show that $C \in \mathrm{E}_{2k'+1}$ contrary to assumption. So fix x. Then $C(x)$ can be computed in time $O(2^{2k'+1})$ steps as follows.

  - First decide whether $x \in D$ (Time: $poly(|x|)$).
  - If $x \in D$ then $C(x) = C \cap D(x)$ and $C \cap D(x)$ can be computed in time $O(2^{2k'+1})$ by assumption. So w.l.o.g. assume $x \notin D$.
  - Then either $|f(x)| \leq 2|x|$ or $|f(x)| > 2|x|$ but $f(x) = f(y)$ for some $y < x$. In the former case, by $A \in \mathrm{E}_{k'}$, $C(x) = A(f(x))$ can be computed in $O(2^{2k'})$ steps. So assume the latter. Let y_0 be the least y such that $f(y) = f(x)$. Then $y_0 \in D$ and, by our assumption that P = PSPACE, y_0 can be found in $poly(|x|)$ steps. Moreover,

    $$C(x) = A(f(x)) = A(f(y_0)) = C \cap D(y_0)$$

    whence, by $y_0 < x$ and by $C \cap D \in \mathrm{E}_{2k'+1}$, $C(x)$ can be computed in $O(2^{2k'+1})$ steps.

- f is one-to-one and length increasing on D.

  This is immediate by definition of D.

- For any string $x \neq \lambda$ there is a string y with $|x| = |y|$ and $xy \notin f(D)$.

  This is shown as follows. Since f is one-to-one on D and since, for any $z \in D$, $|f(z)| \geq 2|z| + 1$, it follows that (for $n \geq 1$)

  $$|f(D) \cap \Sigma^{2n}| \leq |D \cap \Sigma^{<n}| \leq |\Sigma^{<n}| = 2^n - 1 < 2^n = |\Sigma^n|.$$

  So, for any string x of length $n \geq 1$ there is a string y of length n such that $xy \notin f(D)$.

We exploit the above properties of D in order to define the required set B and a p-1-li-reduction g of B to A as follows.

We let

$$g(x) = \begin{cases} f(x) & \text{if } x \in D \\ xy_x & \text{otherwise} \end{cases}$$

where

$$y_x = \mu y\, (|y| = |x| \;\&\; xy \notin f(D)).$$

Then g is one-to-one and length increasing. Moreover, by our P = PSPACE assumption, g is polynomial-time computable, since finding y_x requires only $poly(|x|)$ space. It follows that, for

$$B = (C \cap D) \cup \{x \notin D : xy_x \in A\},$$

$B \leq^p_{1\text{-}li} A$ via g. So it only remains to show that $B \in \mathrm{E}$ and $B \notin \mathrm{E}_k$.

For a proof of $B \in \mathrm{E}$, by $D \in \mathrm{P}$, it suffices to show that $B \cap D \in \mathrm{E}$ and $B \cap \overline{D} \in \mathrm{E}$. The former follows from $B \cap D = C \cap D$ and $C \in \mathrm{E}$. The latter follows from the fact that $|g(x)| = 2|x|$ for $x \in \overline{D}$ and the fact that $A \in \mathrm{E}_{k'}$ whence $B(x) = A(g(x))$ can be computed in $O(2^{2k'|x|})$ steps.

For a proof of $B \notin \mathrm{E}_k$, it suffices to show that $B \cap D \notin \mathrm{E}_k$. But, by $B \cap D = C \cap D$, this is immediate by our observation above that $C \cap D \notin \mathrm{E}_{2k'+1}$.

This completes the proof. □

We do not know whether in Lemma 9.12 the assumption that P = PSPACE can be dropped. So we have to leave a complete characterization of the E-nontriviality notions of the 1-query reducibilities as an open question.

Open Problem 9.13 What are the relations among 1-E-nontriviality, 1-*li*-E- nontriviality, and *m*-E-nontriviality (for sets in E)? Is the answer to this question oracle dependent?

9.4 Strong Nontriviality Under 1-Query Reducibilities

In contrast to E-nontriviality, for strong E-nontriviality, we can give a complete characterization of the relations among the variants of this notion under the 1-query reducibilities.

Lemma 9.14 *Let* $A \in \mathrm{E}$ *be strongly* 1-*tt-nontrivial for* E. *Then* A *is strongly m-nontrivial for* E.

PROOF. By Theorem 9.3 it suffices to show that there is an E_1-bi-immune set $B \in \mathrm{E}$ such that $B \leq^p_m A$. By strong 1-*tt*-nontriviality we may choose an E_1-bi-immune set $C \in \mathrm{E}$ such that $C \leq^p_{1\text{-}tt} A$, say $C \leq^p_{1\text{-}tt} A$ via the selector function g and the evaluator h.

Now let

$$B(x) = \begin{cases} 1 - C(x) & \text{if } h(x,0) > h(x,1) \\ C(x) & \text{otherwise.} \end{cases}$$

Then, as in the proof of Lemma 9.9, $B \in \mathrm{E}$ and $B \leq^p_m A$.

It remains to show that B is E_1-bi-immune. For a contradiction assume that B is not E_1-bi-immune. Then, by symmetry, w.l.o.g. there is an infinite set $D \subseteq B$ such that $D \in \mathrm{E}_1$. Distinguish the following two cases.

If $D_0 = D \cap \{x : h(x,0) > h(x,1)\}$ is infinite then $D_0 \in \mathrm{E}_1$ and $D_0 \subseteq \overline{C}$. Otherwise, for $D_1 = D \setminus D_0$, D_1 is infinite, $D_1 \in \mathrm{E}_1$, and $D_1 \subseteq C$. In either case this contradicts E_1-bi-immunity of C. □

Lemma 9.15 *Let $A \in \mathrm{E}$ be strongly m-nontrivial for* E*. Then A is strongly m-li-nontrivial for* E*.*

PROOF. By Theorem 9.3 it suffices to show that there is an E_1-bi-immune set $B \in \mathrm{E}$ s.t. $B \leq^p_{m-li} A$. Assume $A \in \mathrm{E}_k$. By strong m-nontriviality of A we may choose an E_{k+1}-bi-immune set $B \in \mathrm{E}$ s.t. $B \leq^p_m A$, say $B \leq^p_m A$ via function f. Now we will show that $B \leq^p_{m-li} A$.

Let $D = \{x : |f(x)| \leq |x|\}$. Note, that D is finite. Otherwise by $D \in \mathrm{P}$ and by E_{k+1}-bi-immunity of B, $D \cap B$ would also be infinite; and $D \cap B$ would be an infinite subset of B in E_k, because to decide $x \in D \cap B$ we need to decide $|f(x)| \leq |x|$ and $f(x) \in A$. But that contradicts the assumption that B is E_{k+1}-bi-immune.

Let $y_0 = max(D)$, $|z_0| > |y_0|$, where $z_0 \in A$, $|z_1| > |y_0|$, where $z_1 \notin A$.

Then the following function $f'(x)$ will be many-one, length-increasing and will reduce B to A:

$$f'(x) = \begin{cases} f(x) & \text{if } |f(x)| > |x| \\ z_0 & \text{if } |f(x)| \leq |x| \text{ and } x \in B \\ z_1 & \text{if } |f(x)| \leq |x| \text{ and } x \notin B \end{cases}$$

□

Theorem 9.16 *For any set $A \in \mathrm{E}$ the following are equivalent.*

1. *A is strongly m-li-nontrivial for* E*.*
2. *A is strongly m-nontrivial for* E*.*
3. *A is strongly* 1-*tt-nontrivial for* E*.*

PROOF. The nontrivial implications hold by Lemmas 9.15 and 9.14. □

In contrast to the preceding theorem, however, strong m-nontriviality for E and strong 1-nontriviality for E differ.

Theorem 9.17 *There is a strongly m-*E*-nontrivial set which is weakly* 1-E*-trivial.*

PROOF. We have shown that there is a tally set $A \in \mathrm{E}$ which is strongly m-E-nontrivial (Corollary 5.11). So it suffices to show that no tally set is strongly 1-E-nontrivial. This is established by observing that no set which is p-1-reducible to a tally set is P-coimmune. Namely, if $B \leq^p_1 A$ via f and A is tally then $N = \{x : f(x) \notin \{0\}^*\}$ is infinite and polynomial-time computable, and $N \subseteq \overline{B}$. □

Finally, strong 1-nontriviality for E and strong 1-li-triviality for E coincide.

Theorem 9.18 *For any set $A \in \mathrm{E}$ the following are equivalent.*

1. *A is strongly 1-li-nontrivial for E.*

2. *A is strongly 1-nontrivial for E.*

PROOF. (IDEA). For a proof of the nontrivial implication assume that A is strongly 1-E-nontrivial. In order to show that A is strongly 1-li-E-nontrivial,by Theorem 9.3, it suffices to show that there is an E_1-bi-immune set $\hat{B} \in \mathrm{E}$ such that $\hat{B} \leq^p_{1\text{-}li} A$. Fix k such that $A \in \mathrm{E}_k$ and, by strong 1-E-nontriviality of A, fix an E_1-bi-immune set B such that $B \leq^p_1 A$, say via f. Then, for $\hat{B} = B_{k+1} = \{x : 0^{|x|^{k+1}}1x \in B\}$, $\hat{B} \in \mathrm{E}$ and $\hat{B}$ is E_{k+1}-bi-immune (see the proof of Theorem 9.2 above). Moreover, $\hat{B} \leq^p_1 A$ via $g(x) = f(0^{|x|^{k+1}}1x)$ and, by $A \in \mathrm{E}_k$ and by E_{k+1}-bi-immunity of $\hat{B}$, $|x| < |g(x)|$ for almost all x. So we can convert g into a p-1-li-reduction provided that $A \setminus range(g)$ and $\overline{A} \setminus range(g)$ are infinite. For a proof of the latter let $D = \{0\}^*$. Then $f(D)$ is infinite (since f is one-to-one) and (by definition of g and by f being one-to-one) $f(D) \cap range(g) = \emptyset$. So it suffices to argue that $A \cap f(D)$ and $\overline{A} \cap f(D)$ are infinite. For a contradiction assume not. Then, by symmetry, w.l.o.g. $f(D)$ is almost contained in A. So, by $B \leq^p_1 A$ via f, there is a finite variant of $D = \{0\}^*$ which is contained in B. So B is not P-immune contrary to choice of B. □

The above results can be summarized as follows.

Theorem 9.19 *For $A \in \mathrm{E}$ the following and only the following implications hold in general:*

$$\begin{array}{c}
\boxed{\begin{array}{c} A \textit{ is strongly } 1\text{-}li\text{-}\mathrm{E}\textit{-nontrivial} \\ \Updownarrow \\ A \textit{ is strongly } 1\text{-}\mathrm{E}\textit{-nontrivial} \end{array}} \\
\Downarrow \\
\boxed{\begin{array}{c} A \textit{ is strongly } m\text{-}li\text{-}\mathrm{E}\textit{-nontrivial} \\ \Updownarrow \\ A \textit{ is strongly } m\text{-}\mathrm{E}\textit{-nontrivial} \\ \Updownarrow \\ A \textit{ is strongly } 1\text{-}tt\text{-}\mathrm{E}\textit{-nontrivial} \end{array}}
\end{array} \tag{9.7}$$

Moreover, we can summarize the results of this and the two preceeding subsections as follows. Assuming P = PSPACE the following and (up to transitive closure) only the following implications hold in general:

$$\begin{array}{ccccc}
\boxed{\begin{array}{c} A\ 1\text{-}\mathit{li}\text{-E-cpl} \\ \Updownarrow \\ A\ 1\text{-E-cpl} \\ \Updownarrow \\ A\ m\text{-}\mathit{li}\text{-E-cpl} \\ \Updownarrow \\ A\ m\text{-E-cpl} \\ \Updownarrow \\ A\ 1\text{-}\mathit{tt}\text{-E-cpl} \end{array}}
& \begin{array}{c} \Rightarrow \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}
& \begin{array}{c} \boxed{\begin{array}{c} A\ 1\text{-}\mathit{li}\text{-E-snt} \\ \Updownarrow \\ A\ 1\text{-E-snt} \end{array}} \\ \Downarrow \\ \boxed{\begin{array}{c} A\ m\text{-}\mathit{li}\text{-E-snt} \\ \Updownarrow \\ A\ m\text{-E-snt} \\ \Updownarrow \\ A\ 1\text{-}\mathit{tt}\text{-E-snt} \end{array}} \end{array}
& \begin{array}{c} \\ \\ \\ \\ \\ \\ \Rightarrow \\ \\ \\ \end{array}
& \boxed{\begin{array}{c} A\ 1\text{-}\mathit{li}\text{-E-nt} \\ \Updownarrow \\ A\ 1\text{-E-nt} \\ \Updownarrow \\ A\ m\text{-}\mathit{li}\text{-E-nt} \\ \Updownarrow \\ A\ m\text{-E-nt} \\ \Updownarrow \\ A\ 1\text{-}\mathit{tt}\text{-E-nt} \end{array}}
\end{array} \tag{9.8}$$

Without the assumption that P = PSPACE the following questions remain:

- Is every *m*-E-nontrivial set 1-E-nontrivial?
- Is every 1-E-nontrivial set 1-*li*-E-nontrivial?
- Is every strongly *m*-E-nontrivial set 1-E-nontrivial or even 1-*li*-E-nontrivial?

9.5 Nontriviality and Strong Nontriviality Under Multi-Query Reducibilities

In this section we give complete separation results for the multi-query reducibilities by showing that, for $r, r' \in \{k-tt\ (k \geq 1), btt, tt, T\}$ such that r is strictly stronger than r', there is an r'-E-complete set A which is not r-E-nontrivial. We first separate truth-table from Turing reducibility.

Theorem 9.20 *There is a T-*E*-complete set A such that*

$$\forall\, B\ (B \leq_{tt}^{p} A \Rightarrow B \in \mathrm{E}_6). \tag{9.9}$$

So, in particular, A is tt-trivial for E *and* EXP.

(The level E_6 in (9.9) is not optimized. For the following it will be only of interest that we obtain (9.9) for some level E_k.)

Corollary 9.21 *There is a T-*E*-complete set A such that A is tt-trivial for* E.

PROOF. This is immediate by Theorem 9.20. □

We also get the corresponding separation for EXP in place of E.

Corollary 9.22 *There is a T-*EXP*-complete set A such that A is tt-trivial for* EXP.

PROOF. This is immediate by Theorem 9.20 since, for $A \in \mathrm{E}$, T-E-completeness and T-EXP-completeness coincide. □

PROOF OF THEOREM 9.20. Given an m-E-complete set $C \in \mathrm{E}_1$, it suffices to define a set A such that

$$A \in \mathrm{E}_1, \tag{9.10}$$

$$C \leq^p_T A, \tag{9.11}$$

and (9.9) holds.

For guaranteeing (9.11) we define a p-T-reduction of C to A based on the following coding schema. For any string $z \neq \lambda$ we let

$$CODE(z) = \{\hat{z}y : |y| \leq 3|z|^2 + 1\}$$

where

$$\hat{z} = 0^{4|z|}1z,$$

define a unique string $code(z)$ of length $3|z|^2 + 1$ such that

$$C(z) = code(z)(3|z|^2), \tag{9.12}$$

and let

$$A \cap CODE(z) = \{\hat{z}y : y \sqsubseteq code(z)\}. \tag{9.13}$$

I.e., we will ensure that there is a unique string of maximal length in $CODE(z)$, namely $\hat{z}code(z)$, such that the strings in $CODE(z)$ which are elements of A are just the initial segments of this string extending $\hat{z}$, and the last bit of this string will tell us whether or not $z \in C$. Note that using A as an oracle, we can inductively compute this string by a standard prefix search. So, obviously, this will ensure $C \leq^p_T A$.

Note that

$$z \neq z' \Rightarrow CODE(z) \cap CODE(z') = \emptyset$$

and

$$w \in CODE(z) \Rightarrow 5|z| + 1 \leq |w| \leq 5|z| + 1 + 3|z|^2 + 1. \tag{9.14}$$

Moreover, a string will be put into A only for the sake of coding C into A, hence

$$A \subseteq \bigcup_{z \in \Sigma^+} \{\hat{z}y : y \sqsubseteq code(z)\} \subseteq \bigcup_{z \in \Sigma^+} CODE(z). \tag{9.15}$$

The code $code(z)$ of a string z of length $n \geq 1$ will consist of n parts of length $3n$ each and the final coding bit, i.e.,

$$code(z) = v^z_1 \ldots v^z_n\, C(z) \quad (n = |z|, |v^z_1| = \cdots = |v^z_n| = 3n). \tag{9.16}$$

The components v^z_m of $code(z)$ play a central role in our strategy for satisfying (9.9). We will ensure that

$$v^z_1 \dots v^z_m \ (1 \leq m \leq n; n = |z|) \text{ can be computed in } O(poly(n) \cdot 2^{4m}) \text{ steps.} \quad (9.17)$$

By $C \in \mathrm{E}_1$, (9.16) and (9.17) imply

$$code(z) \text{ can be computed in } O(2^{5n}) \text{ steps } (n = |z|). \quad (9.18)$$

Note that this implies $A \in \mathrm{E}_1$. Namely, given a string x, in polynomial time we can tell whether x is in a code set $CODE(z)$ and if so compute the corresponding z. If x is not in any code set then $A(x) = 0$. If $x \in CODE(z)$ then $x \in A$ if and only if $\hat{z} \sqsubseteq x \sqsubseteq \hat{z}code(z)$ where $\hat{z}$ can be computed in $poly(|z|)$ steps and, by (9.18), $code(z)$ can be computed in $O(2^{5|z|})$ steps. Since, by (9.14), $5|z| \leq |x|$, it follows that $A(x)$ can be determined in $O(2^{|x|})$ steps.

In the remainder of the proof we describe our strategy for satisfying (9.9). We start with some notation.

Fix a standard enumeration $\langle M_e : e \geq 0 \rangle$ of the polynomial-time bounded oracle Turing machines such that (for any oracle) the run time of M_e on inputs of length n is bounded by $p_e(n)$ where the polynomials p_e are chosen such that $n \leq p_e(n) \leq p_{e+1}(n)$ and $p_e(n)^2 < 2^n$ for all e and n with $e \leq n$. Let

$$Q_e(x) = \{y^0_{e,x}, \dots, y^{k_{e,x}}_{e,x}\} \text{ where } y^0_{e,x} < \dots < y^{k_{e,x}}_{e,x}$$

be the set of oracle queries made by M_e on input x if working with the empty oracle set. Note that, for e and x such that $e \leq |x|$, $Q_e(x)$ consists of less than $p_e(|x|) < 2^{|x|}$ strings, each having length less than $p_e(|x|) < 2^{|x|}$. I.e.,

$$k_{e,s} < p_e(|x|) < 2^{|x|} \ \& \ \forall\, j \leq k_{e,s} \ (|y^j_{e,x}| < p_e(|x|) < 2^{|x|}). \quad (9.19)$$

Moreover, since the elements of $Q_e(x)$ are produced when running M_e on input x with the empty oracle, by applying a standard sorting algorithm, we can enumerate the elements $y^0_{e,x}, \dots, y^{k_{e,x}}_{e,x}$ of $Q_e(x)$ in order of magnitude in time less than $O(p_e(n)^2) \leq O(2^n)$. Finally, note that if M_e describes a p-tt-reduction then M_e is nonadaptive, i.e., the query set of M_e on input x does not depend on the oracle set whence $Q_e(x)$ is the query set of $M^A_e(x)$.

Now in order to satisfy (9.9) we ensure that, for a machine M_e and an input x of length $|x| > e$, for any query $y^j_{e,x}$ in a code set $CODE(z)$ where $|x| \leq |z|$ the question whether $y^j_{e,x}$ is an initial segment of $\hat{z}code(z)$ (hence in A) does only depend on the initial segment $v^z_1 \dots v^z_{|x|}$ of $code(z)$:

$$\begin{aligned} &\forall\, e\, \forall\, x,z\, \forall\, j \leq k_{e,x} \ [e < |x| \leq |z| \ \& \ y^j_{e,x} \in CODE(z) \\ &\quad \Rightarrow \ (y^j_{e,x} \sqsubseteq \hat{z}code(z) \Leftrightarrow y^j_{e,x} \sqsubseteq \hat{z}v^z_1 \dots v^z_{|x|})] \end{aligned} \quad (9.20)$$

That this (together with (9.17)) is sufficient for establishing (9.9), is shown as follows. Given B such that $B \leq_{tt}^{p} A$, fix e such that $B \leq_{tt}^{p} A$ via M_e, i.e., such that $B(x) = M_e^A(x)$ for all strings x where M_e is nonadaptive. Then, given x with $|x| > e$, by simulating $M_e^{\emptyset}(x)$, in $poly(|x|)$ steps we can list the queries $y_{e,x}^{0}, \ldots, y_{e,x}^{k_{e,x}}$ used in the reduction. So, given $A(y_{e,x}^{0}), \ldots, A(y_{e,x}^{k_{e,x}})$, we can compute $B(x)$ in $poly(|x|)$ steps using the identity $B(x) = M_e^A(x)$ by simulating M_e on input x and by answering all oracle queries using the list $A(y_{e,x}^{0}), \ldots, A(y_{e,x}^{k_{e,x}})$. Hence, in order to show that $B \in \mathrm{E}_6$, it suffices to argue that, for given $j \leq k_{e,x}$, we can compute $A(y_{e,x}^{j})$ in $O(2^{5|x|})$ steps. (Since $k_{e,x}$ is polynomially bounded in $|x|$, this implies that $O(2^{6|x|})$ will bound the total number of steps required for computing $B(x)$.) This is done as follows. Given $y_{e,x}^{j}$, first decide whether $y_{e,x}^{j} \in CODE(z)$ for some z and if so determine the unique corresponding string z. Since $|y_{e,x}^{j}|$ is polynomially bounded in $|x|$ it follows from the definition of the code sets that this can be done in $poly(|x|)$ steps and that $|z|$ is polynomially bounded in $|x|$ (if exists). Now, if $y_{e,x}^{j}$ is not in any code set then $A(y_{e,x}^{j}) = 0$ by construction. If $y_{e,x}^{j} \in CODE(z)$ then distinguish the following two cases.

If $|z| < |x|$ then, by (9.18), $\hat{z}code(z)$ can be computed in $O(2^{5|z|})$ hence $O(2^{5|x|})$ steps, and, by (9.13), $A(y_{e,x}^{j}) = 1$ if and only if $\hat{z} \sqsubseteq y_{e,x}^{j} \sqsubseteq \hat{z}code(z)$.

Finally, if $|x| \leq |z|$ then, by (9.17), $\hat{z}v_1^z \ldots v_{|x|}^z$ can be computed in $O(poly(|z|)2^{4|x|})$ hence (by $|z|$ being polynomially bounded in $|x|$) in $\leq O(2^{5|x|})$ steps, and, by (9.20), $A(y_{e,x}^{j}) = 1$ if and only if $\hat{z} \sqsubseteq y_{e,x}^{j} \sqsubseteq \hat{z}v_1^z \ldots v_{|x|}^z$.

Given z ($|z| = n$) it remains to define the components $v_1^z, \ldots, v_n^z$ of $code(z)$ in such a way that (9.16), (9.17) and (9.20) are satisfied. This is inductively done as follows. Given m with $1 \leq m \leq n$ and the strings $v_1^z, \ldots v_{m-1}^z$ (where, for $m = 1$, $\hat{z}v_1^z \ldots v_{m-1}^z = \hat{z}$), let v_m^z be the least string v of length $3n$ such that

$$\forall\, e < m \,\forall\, x \in \Sigma^m \,\forall\, j \leq k_{e,x}\, (\hat{z}v_1^z \ldots v_{m-1}^z v \not\sqsubseteq y_{e,x}^{j}). \tag{9.21}$$

Now, to show that the strings v_m^z are well defined and have the required properties, we first observe that given m with $1 \leq m \leq n$ and the strings $v_1^z, \ldots v_{m-1}^z$, there is a string v satisfying (9.21): Let

$$Q = \bigcup_{e<m,|x|=m} Q_e(x) = \{y_{e,x}^{j} : e < m \;\&\; x \in \Sigma^m \;\&\; j \leq k_{e,x}\}.$$

Then it suffices to show that there is a string v of length $3n$ such that $\hat{z}v_1^z \ldots v_{m-1}^z v$ is not extended by any string in Q. Obviously this will be the case if there are more strings v of length $3n$ than strings in Q, i.e., if $|Q| < 2^{3n}$. But the latter follows from the fact that, by $m \leq n$, there are $m \leq n < 2^n$ numbers $e < m$, $2^m < 2^n$ strings $x \in \Sigma^m$, and, by $e < m = |x|$ and by (9.19), $k_{e,x} < 2^m < 2^n$.

So v_m^z exists, and, by definition, $|v_m^z| = 3n$ in accordance with (9.16). Moreover, (9.17) is immediate by the fact that (9.21) holds for $v = v_m^z$.

Finally, for a proof of (9.17), it suffices to show that, given $\hat{z}$ and $v_1^z, \ldots, v_{m-1}^z$, v_m^z can be computed in $O(poly(n) \cdot 2^{4m})$ steps. Since v_m^z is the least string v of length $3n$ such that $\hat{z}v_1^z \dots v_{m-1}^z v$ is not extended by any string in Q, it suffices to show that Q can be enumerated in time $O(2^{2m})$. (Then, a fortiori, $|Q| \leq O(2^{2m})$. So, for finding v_m^z, it suffices to compare $\hat{z}v_1^z \dots v_{m-1}^z v$ for the first $O(2^{2m})$ strings v of length $3n$ with the elements of Q. Obviously, this can be done in

$$O(O(2^{2m}) \cdot (|\hat{z}v_1^z \dots v_{m-1}^z| + 3n) \cdot O(2^{2m})) \leq O(poly(n) \cdot 2^{4m})$$

steps.) But the latter is straightforward. Since for $e < m$ and x with $|x| = m$, $Q_e(x)$ can be produced in $p_e(m)$ steps, it follows by choice of the polynomial p_e that the set Q above can be enumerated in

$$O(m \cdot 2^m \cdot p_e(m)) \leq O(2^{2m})$$

steps.

This completes the proof of Theorem 9.20. □

We now separate the nontriviality notions for E under the different truth-table type reducibilities.

Theorem 9.23 *(a) Let $k \geq 1$. There is a $(k+1)$-tt-complete set A in* E *which is k-tt-*E*-trivial.*

(b) There is a tt-complete set A in E *which is btt-*E*-trivial.*

The proof of Theorem 9.23 uses a variant of the speed-up technique we have used in the proof of Lemma 6.2 already where we compared nontriviality for EXP and E.

PROOF OF THEOREM 9.23.

Since the proofs of the two parts are very similar, we first give a detailed proof of part (a) and then give only some hints how the proof has to be changed in order to prove part (b).

(a)

We construct a set $A \in O(2^{n^2})$ such that:

$$\text{A is } (k+1)\text{-tt-hard for E} \tag{9.22}$$

$$\forall B \in \mathrm{E}(B \leq_{k-tt}^p A \Rightarrow B \in DTIME(2^n)). \tag{9.23}$$

Then any set $\hat{A} \in \mathrm{E}$ with $\hat{A} =_m^p A$ will be $(k+1)$-*tt*-complete for E but *k*-*tt*-E-trivial.

In order to satisfy (9.22) we fix an E-complete set $C \in \mathrm{E}_1$ and we ensure $C \leq_{k+1-tt}^p A$. For the latter let

$$CODE(x) = \{xz_0^l, \dots, xz_k^l\},$$

where l is chosen minimal s.t. $|\Sigma^l| = 2^l \geq k+1$. Then it suffices to ensure that

$$x \in C \Leftrightarrow |A \cap CODE(x)| \text{ odd.} \tag{9.24}$$

Note, that for any x and x' the following is true:

$$x < x' \Rightarrow \forall y \in CODE(x)\ \forall y' \in CODE(x')\ (y < y').$$

By construction we will have

$$A \subseteq \bigcup_{x \in \Sigma^*} CODE(x) =: CODE. \tag{9.25}$$

At stage s of the construction we define $A \cap CODE(z_s)$.

Our strategy for satisfying (9.23) uses ideas from the proof of Lemma 6.2.

Fix an enumeration $\{E_e : e \geq 0\}$ of E such that for x with $|x| > e$, $E_e(x)$ can be computed in time $2^{e|x|}$.

Fix an enumeration $\{(\overrightarrow{g_e}, h_e) : e \geq 0\}$ of all p-k-tt-reductions where $\overrightarrow{g_e} = (g_{e,1}, ..., g_{e,k})$ is a k-tuple of polynomial-time bounded selection functions and h_e is a corresponding evaluator function such that, for a common time bound p_e, $p_e((|x|+l)^2) \leq 2^{|x|}$ for all x with $|x| > e$. Moreover, without loss of generality, assume

- $g_{e,1}(x) < ... < g_{e,k}(x)$
- $g_{e,1}(x), ..., g_{e,k}(x) \in CODE.$

(In case if some $g_{e,i}$ is not in $CODE$, we can redefine the evaluator funtion h_e so that it uses 0 instead of querying (this we can allow by (9.25)) and replace this query with another one, which is in $CODE$ and just not use it in evaluator function. In case if the queries are not ordered we can manually order them.)

We will meet the following requirements (for $e \geq 0$, $e = \langle e_0, e_1 \rangle$):

$$\Re_e : E_{e_0} \leq^p_{k-tt} A \text{ via } (\overrightarrow{g_{e_1}}, h_{e_1}) \Rightarrow$$

$$\forall^\infty x\, \forall i \leq k\ (i \text{ is } (e_1, x)\text{-critical } \Rightarrow |x| > 2^{-e} \cdot |g_{e_1,i}(x)|^2).$$

Here we say that i is (e,x)-*critical* if there are $j_i, ..., j_k$ and $j'_i, ..., j'_k$ such that

$$\begin{aligned} h_e(x, A(g_{e,1}(x)), ..., A(g_{e,i-1}(x)), j_i, ..., j_k) \neq \\ h_e(x, A(g_{e,1}(x)), ..., A(g_{e,i-1}(x)), j'_i, ..., j'_k). \end{aligned} \tag{9.26}$$

In addition to meeting the above requirements we will ensure that A obeys the following complexity bounds (where α is a real number).

$$\forall\, \alpha > 0\ (A \in \mathrm{DTIME}(2^{\alpha \cdot n^2})). \tag{9.27}$$

Observe that $A \in O(2^{n^2})$ is immediate by (9.27).

Now we will show that (9.27) implies (9.23).

Fix $B \in \mathrm{E}$ such that $B \leq^p_{k-tt} A$. To show that $B \in \mathrm{E}_1$ we do the following.

Fix $e = \langle e_0, e_1 \rangle$ such that $B = E_{e_0}$ and $B \leq^p_{k-tt} A$ via $(\overrightarrow{g_{e_1}}, h_{e_1})$. By requirement $\mathfrak{R}_e$ we may fix n_0 such that for x with $|x| \geq n_0$

$$\forall i \leq k\ (i\ (e_1,x) - \text{critical} \Rightarrow |x| > 2^{-e}|g_{e_1,i}(x)|^2) \tag{9.28}$$

holds.

Then, for x with $|x| \geq n_0$, $B(x)$ can be computed in $O(2^{|x|})$ steps as follows.

- Compute $g_{e_1,1}(x), ..., g_{e_1,k}(x)$. This can be done in $poly(|x|)$ steps.
- For $1 \leq i \leq k$ let

$$y_i = \begin{cases} A(g_{e_1,i}(x) & if|x| > 2^{-e}|g_{e_1,i}(x)|^2 \\ 0 & \text{otherwise.} \end{cases}$$

  By (9.27) for $\alpha = 2^{-e}$ this can be done in $O(2^{|x|})$ steps.
- Compute $y = h_{e_1}(x, y_1, ..., y_k)$. This can also be done in $poly(|x|)$ steps.

We claim that $B(x) = y$.

For a contradiction assume that $B(x) \neq y$. Then

$$B(x) = E_{e_0}(x) = h_{e_1}(x, A(g_{e_1,1}(x)), ..., A(g_{e_1,k}(x)))$$

and $y = h_{e_1}(x, y_1, ..., y_k)$ differ. So, for some i, $A(g_{e_1,i}(x)) \neq y_i$, and, for the least such i, i is (e_1,x)-critical. But then, by (9.28), $|x| > 2^{-e} \cdot |g_{e_1,i}(x)|^2$. So, by definition, $y_i = A(g_{e_1,i}(x))$, and that contradicts that for chosen i, $A(g_{e_1,i}(x)) \neq y_i$.

We now turn to the construction of A and describe stage s of the construction where $A \cap CODE(z_s)$ is defined.

We say that requirement $\mathfrak{R}_e$ *requires attention* at stage s if

- $e < |z_s|$,
- $\mathfrak{R}_e$ is not satisfied at any stage $t < s$,

and one of the following holds.

$$\text{There is an } \mathfrak{R}_e\text{-commitment } (y_i, j_i), ..., (y_k, j_k) \text{ at the end of stage } s-1 \text{ and } y_i \in CODE(z_s) \tag{9.29}$$

or there is no current $\mathfrak{R}_e$ commitment and

$$\exists x\ \exists i \leq k\ (|x| \leq 2^{-e}(|z_s| + l)^2\ \&\ (i > 0 \Rightarrow g_{e_1,i-1}(x) \notin CODE(z_s))\ \&\ g_{e_1,i}(x) \in CODE(z_s)\ \&\ i\ (e_1,x)\text{-critical}) \tag{9.30}$$

(Note that, by $g_{e_1,i}(x) \in CODE(z_s)$ and $g_{e_1,i-1} \notin CODE(z_s)$, the question whether i is (e_1,x)-critical or not depends only on the part of A defined prior to stage s).

If some requirement requires attention then fix e minimal such that $\mathfrak{R}_e$ requires attention. We say that $\mathfrak{R}_e$ is *active* at stage s.

If $\mathfrak{R}_e$ requires attention via (9.29) then let $(y_i, j_i), ..., (y_k, j_k)$ be the $\mathfrak{R}_e$- commitment at the end of stage $s-1$, otherwise define $(y_i, j_i), ..., (y_k, j_k)$ as follows. Fix such x and i as in (9.30) minimal. Let $y_i = g_{e_1,i}(x), ..., y_k = g_{e_1,k}(x)$ and fix $j_i, ..., j_k$ minimal such that

$$\mathrm{E}_{e_0}(x) \neq h_{e_1}(x, A(g_{e_1,1}(x)), ..., A(g_{e_1,i-1}(x)), j_i, ..., j_k).$$

Then, in either case proceed as follows.

- Let
$$\mathrm{P}_s = \{y_r : i \leq r \leq k \ \& \ j_r = 1 \ \& \ y_r \in CODE(z_s)\}$$
$$\mathrm{N}_s = \{y_r : i \leq r \leq k \ \& \ j_r = 0 \ \& \ y_r \in CODE(z_s)\}$$
and fix $p \leq k$ minimal such that $y_p \notin CODE(z_s)$ (if there is no such p then let $p = k+1$).

- Cancel all $\mathfrak{R}_{e'}$-commitments where $e < e'$. If $e < e'$ and the current $\mathfrak{R}'_e$-commitment is cancelled then we say that requirement $\mathfrak{R}_{e'}$ is *injured* by requirement $\mathfrak{R}_e$.

- If $p \leq k$ then let $(y_p, j_p), ..., (y_k, j_k)$ be the new $\mathfrak{R}_e$*-commitment*. If $p = k+1$ then say that $\mathfrak{R}_e$ is *satisfied*.

- Define $A \cap CODE(z_s)$ by
$$A \cap CODE(z_s) = \begin{cases} \mathrm{P}_s \cup \{y\} & \text{if } |\mathrm{P}_s| \text{ even and } C(z_s) = 1 \\ & \text{or } |\mathrm{P}_s| \text{ odd and } C(z_s) = 0 \\ \mathrm{P}_s & \text{otherwise} \end{cases}$$
where y is the least element of $CODE(z_s)$ such that $y \notin P_s \cup N_s$ (Note that $|\mathrm{P}_s \cup \mathrm{N}_s| \leq k$ and $|CODE(z_s)| = k+1$).

If no requirement requires attention then let y be the least string in $CODE(z_s)$ and let

$$A \cap CODE(z_s) = \begin{cases} \emptyset & \text{if } C(z_s) = 0 \\ \{y\} & \text{if } C(z_s) = 1 \end{cases}$$

This completes the construction.

Note that the definition of $A \cap CODE(z_s)$ at stage s ensures that (9.24) holds. So, in order to show that A has the required properties, it suffices to show that

(9.27) holds and all requirements are met. We do this by establishing a series of claims.

Claim 1. Every requirement $\mathfrak{R}_e$ is active at most finitely often.

Proof. The proof is by induction. Fix e and, by inductive hypothesis, choose s_0 such that no requirement $\mathfrak{R}_{e'}$ with $e' < e$ becomes active after stage s_0. Then $\mathfrak{R}_e$ will not be injured after stage s_0.

Now, for a contradiction, assume that $\mathfrak{R}_e$ is active at infinitely many stage $s > s_0$, say at stages $s_1 < s_2 < s_3 \dots$. Now $\mathfrak{R}_e$ is not satisfied at any of these stages since otherwise it will cease to require attention. So, by construction, at the end of any stage s_n, $n \geq 1$, there will be some commitment $(y_p, j_p), ..., (y_k, j_k)$ attached to $\mathfrak{R}_e$ and, since $\mathfrak{R}_e$ is not injured after stage s_0, no such commitment will be cancelled. So at the following stage at which $\mathfrak{R}_e$ will become active, i.e, at stage s_{n+1}, $\mathfrak{R}_e$ will require attention via (9.29). But then, by construction, the commitment attached to $\mathfrak{R}_e$ at the end of stage s_{n+1} will be a proper suffix of $(y_p, j_p), ..., (y_k, j_k)$. But this can happen only finitely often contrary to assumption.

Claim 2. Every requirement $\mathfrak{R}_e$ requires attention at most finitely often.

Proof. By Claim 1 fix a stage s_0 such that no requirement $\mathfrak{R}_{e'}$ with $e' \leq e$ is active after stage s_0. Then $\mathfrak{R}_e$ will not require attention at any stage $s > s_0$ (since otherwise $\mathfrak{R}_e$ or some $\mathfrak{R}_{e'}$ will become active at stage s contrary to choice of s_0).

Claim 3. If requirement $\mathfrak{R}_e$ is satisfied at some stage s then $\mathfrak{R}_e$ is met.

Proof. Assume that $\mathfrak{R}_e$ is satisfied at stage s. Then there is the least stage $s' < s$ such that $\mathfrak{R}_e$ is active at stage s' and $\mathfrak{R}_e$ is not injured at any stage t with $s' \leq t \leq s$. Then at stage s', $\mathfrak{R}_e$ requires attention via (9.30). So there is a string x and a sequence $(y_i, j_i), ..., (y_k, j_k)$ such that $y_i = g_{e_1,i}(x), ..., y_k = g_{e_1,k}(x)$, and

$$E_{e_0}(x) \neq h_{e_1}(x, A(g_{e_1,1}(x)), ..., A(g_{e_1,i-1}(x)), j_i, ..., j_k). \tag{9.31}$$

Now we distinguish two cases.

- Case 1: $s' = s$. Then $y_i, ..., y_k \in CODE(z_{s'})$ and we let $A(g_{e_1,m}(x)) = j_m$ for $i \leq m \leq k$ at stage s. So, by (9.31),

  $$E_{e_0}(x) \neq h_{e_1}(x, A(g_{e_1,1}(x)), ..., A(g_{e_1,k}(x))).$$

  Whence $\mathfrak{R}_e$ is met.

- Case 2: $s' < s$. Then Let $s_1 = s' < s_2 < ... < s_n = s$ be the stages t, $s' \leq t \leq s$, at which $\mathfrak{R}_e$ is active. Then, by construction, there are numbers $i = p_0 < p_1 < p_2 < ... < p_n = k+1$ such that $(y_{p_m}, j_m), ..., (y_k, j_k)$ is the $\mathfrak{R}_e$ commitment at the end of stage s_m and $A(y_q)$ was set to j_q at stage s_m for $p_{m-1} \leq q \leq p_m$. It follows by (9.31)

  $$E_{e_0}(x) \neq h_{e_1}(x, A(g_{e_1,1}(x)), ..., A(g_{e_1,k}(x))).$$

  So $\mathfrak{R}_e$ is met.

Claim 4. Every requirement R_e is met.

Proof. For a contradiction assume that $\mathfrak{R}_e$ is not met.

Fix e_0 and e_1 such that $e = \langle e_0, e_1 \rangle$. Moreover, by Claim 2, fix s_0 such that no requirement $\mathfrak{R}_{e'}$ with $e' \leq e$ will require attention after stage s_0 where without loss of generality $e < |z_s|$.

Note that, by Claim 3, $\mathfrak{R}_e$ is never satisfied.

Moreover, if there is an $\mathfrak{R}_e$-commitment $(y_i, j_i), ..., (y_k, j_k)$ at the end of stage $s-1$ then $y_i \in CODE(z_{s'})$ for some $s' > s-1$ (This easily follows by induction on s). So, since $\mathfrak{R}_e$ acts only finitely often, we may fix $s_1 > s_0$ such that there will be no $\mathfrak{R}_e$-commitment at the end of any stage $s \geq s_1$.

Hence there is no R_e-commitment at stage s_0. Since $\mathfrak{R}_e$ is not met, $E_{e_0} \leq^p_{k-tt}$ A via $(\overrightarrow{g_{e_1}}, h_{e_1})$ and

$$\exists^\infty x\ \exists i \leq k\ (|x| \leq 2^{-e} \cdot |g_{e_1,i}(x)|^2\ \&\ i \text{ is } (e_1,x)\text{-critical}). \tag{9.32}$$

Now we have to get such x that (9.30) holds. Since we have infinitely many x as in (9.32), it suffices to find $s' > s_0$ such that $g_{e_1,i}(x) \in CODE(z'_s)$ holds. To do so we take any x like in (9.32) such that $|g_{e_1,i}(x)| > |z_{s_0}| + l$. Then we choose such s' that $g_{e_1,i}(x) \in CODE(z_{s'})$ and $\mathfrak{R}_e$ will require attention by (9.30).

Claim 5. There is a procedure M which on input z_s uses $A \restriction z_s 0^l$ as an oracle and runs in time $O(2^{\frac{1}{e+1}(|z_s|+l)^2})$ such that, for $e < |z_s|$, $e = \langle e_0, e_1 \rangle$, M computes the least x and i witnessing (9.30) *(if there are such x and i) and computes $E_{e_0}(x)$.*

Proof. In order to find the least x and the corresponding least i such that x and i witness (9.30) (if there are such x and i). For x with

$$|x| \leq 2^{-e} \cdot (|z_s| + l)^2 \tag{9.33}$$

we have to do the following

(α) Compute $g_{e_1,1}(x), ..., g_{e_1,k}(x)$.

(β) Find i minimal such that $g_{e_1,i}(x) \in CODE(z_s)$. If there is such i proceed to the next x.

(γ) Compute $A(g_{e_1,1}(x)), ..., A(g_{e_1,i-1}(x))$.

(δ) For each $j_i, ..., j_k, j'_i, ..., j'_k \in \{0,1\}$ check whether (9.26) holds. If so, output (x,i). Otherwise proceed to the next x.

Now, by (9.33) and by choice of $\{(\overrightarrow{g_e}, h_e) : e \geq 0\}$, ($\alpha$) can be done in

$$O(2^{|z_s|})$$

steps. Then (β) can be done in

$$O(|z_s|)$$

steps. In order to compute $A(g_{e_1,j}(x))$ $(1 \leq j \leq i-1)$ from $A \restriction z_s 0^l$ we have to compute m with $z_m = g_{e_1,j}(x)$, look up the $m+1$-th bit b of $A \restriction z_s 0^l$ and set $A(g_{e_1,j}(x)) = b$. Finding m requires $poly(|z_s|)$ steps while the time required for looking up $(A \upharpoonright z_s0^l)(m)$ is bounded by the length of $A \upharpoonright z_s0^l$, i.e., by $O(2^{|z_s|})$. So, (γ) can be done in

$$O(2^{|z_s|})$$

steps. Finally, for carrying out (δ), we have to look at constantly many tuples $j_i,...,j_k,j'_i,...,j'_k \in \{0,1\}$ and for each such tuple we have to check (9.26). Now, by choice of functions h_e, by (9.33) and by (9.30) this can be done in

$$O(2^{|z_s|})$$

steps.

So, for fixed x,the above can be computed in $O(2^{|z_s|})$ steps. By (9.33) the time for finding the least x and the corresponding i with (9.30) is bounded by

$$2^{2^{-e}\cdot(|z_s|+l)^2}\cdot O(2^{|z_s|}) = 2^{2^{-e}\cdot(|z_s|+l)^2+O(|z_s|)} \leq 2^{2^{\frac{1}{e+1}}\cdot(|z_s|+l)^2}$$

steps.

Finally, for the least x and i as above such that (9.30) holds we have to compute $E_{e_0}(x)$. By choice of the sets E_e and by (9.33) this can be done in (for all $e \geq 5$)

$$O(2^{e_0(|x|)}) \leq O(2^{e_0\cdot 2^{-e}\cdot(|z_s|+l)^2})$$
$$\leq O(2^{e\cdot 2^{-e}\cdot(|z_s|+l)^2})$$
$$\leq O(2^{\frac{1}{e+1}(|z_s|+l)^2})$$

steps.

Claim 6. Let

$$SAT(s) = \{e : \exists\, t \leq s\ (\mathfrak{R}_e \textit{ is satisfied at stage } t)\},$$

$$COM(s) = \{\langle e,\alpha\rangle : \alpha \textit{ is the } \mathfrak{R}_e\textit{-commitment at the end of stage } s\}$$

where e is such that $\mathfrak{R}_e$ is active at stage s. Then, for any $k \geq 1$ there is a procedure which computes $SAT(s)$, $COM(s)$ and $A \upharpoonright z_{s+1}0^l$ in $O(2^{\frac{1}{k}(|z_s|+l)^2})$ steps.

Proof. Fix $k \geq 1$. It suffices to give a procedure for computing $SAT(s)$, $COM(s)$ and $A \upharpoonright z_{s+1}0^l$ from z_s, $SAT(s-1)$, $COM(s-1)$ and $A \upharpoonright z_s0^l$ in $O(2^{\frac{1}{k+1}(|z_s|+l)^2})$ steps (where SAT(-1)= $\emptyset$, $COM(-1) = \{0\}$ and $A \upharpoonright z_00^l = \emptyset$). Then, given z_s we can inductively compute

$$SAT(0),...,SAT(s),COM(0),...,COM(s),A \upharpoonright z_{s+1}0^l$$

in total of

$$O(s\cdot 2^{|z_s|}\cdot 2^{\frac{1}{k+1}(|z_s|+l)^2}) \leq O(2^{|z_s|}\cdot 2^{\frac{1}{k+1}(|z_s|+l)^2}) \leq O(2^{\frac{1}{k}(|z_s|+l)^2})$$

steps.

We may fix a stage s_0 such that all requirements $\mathfrak{R}_e$ with $e \leq k$ are satisfied at some stage $m \leq s_0$.

Now, in order to compute $SAT(s)$, $COM(s)$ and $A \restriction z_{s+1}0^l$ from z_s, $SAT(s-1)$, $COM(s-1)$ and $A \restriction z_s 0^l$ for $s > s_0$ we can proceed as follows.

First, we find e minimal such that $|z_s| \geq e > k$ and requirement $\mathfrak{R}_e$ requires attention at stage s (if any).

By Claim 5 we can decide whether (9.30) holds in time $O(2^{\frac{1}{e+1}(|z_s|+l)^2})$ and, if this holds, fix such x and i minimal (Note, that we can use Claim 5 since we can substitute the oracle with the given $A \restriction z_s 0^l$).

Using $COM(s-1)$ we can retrieve active requirement $\mathfrak{R}_{e'}$ and the $\mathfrak{R}_{e'}$- commitment at previous stage $s-1$. Hence, (9.29) can be decided in polynomial time. That means that we can decide whether $\mathfrak{R}_e$ requires attention in time

$$O(2^{|z_s|+l} + 2^{\frac{1}{e+1}(|z_s|+l)^2}) \leq O(2^{\frac{1}{e+1}(|z_s|+l)^2}).$$

Now we have enought information to simulate the stage s of the construction without having to search for a requirement that requires attention. The the whole stage s can be done in polynomial time, hence in $O(2^{|z_s|+l})$.

In the end of stage s, if requirement $\mathfrak{R}_e$ is satisfied then let $SAT(s) = SAT(s-1) \cup \{e\}$ otherwise let $SAT(s) = SAT(s-1)$.

Then let $COM(s) = \langle e, \alpha \rangle$ where α is equal to the current $\mathfrak{R}_e$-commitment.

Finally, let $A \restriction z_{s+1}0^l = A \restriction z_s 0^l \cup \{A \cap CODE(z_s)\}$.

Claim 7. (9.27) *holds.*

Proof. Given α take k such that $\frac{1}{k} \leq \alpha$. Then, given x, it suffices to compute $A(x)$ in $O(2^{\frac{1}{k}|x|^2})$ steps. This is done as follows. First we find z_s such that $x \in CODE(z_s)$. Then $A(x)$ can be computed from $A \restriction z_{s+1}0^l$. By Claim 6 latter can be done in $O(2^{\frac{1}{k}(|z_s|+l)^2})$ steps, hence, by $|x| = |z_s| + l$, in $O(2^{\frac{1}{k}|x|^2})$ steps.

This completes the proof of part (a).

(b) For a proof of part (b) it suffices to construct a set $A \in O(2^{n^2})$ such that:

$$\text{A is tt-hard for E} \tag{9.34}$$

$$\forall B \in \mathrm{E}(B \leq^p_{btt} A \Rightarrow B \in DTIME(2^n)). \tag{9.35}$$

Then any set $\hat{A} \in \mathrm{E}$ with $\hat{A} =^p_m A$ will be tt-complete for E but btt-E-trivial.

In order to satisfy (9.22) we fix an E-complete set $C \in \mathrm{E}_1$ and we ensure $C \leq^p_{tt} A$ by the following coding schema. Let

$$CODE(x) = \{0^{|x|}1xz_l^{|x|} : l \leq |x|\}.$$

Then it suffices to ensure that

$$x \in C \Leftrightarrow |A \cap CODE(x)| \text{ odd}.$$

Note, that for any x and x' the following is true:

$$x < x' \Rightarrow \forall y \in CODE(x)\ \forall y' \in CODE(x')\ (y < y').$$

By construction we will have

$$A \subseteq \bigcup_{x\in\Sigma^*} CODE(x) =: CODE.$$

At stage s of the construction we define $A \cap CODE(z_s)$.

This coding will be flexible enough to allow us to satisfy (9.35) by some diagonalization argument similar to the one used in part (a).

Now, of course, the requirements $\mathfrak{R}_e$ in the proof of the part (a) have to be modified so that they capture k-tt-reductions for all $k \geq 1$, not just for a fixed k as there. □

9.6 Summary for E

Our results on the relations among the nontriviality and strong nontriviality notions for E under the various polynomial-time reducibilities give a complete picture of the relations in diagram (9.1) if we omit the case of the notions based on p-1- and p-1-li-reducibility (and add p-m-li).

Theorem 9.24 *For $A \in$ E the following and (up to transitive closure) only the following implications hold in general ($k \geq 2$):*

$$\begin{tikzcd}
\boxed{\begin{array}{c} A\ m\text{-}li\text{-}\mathrm{E}\text{-}cpl \\ \Updownarrow \\ A\ m\text{-}\mathrm{E}\text{-}cpl \\ \Updownarrow \\ A\ 1\text{-}tt\text{-}\mathrm{E}\text{-}cpl \end{array}} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \boxed{\begin{array}{c} A\ m\text{-}li\text{-}\mathrm{E}\text{-}snt \\ \Updownarrow \\ A\ m\text{-}\mathrm{E}\text{-}snt \\ \Updownarrow \\ A\ 1\text{-}tt\text{-}\mathrm{E}\text{-}snt \end{array}} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \boxed{\begin{array}{c} A\ m\text{-}li\text{-}\mathrm{E}\text{-}nt \\ \Updownarrow \\ A\ m\text{-}\mathrm{E}\text{-}nt \\ \Updownarrow \\ A\ 1\text{-}tt\text{-}\mathrm{E}\text{-}nt \end{array}} \arrow[d, Rightarrow] \\
A\ k\text{-}tt\text{-}\mathrm{E}\text{-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-}\mathrm{E}\text{-}snt \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-}\mathrm{E}\text{-}nt \arrow[d, Rightarrow] \\
A\ (k+1)\text{-}tt\text{-}\mathrm{E}\text{-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-}\mathrm{E}\text{-}snt \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-}\mathrm{E}\text{-}nt \arrow[d, Rightarrow] \\
A\ btt\text{-}\mathrm{E}\text{-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ btt\text{-}\mathrm{E}\text{-}snt \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ btt\text{-}\mathrm{E}\text{-}nt \arrow[d, Rightarrow] \\
A\ tt\text{-}\mathrm{E}\text{-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-}\mathrm{E}\text{-}snt \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-}\mathrm{E}\text{-}nt \arrow[d, Rightarrow] \\
A\ T\text{-}\mathrm{E}\text{-}cpl \arrow[r, Rightarrow] & A\ T\text{-}\mathrm{E}\text{-}snt \arrow[r, Rightarrow] & A\ T\text{-}\mathrm{E}\text{-}nt
\end{tikzcd} \tag{9.36}$$

9.7 Nontriviality for EXP with Respect to Other Reducibilities

We conclude our analysis of nontriviality and strong nontriviality under the various polynomial-time reducibilities by looking at these notions for the polynomial exponential-time class EXP in place of E. We will only look at the case of the multi-query reducibilites where some of the arguments used in case of E do not carry over to EXP. In fact, as our first result of this section shows, the proper hierarchy of the r-E-nontriviality notions (see the right column in (9.36)) for the multi-query reducibilites partially collapses here.

Theorem 9.25 *For any set $A \in \mathrm{EXP}$ the following are equivalent.*

1. *A is m-nontrivial for* EXP.
2. *A is tt-nontrivial for* EXP.

PROOF. For a proof of the nontrivial direction assume that A is tt-nontrivial for EXP. We have to show that A is m-nontrivial for EXP.

Fix $k \geq 1$. Then it suffices to show that there is a set B such that $B \leq_m^p A$ and $B \notin \mathrm{EXP}_k$.

By tt-nontriviality of A, fix C such that $C \in \mathrm{EXP} \setminus \mathrm{EXP}_{4k}$ and $C \leq_{tt}^p A$. Moreover, fix a nonadaptive, oracle Turing machine M such that $C \leq_{tt}^p A$ via M and let p be a polynomial time-bound for M. For any input string x let $q(x,n)$ be the nth query of M on input x (if there is an nth query) and let $q(x,1),\dots,q(x,n_x)$ be a list of all queries on input x. Define the set B by

$$B = \{1^{|x|}0xz_n : n \leq n_x \ \&\ q(x,n) \in A\}.$$

Then $B \leq_m^p A$ via f for f defined by

$$f(y) = \begin{cases} q(x,n) & \text{if } y = 1^{|x|}0xz_n \ \&\ n \leq n_x \\ 0 & \text{otherwise.} \end{cases}$$

It remains to show that $B \notin \mathrm{EXP}_k$.

For a contradiction assume $B \in \mathrm{EXP}_k$. Then $x \in C$ can be decided as follows.

- Compute the queries $q(x,0),\dots,q(x,n_x)$ asked by M on input x. This can be done in $poly(|x|)$ steps.
- Using B, compute the answers of A on these queries. Since $|1^{|x|}0xz_n| \leq 3|x|$ (Note that on input x, the number of queries of M is polynomially bounded in the length of x. So $n \leq poly(|x|)$ whence $|z_n| \leq |x|$ for all sufficiently long x.) it follows, by assumption on B, that this can be done in $poly(|x|) \cdot 2^{3|x|^k}$ steps.

- Using these answers of the oracle, simulate the computation $M^A(x)$. This can be done in $poly(|x|)$ steps.

Since

$$poly(|x|) \cdot 2^{3|x|^k} \leq O(2^{|x|^{k+1}})$$

the above computation of $C(x)$ can be done in $O(2^{|x|^{k+1}})$ steps. It follows that $C \in \mathrm{EXP}_{k+1}$ contrary to assumption. □

Remark 9.26 For an E-*tt*-nontrivial set $A \in \mathrm{E}$ we can duplicate the above argument as follows. Assuming that A is *tt*-nontrivial for E, take a set C such that $C \in \mathrm{E} \setminus \mathrm{E}_{4k}$ and $C \leq_{tt}^{p} A$, and let B be the set obtained from C as above. Then $B \leq_m^p A$ and $B \notin \mathrm{E}_k$. We cannot argue, however, that B is in E. So this argument does not contradict our previous result that *m*-nontriviality and *tt*-nontriviality for E do not coincide.

Note that the above argument cannot be refined to show that *m*-nontriviality for EXP and *T*-nontriviality for EXP coincide. In Corollary 9.22 we have already shown that there is a *T*-EXP-complete set A such that A is *tt*-trivial for EXP. So, in particular, *tt*-EXP-nontriviality and *T*-EXP-nontriviality differ.

Also, in contrast to the collapse of the *r*-EXP-nontriviality hierachy in Theorem 9.25 the hierarchy for *strong* *r*-EXP-nontriviality is proper.

Theorem 9.27 *(a) Let $k \geq 1$. There is a $(k+1)$-tt-complete set A in* EXP *which is weakly k-tt-*EXP*-trivial.*

(b) There is a tt-complete set A in EXP *which is weakly btt-*EXP*-trivial.*

Proof. Since the proofs of the two parts of the theorem are similar, we only sketch the proof of the separation of *k-tt* and $(k+1)$-*tt*.

We construct a set A such that

$$A \in \mathrm{E}_1 \tag{9.37}$$

$$A\ (k+1)\text{-}tt\text{-EXP-hard} \tag{9.38}$$

$$A \text{ weakly } k\text{-}tt\text{-EXP-trivial} \tag{9.39}$$

hold.

In order to satisfy (9.38) we fix an *m*-EXP-complete set $C \in \mathrm{E}_1$ and ensure

$$\forall\, x\, (x \in C \Leftrightarrow |A \cap \{xy_0, \ldots, xy_k\}| \text{ odd}) \tag{9.40}$$

where $y_0, \ldots, y_k$ are the first $k+1$ strings of length l where l is chosen minimal such that $k+1 \leq 2^l$.

Obviously, this suffices to satisfy (9.38).

For describing our strategy for satisfying (9.39) we first have to introduce some notation.

Fix an enumeration $\{(\vec{g}_e, h_e) : e \geq 0\}$ of the *p-k-tt*-reductions (where $\vec{g}_e = (g_{e,1}, \ldots, g_{e,k})$) such that, for x with $|x| > e$, $g_{e,i}(x)$ and $h_e(x)$ can be computed in $O(2^{|x|})$ steps.

Let δ be the iterated exponential function (defined by $\delta(0) = 0$ and $\delta(n+1) = 2^{\delta(n)}$) and let

$$D_e = \{0^{\delta(\langle e,n \rangle)} : n \geq 0\},$$

$$\hat{D}_e = \{g_{e,i}(x) : 1 \leq i \leq k \;\&\; x \in D_e \;\&\; |x| < |g_{e,i}(x)| < 2^{|x|}\},$$

and

$$\hat{D} = \bigcup_{e \geq 0} \hat{D}_e.$$

Note that

$$D_e \in \mathrm{P} \;\&\; \hat{D} \in \mathrm{E}_1 \tag{9.41}$$

and

$$\forall\, n \; (|\hat{D} \cap \Sigma^n| \leq k). \tag{9.42}$$

Now we ensure (9.38) by guaranteeing

$$A \cap \hat{D} = \emptyset. \tag{9.43}$$

That this will guarantee (9.38) is shown as follows. Given a set B such that $B \leq^p_{k\text{-}tt} A$, we have to show that B is not E_1-bi-immune. Fix e such that $B \leq^p_{k\text{-}tt} A$ via $(\vec{g}_e, h_e)$, i.e., such that

$$\forall\, x \; (B(x) = h_e(A(g_{e,1}(x)), \ldots, A(g_{e,k}(x)))).$$

By (9.41) it suffices to show that, for almost all $x \in D_e$, $B(x)$ can be computed in $O(2^{|x|})$ steps. Fix n_0 such that, for x with $|x| \geq n_0$,

$$max\{|g_{e,i}(x)| : 1 \leq i \leq k\} < 2^{|x|}.$$

Then, for $x \in D_e$ with $|x| \geq n_0$,

$$h_e(A(g_{e,1}(x)), \ldots, A(g_{e,k}(x)))$$

can be computed in $O(2^{|x|})$ steps since, for i with $|g_{e,i}(x)| > |x|$, $A(g_{e,i}(x)) = 0$ and, for i with $|g_{e,i}(x)| \leq |x|$, $A(g_{e,i}(x))$ can be computed in $O(2^{|x|})$ steps by (9.37).

Finally, (9.42) ensures that guaranteeing (9.43) does not interfer with (9.40). Namely, for any x we can define A on $\{xy_0, \ldots, xy_k\}$ as follows.

If $x \notin C$ then let $A \cap \{xy_0, \ldots, xy_k\} = \emptyset$. Otherwise, choose $i \leq k$ minimal such that $xy_i \notin \hat{D}$ and let $A \cap \{xy_0, \ldots, xy_k\} = \{xy_i\}$. (Note that, by $C \in \mathrm{E}_1$ and by the second part of (9.41), this can be done in time $O(2^{|x|})$ whence (9.37) is satisfied.)

□

We can summarize the above results on strong nontriviality and nontriviality for EXP under the multi-query reducibilities as follows.

Theorem 9.28 *For $A \in$ EXP the following and (up to transitive closure) only the following implications hold in general ($k \geq 2$):*

$$\begin{tikzcd}
A\ 1\text{-}tt\text{-EXP-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ 1\text{-}tt\text{-EXP-}snt \arrow[d, Rightarrow] & A\ 1\text{-}tt\text{-EXP-}nt \arrow[d, Leftrightarrow] \\
A\ k\text{-}tt\text{-EXP-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-EXP-}snt \arrow[d, Rightarrow] & A\ k\text{-}tt\text{-EXP-}nt \arrow[d, Leftrightarrow] \\
A\ (k+1)\text{-}tt\text{-EXP-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-EXP-}snt \arrow[d, Rightarrow] & A\ (k+1)\text{-}tt\text{-EXP-}nt \arrow[d, Leftrightarrow] \\
A\ btt\text{-EXP-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ btt\text{-EXP-}snt \arrow[d, Rightarrow] & A\ btt\text{-EXP-}nt \arrow[d, Leftrightarrow] \\
A\ tt\text{-EXP-}cpl \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-EXP-}snt \arrow[r, Rightarrow] \arrow[d, Rightarrow] & A\ tt\text{-EXP-}nt \arrow[d, Rightarrow] \\
A\ T\text{-EXP-}cpl \arrow[r, Rightarrow] & A\ T\text{-EXP-}snt \arrow[r, Rightarrow] & A\ T\text{-EXP-}nt
\end{tikzcd} \tag{9.44}$$

CHAPTER 10

Conclusion

In our thesis we have discussed some new weak completeness and hardness notions for the exponential time classes E and EXP. We focused on the concepts defined for the linear exponential time class E but we also discussed the concepts for the polynomial exponential time class EXP and clarified the relations among the concepts for these two complexity classes (see Chapter 6). Moreover, our focus was on completeness, i.e., on the analysis of the weak hardness notions for sets in E, but we also looked at the corresponding hardness notions on sets in general. In particular, in Chapter 7, we addressed and completely answered the question whether being weakly hard is typical or not for a set in general or for a computable set.

From the three new concepts we have introduced, nontriviality, strong nontriviality and compression completeness, it seems to us that nontriviality is the most interesting one. As pointed out by us, it may be viewed as the weakest weak hardness notion. Moreover, in contrast to the previously introduced weak hardness notions, measure hardness and category hardness, nontriviality is a quite simple concept requiring only very basic notions from complexity theory. Finally, nontriviality is closely related to the hierarchical structure of E and, as we have shown, it reflects some basic properties of this exponential time class. In particular, strength and limitations of the padding technique can be described in terms of nontriviality.

Strong nontriviality, which may be viewed as the analog of nontriviality in the setting of almost-everywhere complexity, is of particular interest for the structural analysis of the exponential time classes. In particular, there is a close relation between strong nontriviality and the important concept of bi-immunity. So our analysis of strong nontriviality yielded a number of new results on the distribution of the E_1-bi-immune sets among the exponential-time sets, and some of the open problems on strong nontriviality can be phrased as problems on bi-immune sets.

The third of our new concepts, compression completeness, has less significant relations to the basic concepts of complexity theory, but it may play a role as a useful link between our new quite general weak completeness notions, nontriviality and strong nontriviality, and the much more restricted weak completeness notions in the literature, measure completeness and category completeness.

In our analysis of nontriviality and strong nontriviality yielded we isolated a number of basic properties implying triviality or nontriviality and we provided some natural examples of trivial but intractable problems (see Chapter 3). Moreover, we obtained some interesting properties of the nontrivial and trivial sets. In particular, we have shown that trivial sets do not help (i.e., joining an incomplete set with a trivial set will yield an incomplete set again) and that joining trivial sets will yield trivial sets again. As we have also shown, these properties distinguish nontriviality from all of the other weak completeness notions (see Chapter 8). Moreover, we have distinguished all weak completeness concepts by describing the minimum density of sets with these properties thereby proving a strict hierarchy theorem for these notions (Chapter 5).

Finally we have studied some generalizations of our new weak completeness notions by replacing the underlying polynomial-time many-one reducibility by some more general polynomial-time reducibilities. Here we obtained some surprising differences between the corresponding notions for E and EXP. While, for the multi-query reducibilities, more general reducibilities also yield more general nontriviality notions for E, for EXP the nontriviality notions for the multi-query reducibilities collapse as long as there are no nonadaptive queries (see Chapter 9).

Bibliography

K. Ambos-Spies. Minimal pairs for polynomial time reducibilities. In *Computation theory and logic*, volume 270 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 1987.

K. Ambos-Spies. Polynomial time degrees of NP-sets. In *Trends in theoretical computer science (Udine, 1984)*, volume 12 of *Principles Comput. Sci. Ser.*, pages 95–142. Computer Sci. Press, Rockville, MD, 1988.

K. Ambos-Spies. Honest polynomial time reducibilities and the P = ?NP problem. *J. Comput. System Sci.*, 39(3):250–281, 1989.

K. Ambos-Spies. Resource-bounded genericity. In *Computability, enumerability, unsolvability*, volume 224 of *London Math. Soc. Lecture Note Ser.*, pages 1–59. Cambridge Univ. Press, Cambridge, 1996.

K. Ambos-Spies. Polynomial time reducibilities and degrees. In *Handbook of computability theory*, volume 140 of *Stud. Logic Found. Math.*, pages 683–705. North-Holland, Amsterdam, 1999.

K. Ambos-Spies and T. Kräling. Quantitative aspects of speed-up and gap phenomena. In *Theory and Applications of Models of Computation 2009*, volume 5532 of *Lecture Notes in Comput. Sci.*, pages 88–97. Springer, Berlin, 2009.

K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In *Complexity, logic, and recursion theory*, volume 187 of *Lecture Notes in Pure and Appl. Math.*, pages 1–47. Dekker, New York, 1997.

K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizations over deterministic polynomial time. In *Proceedings of the First Workshop on Computer Science Logic*, volume 329 of *Lecture Notes in Comput. Sci.*, pages 1–16. Springer, Berlin, 1988.

K. Ambos-Spies, E. Mayordomo, and X. Zheng. A comparison of weak completeness notions. *Computational Complexity, Annual IEEE Conference on*, 0:171, 1996a.

K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoret. Comput. Sci.*, 168(1):3–19, 1996b. 19th International Symposium on Mathematical Foundations of Computer Science (Košice, 1994).

K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Theoret. Comput. Sci.*, 172(1-2):195–207, 1997.

J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural complexity. II.* Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 1990.

L. Berman. On the structure of complete sets: almost everywhere complexity and infinitely often speedup. In *17th Annual Symposium on Foundations of Computer Science (Houston, Tex., 1976)*, pages 76–80. IEEE Comput. Soc., Long Beach, Calif., 1976.

H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. *J. Comput. System Sci.*, 54(3):393–399, 1997. Tenth Annual Conference on Structure in Complexity Theory (Minneapolis, MN, 1995).

S. A. Cook. The complexity of theorem-proving procedures. In *Proc. Third Annual ACM Symp. on Theory of Computing*, pages 151 – 158. Association of Computing Machinery, New York, 1971.

M. R. Garey and D. S. Johnson. *Computers and intractability.* W. H. Freeman and Co., San Francisco, Calif., 1979. ISBN 0-7167-1045-5. A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences.

J. G. Geske, D. T. Huỳnh, and A. L. Selman. A hierarchy theorem for almost everywhere complex sets with application to polynomial complexity degrees. In *STACS 87 (Passau, 1987)*, volume 247 of *Lecture Notes in Comput. Sci.*, pages 125–135. Springer, Berlin, 1987.

F. C. Hennie and R. E. Stearns. Two-tape simulation of multitape Turing machines. *J. Assoc. Comput. Mach.*, 13:533–546, 1966.

S. Homer, S. Kurtz, and J. Royer. On 1-truth-table-hard languages. *Theoret. Comput. Sci.*, 115(2):383–389, 1993.

J. E. Hopcroft and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley Publishing Co., Reading, Mass., 1979. Addison-Wesley Series in Computer Science.

D. W. Juedes and J. H. Lutz. The complexity and distribution of hard problems. *SIAM J. Comput.*, 24(2):279–295, 1995a.

D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoret. Comput. Sci.*, 143(1):149–158, 1995b.

R. M. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, pages 85–103. Plenum, New York, 1972.

K.-I. Ko and D. Moore. Completeness, approximation and density. *SIAM J. Comput.*, 10(4):787–796, 1981.

R. E. Ladner. On the structure of polynomial time reducibility. *J. Assoc. Comput. Mach.*, 22:155–171, 1975.

R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial time reducibilities. *Theoret. Comput. Sci.*, 1(2):103–123, 1975.

L. A. Levin. Universal enumeration problems. *Problemy Peredači Informacii*, 9 (3):115–116, 1973.

M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. Graduate Texts in Computer Science. Springer-Verlag, New York, second edition, 1997.

J. H. Lutz. Almost everywhere high nonuniform complexity. *J. Comput. System Sci.*, 44(2):220–258, 1992.

J. H. Lutz. Weakly hard problems. *SIAM J. Comput.*, 24(6):1170–1189, 1995.

E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoret. Comput. Sci.*, 136(2):487–506, 1994.

C.-P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*. Lecture Notes in Mathematics, Vol. 218. Springer-Verlag, Berlin, 1971.

O. Watanabe. A comparison of polynomial time completeness notions. *Theoret. Comput. Sci.*, 54(2-3):249–265, 1987.