Undecidability Results for low complexity time classes*

Rod Downey[†]
Victoria University of Wellington,
André Nies[‡]
The University of Chicago

Abstract

We prove that the theory of EXPTIME degrees with respect to polynomial time Turing and many-one reducibility is undecidable. To do so we use a coding method based on ideal lattices of Boolean algebras which was introduced in Nies [12]. The method can be applied in fact to all time classes given by a time constructible function which dominates all polynomials. By a similar method, we construct an oracle U such that $\mathrm{Th}(\mathrm{NP}^U, \subseteq)$ is undecidable.

1 Introduction

If h is a time constructible function which dominates all polynomials, then, by the methods of the deterministic time hierarchy theorem, DTIME(h) properly contains PTIME. Therefore, a polynomial time reducibility like polynomial time many–one or Turing reducibility induces a nontrivial degree structure on DTIME(h), which is an uppersemilattice with a least element. By the methods of Ladner [10] (also see ([11] or [5, Chapter I.7]), this degree structure is dense. This was so far the only fact known to hold in general for all such structures. Here we prove that all those degree structures are necessarily complicated, because they have an undecidable first–order theory. In fact, this holds for the degree structure induced on any class of computable sets which contains DTIME(h). Thus, for instance the polynomial

*A preliminary version of part of this paper was published in [7]

[†]Partially supported by the New Zealand Marsden Fund for Basic Science under grant VIC-509

[‡]Partially supported by NSF grant DMS–9500983, NSF binational grant INT-9602579 and the New Zealand Marsden Fund for Basic Science under grant VIC-509.

T-degrees and many–one degrees of sets in EXPTIME or in DTIME(2^n) have an undecidable theory.
Our results improve previous undecidability results for degree structures in complexity theory, where no reasonable bound on the complexity of the sets involved could be given. Slaman and Shinoda [13] proved that the theory of the polynomial time Turing-degrees of computable sets interprets $\mathrm{Th}(\mathbb{N}, +, \times)$ (and therefore is undecidable), but left open the case of many-one-reducibility. Three years later, Ambos–Spies and Nies [2] obtained undecidability of the theory of the polynomial time many-one-degrees of computable sets. Both proofs make use of the speed–up technique introduced in [1] (which is reminiscent of Blum's speed–up theorem) in order to show that computably presented ideals can be represented as the intersection of two principal ideals. This technique necessarily produces sets of high complexity (usually nonelementary sets).
Most proofs that a problem is undecidable are indirect: one gives a reduction of a problem which is already known to be undecidable to the problem in question. For theories of structures, a particular type of reduction based on the notion of interpretations of structures is used. It applies the following strengthening for theories of the notion of undecidability: call a theory T in an effective first–order language L *hereditarily undecidable (h.u.)* if each set $X \subseteq T$ which contains the valid L–sentences (i.e. the sentences which can be inferred from $\emptyset$) is undecidable. (Here, a *theory* is a consistent set of first-order sentences in a given language which is closed under logical inference.)
The transfer principle, proved for instance in Burris and Sankappanavar [6], states that, if $\boldsymbol{A}$ is an L_1–structure, $\boldsymbol{B}$ is an L_2–structure and $\boldsymbol{A}$ can be interpreted in $\boldsymbol{B}$ with parameters, then

$$(1) \qquad \mathrm{Th}(\boldsymbol{A}) \text{ h.u. } \Rightarrow \mathrm{Th}(\boldsymbol{B}) \text{ h.u.}$$

See Hodges [9, Ch. 5] for a detailed definition of the concept of interpretations of structures. Here we only need the special case that $\boldsymbol{A}$ is a partial order.

Definition 1.1 *An interpretation (or coding) of $\boldsymbol{A}$ in $\boldsymbol{B}$ with a list of parameters $\overline{p}$ is given by formulas*

$$(2) \qquad \varphi_{dom}(x; \overline{p}), \;\; \varphi_{\leq}(x, y; \overline{p})$$

such that, with an appropriate assignment of a list of elements $\overline{\boldsymbol{b}}$ in $\boldsymbol{B}$ to $\overline{p}$, the second formula defines a preordering on $\{c : \boldsymbol{B} \models \varphi_{dom}(c; \overline{\boldsymbol{b}})\}$ so that the partial order obtained by taking the quotient is isomorphic to $\boldsymbol{A}$.

We make use of coding methods developed in Nies [12], where it is shown that intervals of the lattice $\mathcal{E}$ of r.e. sets under inclusion are either boolean algebras or have an undecidable theory. As a tool, in [12] an undecidability result for the lattice of Σ^0_k-ideals of certain Σ^0_k-boolean algebras is proved. Then, an interpretation of such an ideal lattice of a Σ^0_3-boolean algebra in intervals of $\mathcal{E}$ is given. Our proof proceeds along the same lines: we give an interpretation of the lattice of Σ^0_2–ideals of an appropriate Σ^0_2-boolean algebra, which satisfies the "effective density" criterion needed for the auxiliary undecidability result in [12]. By an application of the transfer principle (1), we obtain the desired undecidability result for our degree structures. The boolean algebra used here is Σ^0_2 because, within a computably presented class $(A_i)_{i\in\omega}$, the question "$A_i \leq^p_r A_j$" is Σ^0_2 in i, j.
Notation We assume that all alphabets Σ contain the symbols $0, 1$. Sets will be subsets of Σ^* unless otherwise mentioned. For sets $X, Y, X \oplus Y$ denotes the set $0X \cup 1Y$.
Given a reducibility $\leq^p_r$, we denote the degree of a computable set X by $\boldsymbol{x}$ and also write $deg^p_r(X)$ for $\boldsymbol{x}$. Rec^p_r is the structure of r-degrees of computable sets. The least element of Rec^p_r, namely the degree consisting of the sets in PTIME, is denoted by $\mathbf{o}$, and $[\mathbf{o}, \boldsymbol{a}]$ denotes the initial interval of r-degrees $\leq \boldsymbol{a}$.
Un upper semilattice is *distributive* if it satisfies

$$(3) \qquad \forall \boldsymbol{x}\forall \boldsymbol{y}\forall \boldsymbol{z}[\boldsymbol{x} \leq \boldsymbol{y} \vee \boldsymbol{z} \;\Rightarrow\; \exists \boldsymbol{y}_0 \leq \boldsymbol{y}\exists \boldsymbol{z}_0 \leq \boldsymbol{z}\; \boldsymbol{x} = \boldsymbol{y}_0 \vee \boldsymbol{z}_0].$$

2 Σ^0_2– boolean algebras

We give a version of the concepts and result from [12] which is suitable for our use. A Σ^0_2*–boolean algebra* is a boolean algebra $\mathcal{B}$ which can be represented as a model

$$(4) \qquad (\mathbb{N}, \preceq, \vee, \wedge)$$

such that $\preceq$ is a Σ^0_2– relation which is a preordering, $\vee, \wedge$ are total computable binary functions, and the quotient structure

$$\mathcal{B} = (\mathbb{N}, \preceq, \vee, \wedge)/\approx$$

is a boolean algebra (where $n \approx m \Leftrightarrow n \preceq m \;\&\; m \preceq n$).

A Σ^0_2–boolean algebra $\mathcal{B}$ is *effectively dense* if there is a computable function F such that

$$x \not\approx 0 \Rightarrow 0 \prec F(x) \prec x. \tag{5}$$

We will identify a subset S of $\mathcal{B}$ with its corresponding preimage $\{n \in \mathbb{N} : n/_{\approx} \in S\}$. Thus, an ideal or a filter of $\mathcal{B}$ is called Σ^0_2 if its preimage is. The Σ^0_2– ideals form a sublattice $\mathcal{I}(\mathcal{B})$ of the distributive lattice of all ideals, because, for Σ^0_2– ideals I, J, the infimum $I \cap J$ and the supremum $I \vee J = \{b \vee c : b \in I \ \& \ c \in J\}^{\approx}$ are Σ^0_2 again.

Theorem 2.1 ([12]) *Suppose $\mathcal{B}$ is a Σ^0_2– boolean algebra which is effectively dense. Then $\mathcal{I}(\mathcal{B})$ has a hereditarily undecidable theory.*

Proof. Relativize the proof in [12] of the corresponding result for r.e. boolean algebras to $\emptyset'$ in order to show that $\mathcal{E}^4$, the partial order of Σ^0_4–sets under inclusion can be interpreted in $\mathcal{I}(\mathcal{B})$ with parameters. Since $\mathcal{E}^4$ has a h.u. theory, an application of the transfer principle (1) gives the desired result. (This works in fact if the function F in (5) is only Δ^0_2.) $\diamondsuit$

3 Undecidability Results

A polynomial time 1-tt reduction of X to Y is a polynomial time Turing reduction where in a computation at most one oracle question is asked. Thus

Definition 3.1 $X \leq^1_{tt} Y$ *if there are polynomial time computable functions $g : \Sigma^{<\omega} \times \{0,1\} \mapsto \{0,1\}$ and $h : \Sigma^{<\omega} \mapsto \Sigma^{<\omega}$ such that*

$$\forall w \in \Sigma^{<\omega} \ [X(w) = g(w, Y(h(x)))].$$

In the following, let $\leq^p_r$ be one of the reducibilities $\leq^p_m, \leq^p_{1-tt}, \leq^p_{btt}, \leq^p_{tt}$ or $\leq^p_T$. Suppose that $h : \mathbb{N} \mapsto \mathbb{N}$ is an increasing time constructible function with $P \subset \mathrm{DTIME}(h)$, so that h eventually dominates all polynomials. Let $\boldsymbol{D}_r(h)$ denote the degree structure induced by $\leq^p_r$ on $\mathrm{DTIME}(h)$.

Theorem 3.2 *The elementary theory of $\boldsymbol{D}_r(h)$ is undecidable.*

Proof. We give an interpretation of $\mathcal{I}(\mathcal{B})$, for an appropriate effectively dense Σ^0_2–boolean algebra $\mathcal{B}$. The plan of the proof is to make $\mathcal{B}$ a very easy, well controlled part of $\boldsymbol{D}_r(h)$, but to use all of $\boldsymbol{D}_r(h)$ to sort out Σ^0_2–ideals of

$\mathcal{B}$. We begin with $\mathcal{B}$. For a degree $\boldsymbol{a} \in \boldsymbol{D}_r(h)$, we let $\mathcal{B}(\boldsymbol{a})$ be the set of complemented elements in $[\mathbf{o}, \boldsymbol{a}]_{\boldsymbol{D}_r(h)} := [\mathbf{o}, \boldsymbol{a}] \cap \boldsymbol{D}_r(h)$, i.e.

$$\mathcal{B}(\boldsymbol{a}) = \{\boldsymbol{x} \leq \boldsymbol{a} : \exists \boldsymbol{y}\ \boldsymbol{x} \wedge \boldsymbol{y} = \mathbf{o}\ \&\ \boldsymbol{x} \vee \boldsymbol{y} = \boldsymbol{a}\}. \tag{6}$$

We will let $\mathcal{B} = \mathcal{B}(\boldsymbol{a})$ where $\boldsymbol{a}$ is the r–degree of a set A enjoying the following strong sparseness property introduced by Ambos-Spies.

Definition 3.3 ([1]) *A is* super sparse *via f if*

1. *f is a strictly increasing, time constructible function $\mathbb{N} \mapsto \mathbb{N}$*
2. *$A \subseteq \{0^{f(k)} : k \in \mathbb{N}\}$ and "$0^{f(k)} \in A$?" can be determined in time $O(f(k+1))$*

Moreover, in addition to [1] we require that

3. *$(\forall r \in \mathbb{N})(a.e.\ n)\ [f(n)^r < f(n+1)]$.*

A string w is relevant *if $w = 0^{f(k)}$ for some k.*

Because of the time-constructibility of f, by a standard argument ([5]) we obtain

Fact 3.4 *The set of relevant strings is in* PTIME. $\diamondsuit$

Polynomial time 1-*tt* reducibility is a reducibility of more technical interest. Here is one application of the notion, due to Ambos-Spies.

Theorem 3.5 ([1]) *Suppose A is super sparse. Then the polynomial time Turing-degree of any set $B \leq_T^p A$ consists of a single 1-tt–degree.* $\diamondsuit$

The proof of Theorem 3.5 is based on the fact that, in a Turing reduction to a super sparse set, all oracle queries except the one of maximal length can be eliminated, since they are so short that they can be answered in time polynomial in the length of the input.
Super sparse sets exist in all the time classes we consider.

Lemma 3.6 ([1]) *Suppose that $h : \mathbb{N} \mapsto \mathbb{N}$ is an increasing time constructible function with* PTIME $\subset$ DTIME(h)*, so that $h(n) \geq n+1$ and h eventually dominates all polynomials. Then there is a super sparse computable $A \in$* DTIME$(h) -$ PTIME.

Sketch of the proof. Let $f(n) = h^{(n)}(0)$. Since h eventually dominates all polynomials, we can construct $A \subseteq \{0^{f(k)} : k \in \mathbb{N}\}$ such that $A \in \textsc{Dtime}(h)$, but still diagonalize against all deterministic polynomial time machines. $\diamondsuit$

In the following let A be the set obtained in the preceding lemma and let $\boldsymbol{a} = \deg_r^p(A)$. Let

$$\mathcal{B} = \mathcal{B}(\boldsymbol{a}).$$

In a sequence of lemmas, we show that $\mathcal{B}$ is an effectively dense Σ_2^0-boolean algebra and interpret $\mathcal{I}(\mathcal{B})$ into $[\mathbf{o}, \boldsymbol{a}]$ without further parameters. While it may be the case that $[\mathbf{o}, \boldsymbol{a}] \not\subseteq \boldsymbol{D}_r(h)$, all the sets we need actually are in $\boldsymbol{D}_r(h)$. In this way we obtain a coding also in $\boldsymbol{D}_r(h)$. A *splitting* (or *split*) of a set B is a set X such that for some $R \in \textsc{Ptime}$, $X = B \cap R$. Note that, since h is hyperpolynomial (i.e., eventually dominates all polynomials), each split of A is in $\textsc{Dtime}(h)$. The advantage of taking a super sparse A is that not only is $\mathcal{B}(\boldsymbol{a})$ indeed a boolean algebra, but in fact it is effectively isomorphic to the boolean algebra of splittings of A, modulo the equivalence relation under which two splittings are identified if there symmetric difference is in $\textsc{Ptime}$. The isomorphism is obtained by mapping a split $A \cap R$ (represented by an index for a machine computing the $\textsc{Ptime}$ set R) to its degree. In this way, $\mathcal{B}$ is well controlled as desired. We could in fact easily ensure that A has no infinite $\textsc{Ptime}$ subsets. In that case $\mathcal{B}$ is isomorphic to the boolean algebra of splits modulo finite sets.

We first show that decomposing a super sparse set A into splits gives complements in $[\mathbf{o}, \boldsymbol{a}]$.

Lemma 3.7 *Suppose that A is super sparse and via f and $A_1 = A \cap R, A_2 = A \cap \overline{R}$ for some $R \in \textsc{Ptime}$. Then A_1 and A_2 form a Turing-minimal pair in the sense that if $Q \leq_T^p A_1, A_2$, then $Q \in P$.*

Proof. By Theorem 3.5, it is sufficient to prove that

$$Q \leq_{1\text{-}tt}^p A_1, A_2 \;\Rightarrow\; Q \in \textsc{Ptime}.$$

Suppose that $Q \leq_{1\text{-}tt}^p A_i$ via g_i, h_i $(i = 1, 2)$ as in Definition 3.1. The idea to show $Q \in \textsc{Ptime}$ is that, if both $h_1(w), h_2(w)$ are relevant oracle queries, then one of them must be much shorter than the other, so that membership of the shorter one in the appropriate oracle set can be determined in time polynomial in the input. The procedure is as follows. Given w, compute $h_1(w)$ and $h_2(w)$. If for some i $h_i(w)$ is not relevant, then $Q(w) = g_i(w, 0)$. Else,

1. if $k = |h_1(w)| = |h_2(w)|$, then see whether $0^k \in R$. If so, then $Q(w) = g_2(w, 0)$, else $Q(w) = g_1(w, 0)$.

2. Otherwise, say $|h_1(w)| < |h_2(w)|$. Evaluate $Q(w) = h_1(w, A_1(v))$, where $v = h_1(w)$. This is possible in polynomial time, because, by the definition of super sparseness, the computation for $A(v)$ takes at most $O(|h_2(w)|)$ many steps. $\diamondsuit$

Next we show that, conversely, each pair of complements in $[\mathbf{o}, \boldsymbol{a}]$ is represented by a decomposition of A into splits.

Lemma 3.8 *Suppose that $\boldsymbol{a}_1 \vee \boldsymbol{a}_2 = \boldsymbol{a}$ and $\boldsymbol{a}_1 \wedge \boldsymbol{a}_2 = \mathbf{o}$. Then there exists a split A_1 of A such that $A_1 \in \boldsymbol{a}_1$ and $A_2 = A - A_1 \in \boldsymbol{a}_2$. In particular, $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \boldsymbol{D}_r(h)$.*

Proof. It is sufficient to consider the case that $r \in \{m, 1\text{-}tt\}$. It is well known that $\leq_m^p$ and $\leq_{1\text{-}tt}^p$ induce distributive uppersemilattices, as defined in (3), on the computable sets. This is because, if $X \leq_r^p Y \oplus Z$, then there is $R \in$ PTIME such that $X \cap R \leq_r^p Y$ and $X \cap \overline{R} \leq_r^p Z$ (provided that $r \in \{m, 1\text{–}tt\}$). Now, pick sets $B_i \in \boldsymbol{a}_i$ and apply this to $A \leq_r^p B_1 \oplus B_2$ in order to obtain R. It is sufficient to show that in fact $A_1 = A \cap R \equiv_r^p B_1$ and $A_2 = A \cap \overline{R} \equiv_r^p B_2$. Notice that since $B_1 \leq_r^p A_1 \oplus A_2$, there is $Q \in$ PTIME such that $B_1 \cap Q \leq_r^p A_1$ and $B_1 \cap \overline{Q} \leq_r^p A_2$. But B_1, A_2 form an $r-$ minimal pair, so $B_1 \cap \overline{Q} \in$ PTIME and therefore $B_1 \equiv_r^p B_1 \cap Q \leq_r^p A_1$. $\diamondsuit$

Finally, we show that the order is preserved when passing from splits modulo PTIME-subsets of A to degrees.

Lemma 3.9 *Let $P, Q \in$ PTIME. Then*

$$A \cap P \leq_r^p A \cap Q \Leftrightarrow A \cap (P - Q) \in \text{PTIME}.$$

Proof. The implication from right to left is immediate. For the other implication, notice that $A \cap P$ splits into $A \cap P \cap Q$ and $A \cap (P - Q)$. But $A \cap (P - Q)$ and $A \cap Q$ form a T-minimal pair by Lemma 3.7. Therefore if $A \cap P \leq_r^p A \cap Q$, then $A \cap (P - Q) \in$ PTIME. $\diamondsuit$

Let $(P_e)_{e \in \mathbb{N}}$ be an effective listing of the polynomial time sets. Through the preceding lemmas we have obtained a representation of $\mathcal{B}$ in the sense of (4): let $e \in \mathbb{N}$ represent $\deg_r(A \cap P_e)$. The computable functions $\vee, \wedge$ on $\mathbb{N}$ are obtained by taking unions and intersections of polynomial time sets. Clearly, "$A \cap P_e \subseteq A \cap P_i$" is Σ_2^0 in e, i.

Lemma 3.10 *$\mathcal{B}$ is an effectively dense Σ^0_2-boolean algebra.*

Proof. It remains to be proved that $\mathcal{B}$ is effectively dense. By Ladner's delayed diagonalization technique [10], given a splitting $A \cap P_e$, we can effectively obtain $Q = P_{F(e)} \subseteq P_e$ such that $A \cap P_e \notin$ PTIME implies that $A \cap Q, A \cap (P - Q) \notin$ PTIME. For details, see Balcazar e.a. [5, proof of Theorem 7.3]. $\diamondsuit$

This concludes our analysis of $\mathcal{B}$. Next we show how to obtain a coding of $\mathcal{I}(\mathcal{B})$ in $[\mathbf{o}, \boldsymbol{a}]$. The idea is to represent a Σ^0_2– ideal I by a degree $\boldsymbol{c}_I$ such that

$$I = \{\boldsymbol{x} \in \mathcal{B} : \boldsymbol{x} \leq \boldsymbol{c}_I\}.$$

Clearly any ideal defined in this way must be Σ^0_2 (even if $\boldsymbol{c}_I$ is just the degree of any computable set, not necessarily in $[\mathbf{o}, \boldsymbol{a}]$). The final lemma will show that, conversely, each Σ^0_2 ideal can be represented in that way by a degree $\boldsymbol{c}_I \leq \boldsymbol{a}$. Then one obtains the desired (parameter free) coding of $\mathcal{I}(\mathcal{B})$ in $[\mathbf{o}, \boldsymbol{a}]$: the formulas for Definition 1.1 are $\varphi_{dom}(c) \Leftrightarrow c = c$ and

$$\varphi_{\leq}(c_1, c_2) \equiv \forall x \text{ complemented } (x \leq c_1 \Rightarrow x \leq c_2).$$

Lemma 3.11 *Suppose that A is super sparse via f. Then for each Σ^0_2 ideal $I \lhd \mathcal{B}(\boldsymbol{a})$ there is $\boldsymbol{c}_I \leq \boldsymbol{a}$ such that $\forall \boldsymbol{x} \in \mathcal{B}(\boldsymbol{a})$ $(\boldsymbol{x} \in I \Leftrightarrow \boldsymbol{x} \leq \boldsymbol{c}_I)$.*

Proof of Lemma 3.11 Recall that w is relevant if $w = 0^k$ for some $k \in$ range(f). We will build $C_I \leq^p_m A$ via a g which is computable in polynomial time. By Theorem 3.5 it is sufficient to consider the cases of $\leq^p_m$ and $\leq^p_{1-tt}$ reducibility. Since I is a Σ^0_2-ideal, there is a function $q \leq_T \emptyset'$ such that range$(q) = \{e : \deg^p_r(P_e \cap A) \in I\}$. By the Limit Lemma in Soare [14], there is a computable function $q(e,t)$ such that $q(e) = \lim_t q(e,t)$. If we consider m-reducibility, let (h_j) be an effective list of all polynomial time m-reductions. If we consider 1-tt-reducibility, let $(g_j), (h_j)$ be effective lists of all polynomial time functions g, h as in Definition 3.1. We meet the coding requirements

$$K_e : A \cap P_{q(e)} \leq^p_m C_I$$

by specifying polynomial time m-reductions to C_I. To do so, we assign *K_e-coding locations* to elements certain relevant 0^s. If $s = f(m)$, a K_e-coding location for 0^s will have the form 0^n, $n = \langle e, r\rangle$, where $r \geq e$ and $f(m) \leq n < f(m+1)$. We will ensure that K_e-coding locations exists for all sufficiently long relevant 0^s. We require that in n steps one can determine that $0^s \in P_u$, where u is the current guess at $q(e) = \lim_t q(e,t)$. We define C_I by specifying a polynomial time computable g such that $C_I = g^{-1}(A)$, mapping coding locations for relevant strings 0^s to 0^s. Thus, eventually just the relevant $0^s \in P_{q(e)}$ are assigned a K_e-coding location, which is in C_I just if 0^s is in A. An appropriate choice of the K_e-coding locations will ensure that the requirements

$$H_{\langle i,j\rangle} : A \cap P_i \leq_r^p C_I \text{ via } [g_j,]\ h_j \Rightarrow A \cap P_i \leq_r^p \oplus_{m \leq k} A \cap P_{q(m)}\ (k = \langle i,j\rangle)$$

are met. We can suppose that computing $h_j(x)$ takes at most $p_j(|x|)$ steps, where

$$p_j(n) = (n+2)^j.$$

The main idea of the proof is how to ensure that the coding of K_e does not interfere with the requirements H_i, $i < e$. We make the length of any K_e-coding location for 0^s exceed $p_{e-1}(s)$.

The algorithm for g.
Given an input x, $n = |x|$, first determine in quadratic time the maximal $s \leq n$ such that 0^s is relevant. This is possible by the time constructibility of f. Now proceed as follows.

1. See if there are e, r such that $x = 0^{\langle e,r\rangle}$
2. perform computations $q(e,0), q(e,1), \ldots$ till n steps have passed and let u be the last value (or $u = 0$ if there was no value so far).
3. see if $0^s \in P_u$ in n steps
4. check if $p_{e-1}(s) \leq n$.

If (1) and (3) are answered affirmatively and the computation in (4) stops, then let $g(x) = 0^s$ (so x is a K_e-coding location for 0^s). Else let $g(x)$ be the string $(1) \notin A$. This completes the algorithm. Clearly the algorithm takes at most $O(n^2)$ steps.

Let $C_I = g^{-1}(A)$. We verify that C_I has the required properties.
Claim 1. Let $q(e) = \lim_t q(e,t)$. Then $A \cap P_{q(e)} \leq_m^p C_I$.
Proof. Let $p(s)$ be a polynomial which dominates $p_{e-1}(s)$ and the number of steps it takes to compute $P_{q(e)}$ on the input 0^s. Pick an $s_0 = f(m)$ such that the value returned in (2.) of the algorithm is $q(e)$ for all $s \geq s_0$ and

also that, by super sparseness, $\langle e, p(f(k))\rangle < f(k+1)$ for all $k \geq m$. Then for all $s \geq s_0$, 0^s relevant,

$$0^s \in A \cap P_{q(e)} \;\Leftrightarrow\; 0^{\langle e,p(s)\rangle} \in C_I.$$

Claim 2. The requirements $H_{\langle i,j\rangle}$ are met.
Proof. We first consider the case of m-reducibility. Suppose that $A \cap P_i \leq_r^p C_I$ via h_j. We obtain an m-reduction of $A \cap P_i$ to $\bigoplus_{m<k} A \cap P_{q(m)}$ $(k = \langle i, j\rangle)$ as follows. Given a relevant string 0^s, first compute $x = h_j(0^s)$. Since $0^s \in A \cap P_i \;\Leftrightarrow\; x \in C_I$, it is sufficient to determine if $x \in C_I$. Run the algorithm for g on input x. If $g(x) = (1)$ then $x \notin C_I$. Otherwise x is a coding location.
Case 1: $|x| < s$. Then give $A(g(x))$ as an answer. Since A is super sparse and $|g(x)| < s$, this answer can be found in time $O(s)$.
Case 2: $n = |x| \geq s$.
We can suppose that $s \geq s_0$ where s_0 is so large that for all relevant $t \geq s_0$ $|h_j(0^t)|$ is less than the least relevant number bigger than t (by Condition (3.) in Definition 3.3), and also the computation in Step 2 of the algorithm for g with input 0^t gives the final value $q(e)$ for each $e \leq k$. By the main idea , if $x \in C_I$, then x must be a coding location for a requirement K_e, $e \leq k$. Since $s \geq s_0$, $x \in C_I \Leftrightarrow g(x) \in A \cap P_{q(e)}$.

To prove Claim 2 for 1-tt reducibility, suppose that $A \cap P_i \leq_{1-tt}^p C_I$ via g_j, h_j. In Case 2, as before obtain an answer $b \in \{0, 1\}$ to "$x \in C_I$?", depending on a query to the oracle set. Now give as an output $g_j(x, b)$.

Because h is hyperpolynomial, all the sets $A \cap P_e$, as well as the sets C_I are in DTIME(h). By the preceding result, we obtain a coding of $\mathcal{I}(\mathcal{B})$ in $\boldsymbol{D}_r(h)$ with parameter $\boldsymbol{a}$. Because of the transfer principle (1) and Theorem 2.1 this implies that Th($\boldsymbol{D}_r(h)$) is undecidable. Observe that all sets involved are tally sets, i.e. subsets of $\{0\}^*$. So we have also proved that the r-degrees of tally sets in DTIME(h) have an undecidable theory. $\diamondsuit$

Note. If PTIME = NP, then the polynomial time honest degrees below any super sparse set form a boolean algebra (Ambos-Spies and Yang [3]). So the dishonesty of the reduction of C_I to A in the proof of Lemma 3.11 seems to be inevitable.

4 Oracle results

One can relativize a polynomial time reducibility $\leq_r^p$ to a computable oracle U by replacing the underlying Turing machine model by an oracle Turing machine. We denote this relativized reducibility by $\leq_r^U$. The relativization process is most natural for $\leq_T^p$, since

$$X \leq_T^U Y \Leftrightarrow X \oplus U \leq_T^p Y \oplus U.$$

Thus, if $\boldsymbol{a} = \deg_T^p(A)$, then the $\leq_T^U$-degrees of the computable sets are isomorphic to the end segment $\{\boldsymbol{x} \in Rec_T^p : \boldsymbol{x} \geq \boldsymbol{a}\}$.
An interesting question arising from Theorem 3.2 is:

(7) $\quad\quad \text{PTIME} \neq \text{NP} \Rightarrow \text{Th}(\text{NP}, \leq_T^p)$ is undecidable ?

Let $\text{EXPTIME} = \bigcup_{k \in \mathbb{N}} \text{DTIME}(2^{(n^k)})$. We show that the conclusion holds when relativized to any computable oracle U such that $\text{NP}^U = \text{EXPTIME}^U$. Such U exist by a result of Heller [8]. Clearly EXPTIME^U is closed downwards under $\leq_T^U$.

Theorem 4.1

$$\text{NP}^U = \text{EXPTIME}^U \Rightarrow \text{Th}(\text{NP}^U, \leq_T^U) \textit{ is undecidable.}$$

Proof. To relativize the notion of a super sparse sets to U, we change the second condition in Definition 3.3: we now require that "$0^{f(k)} \in A$?" can be determined in time $O(f(k+1))$ with the help of the oracle U. All the arguments used in order to prove Theorem 3.2 are relativizable, including Ambos-Spies' Theorem 3.5. For instance, Lemma 3.6 relativized to U states the existence of a U-super sparse $A \notin \text{PTIME}^U$ such that A can be computed in time $h(n)$ with oracle U. We apply this with $h(n) = 2^n$.
Notice that the boolean algebra $\mathcal{B}$ remains Σ_2^0 because U is computable. So we obtain a coding of $\mathcal{I}(\mathcal{B})$ in the structure R_A^U of $\leq_T^U$-degrees below A. (Of course, R_A^U is isomorphic to the interval $[\boldsymbol{u}, \boldsymbol{a}]$ of polynomial time T-degrees, where $\boldsymbol{a} = \deg_T^p(A \oplus U)$). Since $\text{NP}^U = \text{EXPTIME}^U$, R_A^U is an initial interval of the $\leq_T^U$-degrees of NP^U-sets. So we obtain a coding of $\mathcal{I}(\mathcal{B})$ in $(\text{NP}^U, \leq_T^U)$.
$\diamondsuit$

Next we consider relativizations of the lattice of NP sets under inclusion. It is not known if NP = CoNP, i.e. whether this lattice is a boolean algebra. The strongest possible analog to the question (7) would thus be:

(8) $$\mathrm{NP} \neq \mathrm{CoNP} \;\Rightarrow\; \mathrm{Th}(\mathrm{NP}, \subseteq) \text{ is undecidable ?}$$

One can construct oracles X, U such that $\mathrm{NP}^X = \mathrm{CoNP}^X$ and $\mathrm{NP}^U \neq \mathrm{CoNP}^U$. Here we extend the second oracle result:

Theorem 4.2 *There is a computable oracle U such that*

$$\mathrm{Th}(\mathrm{NP}^U, \subseteq) \textit{ is undecidable.}$$

Proof. We again develop a coding with parameters of a lattice $\mathcal{I}(\mathcal{B})$, where $\mathcal{B}$ is an effectively dense Σ^0_2-boolean algebra. But here we use the language of filters rather than ideals. The proof necessarily produces an oracle U such that $\mathrm{NP}^U \neq \mathrm{CoNP}^U$. In fact we make $\mathcal{B}$ a boolean algebra which is closely related to

$$\mathcal{C}^U := \mathrm{NP}^U \cap \mathrm{CoNP}^U,$$

and use the rest of NP^U to represent $\mathcal{I}(\mathcal{B})$. A similar idea was used in the proof of Theorem 3.2. *Let the variables R, S range over $\mathcal{C}^U$.* We use the concept of oracle nondeterministic Turing machine (oracle NTM) which is described in Balcazar e.a. [5].

Outline of the proof. The construction of U extends Baker e.a. [4]. As a parameter, we determine a set $Q \in \mathrm{NP}^U - \mathcal{C}^U$, where for some polynomial time $S \subseteq \{0\}^*$,

(9) $$Q = \{w \in S : \exists v \in U \; |v| = |w|\}.$$

Then we let $\mathcal{B} = \mathcal{B}(Q)/_{\mathcal{R}(Q)}$, where

(10) $$\begin{aligned} \mathcal{B}(Q) &= \{Q \cap R : R \in \mathcal{C}^U\}, \\ \mathcal{R}(Q) &= \{R \in \mathcal{C}^U : R \subseteq Q\}, \\ \mathrm{Co}\mathcal{R}(Q) &= \{Q - R : R \in \mathcal{R}(Q). \end{aligned}$$

Clearly $\mathcal{R}(Q)$ is an ideal of $\mathcal{B}(Q)$. With an appropriate numbering of NP^U, $\mathcal{B}$ is an effectively dense Σ^0_2-boolean algebra. A filter $\mathcal{F}$ of $\mathcal{B}(Q)$ is *2- acceptable* if $\mathrm{Co}\mathcal{R}(Q) \subseteq \mathcal{F}$ and $\mathcal{F}$ has a Σ^0_2-index set. The construction of U will ensure that $\mathcal{F}$ is 2-acceptable iff for some $D \subseteq Q$ in NP^U,

$$(11) \qquad \mathcal{F} = \{X \in \mathcal{B}(Q) : \exists R \in \mathcal{R}(Q)[D - X \subseteq R]\}.$$

Hence the class of 2-acceptable filters is uniformly definable in NP^U. Moreover it is in 1-1 correspondence with the class of Σ^0_2-filters of $\mathcal{B} = \mathcal{B}(Q)/_{\mathcal{R}(Q)}$, and hence to $\mathcal{I}(\mathcal{B})$ (since complementation in a Σ^0_2- boolean algebra is a Δ^0_2 operation). In this way we code $\mathcal{I}(\mathcal{B})$ into NP^U with a parameter Q.

The details. First we need an appropriate listing of $\mathcal{C}^U$. We rely on the fact that U, and therefore Q, is given by a construction in stages which at stage s determines $U^{=s} = U \cap \Sigma^s$.

Lemma 4.3 *There is a uniformly computable pair of sequences $(C_e), (\widetilde{C}_e)$ such that*

(i) for each e we are effectively given oracle NTMs computing $C_e, \widetilde{C}_e$ with time bound $(n+2)^e$

(ii) $C_e \cap \widetilde{C}_e =^* \emptyset$ and $C_e \cup \widetilde{C}_e =^* \Sigma^{<\omega}$.

Proof. Fix some listing of all oracle NTM (N_k) such that N_k has time bound $(n+2)^k$. We write N_i^U for the set accepted by N_i when the oracle is U. To determine C_e, $e = \langle i, j\rangle$, we assume that N_i^U is the complement of N_j^U until, if ever, this can be refuted in real time based on oracle queries whose answer has been already determined. Given input w, to obtain $C_e(w), \widetilde{C}_e(w)$, run $s = |w|$ steps of the following:

> in lexicographical order, for strings x such that $(|x|+2)^e < s$, see whether $x \in N_i^U \Leftrightarrow x \in N_j^U$. If so, stop.

If we stop in $\leq s$ steps, then our assumption was wrong, so arbitrarily let $C_e(w) = 0, \widetilde{C}_e(1) = 1$. Else let $C_e(w) = N_i^U(w), \widetilde{C}_e(w) = N_j^U(w)$.
Clearly (i) and (ii) are satisfied. Moreover, if N_i^U actually is the complement of N_j^U, then $C_e = N_i^U$ and $\widetilde{C}_e = N_j^U$. $\Diamond$

Notice that $\mathcal{B}(Q) = \{Q \cap C_e : e \in \mathbb{N}\}$, so we obtain a presentation in the sense of (4) for $\mathcal{B}(Q)$, and hence for $\mathcal{B}$. Moreover, $\mathcal{B}$ with this presentation is a Σ^0_2-boolean algebra, because U is computable:

$$e \preceq i \;\Leftrightarrow\; Q \cap (C_e - C_i) \in \mathcal{R}(Q) \;\Leftrightarrow\; \exists j\; Q \cap (C_e - C_i) = C_j \subseteq Q,$$

and the matrix of the last expression is Π^0_1.
It remains to be proved that $\mathcal{B}$ is effectively dense. This is implied by the following relativizable lemma.

Lemma 4.4 *If B is decidable and $B \notin$ CoNP, then one can in an effective way from a decision procedure for B determine a set $R \in$ PTIME such that $B \cap R, B - R \notin$ CoNP.*

Proof. An easy application of the delayed diagonalization technique, similar to the proof of Lemma 3.10. $\diamondsuit$

Effective density of $\mathcal{B}$ is obtained as follows: given e, consider $B = Q \cap C_e$. Applying the previous lemma relativized to U yields $R \in \text{PTIME}^U$ such that $B \notin \text{CoNP} \;\Rightarrow\; B \cap R, B - R \notin \text{CoNP}^U$. Using $\emptyset'$ as an oracle one can compute $i = F(e)$ such that $B \cap R = Q \cap C_i$. So $\mathcal{B}$ is effectively dense via F.
We next describe how to ensure $Q \notin \mathcal{C}^U$ and introduce a first version of the set S needed for (9). Using the technique of Baker e.a. [4], for each e, we produce a witness w such that $Q(w) = N_e^U(w)$. Thus we meet the requirements

$$R_e : Q \neq \Sigma^{<\omega} - N_e^U.$$

If w is our witness and we see an accepting computation $N_e^U(w) = 1$, we have to put a string u of the same length as w into U which is not an oracle query asked in that computation (or in accepting computations for requirements which have already been satisfied). Let $S = \{0^{s_0}, 0^{s_1}, \ldots\}$, where $s_0 = 0$ and, for $k > 0$

$$(12) \qquad s_k = \min\{s > s_{k-1} : s > (s_{k-1}+2)^{k-1} \;\&\; 2^s > G_k(s)\}.$$

Here $G_k(s) = (s+2)^k$, but this definition of $G_k(s)$ will be modified when we add further requirements. Clearly $S \in$ PTIME (apply the logarithm with base 2 to "$2^s > G_k(s)$").
Construction of U, Part 1.
For each string w, $U(w) = 0$ unless otherwise specified.

> To determine $U^{=s}$ for $s = s_k$, check whether there is an $e < k$ such that R_e is not yet met, namely

$$\forall w \in S[|w| < s \;\Rightarrow\; N_e^U(w) \neq Q(w)].$$

If not, $U^{=s} = \emptyset$. If so for e minimal, we meet requirement R_e: see whether $N_e^U(0^s) = 1$ via some accepting computation Γ based on the current oracle. Let $u \in \Sigma^s$ be the lexicographically first string which is not an oracle query in Γ, and define $U(u) = 1$, thereby causing $Q(0^s) = 1$.

Next we describe how we obtain, for each 2-acceptable $\mathcal{F}$ a set $D \subseteq Q$ in NP^U satisfying (11). We identify subsets of $\mathcal{B}$ and their preimages under the canonical map associated with the presentation (4). Note that there is an effective listing $(\mathcal{F}_e)_{e>0}$ of Σ_2^0-indices for 2-acceptable filters: let $\mathcal{F}_e$ be the filter generated by $\mathrm{Co}\mathcal{R}(Q)$ and the $e-1$-th Σ_2^0-set. (We need $e > 0$ for notational reasons.)
Since each $\mathcal{F}_e$ is infinite (when viewed as a subset of $\mathbb{N}$), there is a binary function $\alpha \leq_T \emptyset'$ such that, for all $e > 0$,

$$\mathcal{F}_e = \{\alpha_e(n) : n \in \mathbb{N}\}.$$

By the Limit Lemma in Soare [14], there is a computable β such that, for each $n, e > 0$, $\alpha(e,n) = \lim_k \beta(e,n,k)$. We can assume that

$$\beta(e,n,k) < k. \tag{13}$$

To obtain a good representation of $\mathcal{F}_e$, let

$$F^e_{n,k} = Q \cap \bigcap_{m \leq n} C_{\beta(e,m,k)}. \tag{14}$$

Then, for each n, $F^e_n = \lim_k \; F^e_{n,k}$ exists in the sense that an index for an oracle NTM obtained from (14) stabilizes. Moreover, the sequence $F^e_0 \supset F^e_1 \supset \ldots$ generates $\mathcal{F}_e$.
For $e > 0$, let

$$D_e = \{0^{s_k+e} : e < k \;\&\; \exists w \in U \; |w| = s_k + e\}. \tag{15}$$

For the inclusion "$\subseteq$" in (11), we ensure that

$$\forall m \; D_e \subseteq^* F^e_m. \tag{16}$$

Then $X \in \mathcal{F}_e \;\Rightarrow\; \exists m F_m^e \subseteq X \;\Rightarrow\; D_e - X$ finite.
For the converse inclusion, we meet the requirements

$$P_{\langle e,m\rangle} : |F_m^e \cap \widetilde{C}_m| = \infty \;\Rightarrow\; D_e \cap \widetilde{C}_m \neq \emptyset.$$

Then, if $X = Q \cap C_i \notin \mathcal{F}_e$, we can deduce that $D_e - X \not\subseteq R$ for each $R \in \mathcal{R}(Q)$. Observe that $X \cup R \notin \mathcal{F}_e$ because $\mathrm{Co}\mathcal{R}(Q) \subseteq \mathcal{F}_e$. Choose an m such that $X \cup R = Q \cap C_m$, and also that $\widetilde{C}_m$ is the complement of C_m. Then the hypothesis of $P_{\langle e,m\rangle}$ is satisfied, thus $D_e \cap \widetilde{C}_m \neq \emptyset$, which means that $D_e - X \not\subseteq R$.
We extend the construction by putting at most one element of length $s_k + e$, $0 < e < k$ into U in order to meet the P-type requirements: according to (15) this will determine the sets D_e. After presenting the construction we will determine an appropriate choice of the function $G_k(s)$ needed in (12).

Construction of U, Part 2.

> For $s = s_k$, after determining $U^{=s}$, if we placed some string of length s into U, we also do the following: search for a minimal $\langle e,m\rangle < k, e > 0$ such that $P_{\langle e,m\rangle}$ is not yet *satisfied*, namely
>
> (17) $$D_e \cap \widetilde{C}_m \cap \Sigma^{<s} = \emptyset,$$
>
> and also (based on the current oracle)
>
> (18) $$0^s \in F_{m,k}^e \cap \widetilde{C}_m.$$
>
> If $\langle e,m\rangle < k$ exists, find a $w \in \Sigma^{s+e}$ which does not occur as an oracle query in an accepting computation in (18), and also not in the accepting computation Γ from Part 1, stage s. Define $U(w) = 1$. We say that $P_{\langle e,m\rangle}$ *receives attention.*

Now to make sure we can find w, we have to count relevant accepting computations and define $G_k(s)$ appropriately. For a Q-type requirement there is at most one, and to determine $0^s \in F_{m,k}^e$ we need at most $k+1$ many, see (14). Notice that these computations have a time bound $(s+2)^k$, by the property (13). There is one more accepting computation for $0^s \in \widetilde{C}_m$. So the definition

$$G_k(s) = (k+3)(s+2)^k$$

is as desired.

Clearly U is computable and $Q \in \mathrm{NP}^U$. The R-type requirements are met for the same reasons as before. No requirement is ever injured by a "later" U-change by the fact that $s_k > (s_{k-1}+2)^{k-1}$ and the construction. So by the condition (17), each requirement receives attention at most once. We conclude that (16) holds: given $e > 0$ and m, choose a k such that for $n < m$, $\beta(e,n,k)$ has reached its limit and $P_{\langle e,n\rangle}$ does not receive attention from s_k on. If a requirement causes $v \in D_e$ at a stage $s \geq s_k$, then $s = s_h + e$ for some $h \geq k$ and the requirement is $P_{\langle e,n\rangle}$ for some $n > m$. Hence $v \in F^e_{n,h} \subseteq F^e_m$. To prove that $P_{\langle e,m\rangle}$ is met, suppose that $|F^e_m \cap \widetilde{C}_m| = \infty$. Choose a k such that $\beta(e,m,k)$ has reached its limit and no requirement P_u, $u < \langle e,m\rangle$ receives attention at a stage $\geq s_k$. Since $F^e_m \subseteq Q \subseteq \{0^{s_i} : i \in \mathbb{N}\}$, there is an $s = s_h \geq s_k$ such that $0^s \in F^e_m \cap \widetilde{C}_m$. Since $P_{\langle e,m\rangle}$ has the highest priority at s, we cause $0^s \in D_e$. So $P_{\langle e,m\rangle}$ is met. $\Diamond$

References

[1] K. Ambos-Spies. Inhomogeneities in the polynomial time degrees. *Information Processing Letters*, 22:113–117, 1986.

[2] K. Ambos-Spies and A. Nies. The theory of polynomial many-one degrees of recursive sets in undecidable. In *STACS 92*, volume 577 of *Lecture Notes in Computer Science*, pages 209–210. Springer–Verlag, 1992.

[3] K. Ambos-Spies and D. Yang. Honest polynomial-time degrees of elementary recursive sets. In *CSL: 3rd Workshop on Computer Science Logic*. LNCS, Springer-Verlag, 1990.

[4] T. Baker, J. Gill, and R. Solovay. Relativizations of the $\mathcal{P} =? \mathcal{NP}$ question. *SIAM Journal on Computing*, 4(4):431–442, December 1975.

[5] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*, volume 11 of *EATCS Monographs on Theoretical Computer Science*. Springer–Verlag, Heidelberg, 1988.

[6] S. Burris and H. P. Sankappanavar. Lattice theoretic decision problems in universal algebra. *Algebra Universalis*, 5:163–177, 1975.

[7] R. Downey and A. Nies. Undecidability results for low complexity degree structures. In *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, pages 128–132, 1997.

[8] H. Heller. Relativized polynomial hierarchies extending two levels. *Mathematical Systems Theory*, 17(2):71–84, 1984.

[9] W. Hodges. *Model Theory*, volume 42 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, Cambridge, 1993.

[10] R. Ladner. On the structure of polynomial time reducibility. *J. Assoc. Comput. Mach.*, 22(1):155–171, January 1975.

[11] L. Landweber, R. Lipton, and E. Robertson. On the structure of NP and other complexity classes. *J. Theoretical Comp. Sc.*, 15:181–200, 1981.

[12] A. Nies. Intervals of the lattice of computably enumerable sets and effective boolean algebras. *Bull. Lond. Math. Soc.*, 29:683–92, 1997.

[13] J. Shinoda and T. A. Slaman. On the theory of the PTIME degrees of the recursive sets. In *Annual Conference on Structure in Complexity Theory*, 1988.

[14] R. I. Soare. *Recursively Enumerable Sets and Degrees*. Perspectives in Mathematical Logic, Omega Series. Springer–Verlag, Heidelberg, 1987.

Department of Mathematics, P.O. Box 600, Victoria University, Wellington, New Zealand, e-mail Rod.Downeyvuw.ac.nz
Department of Mathematics, The University of Chicago, Chicago IL 60637, USA, e-mail niesmath.uchicago.edu