On p-Separability

Devdatt Dubhashi*

TR 89-973
February 1989

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

*Research supported by NSF grant CCS-8806979.

On p-Separability

Devdatt P. Dubhashi*
Department of Computer Science
Cornell University
Ithaca, NY 14853

February 27, 1989

Abstract

We introduce the notion of p-separability in analogy with the recursion-theoretic notion of recursive separability. The existence of p-inseparable sets in $\mathcal{NP}$ is related to structural properties of complexity classes. Sparseness is related to p-separability and structural conditions for the existence of sparse p-inseparable sets in $\mathcal{NP}$ are given. Using the notion we obtain sets hard for the Σ_2^0 and Π_2^0 levels of the Kleene Arithmetic Hierarchy. Some independence results are shown to follow.

1 Introduction

In Recursive Function Theory, two sets A and B are said to be *recursively-inseparable* if whenever $A \subseteq C$ and C is recursive, then $B \cap C \neq \emptyset$. [8, pages-93-94], [9, page 23], [7, page 84]. As shown in [7], the Gödel Incompleteness Theorem for Arithmetic can be deduced from the existence of recursively- enumerable (r.e.) sets that are recursively inseparable : in this way, the recursively inseparable sets establish a link between recursive-function theory and logic.

We investigate here, the corresponding resource-bounded notion. *p(polynomial-time)-separability*. This paper is organised as follows. In §2. we define the notion of p-(in)separability. and relate the existence of p-inseparable sets in NP to certain structural properties of complexity classes. In §3, we relate p-separability to *sparseness* and give structural conditions

*Supported by NSF grant CCS-8806979

paralleling those of §2 for the existence of sparse p-inseparable sets in NP. In §4, we obtain complete sets in the Σ_2^0 and Π_2^0 levels of the Kleene Arithmetic Hierarchy using the notion of p-inseparability. Some independence results immediately follow from these, including a sharp form of Godel's Incompleteness Theorem for Arithmetic.

2 p-Separability : Definition and Properties

We use the conventions of [6] for automata-theoretic concepts. We will let $\{M_i\}_{i\geq 0}$ stand for any acceptable enumeration of Turing Machines (TMs). In general the M_i are arbitrary TMs ; when we wish to refer to a listing of explicitly clocked TMs, we will state this and specify the resource bound in question.

In exact analogy with the recursive-function theory concept, we introduce the

Definition 2.1 (p-Separability) *Let $A, B \subseteq \Sigma^*$. Then A, B are p-separable iff there exists a set C in $\mathcal{P}$ such that $A \subseteq C$ and $C \cap B = \emptyset$.(Observe that for A, B to be p-separable, it is necessary that A, B be disjoint.) If A, B are not p-separable, then A, B are p-inseparable.*

In recursive-function theory, it is possible to explicitly exhibit two r.e. sets which are recursively inseparable. It is quite natural to ask : Are there sets in $\mathcal{NP}$ that are p-inseparable ? The next theorem shows that the answer depends on certain structural properties of the classes $\mathcal{P}$, $\mathcal{NP}$ and $co-\mathcal{NP}$.

Theorem 2.1 *1. If there exist disjoint p-inseparable sets in $\mathcal{NP}$, then $\mathcal{P} \neq \mathcal{NP}$.*

2. If $\mathcal{P} \neq \mathcal{NP} \cap co-\mathcal{NP}$, then there exist p-inseparable sets in $\mathcal{NP}$.

Proof

1. If $\mathcal{P} = \mathcal{NP}$ then clearly any two disjoint sets in $\mathcal{NP}$ are p-separable.

2. Let $A \in \mathcal{NP} \cap co-\mathcal{NP} \setminus \mathcal{P}$. Then $A, \overline{A}$ are in $\mathcal{NP}$ and we claim they are p-inseparable. Otherwise, if $A \subseteq C$, $C \in \mathcal{P}$ and $C \cap \overline{A} = \emptyset$ then $A = C \in \mathcal{P}$ contrary to assumption.$\square$

If there are p-inseparable sets in $\mathcal{NP}$, then one may conjecture that any two disjoint $\mathcal{NP}$-complete sets are p-inseparable. This is false. Let $SAT_i = \{\langle i, F\rangle : F \in SAT\}$ for $i = 0, 1$. Then, SAT_0, SAT_1 are $\mathcal{NP}$-complete and disjoint, but easily p-separable. However, the following result is true.

Proposition 2.2 *If there exist p-inseparable sets in $\mathcal{NP}$, then there exist $\mathcal{NP}$-complete sets are p-inseparable.*

Proof Let $A, B \in \mathcal{NP}$ be p-inseparable, and consider the sets $A \oplus SAT, B \oplus SAT$. These are clearly $\mathcal{NP}$-complete. Assume, to reach a contradiction, that $A \oplus SAT \subseteq L(M)$ and $B \oplus SAT \cap L(M) = \emptyset$, where M is a polynomial-time TM. Define a TM M' such that

$$x \in L(M') \leftrightarrow \langle 0, x\rangle \in L(M)$$

Then, M' is a polynomial-time TM that separates A and B, a contradiction. □

3 Sparseness and p-Separability

A set S is said to be *sparse* if there exists a polynomial p such that for all $n \geq 0$, $card(S \cap \Sigma^{\leq n}) \leq p(n)$. A special kind of sparse set is a *tally* set T which is a set over a single letter alphabet. Tally sets are the sparsest possible non-trivial sets, since they have at most one string of each length. See [1] for the significance of sparse sets in complexity theory.

Intuitively, sparse sets should be easy to separate : one does not have to include too much to capture one set and it is easy to avoid "hitting the skinny other set". The next result shows that this intuition is not entirely right.

Proposition 3.1 *There exist tally sets in $\mathcal{EXPTIME}$ that are p-inseparable.*

Proof We construct $T_1, T_2 \subseteq 0^*$ by diagonalising over all polynomial-time TMs, M_i. Let $\pi : \omega \times \omega \to \omega$ be an easily computed pairing function. I define the predicate $Accept(M, x, n) \leftrightarrow M$ accepts x in $\leq n$ steps.

Define

$$T_1 = \{0^{\pi(i,j)} : \neg Accept(M_i, \pi(i,j), 2^{\pi(i,j)})\}$$

$$T_2 = \{0^{\pi(i,j)} : Accept(M_i, \pi(i,j), 2^{\pi(i,j)})\}$$

It is easy to see that T_1, T_2 are in EXPTIME. To see that they are p-inseparable, suppose $T_1 \subseteq L(M_i)$ and suppose M_i runs in time $p(n)$. Choose j so that $2^{\pi(i,j)} \geq p(\pi(i,j))$. Then, if $0^{\pi(i,j)} \in L(M_i), 0^{\pi(i,j)} \in T_2$ and $L(M_i) \cap T_2 \neq \emptyset$. On the other hand if $0^{\pi(i,j)} \notin L(M_i)$ then $0^{\pi(i,j)} \in T_1$ and $T_1 \not\subseteq L(M_i)$. Therefore T_1, T_2 are p-inseparable. $\square$

How about sparse p-inseparable sets in $\mathcal{NP}$? The next result uses ideas of [5] to relate the existence of tally sets in $\mathcal{NP}$ that are p-inseparable to conditions between complexity classes parallel to those of Theorem 2.1.

Theorem 3.2 *1. If there exist disjoint tally sets in $\mathcal{NP}$ that are p-inseparable, then $\mathcal{EXPTIME} \neq \mathcal{NEXPTIME}$*

2. If $\mathcal{EXPTIME} \neq \mathcal{NEXPTIME} \cap co-\mathcal{NEXPTIME}$ then there exist tally sets in NP that are p-inseparable.

Proof

1. If $T \subseteq 0^*$ is a tally set in $\mathcal{NP}$, then the set $\{n : 0^n \in T\}$ is in $\mathcal{NEXPTIME}$.So if $\mathcal{EXPTIME} = \mathcal{NEXPTIME}$ then $T \in \mathcal{P}$,and any two disjoint tally sets in $\mathcal{NP}$ would be p-separable.

2. Let $A \in \mathcal{NEXPTIME} \cap co-\mathcal{NEXPTIME} \setminus \mathcal{EXPTIME}$. Then $A, \overline{A} \in \mathcal{NEXPTIME}$. Let $T_A = \{0^n : n \in A\}$ and $T_{\overline{A}} = \{0^n : n \in \overline{A}\}$. Then $T_A, T_{\overline{A}}$ are in $\mathcal{NP}$ and are p-inseparable. The last fact is true because otherwise T_A is in $\mathcal{P}$ and $A \in \mathcal{EXPTIME}$, a contradiction. $\square$

4 p-Separability and the Arithmetic Hierarchy

In this section we use the concept of p-(in)separability to obtain sets hard for the Σ_2^0 and Π_2^0 levels of the Kleene Arithmetic Hierarchy. [8,9] These sets are used to prove a representation-free independence result and a sharp form of the Godel- Incompleteness Theorem for Arithmetic.

It is well known (see for instance, the aforementioned references) that

Proposition 4.1 *The set*

$$INF = \{i : L(M_i) \textit{is infinite}\}$$

is $\leq_m$-complete for the class Π_2^0. $\square$

Using Proposition 4.1 , we obtain

Theorem 4.2 *The set,*

$$INSEP = \{(i,j) : L(M_i), L(M_j) \textit{are p-inseparable}\}$$

is $\leq_m$-hard for Π_2^0. The set,

$$SEP = \{(i,j) : L(M_i), L(M_j) \textit{are p-separable}\}$$

is $\leq_m$-hard for Σ_2^0.

Proof We will exhibit a reduction $i \mapsto (\sigma(i), \rho(i))$ from INF to INSEP.

Let M_1, M_2 be TMs such that $L(M_1), L(M_2)$ are p-inseparable. (From Proposition 3.1 we know that these exist.) $M_{\sigma(i)}$ is the TM that on input x, simulates M_i on inputs $y \leq x$ in a dovetailed fashion. If M_i ever accepts some such y, $M_{\sigma(i)}$ simulates M_1 on x. $M_{\rho(i)}$ is the same except it simulates M_2. Thus,

$$i \in INF \rightarrow L(M_{\sigma(i)}) = L(M_1) \text{and} L(M_{\rho(i)}) = L(M_2)$$

and

$$i \notin INF \rightarrow L(M_{\sigma(i)}), L(M_{\rho(i)}) \text{are finite}$$

Therefore,

$$i \in INF \leftrightarrow (\sigma(i), \rho(i)) \in INSEP$$

and we see that $INF \leq_m INSEP$.

$\overline{INSEP}$ is $\leq_m$-hard for Σ_2^0 and clearly $SEP \equiv_m \overline{INSEP}$. We conclude that SEP is $\leq_m \text{hard} - for \Sigma_2^0.\Box$

Corollary 4.3 $SEP \notin \Sigma_1^0$.

Proof By the Kleene-Post Hierarchy Theorem ([8,9]), $\Sigma_1^0 \subset \Sigma_2^0$ and SEP is Σ_2^0-hard. Hence $SEP \notin \Sigma_1^0.\Box$

From Theorem 4.2 and Corollary 4.3, we obtain a representation- free independence result in the style of [3].

Theorem 4.4 *Let $\mathcal{F}$ be a sound, recursively axiomatised formal system which is strong enough to express properties of TM-computations. (For instance, $\mathcal{F}$ can be Peano Arithmetic (PA) or Zermelo-Fraenkel Set Theory (ZFC).) Then there exist TMs M_i, M_j such that $L(M_i), L(M_j)$ are p-separable, but for no polynomial-time TM M_e, can $\mathcal{F}$ prove that "$L(M_e)$ separates $L(M_i)$ and $L(M_j)$".(Here, "s" refers to the appropriate expression of the statement s in the formal system $\mathcal{F}$.)*

Proof Otherwise,

$SEP = \{(i,j) : \exists e \exists d$ (d is a proof in $\mathcal{F}$ of " $L(M_e)$ separates$L(M_i), L(M_j)$")$\}$

and $SEP \in \Sigma_1^0$ contradicting Corollary 4.3.□

We convert this into a statement of a very sharp form of the Godel Incompleteness Theorem. It asserts that there is a not-very-complex statement in Arithmetic that no formal system can prove.

Corollary 4.5 *For any sufficiently powerful formal system $\mathcal{F}$ of Arithmetic,, there is a $\forall\exists$ formula $\varphi(i,j,e)$ with parameters i,j and e such that for some choice of the parameters,φ is true ($\mathcal{N} \models \varphi$) but $\mathcal{F} \not\vdash \varphi$.*

Proof Using Godel's well-known arithmetisation of Turing Machines, let φ be the formula of Arithmetic such that

$$\varphi(i,j,e) \rightarrow L(M_i) \subseteq L(M_e) \wedge L(M_e) \cap L(M_j) = \emptyset$$

Here, M_e is an explicitly-clocked polynomial-time TM. This is a $\forall\exists$-formula with parameters. The result now follows from Theorem 4.4 . □

Remark Theorem 4.4 and the above corollary are incompleteness results and have a recursion-theoretic interpretation along the lines of a recursion-theoretic interpretation of Godel's Incompleteness Theorem. As in [2], the Godel Incompleteness Theorem can be understood as arising from the fact that while the theorems of Peano Arithmetic (and indeed any recursively axiomatised formal system) form a r.e. set, the set

$$Th(\mathcal{N}) = \{\varphi : \mathcal{N} \models \varphi\}$$

is *productive*.([8]) The sets INSEP and SEP being complete at the Π_2^0 and Σ_2^0 levels of the Arithmetic Hierarchy, are also productive, and the incompleteness results arise directly out of this fact.◇

5 Concluding Remarks

We have introduced the concept of p-separability and used it to [illegible] structural properties of complexity classes. We also used it to obta[illegible] sets in the Arithmetic heirarchy with applications to logical proble[illegible] results here go further to illustrate the "importance of being Π_2- ha[illegible] Both the structural complexity aspects and logical aspects of the [illegible] p-separability, we feel, are worth investigating further.

References

[1] Berman,L. and J. Hartmanis : " On Isomorphisms and density of NP nad other complete sets." *SIAM J. Computing*, 6:2, 1977 305-322.

[2] Cutland, N : Computability Cambridge University Press, 1980

[3] Hartmanis,J. " Independence results about context-free languages and lower bounds." *Inform. Process. Lett.* 20:5. 1985 241-248.

[4] Hartmanis J . "On the importance of being Π_2-hard". TR 88-961, Department of Computer Sceinec, Cornell University, Jan 1989.

[5] Hartmanis,J.,V.Sewelson and N.Immerman : "Sparse sets in NP-P : Exptime versus Nexptime " 15th STOC, 382-391.

[6] Hopcroft,J. and J.D. Ullman : Introduction to Automata Theory, Languages and Computation. Addison Wesley, 1979.

[7] Machtey,M. and P.Young : Introduction to the General Theory of Algorithms. North Holland, 1978.

[8] Rogers, H Jr. : Theory of Recursive Functions and Effective Computability. McGraw Hill, 1967.

[9] Soare,R.I. : Recursively Enumerable Sets and Degrees. Springer Verlag, 1987.