Theoretical Computer Science 51 (1987) 177-204
North-Holland

DIAGONALIZATIONS OVER POLYNOMIAL TIME COMPUTABLE SETS*

Klaus AMBOS-SPIES, Hans FLEISCHHACK and Hagen HUWIG
Lehrstuhl für Informatik II, Universität Dortmund, D-4600 Dortmund 50, Fed. Rep. Germany

Communicated by P. Young
Received April 1985
Revised July 1986

Abstract. A formal notion of diagonalization is developed which allows to enforce properties that are related to the class of polynomial time computable sets (the class of polynomial time computable functions respectively), like, e.g., p-immunity. It is shown that there are sets—called p-generic—which have all properties enforceable by such diagonalizations. We study the behaviour and the complexity of p-generic sets. In particular, we show that the existence of p-generic sets in NP is oracle dependent, even if we assume $P \neq NP$.

1. Introduction

In recent publications structural properties of recursive sets like p-immunity (see, e.g., [6, 10]), non-p-selectivity [19] and non-p-mitoticity [1] have been studied. These properties have in common that no polynomial time computable set has any of these properties. So the existence of a set with one of these structural properties in the class NP of nondeterministically polynomial time computable sets would separate P from NP. The existence of recursive sets which enjoy some of these properties has been proved by diagonalization arguments. In some cases it has been shown that the existence of such sets in NP is oracle dependent.

In this paper we formally characterize a class of diagonalizations over the classes P and PF of polynomial time computable sets and functions respectively, called p-standard diagonalizations. This notion does not cover all diagonalization arguments over P but it is restricted to diagonalizations which yield witnesses of low complexity for the desired properties. In part this is achieved by considering only such properties which are shared by some tally set, i.e., by a set over a single-letter alphabet. Despite those restrictions, the common diagonalization arguments over P are covered by p-standard diagonalizations, as we demonstrate by a great number of examples. For instance, the above-mentioned structural properties can all be enforced by p-standard diagonalizations. We show that there exist recursive sets,

* The results of this paper have been presented at the 11th ICALP '84, Antwerp, Belgium (see [3]).

called p-generic sets, which have *all* properties enforceable by p-standard diagonalizations.

The existence of p-generic sets in NP is shown to be oracle dependent. We prove this by constructing recursive oracles A and B such that $P^A \neq NP^A$, $P^B \neq NP^B$ and there is a p^A-generic set in NP^A but NP^B contains no p^B-generic set. For properties Q enforceable by diagonalization over P this yields a new method for proving the existence of an oracle A such that some set in NP^A fulfils Q^A: to ensure this it will suffice to show that, in the unrelativized case, Q is enforceable by a p-standard diagonalization and that this fact relativizes.

After some preliminaries in Section 2, our diagonalization notion is introduced in Section 3. The existence of p-generic sets is proved in Section 4. In Section 5 some applications of p-standard diagonalizations are given. For instance, it is shown that p-generic sets distinguish the various notions of strong polynomial time reducibility introduced in [14]. Section 6 is devoted to the complexity of p-generic sets. Limitations of p-standard diagonalizations are discussed in Section 7. It is shown that a p-standard diagonalization does not suffice for diagonalizing over polynomial time bounded Turing reductions. A stronger diagonalization concept overcoming this shortcoming is introduced in Section 8. Again it is proved that there are sets—called strongly p-generic—possessing all properties enforceable by this extended diagonalization concept. Strongly p-generic sets can be constructed in double exponential time. For any relativization, however, strongly p-generic sets are not in NP (see [8]), whence they cannot serve for strong separation results for relativized P and NP. In the final Section 9, we compare our diagonalization concepts with the common diagonalization concepts in computational complexity theory and recursive function theory.

Our study of p-generic sets has been inspired by genericity notions for recursively enumerable sets introduced by Jockusch [11] and Maass [17]. Moreover, a conversation of the first author with C. Jockusch Jr and J. Mohrherr was stimulating for this research.

2. Preliminaries

Lower case letters from the middle of the alphabet stand for elements of $\mathbb{N}$, the set of nonnegative integers. $\Sigma = \{0, 1\}$. x, y, z denote *strings*, i.e., elements of Σ^*, capital letters A, B, $C, \ldots$ stand for recursive subsets of Σ^*. A set A is called *tally* if $A \subseteq \{0\}^*$. $|x|$ is the length of x and, for $n < |x|$, $x(n)$ is the $(n+1)$st component of x, i.e., $\langle i_0, \ldots, i_{k-1}\rangle(n) = i_n$. $x * y$ is the concatenation of x and y. Sometimes we abbreviate $x * \langle i\rangle$ by xi ($x \in \Sigma^*$, $i \in \Sigma$). We say x extends y if $x = y * z$ for some z. The lexicographical ordering on strings is denoted by $<$.

We identify a set and its characteristic function; i.e., $x \in A$ iff $A(x) = 1$ and $x \notin A$ iff $A(x) = 0$.

$A \upharpoonright n$ denotes the restriction of the characteristic function of A to arguments of length less than n; i.e., $A \upharpoonright n : \Sigma^{<n} \to \{0, 1\}$, where $\Sigma^{<n} = \{x \in \Sigma^* : |x| < n\}$ and, for

$x \in \Sigma^{<n}$, $x \in A$ iff $A{\upharpoonright}n(x) = 1$. For tally A, we interpret $A{\upharpoonright}n$ as a string, i.e., we let $A{\upharpoonright}n = x$, where $|x| = n$ and $\forall k < n\ (x(k) = A(0^k))$. We write $A =^* B$ iff $(A - B) \cup (B - A)$ is finite. $A \oplus B = \{\langle 0\rangle * x : x \in A\} \cup \{\langle 1\rangle * x : x \in B\}$.

P (NP) is the class of subsets of Σ^* which are (non)deterministically computable in polynomial time. PF is the class of deterministically in polynomial time computable functions from Σ^* to Σ^*. $\{P_n : n \in \mathbb{N}\}$ and $\{f_n : n \in \mathbb{N}\}$ are effective enumerations of P and PF respectively. $\{M_n^X : n \in \mathbb{N}\}$ and $\{p_n : n \in \mathbb{N}\}$ are standard enumerations of the deterministic polynomial time oracle machines (with oracle X) and their respective polynomial bounds. We write $x \in M_n^X$ ($x \notin M_n^X$) iff M_n^X accepts (refutes) x.

We say a string y is *used* in the computation $M_n^X(x)$ if the oracle X is queried about y. Note that at most $p_n(|x|)$ strings—and only strings of length $< p_n(|x|)$—are used in the computation $M_n^X(x)$.

A is a polynomial time many-one ($(p\text{-}m)$-)reducible to B, $A \leq_m^p B$, if, for some n, $\forall x\ (A(x) = B(f_n(x)))$. A is polynomial time Turing ($(p\text{-T})$-)reducible to B, $A \leq_T^p B$, if $A = M_n^B$ for some n. We write $A =_{m(T)}^p B$ iff $A \leq_{m(T)}^p B$ and $B \leq_{m(T)}^p A$. The $(p\text{-}m(T))$-degree of A is denoted by $\deg_{m(T)}^p A$. P^A is the set of deterministic polynomial time sets relative to A, i.e., $P^A = \{B : \exists n\ (B = M_n^A)\}$.

3. Diagonalizations over polynomial time computable sets and functions

The goal of this section is to develop a formal characterization of a class of diagonalization arguments over polynomial time computable sets and functions, which subsumes the common diagonalizations over P. In Section 9 we will compare our diagonalization notion with other concepts in the literature.

We start with analysing three typical constructions by diagonalizations, namely that of

(i) a recursive set A_1 which is not in P,

(ii) a recursive *p-immune* set A_2 (see [6, 10]), i.e., an infinite set A_2 which does not contain any infinite subset which is in P, and

(iii) a recursive *non-$(p\text{-}m)$-autoreducible* set A_3 (see [1]), i.e., a set which cannot be nontrivially $(p\text{-}m)$-reduced to itself (to be more precise, there is no function f such that $A_3 \leq_m^p A_3$ via f and $\forall x\ (f(x) \neq x)$).

Sets A_i ($i = 1, 2, 3$) with the desired properties are effectively constructed in stages, where, at stage $s+1$, membership in A_i is determined for strings of length s. So $A_i{\upharpoonright}s$ is completed by the end of stage s, whence A_i is recursive by the effectivity of the construction. The constructions have in common that the condition we want to satisfy is broken down into an infinite list of simpler requirements, namely,

R_e^1: $A_1 \neq P_e$;

R_e^2: $|P_e| = \infty \Rightarrow P_e \not\subseteq A_2$;

R_e^3: $\forall x (f_e(x) \neq x) \Rightarrow$ not $A_3 \leq_m^p A_3$ via f_e

(with $e \in \mathbb{N}$), respectively. (In the case of set A_2, we have to make sure additionally that A_2 is infinite. We will ignore this task for the moment and come back to it later.)

The fact that A_1 meets requirement R^1_e can be expressed as follows. Let $C^1_e = \{X \upharpoonright s : \exists x\ (|x| < s\ \&\ X(x) \neq P_e(x))\}$. Then A_1 meets R^1_e iff $A_1 \upharpoonright s \in C^1_e$ for some s. Similarly, A_i meets R^i_e, $i = 2, 3$, iff the premise of R^i_e is false or $A_i \upharpoonright s \in C^i_e$ for some s, where

$$C^2_e = \{X \upharpoonright s : \exists x\ (|x| < s\ \&\ X(x) = 0\ \&\ P_e(x) = 1)\}$$

and

$$C^3_e = \{X \upharpoonright s : \exists x, y\ (|x|, |y| < s\ \&\ f_e(x) = y\ \&\ X(x) \neq X(y))\}.$$

So, by determining an initial segment of A_i in an appropriate way, we can guarantee that A_i meets the requirement R^i_e. Moreover, assuming that the premise of R^i_e is correct, there are infinitely many stages s such that, for given $A_i \upharpoonright s$, there is a 1-step extension $A_i \upharpoonright s+1$ of $A_i \upharpoonright s$ with $(A_i \upharpoonright s+1) \in C^i_e$. So, intuitively speaking, either the premise of R^i_e fails, whence R^i_e is met trivially, or in the course of the construction of A_i there are infinitely many chances to ensure R^i_e by appropriately extending the so far enumerated part of A_i with length 1. For R^1_e this is obvious since, for any s, any $A \upharpoonright s$ and any string x of length s, we obtain an extension $(A \upharpoonright s+1) \in C^1_e$ of $A \upharpoonright s$ by choosing $A \upharpoonright s+1$ so that $A(x) \neq P_e(x)$.

For R^2_e consider such s where, for some x of length s, $P_e(x) = 1$ and choose $A \upharpoonright s+1$ with $(A \upharpoonright s+1)(x) = 0$. By the premise of R^2_e, infinitely many such stages s exist. Finally, for R^3_e consider stages s such that there are strings x and y with $x \neq y$, $|x| \leq |y| = s$ and $f_e(x) = y$ or $f_e(y) = x$. (Note that by premise of R^3_e infinitely many such stages s must exist.) Given $A \upharpoonright s$, we then choose an extension $A \upharpoonright s+1$ of $A \upharpoonright s$ such that $(A \upharpoonright s+1)(x) \neq (A \upharpoonright s+1)(y)$. Note that in contrast to the requirements R^1_e and R^2_e, where the strings of length s in A can be chosen independently from $A \upharpoonright s$, in case of R^3_e the extension depends on the previously constructed initial segment of A. Namely, for x and y as above such that $|x| < |y|$, i.e., $|x| < s$, the value of $A(y)$ is determined by the previously specified value of $A(x)$. This dependence is typical for more involved diagonalization arguments.

The above argument shows that A_i meets requirement R^i_e iff

$$\begin{aligned}&\textbf{if } \exists^\infty s\ \exists (X \upharpoonright s+1) \in C^i_e\ (X \upharpoonright s+1 \text{ extends } A_i \upharpoonright s)\\ &\textbf{then } \exists s\ (A_i \upharpoonright s \in C^i_e).\end{aligned} \tag{3.1}$$

This fact is (implicitly) used in the usual construction of the sets A_i: At stage $s+1$ of the construction we choose $e \leq s$ minimal (if there is any) such that R^i_e is not yet met at stage s (i.e., $\nexists t \leq s\ (A_i \upharpoonright t \in C^i_e)$) and R^i_e can be ensured at stage $s+1$ (i.e., there is some $X \upharpoonright s+1$ extending $A_i \upharpoonright s$ such that $(X \upharpoonright s+1) \in C^i_e$). Then we let $A_i \upharpoonright s+1 = X \upharpoonright s+1$ for such an extension, thus meeting R^i_e. So, for given e and for s_e such that, for all $e' < e$,

$$\exists t\ (A_i \upharpoonright t \in C^i_{e'}) \Rightarrow \exists t < s_e\ (A_i \upharpoonright t \in C^i_{e'}),$$

at any stage $s > s_e$ requirement R^i_e will have highest priority for becoming satisfied in the above-described way. Hence, if the premise of (3.1) is correct, then $A_i \upharpoonright s \in C_e^i$ for some s.

So (3.1) is satisfied for each e eventually, thus implying that A_i has the desired property.

The fact that a property which can be enforced by diagonalization can be ensured by an infinite list of conditions of the form (3.1) is not limited to diagonalizations over P but it applies to diagonalizations over any complexity class (see Section 9 below). What is typical for diagonalizations over P is the complexity of the classes C_e^i in (3.1), namely, for an appropriate encoding, $C_e^i \in \mathrm{P}$. This is of great importance since, in general, we are interested in getting sets A_i of as low a complexity as possible and the complexity of A_i depends on the complexity of the condition sets C_e^i. If we more closely analyse the complexity of A_i in the above outlined construction, we see that the computation of $A_i(x)$ for a string x of length s depends on tests of the form $A_i \upharpoonright t \in C_i^e$, $t \leq s$, where $|A_i \upharpoonright t| \leq 2^t$, and on a search among the 2^{2^s} possible extensions $X \upharpoonright s+1$ of $A_i \upharpoonright s$. The complexity can be exponentially decreased by considering only *tally* sets. By requiring A_i to be tally, $A_i \upharpoonright t$ can be interpreted as a string of length t (cf. Section 2) and there are only two possible extensions $X \upharpoonright s+1$ of $A_i \upharpoonright s$, namely, $A_i \upharpoonright s * \langle 0 \rangle$ and $A_i \upharpoonright s * \langle 1 \rangle$.

So, for tally sets A_i, the sets C_e^1, C_e^2, C_e^3 can be written as

$$C_e^1 = \{x : \exists n < |x| \ (x(n) \neq P_e(0^n))\},$$

$$C_e^2 = \{x : \exists n < |x| \ (x(n) = 0 \ \& \ P_e(0^n) = 1)\},$$

$$C_e^3 = \{x : \exists m,n < |x| \ (f_e(0^m) = 0^n \ \& \ x(m) \neq x(n))\}$$

and (3.1) now becomes

$$\exists^\infty s \ \exists j \leq 1 \ (A_i \upharpoonright s * \langle j \rangle \in C_e^i) \Rightarrow \exists s \ (A_i \upharpoonright s \in C_e^i). \tag{3.1'}$$

As one can easily check, C_e^1, C_e^2, $C_e^3 \in \mathrm{P}$.

The above analysis of examples for diagonalizations over P and PF leads us to the following central definition.

Definition 3.1. A property Q of languages over the alphabet Σ can be enforced by a *p-standard diagonalization* if there is a sequence $\{C_e : e \in \mathbb{N}\}$ of polynomial time computable sets such that, for any tally set A, the following holds: if, for every $e \in \mathbb{N}$,

$$\exists^\infty s \ \exists i \leq 1 \ (A \upharpoonright s * \langle i \rangle \in C_e) \Rightarrow \exists s \ (A \upharpoonright s \in C_e), \tag{3.2}$$

then A has property Q.

Note that only those properties can be enforced by a p-standard diagonalization which are shared by some tally set. At first sight, this is a severe restriction. For most structural properties studied in the context of the (P-NP)-problem, however, tally witnesses are known (see Section 5). The restriction to tally sets will allow us to construct 'universal' sets for p-standard diagonalizations in relativized NP (see Sections 4 and 6). Without this restriction a similar result cannot be obtained (see Section 9).

As shown above, being not in P and non-(p-m)-autoreducibility can be enforced by p-standard diagonalizations. In case of p-immunity in the above argument, we ignored the task of making A_2 infinite. Since any set not in P is infinite, by the following lemma we may conclude that p-immunity can be enforced by p-standard diagonalizations too. Further examples of enforceable properties are given in Section 5.

Lemma 3.2. *Let* Q_1 *and* Q_2 *be properties of languages over* Σ.

(a) *If* Q_1 *and* Q_2 *can be enforced by p-standard diagonalizations, then so can the conjunction* Q_1 & Q_2 *of* Q_1 *and* Q_2.

(b) *If* Q_1 *can be enforced by a p-standard diagonalization and* Q_1 *implies* Q_2, *then* Q_2 *can be enforced by a p-standard diagonalization.*

Proof. (a): Let $\{C_e^1 : e \in \mathbb{N}\}$ and $\{C_e^2 : e \in \mathbb{N}\}$ be sequences of polynomial time computable sets which enforce Q_1 and Q_2 respectively. Then the sequence $\{C_e : e \in \mathbb{N}\}$, where $C_{2e} = C_e^1$ and $C_{2e+1} = C_e^2$, enforces Q_1 & Q_2.

(b): Immediate. □

4. p-Generic sets

We will now show that there are tally recursive sets which have *all* properties which can be enforced by p-standard diagonalizations. So any property Q which can be enforced by a p-standard diagonalization is shared by a (tally) recursive set.

Definition 4.1. A tally set A is *p-generic* if, for every polynomial time computable set C,

$$\exists^\infty s\, \exists i \leq 1\, (A \upharpoonright s * \langle i \rangle \in C) \Rightarrow \exists s\, (A \upharpoonright s \in C). \tag{4.1}$$

If $A \upharpoonright s \in C$, then we say *A hits C*. The name p-genericity stems from a similarity between Definition 4.1 and the definition of a generic set for forcing notions in set theory.

p-Genericity is the strongest property that can be ensured by p-standard diagonalization.

Proposition 4.2.

(i) *p-Genericity can be enforced by p-standard diagonalization.*

(ii) *If A is p-generic and* Q *can be enforced by p-standard diagonalization, then A has property* Q.

(iii) *If* Q *is a property shared by all p-generic sets, then* Q *can be enforced by p-standard diagonalization.*

Proof. (i): Choose $\{C_e : e \in \mathbb{N}\}$ to be the enumeration $\{P_e : e \in \mathbb{N}\}$ of P.

(ii): Any sequence $\{C_e : e \in \mathbb{N}\}$ of polynomial time computable sets is contained in $\{P_e : e \in \mathbb{N}\}$.

(iii) Immediate by (i) and Lemma 3.2(b). □

Note that no p-generic set can be in P since—as mentioned in the preceding section—the property of being not in P can be ensured by a p-standard diagonalization. We now show that p-generic sets actually exist.

Theorem 4.3. *There is a recursive p-generic set.*

Proof. The proof is a standard diagonalization argument like the ones described in Section 3. Still we give a fairly detailed proof since, for later refinements of Theorem 4.3, we will have to refer to the construction below.

We effectively construct a p-generic set A in stages. To make A p-generic it suffices to meet the requirements

$$\mathbf{R}_e\colon \exists s\, \exists^\infty i \le 1\ (A{\upharpoonright}s * \langle i\rangle \in P_e) \Rightarrow \exists s\ (A{\upharpoonright}s \in P_e) \quad (e \in \mathbb{N}).$$

At stage $s+1$ of the construction below, we determine the value of $A(0^s)$. So, by the end of stage s, $A{\upharpoonright}s$ will be defined and can be used in the description of stage $s+1$.

We say $\mathbf{R}_e$ is *satisfied at (the end of) stage s* if, for some $t \le s$, $A{\upharpoonright}t \in P_e$. Note that once $\mathbf{R}_e$ is satisfied at some stage, it is satisfied at all later stages and $\mathbf{R}_e$ is met. Requirement $\mathbf{R}_e$ *requires attention at stage* $s+1$ if it is not satisfied at stage s and $A{\upharpoonright}s * \langle i\rangle \in P_e$ for some $i \le 1$. If $\mathbf{R}_e$ requires attention at stage $s+1$, then at stage $s+1$ we can ensure that $A{\upharpoonright}s+1 \in P_e$ (and thus that $\mathbf{R}_e$ is satisfied) by choosing the appropriate value for $A(0^s)$. It might happen that at some stages more than one requirement requires attention. In this case we give the requirement with *least* index among the requirements asking for attention *highest priority* and ignore the other ones.

We now give the construction of A.

Stage 0: Do nothing.

Stage $s+1$: If no requirement $\mathbf{R}_e$, $e \le s$, requires attention, then let $A(0^s) = 0$. Otherwise, choose e and i minimal (in this order) such that $\mathbf{R}_e$ requires attention and $A{\upharpoonright}s * \langle i\rangle \in P_e$. Set $A(0^s) = i$ and say $\mathbf{R}_e$ is *active*.

This completes the construction.

Obviously, the construction is effective and $A{\upharpoonright}s$ is defined by the end of stage s. So A is recursive. That the requirements $\mathbf{R}_e$ are met and thus that A is p-generic follows from the following claim.

Claim. *For every e, $\mathbf{R}_e$ requires attention only finitely often and is met.*

The claim is proved by induction on e. Fix e and, by inductive hypothesis, assume the claim correct for $e' < e$. Then we can choose s_0 such that no requirement $\mathbf{R}_{e'}$,

$e' < e$, requires attention after stage s_0. Now if R_e requires attention at some stage $s_1 > s_0$, then R_e becomes active at stage s_1 and—as pointed out above—is satisfied at all later stages. So R_e does not require attention after stage s_1.

To see that R_e is met, w.l.o.g., assume that $\exists^\infty s\ \exists i \leq 1\ (A{\upharpoonright}s*\langle i\rangle \in P_e)$. We have to show that R_e is satisfied at some stage and thus A hits P_e. But if this were not the case, then R_e would require attention at infinitely many stages, a contradiction. This also completes the proof of the theorem. □

It is a general experience that there is no property Q such that both Q and the complementary property $\bar{\mathrm{Q}}$ can be ensured by diagonalizations. For p-standard diagonalizations, this experience can be formally verified.

Corollary 4.4. *There is no property* Q *such that* Q *and* $\bar{\mathrm{Q}}$ *can be enforced by p-standard diagonalizations.*

Proof. To construct a contradiction, assume that Q and $\bar{\mathrm{Q}}$ are enforceable by p-standard diagonalization. Then, by Proposition 4.2, $A \in \mathrm{Q}$ and $A \in \bar{\mathrm{Q}}$ for any p-generic set A. So there are no p-generic sets, contrary to Theorem 4.3. □

In the following two sections we will first study properties of p-generic sets and then consider questions related to the complexity of such sets.

5. Properties of p-generic sets

In this section we will investigate some properties of p-generic sets and give more examples of properties which can be enforced by p-standard diagonalizations. We thereby reprove some known structural results (simplifying the original proofs) but we also prove some new results, e.g., on the structure of the polynomial time one-one degrees.

We first note that p-genericity is invariant under finite variations and that the complement of a p-generic set relative to $\{0\}^*$ is p-generic, too.

Theorem 5.1. *Let A be p-generic. Then,*
(i) *$\{0\}^* - A$ is p-generic and*
(ii) *for any $B \subseteq \{0\}^*$ such that $B =^* A$, B is p-generic.*

Proof. (i): Let $C \in \mathrm{P}$ be given. Then,

$$C' = \{x' : \exists x \in C\ (|x'| = |x|\ \&\ \forall n < |x|\ (x'(n) = 1 - x(n)))\}$$

is in P and, for any s and $i \leq 1$,

$$A{\upharpoonright}s*\langle i\rangle \in C' \text{ iff } (\{0\}^* - A){\upharpoonright}s*\langle 1-i\rangle \in C.$$

So p-genericity of A implies p-genericity of $\{0\}^* - A$.

(ii): Fix $B \subseteq \{0\}^*$ such that $B =^* A$, say $\forall s \geq s_0\, (B(0^s) = A(0^s))$, and let any $C \in \mathrm{P}$ be given. Then,

$$C'' = \{A \upharpoonright s_0 * x : B \upharpoonright s_0 * x \in C\}$$

is in P and, for $s > s_0$ and $i \leq 1$,

$$A \upharpoonright s * \langle i \rangle \in C'' \text{ iff } B \upharpoonright s * \langle i \rangle \in C.$$

So again p-genericity of A implies p-genericity of B. □

By equation (4.1), a p-generic set A hits any set $C \in \mathrm{P}$ if it has infinitely many chances to do so, i.e., if there are infinitely many s such that $A \upharpoonright s * \langle i \rangle \in C$ for some i. The following theorem implies that if A has infinitely many chances to hit C, then A hits C not just once but infinitely often. In a p-standard diagonalization we only consider extensions of length 1. One might conjecture that considering longer extensions will give more powerful diagonalization concepts. The following theorem shows that a p-generic set A will still hit any set $C \in \mathrm{P}$ if there are infinitely many chances to hit C by extensions of any constant length, i.e., if

$$\exists n\, \exists^\infty s\, \exists x\, (|x| = n \;\&\; A \upharpoonright s * x \in C).$$

Intuitively speaking, this shows that p-generic sets also have all those properties which are enforceable by finitely iterated p-standard diagonalizations, i.e., diagonalizations with any constant look-ahead instead of look-ahead of length 1.

So, by Proposition 4.2(i), such iterated diagonalizations are not more powerful than simple p-standard diagonalizations. In Section 7 we will show, however, that considering extensions of nonconstant length gives rise to a stronger diagonalization concept.

Theorem 5.2. *Let A be p-generic. Then, for all $C \in \mathrm{P}$, the following holds:*

$$\text{if } \exists n \geq 1\, \exists^\infty s\, \exists x\, (|x| \leq n \;\&\; A \upharpoonright s * x \in C), \text{ then } \exists^\infty s\, (A \upharpoonright s \in C). \tag{5.1}$$

Proof. We prove by induction on n that, for all $C \in \mathrm{P}$, it holds that

$$\exists^\infty s\, \exists x \quad (|x| = n \;\&\; A \upharpoonright s * x \in C) \Rightarrow \exists^\infty s\, (A \upharpoonright s \in C). \tag{5.2}$$

Basic step ($n = 1$): Fix $C \in \mathrm{P}$ and assume that the premise of (5.2) holds. Let

$$C_m = \{x : |x| \geq m \;\&\; x \in C\} \quad (m \in \mathbb{N}).$$

Then $C_m \in \mathrm{P}$ and $\exists^\infty s\, \exists i \leq 1\, (A \upharpoonright s * \langle i \rangle \in C_m)$. So, by p-genericity of A, A hits each C_m and thus A hits C infinitely often.

Inductive step: Fix C and assume

$$\exists^\infty s\, \exists x \quad (|x| = n + 1 \;\&\; A \upharpoonright s * x \in C). \tag{5.3}$$

To show that A hits C infinitely often, let

$$C' = \{x : \exists i \leq 1 \ (x * \langle i \rangle \in C)\}.$$

Then $C' \in \mathrm{P}$ and, by (5.3),

$$\exists^\infty s \, \exists x \quad (|x| = n \ \& \ A \upharpoonright s * x \in C').$$

So, by the inductive hypothesis, $\exists^\infty s \ (A \upharpoonright s \in C')$, i.e. $\exists^\infty s \, \exists i \leq 1 \ (A \upharpoonright s * \langle i \rangle \in C)$. It follows, again by inductive hypothesis, that A hits C infinitely often. □

In the remainder of this section we will give some examples of properties which can be enforced by p-standard diagonalizations. In Section 3 we have already shown that not being in P and p-immunity are such properties. Recall that A is *p-selective* if there is a polynomial time computable function $f: \Sigma^* \times \Sigma^* \to \Sigma^*$ such that

$$\forall x, y \in \Sigma^* \quad (f(x, y) \in \{x, y\} \text{ and } (A \cap \{x, y\} \neq \emptyset \Rightarrow f(x, y) \in A))$$

(cf. [19]).

Theorem 5.3. *Let A be p-generic. Then*

(i) $A \notin \mathrm{P}$;

(ii) *A is p-immune*;

(iii) *A is not p-selective.*

Proof. It remains to prove (iii). For a contradiction, assume that A is p-selective, i.e., for some polynomial time computable f,

$$\forall x, y \in \Sigma^* \quad [f(x, y) \in \{x, y\} \text{ and } (A \cap \{x, y\} \neq \emptyset \Rightarrow f(x, y) \in A)], \tag{5.4}$$

where w.l.o.g., $f(\{0\}^* \times \{0\}^*) \subseteq \{0\}^*$. Then, for the set

$$C = \{x : \exists n \ (|x| = n+2 \ \& \ [f(0^n, 0^{n+1}) = 0^n \Rightarrow x(n) = 0 \ \& \ x(n+1) = 1]$$
$$\& \ [f(0^n, 0^{n+1}) = 0^{n+1} \Rightarrow x(n) = 1 \ \& \ x(n+1) = 0])\},$$

$C \in \mathrm{P}$. Moreover, $\forall s \, \exists x \ (|x| = 2 \ \& \ A \upharpoonright s * x \in C)$ whereas, by (5.4), $\nexists s \ (A \upharpoonright s \in C)$. By Theorem 5.2, this is impossible. □

Parts (ii) and (iii) of Theorem 5.3 show that p-generic sets are free of certain redundancies; e.g., by immunity, they do not contain infinite trivial, i.e., polynomial time computable, parts. The lack of further redundancy properties follows from the next theorem and its corollaries.

Theorem 5.4. *Let A, B be recursive sets such that $B \subseteq A$ and A is p-generic. Then the following hold*:

(a) *if $A \leq^p_m B$ via f, then*

$$\exists n_0 \, \forall n \geq n_0 \, \exists m \leq n \quad (f(0^n) = 0^m); \tag{5.5}$$

(b) *if $B \leq^p_m A$ via f and $f(\{0\}^*) \subseteq \{0\}^*$, then* (5.5) *holds*;

(c) *if $A \leq^p_m A$ via f, then*

$$\exists n_0 \, \forall n \geq n_0 \quad (f(0^n) = 0^n). \tag{5.6}$$

Proof. (a): Fix f such that $A \leqslant_m^p B$ via f and, for a contradiction, assume that (5.5) fails. Then

$$\exists^\infty n \quad (f(0^n) \notin \{0^0, \ldots, 0^n\}). \tag{5.7}$$

First assume that

$$\exists^\infty n \quad (0^n \in A \,\&\, f(0^n) \notin \{0^0, \ldots, 0^n\}) \tag{5.8}$$

holds. Since $A = f^{-1}(B)$ and $B \subseteq \{0\}^*$, this implies that $\{n : 0^n \in A \,\&\, \exists m > n\ (f(0^n) = 0^m)\}$ is infinite. Hence, there are infinitely many s such that $A \upharpoonright s * \langle 0 \rangle \in C$ for the polynomial time computable set

$$C = \{x0 : \exists n < |x|\ (f(0^n) = 0^{|x|} \,\&\, x(n) = 1)\}.$$

So A hits C, i.e., $A(0^n) = 1 \neq 0 = A(f(0^n))$ for some n. Since $B \subseteq A$ this implies $A(0^n) \neq B(f(0^n))$, a contradiction.

So (5.8) fails, whence there is a number n_0 such that

$$\forall n \geqslant n_0 \quad (f(0^n) \notin \{0^0, \ldots, 0^n\} \Rightarrow 0^n \notin A).$$

So the polynomial time computable set

$$D = \{0^n : n \geqslant n_0 \text{ and } f(0^n) \notin \{0^0, \ldots, 0^n\}\}$$

is contained in $\{0\}^* - A$. Moreover, by (5.7), D is infinite. It follows that $\{0\}^* - A$ is not p-immune, contrary to Theorems 5.1 and 5.3.

(b): The proof is very similar to the proof of part (a). Fix f such that $B \leqslant_m^p A$ via f and $f(\{0\}^*) \subseteq \{0\}^*$ and, for a contradiction, assume that (5.5) fails. Then $\exists^\infty n\, \exists m > n\ (f(0^n) = 0^m)$. So either

$$\exists^\infty n \quad (0^n \notin A \text{ and } \exists m > n\ (f(0^n) = 0^m))$$

in which case A will hit the set

$$\{x1 : \exists n < |x|\ (f(0^n) = 0^{|x|} \,\&\, x(n) = 0)\},$$

contrary to $B = f^{-1}(A)$; or, for some n_0, the infinite set

$$\{0^n : n \geqslant n_0 \,\&\, f(0^n) \notin \{0^0, \ldots, 0^n\}\} \in \mathrm{P}$$

is contained in A, contrary to p-immunity of A.

(c): Fix f such that $A \leqslant_m^p A$ via f and, for a contradiction, assume that $f(0^n) \neq 0^n$ for infinitely many n. Then, by part (a), $\exists^\infty n\, \exists m < n\ (f(0^n) = 0^m)$. So, for infinitely many s, there is some $i \leqslant 1$ such that $A \upharpoonright s * \langle i \rangle \in C$ for the polynomial time computable set

$$C = \{xi : \exists n < |x|\ (f(0^{|x|}) = 0^n \,\&\, x(n) \neq i)\}.$$

This implies that A hits C, whence $A(0^n) \neq A(f(0^n))$ for some n, a contradiction. □

Theorem 5.4 has a series of interesting corollaries.

Corollary 5.5. *Let A be p-generic. Then, for any subset B of A, $A =^p_m B$ iff $A =^* B$.*

Proof. For a proof of the nontrivial implication, fix f_1 and f_2 such that $A \leq^p_m B$ via f_1 and $B \leq^p_m A$ via f_2, where, w.l.o.g., $f_2(\{0\}^*) \subseteq \{0\}^*$. Then, by Theorem 5.4, there is some number n_0 such that

$$\forall n \geq n_0 \quad (f_1(0^n), f_2(0^n) \in \{0^0, \ldots, 0^n\}).$$

Since $A \leq^p_m A$ via $f_2 \circ f_1$, whence $f_2 \circ f_1(0^n) = 0^n$ for almost all n by Theorem 5.4, this implies $f_1(0^n) = f_2(0^n) = 0^n$ for almost all n. So $A =^* B$. □

Corollary 5.6. *Let A be p-generic and let B be a polynomial time computable set such that $B \cap \{0\}^*$ and $\bar{B} \cap \{0\}^*$ are infinite. Then $A \cap B <^p_m A$, $A \cap \bar{B} <^p_m A$, and $A \cap B$ and $A \cap \bar{B}$ are $(p\text{-}m)$-incomparable.*

Proof. Since, by Theorems 5.1 and 5.3, A and $\{0\}^* - A$ are p-immune, $A \cap B$ and $A \cap \bar{B}$ are infinite. So, by Corollary 5.5, $A \cap B \neq^p_m A$ and $A \cap \bar{B} \neq^p_m A$. Since, for any recursive set A and for any $B \in \mathrm{P}$, $A =^p_m (A \cap B) \oplus (A \cap \bar{B})$, this implies the claims. □

Corollary 5.6 in particular shows that p-generic sets are non-$(p\text{-}m)$-mitotic in the sense of Ambos-Spies [1].

Theorem 5.4 has a further interesting corollary on the p-one-one-degrees of the finite variants of a p-generic set. Recall that A is p-one-one ($(p\text{-}1)$-)reducible to B, $A \leq^p_1 B$, if $A \leq^p_m B$ via a one-to-one function f.

Corollary 5.7. *Let A be p-generic, $x \notin A$.*

(a) $A <^p_1 A \cup \{x\}$.

(b) *The $(p\text{-}m)$-degree of A contains a chain of $(p\text{-}1)$-degrees of the order type of the integers.*

Proof. (a): Obviously, $A \leq^p_1 A \cup \{x\}$ via the one-to-one function f, where

$$f(y) = \begin{cases} y & \text{if } y \in \{0\}^* - \{x\}, \\ y1 & \text{otherwise.} \end{cases}$$

Now, for a contradiction, assume $A \cup \{x\} \leq^p_1 A$, say via g. Then, for each $n \geq 1$, $g^n(x) \in A$. By injectivity of g this implies $g^n(x) \neq g^m(x)$ for $n \neq m$. So, for h defined by

$$h(y) = \begin{cases} g(y) & \text{if } y \neq x, \\ 1 & \text{if } y = x, \end{cases}$$

$A \leq^p_m A$ via h and $\forall n \geq 1$ $(h(g^n(x)) = g^{n+1}(x) \neq g^n(x))$. So there are infinitely many n such that $h(0^n) \neq 0^n$. But this is impossible by Theorem 5.4(c).

(b): Let $\{x_n : n \in \mathbb{N}\}$ and $\{y_n : n \in \mathbb{N}\}$ be sequences of pairwise different strings such that $x_n \in \{0\}^* - A$ and $y_n \in A$. Then, by Theorem 5.1, $A \cup \{x_1, \ldots, x_n\}$ and $A - \{y_1, \ldots, y_n\}$ are p-generic. So by part (a),

$$\cdots <_1^p A - \{y_1, y_2\} <_1^p A - \{y_1\} <_1^p A <_1^p A \cup \{x_1\}$$
$$<_1^p A \cup \{x_1, x_2\} <_1^p \cdots \qquad \square$$

p-Generic sets can also be used to distinguish various notions of polynomial time reducibility such as (p-1)-reducibility, (p-m)-reducibility and variants of p-truth-table ((p-tt)-)reducibility. The following theorem gives a simple proof for some of these separation results which have already been shown by Ladner et al. in [14]. Here we are not able to prove that (p-tt)-reducibility differs from (p-T)-reducibility on the recursive sets. The first reason is that the notion of p-genericity is too weak to diagonalize over (p-T)-reductions as we will see later. On the other hand, in the context of tally languages there is no difference between (p-T)-reductions and (p-tt)-reductions at all, that is, for tally A the following holds: $B \leq_T^p A$ iff $B \leq_{tt}^p A$.

For the formal notion of (p-tt)-reducibility we refer to [14], whereas for the bounded versions we give a slightly different definition which is easier to use in our proofs but does not change the induced reducibility relation.

Definition 5.8. A set A is k-bounded (p-tt)-reducible to a set B ($A \leq_{k\text{-tt}}^p B$) if there is a polynomial time computable function $f_0 : \Sigma^* \times \{0,1\}^k \to \{0,1\}$ and functions $f_1, \ldots, f_k \in \mathrm{PF}$ such that $x \in A$ iff $f_0(x, B(f_1(x)), \ldots, B(f_k(x))) = 1$. A is bounded (p-tt)-reducible to B ($A \leq_{btt}^p B$) if $A \leq_{k\text{-tt}}^p B$ for some $k \geq 1$.

Theorem 5.9. *Let A be p-generic. Then,*

(i) $A \oplus A = \{0^{2n} : 0^n \in A\} \cup \{0^{2n+1} : 0^n \in A\} \not\leq_1^p A$;

(ii) $\bar{A} \not\leq_m^p A$;

(iii) $D_n = \{0^k : \{0^{n\cdot k}, \ldots, 0^{n\cdot k+n-1}\} \subseteq A\} \not\leq_{(n-1)\text{-tt}}^p A$, $n \geq 2$;

(iv) $\bigoplus_{n \in \mathbb{N}} D_n = \{1^n 0^k : 0^k \in D_n\} \not\leq_{btt}^p A$.

Note that $A \oplus A \leq_m^p A$, $\bar{A} \leq_{1\text{-tt}}^p A$, $D_n \leq_{n\text{-tt}}^p A$, and $\bigoplus_{n \in \mathbb{N}} D_n \leq_{tt}^p A$. So p-generic sets provide natural examples of sets proving

$$\leq_{tt}^p \not\Rightarrow \leq_{btt}^p \not\Rightarrow \leq_{(n+1)\text{-tt}}^p \not\Rightarrow \leq_{n\text{-tt}}^p \not\Rightarrow \leq_m^p \not\Rightarrow \leq_1^p$$

(cf. [14]). We also see that, for $n \geq 2$, $\leq_{n\text{-tt}}^p$ is not transitive since $D_{2n} \leq_{2\text{-tt}}^p D_n \leq_{n\text{-tt}}^p A$.

Proof of Theorem 5.9. (i): Assume that $A \oplus A \leq_1^p A$ via f. Fix numbers r and s such that $0^r \in A$ and $0^s \notin A$ and define the function g by letting $g(0^n) = f(0^{2n})$ for $n \neq s$, $g(0^s) = f(0^{2r+1})$, and $g(x) = f(x)$ for $x \in \Sigma^* - \{0\}^*$. Then $A \cup \{0^s\} \leq_1^p A$ via g, contrary to Corollary 5.7.

(ii): Assume that $\bar{A} \leq_m^p A$ via f, where, w.l.o.g., $f(\{0\}^*) \subseteq \{0\}^*$. Define

$$C = \{x : \exists m, n < |x| \, (f(0^m) = 0^n \,\&\, x(m) = x(n))\}.$$

Then $C \in \mathrm{P}$ and there is an $i \leqslant 1$ such that $A \upharpoonright s * \langle i \rangle \in C$ infinitely often. So, since A is p-generic, there is an $s \in \mathbb{N}$ such that $A \upharpoonright s \in C$. It follows that $\bar{A} \not\leqslant_m^p A$ via f, contradicting the assumption.

(iii): To simplify notation, we only prove the case $n=3$. The extension to the general case is straightforward.

For a contradiction, assume $D_3 \leqslant_{2\text{-tt}}^p A$, say via f_0, f_1, f_2. W.l.o.g., we may assume

$$f_1(\{0\}^*) \cup f_2(\{0\}^*) \subseteq \{0\}^* \quad \text{and} \quad \forall k\ (f_1(0^k) < f_2(0^k)).$$

We distinguish the following cases.

Case 1: there are infinitely many k such that $f_2(0^k) > 0^{3k+2}$ and $f_0(0^k, A(f_1(0^k)), 0) \neq f_0(0^k, A(f_1(0^k)), 1)$. Then A has infinitely many chances to hit the polynomial time computable set

$$C = \{x : \exists k, l, m < |x|\ [|x| = m+1\ \&\ f_1(0^k) = 0^l\ \&\ f_2(0^k) = 0^m$$
$$\&\ m > 3k+2\ \&\ f_0(0^k, x(l), x(m)) \neq x(3k) \cdot x(3k+1) \cdot x(3k+2)]\}$$

and thus it hits C. By definition of C, this implies that $D_3 \leqslant_{2\text{-tt}}^p A$ via f_0, f_1, f_2 does not hold: a contradiction.

Case 2: otherwise. Distinguish the following two subcases.

Case 2.1: there are infinitely many k such that $f_1(0^k) > 0^{3k+2}$ and $f_0(0^k, 0, i) \neq f_0(0^k, 1, i)$ for some $i \leqslant 1$. Then, let

$$C = \{x : \exists k, l < |x|\ [|x| = l+1\ \&\ f_1(0^k) = 0^l\ \&\ l > 3k+2$$
$$\&\ \exists i \leqslant 1 (f_0(0^k, x(l), i) \neq x(3k) \cdot x(3k+1) \cdot x(3k+2))]\}.$$

Obviously, $C \in \mathrm{P}$ and A has infinitely many chances to hit C. Hence, by Theorem 5.2, there are infinitely many numbers k such that $f_1(0^k) > 0^{3k+2}$ and

$$f_0(0^k, A(f_1(0^k)), i) \neq A(0^{3k}) \cdot A(0^{3k+1}) \cdot A(0^{3k+2})$$

for some $i \leqslant 1$. Since
Case 1 fails and $f_2(0^k) > f_1(0^k)$, this implies

$$f_0(0^k, A(f_1(0^k)), A(f_2(0^k))) \neq A(0^{3k}) \cdot A(0^{3k+1}) \cdot A(0^{3k+2}) = D_3(0^k)$$

for infinitely many numbers k, contrary to our assumption that $D_3 \leqslant_{2\text{-tt}}^p A$ via f_0, f_1, f_2.

Case 2.2: otherwise. Then there is some k_0 such that, for $k \geqslant k_0$, the value of $f_0(0^k, A(f_1(0^k)), A(f_2(0^k)))$ only depends on $A \upharpoonright 3k+3$. So if we let $\hat{f}_i(0^k) = f_i(0^k)$ if $f_i(0^k) \leqslant 0^{3k+2}$ and $\hat{f}_i(0^k) = 0$ otherwise $(i = 1, 2)$, then $f_0(0^k, A(f_1(0^k)), A(f_2(0^k))) = f_0(0^k, A(\hat{f}_1(0^k)), A(\hat{f}_2(0^k)))$ for $k \geqslant k_0$. Now, let

$$C = \{x : \exists k, l, m < |x|\ [k \geqslant k_0\ \&\ |x| = 3k+3\ \&\ \hat{f}_1(0^k) = 0^l\ \&\ \hat{f}_2(0^k) = 0^m$$
$$\&\ f_0(0^k, x(l), x(m)) \neq x(3k) \cdot x(3k+1) \cdot x(3k+2)]\}.$$

Then $C \in \mathrm{P}$ and, for each string y of length $3k$, $k \geqslant k_0$, there is an extension x of y such that $|x| = 3k+3$ and $x \in C$. So, by Theorem 5.2, A hits C, whence not $D_3 \leqslant_{2\text{-tt}}^p A$ via f_0, f_1, f_2.

(iv) immediately follows from (iii). $\square$

6. On the complexity of p-generic sets

We now turn to the question how complex p-generic sets are. We first note that there are p-generic sets which can be computed in exponential time while, on the other hand, there are p-generic sets of arbitrarily high complexity.

Theorem 6.1. (a) *There is a p-generic set A such that* $A \in \mathrm{DTIME}(2^{cn})$.

(b) *For any recursive set B there is a recursive p-generic A such that* $A \not\leq_T^p B$.

The proof of Theorem 6.1(a) is a straightforward variant of that of Theorem 4.3 based on the observation that, for each requirement R_e, there is a polynomial q_e such that, given $A\upharpoonright s$, we can decide in $q_e(|A\upharpoonright s|) = q_e(s)$ steps whether R_e requires attention and if so, compute the least i such that $A\upharpoonright s*\langle i\rangle \in R_e$ (i.e., the value i 'R_e wants $A(0^s)$ to have'). We omit the proof since Theorem 6.1(a) is a direct consequence of the existence of a universal set for P in $\mathrm{DTIME}(2^n)$ and of Theorem 6.2 below.

To prove (b), merge the requirements of Theorem 4.3 with requirements $\hat{R}_e$: $A \neq M_e^B$ which are handled in the usual way (see [13]).

We say a set U is universal for P if, for some polynomial time computable and invertible bijection $\langle\,,\rangle: \mathbb{N}\times\Sigma^* \to \Sigma^*$, $\{U^{(n)} : n\in\mathbb{N}\} = P$, where $U^{(n)} = \{x : \langle n, x\rangle \in U\}$.

Theorem 6.2. *Let U be universal for* P. *Then there is a p-generic set A such that* $A \leq_T^p U$.

Proof. In the proof of Theorem 4.3, replace all occurrences of P_e by $U^{(e)}$. Then the constructed set A can be (p-T)-reduced to U. □

Theorem 6.2 shows that p-generic sets are not more complicated than universal sets for P. In particular, since there are universal sets of subexponential complexity, there are p-generic sets of subexponential complexity, too. This leads to the question whether—or under which hypotheses—there are p-generic sets in NP.

Before turning to this question, we note that there is no simplest p-generic set.

Theorem 6.3. *Let A be a recursive p-generic set. Then there is a p-generic set $\hat{A}$ such that* $\hat{A} <_m^p A$.

Proof. Let $\hat{A} = \{0^n : 0^{2n} \in A\}$. Obviously, $\hat{A} =_m^p A \cap \{0^{2n} : n\in\mathbb{N}\}$. So $\hat{A} <_m^p A$ by Corollary 5.6. To prove that $\hat{A}$ is p-generic, fix $C \in P$ and assume that $\exists^\infty s\, \exists i \leq 1$ $(\hat{A}\upharpoonright s*\langle i\rangle \in C)$. Let

$$C' = \{x : |x| \text{ is odd } \& \text{ ev}(x) \in C\},$$

where, for $|x| = 2n+1$, $|\text{ev}(x)| = n+1$ and $\text{ev}(x)(i) = x(2i)$, $i \leq n$. Obviously $C' \in P$ and

$$\hat{A}\upharpoonright s*\langle i\rangle \in C \Leftrightarrow (A\upharpoonright 2s+1)*\langle i\rangle \in C'.$$

So, by p-genericity of A, A hits C' and thus $\hat{A}$ hits C. □

The existence of sets with certain structural properties, like p-immunity, in the class NP has been shown to be oracle dependent, i.e., there are (recursive) sets A and B such that there is a set with that (relativized) property in NP^A but no set in NP^B has that property (cf. [10]). We now show that the existence of p-generic sets in NP is oracle dependent, too.

Definition 6.4. For any B, a tally set A is *p^B-generic* if, for every $C \in \mathrm{P}^B$, condition (4.1) holds.

Theorem 6.5. *There are recursive sets A and B such that*
(i) $\mathrm{P}^A \neq \mathrm{NP}^A$ *and there is a set in* NP^A *which is p^A-generic*;
(ii) $\mathrm{P}^B \neq \mathrm{NP}^B$ *and no* NP^B*-set is p^B-generic.*

Proof. (i): We construct a recursive set A in stages such that the NP^A-set

$$D = \{0^n : \exists x \in A \ (|x| = n)\}$$

is p^A-generic. For this sake it suffices to meet the requirements

$$\boldsymbol{R}_e: \quad \exists^\infty s \, \exists i \leq 1 \ (D{\upharpoonright}s * \langle i \rangle \in M_e^A) \Rightarrow \exists s \ (D{\upharpoonright}s \in M_e^A),$$

for all $e \in \mathbb{N}$.

The part of A enumerated by the end of stage s in the construction below is denoted by A_s, and we let D_s be the string of length s such that, for $n < s$, $D_s(n) = 1$ iff $\exists x \in A_s \ (|x| = n)$. We will ensure that for each s there is at most one string of length s in A and if such an x exists, then x is enumerated in A at stage $s+1$. So we will have $A_s = A{\upharpoonright}s$ and $D_s = D{\upharpoonright}s$.

As in the proof of Theorem 4.3, the requirements are assigned priorities, $\boldsymbol{R}_n$ having higher priority than $\boldsymbol{R}_m$ iff $n < m$.

For each requirement $\boldsymbol{R}_e$ and each stage s there will be a finite set $R(e, s) \subseteq \Sigma^*$ called the *restraint set* of $\boldsymbol{R}_e$ at stage s. The purpose of $R(e, s)$ is to ensure for certain strings x that $M_e^{A_s}(x) = M_e^A(x)$ provided that $A \cap R(e, s) = \emptyset$. Strings in $R(e, s)$ can be enumerated in A after stage s only for the sake of requirements of higher priority than $\boldsymbol{R}_e$.

We say $\boldsymbol{R}_e$ is *satisfied at stage* s if, for some $t \leq s$, $D_t \in M_e^{A_s}$ and if all strings x of length $\geq s$ which are used in the computation $M_e^{A_s}(D_t)$ are elements of $R(e, s)$. An intermediate restraint set $\hat{R}(e, s)$ for $\boldsymbol{R}_e$, $e \leq s$, at the beginning of stage $s+1$ is defined by

$$\hat{R}(e, s) = R(e, s) \cup \{x : |x| \geq s \text{ and } x \text{ is used in one of the computations } M_e^{A_s}(D_s * \langle 0 \rangle) \text{ and } M_e^{A_s}(D_s * \langle 1 \rangle)\}.$$

Note, that by the second clause of the definition of $\hat{R}(e, s)$, $A \cap \hat{R}(e, s) = \emptyset$ implies $M_e^A(D_s * \langle i \rangle) = M_e^{A_s}(D_s * \langle i \rangle)$, $i = 0, 1$.

Finally we say R_e *requires attention at stage* $s+1$ if $e \leq s$ and the following hold:

$$R_e \text{ is not satisfied at stage } s; \tag{6.1}$$

$$\exists x \left(|x| = s \text{ and } x \notin \bigcup_{e' \leq e} \hat{R}(e', s) \right); \tag{6.2}$$

$$\exists i \leq 1 \ (M_e^{A_s}(D_s * \langle i \rangle) = 1). \tag{6.3}$$

We now give the *construction of* A and of the restraint sets $R(e, s)$.

Construction of A

Stage 0: $A_0 = R(e, 0) = \emptyset$ for all $e \in \mathbb{N}$.

Stage $s+1$: If no requirement requires attention, then let $A_{s+1} = A_s$, and

$$R(e, s+1) = \begin{cases} \hat{R}(e, s) & \text{if } e \leq s, \\ \emptyset & \text{if } e > s; \end{cases}$$

otherwise choose e and i minimal (in this order) such that R_e requires attention and $M_e^{A_s}(D_s * \langle i \rangle) = 1$. Let

$$A_{s+1} = \begin{cases} A_s & \text{if } i = 0, \\ A_s \cup \{x'\} & \text{if } i = 1, \end{cases}$$

where x' is the least x witnessing condition (6.2), and

$$R(e', s+1) = \begin{cases} \hat{R}(e', s) & \text{if } e' \leq e, \\ \emptyset & \text{if } e' > e \end{cases}$$

Also say R_e is *active*. This completes the construction.

Note that the construction is effective, $A_s = A \upharpoonright s$, and $D_s = D \upharpoonright s$. It follows that A is recursive. To show that the requirements R_e are met, we prove a series of claims.

Claim 1. *If* R_e *is active at stage* $s+1$, *then* R_e *is satisfied at stage* $s+1$.

Proof. If R_e is active at stage $s+1$, then, for some $i \leq 1$, $M_e^{A_s}(D_s * \langle i \rangle) = 1$ and, by definition of A_{s+1}, for the least such i, $D_{s+1} = D_s * \langle i \rangle$. Moreover, any string x used in the computation $M_e^{A_s}(D_s * \langle i \rangle)$ such that $|x| \geq s$ is in $\hat{R}(e, s)$ and no element of $\hat{R}(e, s)$ is in $A_{s+1} - A_s$, whence $M_e^{A_{s+1}}(D_{s+1}) = M_e^{A_s}(D_{s+1}) = 1$. □

Let $R(e) = \{x : \exists s_x \ \forall s \geq s_x \ (x \in R(e, s))\}$ and say R_e is *permanently satisfied* if it is satisfied at some stage s such that $R(e, s) \subseteq R(e)$.

Claim 2. (i) *If no requirement* $R_{e'}$, $e' < e$, *requires attention after stage* s, *then*

$$\forall t \geq s \ (R(e, s) \subseteq R(e, t) \subseteq \hat{R}(e, t) \subseteq R(e)).$$

(ii) $R(e) \cap A = \emptyset$.

Proof. By induction. □

Claim 3. *If $\boldsymbol{R}_e$ is permanently satisfied, then, for some s, $D\uparrow s$ hits M_e^A and $\boldsymbol{R}_e$ is satisfied at every stage $t \geq s$.*

Proof. By Claim 2. □

Claim 4. *$\boldsymbol{R}_e$ requires attention at most finitely often.*

Proof. By induction on e. Fix e and, by inductive hypothesis, choose s_0 such that no requirement $\boldsymbol{R}_{e'}$, $e' < e$ requires attention after stage s_0. Now, if $\boldsymbol{R}_e$ requires attention at a stage $s_1 + 1 > s_0$, then $\boldsymbol{R}_e$ becomes active at stage $s_1 + 1$ and thus, by Claims 2 and 3, $\boldsymbol{R}_e$ is satisfied at stage $s_1 + 1$ and all later stages. So $\boldsymbol{R}_e$ does not require attention after stage $s_1 + 1$. □

Let $r(e, s) = |\bigcup\{\hat{R}(e', s) : e' \leq e\}|$. Note that

$$|\hat{R}(e, s)| \leq \sum_{s' \leq s} 2 \cdot p_e(s').$$

So $\lambda s.r(e, s)$ is bounded by a polynomial. The next claim now follows.

Claim 5. *For each e there is a stage s_e such that $\forall s > s_e\ (r(e, s) < 2^{s+1})$.*

Claim 6. *Requirement $\boldsymbol{R}_e$ is met.*

Proof. W.l.o.g., assume that

$$\exists s\ (D\uparrow s \in M_e^A). \tag{6.4}$$

By Claims 4 and 5, choose $s_1 > e$ such that no requirement $\boldsymbol{R}_{e'}$, $e' \leq e$, requires attention after stage s_1 and such that $\forall s > s_1\ (r(e, s) < 2^{s+1})$. Then, by Claims 2 and 3 and (6.4), $\boldsymbol{R}_e$ is not satisfied at any stage $s > s_1$. Since $\boldsymbol{R}_e$ does not require attention after stage s_1, this implies that, for no $s > s_1$, condition (6.3) holds, i.e.,

$$\forall s \geq s_1\ \forall i \leq 1\ (M_e^{A_s}(D\uparrow s * \langle i\rangle) = 0).$$

By definition of $R(e, s)$, the choice of s_1, and Claim 2, it now follows that

$$\forall s \geq s_1\ \forall i \leq 1\ (M_e^A(D\uparrow s * \langle i\rangle) = 0)$$

and thus that $\boldsymbol{R}_e$ is met. □

The proof of Claim 6 also completes the proof of Theorem 6.5(i).

(ii): Homer and Maass [10] have constructed a recursive oracle B such that $\mathrm{P}^B \neq \mathrm{NP}^B$ and no NP^B-set is p^B-immune. Since the proof of Theorem 5.3 relativizes, i.e., since p^B-generic sets are p^B-immune, this implies that no NP^B set is p^B-generic. This completes the proof of Theorem 6.5. □

Corollary 6.6. *Let Q be a property which can be enforced by a p-standard diagonalization. Furthermore, assume that this fact relativizes. Then there is a recursive set A such that $\mathrm{P}^A \neq \mathrm{NP}^A$ and there is a (tally) NP^A-set with property Q^A.*

Proof. With Theorem 5.6 and the relativized version of Proposition 4.2(ii) this theorem is easily proved. □

Since the common proofs that a property can be enforced by p-standard diagonalization trivially relativize, Corollary 6.6 provides a new, simple approach for obtaining oracle dependence results. To show that the existence of sets with a certain property Q in NP can neither be proved nor be refuted by an argument which relativizes, it suffices to show that $\mathrm{Q}\cap \mathrm{P}=\emptyset$ and Q can be enforced by p-standard diagonalization and that these facts relativize. For instance, by relativizing Theorem 5.3, we obtain the following corollary.

Corollary 6.7. *There are recursive sets A and C such that $C\in \mathrm{NP}^A$ and C is p^A-immune but not p^A-selective.*

7. Limitations of p-standard diagonalizations

Our notion of p-standard diagonalization covers the common diagonalizations over polynomial time computable sets and functions. In particular, it subsumes diagonalizations over polynomial time bounded *many-one* reductions. In general, it does not cover however diagonalizations over polynomial time bounded *Turing* reductions. The latter type of diagonalizations requires us to consider extensions of the set under construction of polynomial length and not just extensions of length 1 (or of constant length), as in the case of p-standard diagonalizations.

To illustrate this limitation on p-standard diagonalizations, we show that, in contrast to Corollary 5.6, there are a p-generic set A and a polynomial time computable set B such that $B\cap\{0\}^*$ and $\bar{B}\cap\{0\}^*$ are infinite and $A\cap B =^p_T A$. To obtain this result, we first prove a lemma.

Lemma 7.1. *There is a p-generic set A such that*

$$\forall n\in\mathbb{N}\quad (0^{2n+1}\in A \Leftrightarrow |A\cap I_n|\geqslant n), \tag{7.1}$$

where $I_n=\{0^{2i}: n^2<i<(n+1)^2\}$.

Proof. The construction of a set A with the desired properties is based on the construction of a p-generic set given in Section 4. We start with some simple observations regarding the *intervals* I_n.

$$\forall x\in I_n\quad (2n+1<|x|), \tag{7.2}$$

$$2n\leqslant |I_n| \quad\text{and}\quad I_n \text{ is finite}, \tag{7.3}$$

$$n\neq m \Rightarrow I_n\cap I_m=\emptyset. \tag{7.4}$$

We call a number s an *n-number* if $0^s\in I_n$.

Now the basic idea for satisfying (7.1) is the following. If a stage s is an n-number, then only requirements R_i, $i \leq n-1$, may become active at stage $s+1$, and if no requirement is active at stage $s+1$, then we let $A(0^s) = A(0^{2^{n+1}})$. Note that, by (7.2), $A(0^{2^{n+1}})$ has been defined at a previous stage. Moreover, since each requirement is active at most once, $A(0^s) = A(0^{2^{n+1}})$ for all but at most $n-1$ n-numbers s by (7.4), whence (7.1) will hold by (7.3).

Using the notation and the requirements of the proof of Theorem 4.3 this leads to the following construction.

Construction

Stage 0: Do nothing.

Stage $s+1$: Define k by $k = n-1$ if s is an n-number, and by $k = s$ otherwise. If no requirement R_e, $e \leq k$, requires attention, let $A(0^s) = A(0^{2^{n+1}})$ if s is an n-number, and $A(0^s) = 0$ otherwise. Otherwise choose e and i minimal (in this order) such that R_e requires attention and $A\upharpoonright s * \langle i \rangle \in P_e$, and set $A(0^s) = i$. Also say that R_e is *active*.

As in the proof of Theorem 4.3, we can show that each requirement R_e requires attention only finitely often, is active at most once, and is met. For the proof that R_e is met, we only have to note that there are only finitely many stages $s+1$ such that s is an n-number for some $n \leq e+1$ (by (7.3)), whence R_e is prevented from acting by the additional restraints introduced in this construction only finitely often. Finally, it follows from the remarks preceding the construction that the constructed set A satisfies (7.1). □

Theorem 7.2. *There is a p-generic set A such that* $A \cap \{0^{2^n} : n \in \mathbb{N}\} =_T^p A$.

Proof. Fix A as in Lemma 7.1 and define $f : \{0\}^* \to \{0\}^*$ by

$$A \cap \{0^{2^{n+1}} : n \in \mathbb{N}\} \leq_T^p A \cap \{0^{2^n} : n \in \mathbb{N}\}.$$

Obviously, this implies $A \cap \{0^{2^n} : n \in \mathbb{N}\} =_T^p A$. □

We conclude this section with a further application of Lemma 7.1. Recall that a one-to-one and onto function $f : \Sigma^* \to \Sigma^*$ or $f : \{0\}^* \to \{0\}^*$ is a *p-isomorphism* if f and its inverse f^{-1} both are polynomial time computable. Note that, with f, f^{-1} is a p-isomorphism, too.

A property Q (of tally sets) is called *p-invariant* if, for $A \in \mathrm{Q}$ and any p-isomorphism $f : \Sigma^* \to \Sigma^*$ ($f : \{0\}^* \to \{0\}^*$), $f(A) \in \mathrm{Q}$ again. As one can easily check, most of the structural properties studied in the literature are p-invariant. For p-immunity this follows from the observation that p-isomorphisms map infinite polynomial time computable sets to such sets again. Similarly, if A is p-selective, if g is a selector function for A, and f a p-isomorphism, then $f \circ g \circ f^{-1}$ is a selector for $f(A)$. In contrast to these observations, p-genericity is not p-invariant.

Theorem 7.3. *p-Genericity is not p-invariant, i.e., there is a p-generic set A and a p-isomorphism* $f:\{0\}^* \to \{0\}^*$ *such that* $f(A)$ *is not p-generic.*

Proof. Fix A as in Lemma 7.1 and define $f:\{0\}^* \to \{0\}^*$ by

$$f(0^s) = \begin{cases} 0^{(2n+2)^2} & \text{if } s = 2n+1, \\ 0^{2n+1} & \text{if } s = (2n+2)^2, \\ 0^s & \text{otherwise.} \end{cases}$$

Then A is p-generic and, obviously, f is a p-isomorphism. We will show that $f(A)$ is not p-generic.

First, observe that, by (7.1),

$$\forall n \in \mathbb{N} \quad (0^{(2n+2)^2} \in f(A) \Leftrightarrow |f(A) \cap I_n| \geq n), \tag{7.5}$$

where $I_n = \{0^{2i} : n^2 < i < (n+1)^2\}$. (Note that $f(A) \cap I_n = A \cap I_n$.) Also note that

$$x \in I_n \Rightarrow |x| < (2n+2)^2. \tag{7.6}$$

Now consider the set

$$C = \{x : \exists n \ (|x| = (2n+2)^2 + 1 \text{ and } x((2n+2)^2) = 0$$
$$\text{iff there are at least } n \text{ numbers } i < |x| \text{ such that}$$
$$x(i) = 1 \text{ and } 0^i \in I_n)\}.$$

Obviously, $C \in \mathrm{P}$. Moreover, by (7.6), if a set B hits C, then

$$\exists n \in \mathbb{N} \quad (0^{(2n+2)^2} \notin B \Leftrightarrow |B \cap I_n| \geq n).$$

So, by (7.5), $f(A)$ does not hit C. On the other hand, every set has infinitely many chances to hit C. Hence, $f(A)$ is not p-generic. □

8. Generalized p-standard diagonalizations and strongly p-generic sets

In this section we will show that our formal diagonalization concept can be extended to cover also diagonalizations over polynomial time Turing reductions. Since in such a reduction the required information is spread out over an interval of polynomial length, we now have to consider extensions of such a length. Again we will see that there is a strongest property which can be enforced by this extended diagonalization concept and that there are recursive sets having this property. Due to the more complicated diagonalization however, these sets are more complex than p-generic sets.

Definition 8.1. (i) A property Q can be enforced by a *generalized p-standard diagonalization* if there is a sequence $\{C_e : e \in \mathbb{N}\}$ of polynomial time computable sets such that, for any tally set A, the following holds: if, for every $e \in \mathbb{N}$,

$$\exists \text{polynomial } p\ \exists^{\infty} s\ \exists x\ (|x| \leqslant p(s)\ \&\ A\upharpoonright s * x \in C_e) \Rightarrow \exists s\ (A\upharpoonright s \in C_e), \tag{8.1}$$

then A has property Q.

(ii) A tally set A is *strongly p-generic* if, for every $C \in \mathrm{P}$,

$$\exists \text{polynomial } p\ \exists^{\infty} s\ \exists x\ (|x| \leqslant p(s)\ \&\ A\upharpoonright s * x \in C) \Rightarrow \exists s\ (A\upharpoonright s \in C). \tag{8.2}$$

Note that any property enforceable by a p-standard diagonalization can be enforced by a generalized p-standard diagonalization. So any *strongly p*-generic is p-generic. Also one can easily see that strong p-genericity is the strongest property enforceable by a generalized p-standard diagonalization and that a property can be enforced by generalized p-standard diagonalization iff it is shared by all strongly p-generic sets. Furthermore, Theorem 5.1 carries over to strongly p-generic sets. Moreover, in contrast to the class of p-generic sets, the class of strongly p-generic sets is p-invariant.

Theorem 8.2. *Strong p-genericity is p-invariant.*

Proof. Let A be strongly p-generic and let $f: \{0\}^* \to \{0\}^*$ be a p-isomorphism. To prove that $f(A)$ is strongly p-generic, fix $C \in \mathrm{P}$ and a polynomial p such that

$$\exists^{\infty} s\ \exists x\ (|x| \leqslant p(s)\ \&\ f(A)\upharpoonright s * x \in C). \tag{8.3}$$

Then it suffices to show $f(A)\upharpoonright s \in C$ for some s.

Let $F: \mathbb{N} \to \mathbb{N}$ be the bijection induced by f on $\mathbb{N}$, i.e., $f(0^n) = 0^{F(n)}$. Then F is polynomial time computable and invertible (with respect to unary representation). So there is a polynomial q such that

$$F(n) \leqslant q(n) \quad \text{and} \quad F^{-1}(n) \leqslant q(n). \tag{8.4}$$

Now, define C' by

$$C' = \{x : \exists y \in C\ (|x| = \max\{F^{-1}(i) : i < |y|\} + 1 \\ \&\ \forall i < |y|\ (y(i) = x(F^{-1}(i))))\}.$$

Obviously, $C' \in \mathrm{P}$ and $0^0 \notin C'$. Moreover, if A hits C', say $(A\upharpoonright s+1) \in C'$, then $f(A)$ hits C, namely $f(A)\upharpoonright s' \in C$ for some number $s' \leqslant q(s)+1$. So, by strong p-genericity of A, it suffices to show

$$\forall n\ \exists s \geqslant n\ \exists x\ (|x| \leqslant r(s)\ \&\ A\upharpoonright s * x \in C'), \tag{8.5}$$

where r is the polynomial $r(n) = q(q(n) + p(q(n)))$.

For a proof of (8.5) fix n and, by (8.3), choose t and y such that $q(n) < t$, $|y| \leqslant p(t)$, and $f(A)\upharpoonright t * y \in C$. Let $z = f(A)\upharpoonright t * y$, $u = \max\{F^{-1}(i) : i < |z|\} + 1$, and let w be any string of length u such that

$$\forall i < |z| \quad (w(F^{-1}(i)) = z(i)).$$

Then $w \in C'$ and, by (8.4), $|w| \leq q(|z|)$, i.e., $|w| \leq q(t+p(t))$. Now let $s = \min\{k : F(k) \geq t\}$. Then, for $i < s$, $F(i) < t$ and thus $w(i) = z(F(i)) = f(A)\ (0^{F(i)})$.

It follows that there is a string x such that $A\uparrow s * x = w$. It remains to show that $|x| \leq r(s)$. First, note that $F(s) \geq t$, whence, by (8.4), $t \leq q(s)$. On the other hand, $|x| \leq |w|$ and, as shown above, $|w| \leq q(t+p(t))$. Hence,

$$|x| \leq q(q(s)+p(q(s))) = r(s). \qquad \square$$

Theorems 7.3 and 8.2 show that there are p-generic sets which are not strongly p-generic. In particular, there is no strongly p-generic set satisfying (7.1). A similar argument shows that there are p-generic but no strongly p-generic sets A satisfying

$$\nexists s > 0 \quad (A\uparrow 2s = A\uparrow s * \langle \underbrace{0, \ldots, 0}_{s\text{-times}} \rangle).$$

The increased power of generalized p-standard diagonalizations is further illuminated by the next theorem which gives an example for a diagonalization of p-Turing reductions captured by generalized p-standard diagonalization but not by p-standard diagonalizations (cf. Theorem 7.2).

Theorem 8.3. *Let A be strongly p-generic and let $B \in \mathrm{P}$ such that $\{0\}^* \cap \bar{B}$ is infinite. Then $A \cap B <_{\mathrm{T}}^{p} A$.*

Proof. Obviously, $A \cap B \leq_{\mathrm{T}}^{p} A$. So it suffices to show $A \not\leq_{\mathrm{T}}^{p} A \cap B$. For a contradiction, assume $A = M^{A \cap B}$, and p is a polynomial bound for M. W.l.o.g., $p(n) > n$. For a string x, let x_B be the string determined by $|x_B| = |x|$, $x_B(n) = x(n)$ for $0^n \in B$ and $x_B(n) = 0$ for $0^n \notin B$. Then, for

$$C = \{x : \exists n\ (|x| = p(n)\ \&\ x(n) \neq M^{x_B}(n))\},$$

$C \in \mathrm{P}$ and, for s such that $0^s \notin B$,

$$\exists x \quad (|x| < p(s)\ \&\ A\uparrow s * x \in C).$$

So, by infinity of $\{0\}^* \cap \bar{B}$ and by strong p-genericity of A, A will hit C. It follows that $A \neq M^{A \cap B}$, contrary to our assumption. $\square$

Corollary 8.4. *Let A be strongly p-generic and let $B \in \mathrm{P}$. Then, $A \cap B =_{\mathrm{T}}^{p} A$ iff $A \cap B =^* A$.*

Proof. We prove the nontrivial implication by contraposition. Assume $A \cap B =_{\mathrm{T}}^{p} A$ but $A - (A \cap B)$ is infinite. Then, $\{0\}^* \cap \bar{B}$ is infinite too, whence $A \cap B \neq_{\mathrm{T}}^{p} A$ by Theorem 8.3. $\square$

Corollary 8.5. *Let A be strongly p-generic and let $B \in \mathrm{P}$ such that $|B \cap \{0\}^*| = |\bar{B} \cap \{0\}^*| = \infty$. Then $A \cap B$ and $A \cap \bar{B}$ are (p-T)-incomparable.*

Proof. Since, for $B \in \mathrm{P}$, $\bar{B} \in \mathrm{P}$ too and since $A =_{\mathrm{T}}^{p} (A \cap B) \oplus (A \cap \bar{B})$, this is an immediate consequence of Theorem 8.3. $\square$

Note that by Corollary 8.5, any strongly p-generic set A is non-(p-T)-mitotic in the sense of Ambos-Spies [1]. We conclude with the proof that strongly p-generic sets actually exist.

Theorem 8.6. *There is a recursive strongly-p-generic set.*

Proof. The proof is similar to that of Theorem 4.3, though somewhat more involved. Given an enumeration $\{p_e : e \in \mathbb{N}\}$ of all polynomials, we construct a recursive set $A \subseteq \{0\}^*$ to meet the requirements

$$R_{\langle e,i\rangle}:\quad \exists^\infty s\, \exists x\, (|x| \leq p_i(s)\ \&\ A\upharpoonright s * x \in P_e) \Rightarrow \exists s\, (A\upharpoonright s \in P_e)$$

The construction of A is in stages. At stage $s+1$ we determine the value of $A(0^s)$. So by the end of stage s the enumeration of $A\upharpoonright s$ is completed.

Construction of A

Stage $s+1$: Requirement $R_{\langle e,i\rangle}$ *requires attention via* x if $\langle e,i\rangle \leq s$, $\nexists t \leq s\, (A\upharpoonright t \in P_e)$, $|x| \leq p_i(s)$, and $A\upharpoonright s * x \in P_e$.

If no requirement requires attention, then let $A(0^s) = 0$. Otherwise, choose $\langle e, i\rangle$ and x minimal (in this order) such that $R_{\langle e,i\rangle}$ requires attention via x, let $A(0^s) = x(0)$ and say $R_{\langle e,i\rangle}$ is *active via* x.

Obviously, the construction is effective and thus A is recursive. That A is strongly p-generic follows from the following claim.

Claim. *For every* e, i, $R_{\langle e,i\rangle}$ *requires attention at most finitely often and is met.*

The claim is proved by induction. Fix $\langle e, i\rangle$ and, by inductive hypothesis, choose s_0 such that no requirement R_n, $n < \langle e, i\rangle$, requires attention after stage s_0. Now distinguish two cases.

Case 1: $\exists s\, (A\upharpoonright s \in P_e)$. Then R_e is met and R_e does not require attention after the least stage s such that $A\upharpoonright s \in P_e$.

Case 2: $\nexists s\, (A\upharpoonright s \in P_e)$. Then distinguish two subcases.

Case 2.1: $\exists s_1\, \forall s \geq s_1\, \forall x\, (|x| \leq p_i(s) \Rightarrow A\upharpoonright s * x \notin P_e)$. Then $R_{\langle e,i\rangle}$ is met trivially and it stops requiring attention after stage s_1.

Case 2.2: otherwise. Then choose $s > s_0$ and x minimal (in this order) such that $|x| \leq p_i(s)\ \&\ A\upharpoonright s * x \in P_e$, say $x = \langle i_0, \ldots, i_k\rangle$. Then—as one can easily see—$R_{\langle e,i\rangle}$ is active at stage $s+m$ via $\langle i_{m-1}, \ldots, i_k\rangle$ for $m = 1, \ldots, k+1$. So $A\upharpoonright(s+k+1) = A\upharpoonright s * x \in P_e$, contrary to assumption. So this case cannot apply. This completes the proof of Theorem 8.6. $\square$

The construction can be modified to give a strongly p-generic set which is recognizable in double exponential time. As the second author has shown in his dissertation [8] however, there is no oracle A such that NP^A contains a strongly p-generic set.

9. Concluding remarks

In this final section we will relate our notion of (generalized) p-standard diagonalizations to other diagonalization concepts in computational complexity theory which can be found in the literature.

The most elementary type of diagonalizations one encounters are diagonalizations over recursively presentable (r.p) classes, i.e., classes of recursive sets which possess a recursive universal set. Since the class P is r.p., the construction of a recursive set $A \notin \mathrm{P}$ is an example for such a diagonalization. For some general results on indexings and diagonals of r.p. classes, see [12]. An important variant of diagonalizations over r.p. classes which in addition, are closed under finite variations (c.f.v.) is the *delayed diagonalization* or *looking back* technique (see, e.g., [7, 13, 15, 18]). Here, starting from a given diagonal, new diagonals with certain additional properties are constructed.

Most applications of the delayed diagonalization technique can be reduced to the following diagonalization lemma due to Schöning ([18], see also [2]): *given diagonals $D_1, \ldots, D_n$ for r.p. and c.f.v. classes $\mathrm{C}_1, \ldots, \mathrm{C}_n$ respectively, there is a diagonal D for the union $\mathrm{C}_1 \cup \cdots \cup \mathrm{C}_n$ of these classes whose complexity is bounded by the sum of the given diagonals for the individual classes, i.e., $D \leq_m^p D_1 \oplus \cdots D_n$.* Delayed diagonalizations have been used to characterize the fine structure of NP under the assumption that $\mathrm{P} \neq \mathrm{NP}$ (see, e.g., [2, 13]).

The diagonalizations considered here are of a more general type, not limited to r.p. classes. For instance, the construction of a p-immune set (cf. Section 3) requires us to diagonalize over the not recursively presentable (in fact not even recursively enumerable) class of infinite recursive sets containing an infinite polynomial time computable set together with the finite sets. We can reduce the task of constructing a p-immune set, however, to the construction of a set A meeting an infinite effective sequence of finitary requirements, namely the requirements

$$\boldsymbol{R}_e: \quad \text{if } P_e \text{ is infinite, then } \bar{A} \cap P_e \neq \emptyset \quad (e \in \mathbb{N})$$

(cf. Section 3). These requirements are finitary in the following sense: if we construct A in stages by determining longer and longer initial segments of A, i.e., by letting $A_s = A \upharpoonright l(s)$, $l: \mathbb{N} \to \mathbb{N}$ some unbounded increasing (recursive) function, then requirement $\boldsymbol{R}_e$ can be met by considering finite extensions of certain initial parts $A \upharpoonright l(s)$ of A, i.e., by an appropriate choice of $l(s+1) > l(s)$ and by an appropriate definition of $A(x)$ for strings x of length $\geq l(s)$ and $< l(s+1)$ (see Section 3). In other words, each requirement $\boldsymbol{R}_e$ corresponds to a *witness set* C_e whose elements are finite initial parts of sets such that a set A meets $\boldsymbol{R}_e$ iff one of its initial parts belongs to C_e.

Diagonalization arguments of the just described type are very common in recursive function theory and are known as *finite extension arguments* (see, e.g., [16]). It is typical for these arguments that there are conflicts among the requirements, i.e., extensions of a given initial part belonging to the witness sets of two distinct requirements will in general be incompatible. On the other hand, no matter how the set A is constructed, in general, for each requirement $\mathbf{R}_e$, there will be infinitely many initial parts $A \upharpoonright l(s)$ of A possessing finite extensions in the witness set C_e of $\mathbf{R}_e$. So, by assigning priorities to the requirements, we can ensure that all requirements will be eventually met (cf. Section 3).

The complexity of diagonals constructed by finite extension arguments depends on both the complexity of the witness sets and on the length of the extensions we have to consider. In contrast to recursive function theory, we here consider only recursive witness sets (since we only have to diagonalize over classes whose elements are recursive sets). This restriction, however, does not automatically lead to recursive diagonals: if the length of the extensions is not bounded, then we cannot decide whether a given initial segment has an extension in some witness set. In recursive function theory, this difficulty is overcome by recursively bounding the length of the extensions in the length of the given initial segment; i.e., given $A_s = A \upharpoonright l(s)$, one only checks extensions of length $f(l(s))$, f some recursive function.

Then possible extensions of admissible lengths belonging to a witness set do not exist for all, but only for certain initial segments. So we cannot meet a requirement at any stage, but we have to wait for appropriate stages. (For this reason, such diagonalizations are also called *wait-and-see* arguments or—as in [5]—*slow diagonalizations.*)

Moreover, due to the bounded search it might happen that some extensions are missed and a requirement is not met. The latter case can be avoided by considering, at stage s for a requirement $\mathbf{R}_e$, not only extensions of $A \upharpoonright l(s)$ of length $f(l(s))$, but but also such extensions of (certain) $A \upharpoonright t$ for $t < l(s)$ and, if necessary, by *replacing* the initial segment $A \upharpoonright l(s)$ by a new extension of some $A \upharpoonright t$. In general, this procedure only yields a recursive approximation to the set A being constructed, i.e., the set A will not be recursive but only Δ_2^0 (see [16]). In a special variant of this technique, an initial segment may be replaced only by an initial segment which contains all the elements of the previously given initial segment, thus ensuring that the constructed set is recursively enumerable. This technique is known as *finite injury priority method.* For a detailed discussion of priority arguments, including ones refining the above described technique by admitting also infinitary requirements, we refer the reader to [20].

Fortunately, the above described obstacles do not occur if we diagonalize over complexity classes or enforce properties related to such classes by diagonalizations. In case of deterministic time or space classes, the complexity of the class is reflected both by the complexity of the witness sets and by the (recursive) bounds on the extensions which have to be considered. So in these cases always (recursively) *bounded extension arguments* will do; i.e., it suffices to consider extensions recursively bounded in the length of the given initial part. (Examples for such bounded extension arguments are, besides the constructions referred to and given in this paper, the constructions of [4] and others which yield recursive oracles separating relativized complexity classes.) In fact, for most applications it suffices to consider extensions of length 1, whence this case is treated separately here leading to the notion of

p-standard diagonalization for length-1 bounded extension arguments related to the class P which yield tally diagonals. The more general concept of generalized p-standard diagonalization aims at a formalization of general finite extension arguments related to P, based on the observation that the polynomial time bounds on the members of P can be reflected by polynomial bounds on the extensions one has to consider. Moreover, we restrict ourselves to diagonalizations over tally sets. As pointed out in Section 3, this decreases the complexity of generic sets by an exponential factor, thus allowing the construction of a (relativized) p-generic set in relativized NP. For a non-tally set G which is generic for length-1-extension diagonalization arguments over arbitrary polynomial time computable sets, the unary encoding $\text{TALLY}(G)$ of G is p-generic. Moreover, using the technique of [8] for proving that there are no strongly p-generic sets in NP, we can show that $\text{TALLY}(G) \notin$ NP, whence $G \notin \text{NTIME}(2^{cn})$ for any number c. So non-tally generic sets are too complex for providing strong separation results for (relativized) P and NP.

For a general treatment of these diagonalization techniques for arbitrary complexity classes see [8]. There, the question of possible tradeoffs between the complexity of the witness sets and the length of the bounds on the admissible extensions is also discussed.

References

[1] K. Ambos-Spies, p-Mitotic sets, in: E. Börger, G. Hasenjäger and D. Rodding, eds., *Logic and Machines: Decision Problems and Complexity*, Lecture Notes in Computer Science **171** (Springer, Berlin, 1984) 1-23.

[2] K. Ambos-Spies, Polynomial time degrees of NP-sets, in: E. Börger, ed., *Current Trends in Theoretical Computer Science* (Computer Science Press, Rockville, MD, 1987).

[3] K. Ambos-Spies, H. Fleischhack and H. Huwig, p-Generic sets, in: J. Paredaens, ed., *Proc. 11th Internat. Coll. on Automata, Languages and Programming*, Lecture Notes in Computer Science **172** (Springer, Berlin, 1984) 58-68.

[4] T. Baker, J. Gill and R. Solvay, Relativizations of the P = ? NP question, *SIAM J. Comput.* **4** (1975) 431-442.

[5] J.L. Balcazar, Separating, strongly separating and collapsing relativized complexity classes, in: M. P. Chytil and V. Koubek, eds., *Mathematical Foundations of Computer Science 1984*, Lecture Notes in Computer Science **176** (Springer, Berlin, 1984) 1-16.

[6] C.H. Bennett and J. Gill, Relative to a random oracle A, $P^A \neq NP^A \neq CO\text{-}NP^A$ with probability 1, *SIAM J. Comput.* **10** (1981) 96-113.

[7] P. Chew and M. Machtey, A note on structure and looking back applied to the relative complexity of computable functions, *J. Comput. System Sci.* **22** (1981) 53-59.

[8] H. Fleischhack, On diagonalizations over complexity classes, Dissertation, Universität Dortmund, 1985.

[9] H. Fleischhack, p-Genericity and strong p-genericity, in: J. Gruska et al., eds., *Mathematical Foundations of Computer Science 1986*, Lecture Notes in Computer Science **233** (Springer, Berlin, 1986) 341-349.

[10] S. Homer and W. Maass, Oracle-dependent properties of the lattice of NP-sets, *Theoret. Comput. Sci.* **24** (1983) 279-289.

[11] C.G. Jockusch Jr., Genericity for recursively enumerable sets, in: J.-D. Ebbinghaus et al., eds., *Recursion Theory Week*, Lecture Notes in Mathematics **1141** (Springer, Berlin, 1985) 203-232.

[12] D. Kozen, Indexing of subrecursive classes, *Theoret. Comput. Sci.* **11** (1980) 277-301.

[13] R.E. Ladner, On the structure of polynomial time reducibility, *J. ACM* **22** (1975) 155-171.
[14] R.E. Ladner, N.A. Lynch and A.L. Selman, A comparison of polynomial time reducibilities, *Theoret. Comput. Sci.* **1** (1975) 103-123.
[15] L. Landweber, R. Lipton and E. Robertson, On the structure of sets in NP and other complexity classes, *Theoret. Comput. Sci.* **15** (1981) 181-200.
[16] M. Lerman, *Degrees of Unsolvability* (Springer, Berlin, 1983).
[17] W. Maass, Recursively enumerable generic sets, *J. Symbolic Logic* **47** (1982) 809-823.
[18] U. Schöning, A uniform approach to obtain diagonal sets in complexity classes, *Theoret. Comput. Sci.* **18** (1982) 95-103.
[19] A.L. Selman, p-Selective sets, tally languages, and the behaviour of polynomial time reducibilities on NP, *Math. Systems Theory* **13** (1979) 55-65.
[20] R.I. Soare, *Recursively Enumerable Sets and Degrees* (Springer, Berlin, 1987).