Types of Separability

Sven Kosub

Theoretische Informatik
Julius-Maximilians-Universität Würzburg
Am Hubland
D-97074 Würzburg, Germany
kosub@informatik.uni-wuerzburg.de

Abstract. In this paper we demonstrate that the studies of structural properties of the boolean hierarchy of NP-partitions are not only worthwhile in their own, e.g., as a framework for capturing the complexity of classification problems but have interesting ties with other research in computational complexity: We discuss the relationships to the study of separable NP sets.

1 Introduction

The notion of separability is a very fundamental one which originally goes back to Lusin who created by introducing it in descriptive set theory a very influential notion (for a list of separation theorems see [Kec95]).

Typically, separability means the following: Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be classes of subsets of M and let $\mathcal{K}_2$ be closed under complements. We say that two disjoint sets A and B belonging to $\mathcal{K}_1$ are separable by sets from $\mathcal{K}_2$ if there exist a set $C \in \mathcal{K}_2$ such that $A \subseteq C$ and $B \subseteq \overline{C}$. We say that the two disjoint sets are inseparable in $\mathcal{K}_2$ if they are not separable by sets from $\mathcal{K}_2$. This notion becomes interesting if $\mathcal{K}_2$ is not greater than $\mathcal{K}_1$.

Separability has been extensively investigated in recursion theory. It has been used to strengthen the fundamental result that there exist recursively enumerable sets that are not recursive by proving that there exists a pair of disjoint recursively enumerable sets that are not separable by recursive sets [Kle50,Tra53] (for a stronger result see [Sho58]). In contrast to this, it is not hard to show that every pair of disjoint complements of recursively enumerable sets is separable by recursive sets. In fact, this property is the reason why the so-called Embedding Theorem (as aimed for the class NP in [KW99,KW00]) cannot hold for the recursively enumerable sets. Furthermore, separability is deeply tied with, e.g., creative sets [Kle50,Usp53] or essential undecidability of formal systems [Tar49].

In complexity theory, finally, separability has also been broadly applied. In 1988, Grollmann and Selman [GS88] showed that weak one-way functions[1] exist if and only if there is a pair of disjoint NP sets that is inseparable in P. The question of whether the latter is possible has subsequently been examined further in [FR94,FFNR96,MV96]. Hemaspaandra *et al.* [HHN$^+$95] pointed out connections between separability and selectivity notions. In particular, they proved that all NP-selective sets are P-selective if and only if all pairs of disjoint NP sets are separable in P. Furthermore separability has been studied in the complexity-theoretic settings of lower bounds for proof systems [Raz94,Raz95,KM98], complexity of Craig interpolants [SP98], P-superterse sets [Bei88], and witness-isomorphic reductions [FHT97].

[1] A weak one-way function is one that has some easy-to-compute extension but no easy-to-invert extension.

The study of separability notions is very closely related to the study of partition classes in the context of the boolean hierarchy of NP-partitions as initiated in [KW99,KW00,Kos00]. In this paper we emphasize how successfully both studies can interact.

2 Preliminaries

We briefly gather basic concepts and notions that are used throughout this paper.

Let $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{N}_+ = \{1, 2, \dots\}$. The cardinality of an arbitrary finite set A is denoted by $\|A\|$. For sets A and B we use $A \setminus B$ to denote the set-difference of A with B, and we use $A \times B$ to denote the cartesian product of A with B. Let $\mathcal{P}(M)$ be the power set of a fixed basic set M. For a set $A \subseteq M$, its complement in the basic set M is denoted by $\overline{A}$, i.e., $\overline{A} = M \setminus A$. Let $\mathcal{K}$ and $\mathcal{K}'$ be classes of subsets of M, i.e., $\mathcal{K}, \mathcal{K}' \subseteq \mathcal{P}(M)$. We define $\mathrm{co}\mathcal{K} =_{\mathrm{def}} \{\ \overline{A} \mid A \in \mathcal{K}\ \}$ and $\mathcal{K} \wedge \mathcal{K}' =_{\mathrm{def}} \{\ A \cap B \mid A \in \mathcal{K}, B \in \mathcal{K}'\ \}$. $\mathrm{BC}(\mathcal{K})$ is the boolean closure of $\mathcal{K}$, i.e., the smallest class which contains $\mathcal{K}$ and which is closed under intersection and complements.

We need some notions from order theory (see e.g., [Grä78,DP90]). A pair $(G, \leq)$ is a poset if $\leq$ is a partial order on the set G. Usually, we talk about the poset G. Where it is necessary we write $(G, \leq)$ to specify the order.

We will make no difference between m-tuples $(x_1, \dots, x_m)$ over a finite set (alphabet) M and words $x_1 \dots x_m$ of length m over M. We fix the finite alphabet $\Sigma = \{0, 1\}$ for considerations about input-output behavior of machines. More generally, let Δ be any finite alphabet. Δ^* is the set of all finite words that can be built with letters from Δ. For $x, y \in \Delta^*$, $x \cdot y$ (or xy for short) denotes the concatenation of x and y. The empty word is denoted by ε. For $x \in \Delta^*$, $|x|$ denotes the length of x. For $n \in \mathbb{N}$, $\Delta^{\leq n}$ is the set of all words $x \in \Delta^*$ with $|x| \leq n$, and $\Delta^{=n}$ is the set of all words $x \in \Delta^*$ with $|x| = n$. If the alphabet Δ is ordered by $\leq$, then let $\leq_{\mathrm{lex}}$ denote the standard lexicographical order on Δ^*, that is, for each $x, y \in \Delta^*$, $x \leq_{\mathrm{lex}} y$ if and only if (a) $x = y$, (b) $|x| < |y|$, or (c) $|x| = |y|$ and there is an i with $x_j = y_j$ for all $j \in \{1, \dots, i-1\}$ but $x_i < y_i$. Usually we consider words x and y of the same length n to be partially ordered by the vector-ordering, that is, $x \leq y$ iff $x_i \leq y_i$ for all $i \in \{1, \dots, n\}$.

The computational model we refer to is the standard Turing machine (for a formal description see, e.g., [WW86,BDG95]). We consider nondeterministic and deterministic versions of Turing machines. We also consider Turing machines that have access to an oracle. The notions translate accordingly to such oracle Turing machines. If we consider an oracle Turing machine M accessing an oracle A then this is denoted by M^A.

Polynomial-time Turing machines are Turing machines that for a fixed polynomial p, make on every input x at most $p(|x|)$ computation steps before reaching a final state. In case of a nondeterministic polynomial-time Turing machine M, the set of all words accepted by M, denoted by $L(M)$, is the set of all words $x \in \Sigma^*$ for which M, on input x, has at least one computation path of at most $p(|x|)$ steps of running, that ends in an accepting final state. NP (P) is the class of all sets that are accepted by nondeterministic (deterministic) polynomial-time Turing machines. NP^B is the class of all sets that are accepted by nondeterministic polynomial-time Turing machine accessing the set B. For a class $\mathcal{K}$, $\mathrm{NP}^{\mathcal{K}}$ consists of all sets that belong to NP^B for some $B \in \mathcal{K}$. The polynomial hierarchy [MS72,Sto77] is inductively defined as follows.

$$\begin{aligned}
\Sigma_0^p &=_{\text{def}} \mathrm{P}, \\
\Sigma_{m+1}^p &=_{\text{def}} \mathrm{NP}^{\Sigma_m^p}, \\
\mathrm{PH} &=_{\text{def}} \bigcup_{m \in \mathbb{N}} \Sigma_m^p.
\end{aligned}$$

UP is the class of all languages that are accepted by nondeterministic polynomial-time Turing machines having for all inputs at most one accepting path.

FP denotes the class of all functions that are computable by a deterministic polynomial-time Turing transducer. We say that a set $A \subseteq \Sigma^*$ is polynomial-time many-one reducible to a set $B \subseteq \Sigma^*$, in symbols $A \leq_m^p B$, if and only if there exists a function $f \in \mathrm{FP}$ such that for all $x \in \Sigma^*$, $x \in A \iff f(x) \in B$. A class $\mathcal{K} \subseteq \mathcal{P}(\Sigma^*)$ is closed under $\leq_m^p$ if for all $A, B \subseteq \Sigma^*$ it holds that $A \leq_m^p B$ and $B \in \mathcal{K}$ imply that $A \in \mathcal{K}$. All classes in the polynomial hierarchy and UP as well are closed under $\leq_m^p$. A set A is $\leq_m^p$-complete for $\mathcal{K}$ if $A \in \mathcal{K}$ and $B \leq_m^p A$ for all $B \in \mathcal{K}$. Satisfiability, denoting the set of all (encodings of) satisfiable propositional formulas, is an example of a set $\leq_m^p$-complete for NP, and Tautology, denoting the set of all (encodings of) tautological propositional formulas, is an example of a set $\leq_m^p$-complete for coNP.

We implicitly use the following correspondence val between Σ^* and $\mathbb{N}$: For $x \in \Sigma^*$, define $\mathrm{val}(x) =_{\text{def}} \|\{y \in \Sigma^* \mid y <_{\text{lex}} x\}\|$. Note that val is polynomial-time computable and invertible.

Finally, let us make some notational conventions about partitions. For any set M, a k-tuple $A = (A_1, \dots, A_k)$ with $A_i \subseteq M$ for each $i \in \{1, \dots, k\}$ is said to be a *k-partition of M* if and only if $A_1 \cup A_2 \cup \dots \cup A_k = M$ and $A_i \cap A_j = \emptyset$ for all i, j with $i \neq j$. The set A_i is said to be the *i-th component of A*. For two k-partitions A and B to be equal it is sufficient that $A_i \subseteq B_i$ for all $i \in \{1, \dots, k\}$. Let $c_A : M \to \{1, \dots, k\}$ be the characteristic function of a k-partition $A = (A_1, \dots, A_k)$ of M, that is, $c_A(x) = i$ if and only if $x \in A_i$. For $\mathcal{K}_1, \dots, \mathcal{K}_k \subseteq \mathcal{P}(M)$ let

$$(\mathcal{K}_1, \dots, \mathcal{K}_k) =_{\text{def}} \left\{ A \mid A \text{ is } k\text{-partition of } M \text{ and } A_i \in \mathcal{K}_i \text{ for all } i \in \{1, \dots, k\} \right\}$$

and for $i \in \{1, \dots, k\}$,

$$(\mathcal{K}_1, \dots, \mathcal{K}_{i-1}, \cdot, \mathcal{K}_{i+1}, \dots, \mathcal{K}_k) =_{\text{def}} (\mathcal{K}_1, \dots, \mathcal{K}_{i-1}, \mathcal{P}(M), \mathcal{K}_{i+1}, \dots, \mathcal{K}_k).$$

For a class $\mathcal{K}$ of k-partitions, let $\mathcal{K}_i =_{\text{def}} \left\{ A_i \mid A \in \mathcal{K} \right\}$ be the *i-th projection of $\mathcal{K}$*. Obviously, $\mathcal{K} \subseteq (\mathcal{K}_1, \dots, \mathcal{K}_k)$. In what follows we identify a set A with the 2-partition $(A, \overline{A})$, and we identify a class $\mathcal{K}$ of sets with the class $(\mathcal{K}, \mathrm{co}\mathcal{K}) = (\mathcal{K}, \cdot) = (\cdot, \mathrm{co}\mathcal{K})$ of 2-partitions.

3 Partition Classes Defined by Posets

In this section we give a short introduction to the boolean hierarchy of NP-partitions and its refinements. The most important point for our purposes is the construction of partitions and partition classes from finite labeled posets. The following can be found in [Kos00].

Let $\mathcal{K}$ be a class with $\emptyset, M \in \mathcal{K}$ and $\mathcal{K}$ is closed under union and intersection.

Definition 1. *Let G be a poset.*

1. *A mapping $S : G \to \mathcal{K}$ is said to be a* $\mathcal{K}$-homomorphism on G *if and only if*

   (a) $\bigcup_{a \in G} S(a) = M$ *and*

   (b) $S(a) \cap S(b) = \bigcup_{c \leq a, c \leq b} S(c)$ *for all $a, b \in G$.*

2. *For any $\mathcal{K}$-homomorphism S on G and $a \in G$, let*

$$T_S(a) =_{\text{def}} S(a) \setminus \bigcup_{b<a} S(b).$$

Lemma 2. *Let G be a poset, and let S be a $\mathcal{K}$-homomorphism on G.*

1. *$T_S(a) \in \mathcal{K} \wedge \text{co}\mathcal{K}$ for every $a \in G$.*
2. *If $a \leq b$ then $S(a) \subseteq S(b)$ for every $a, b \in G$.*
3. *$S(a) = \bigcup_{b \leq a} T_S(b)$ for every $a \in G$.*
4. *The set of all $T_S(a)$ for $a \in G$ yields a partition of M.*

Any pair (G, f) of an arbitrary finite poset G and a function $f : G \to \{1, 2, \ldots, k\}$ is called a *k-poset.*

Lemma 2 provides that the following definitions are sound.

Definition 3. *Let (G, f) be a k-poset. Let $k \geq 2$.*

1. *For a $\mathcal{K}$-homomorphism S on G,* the k-partition defined by (G, f) and S *is given by*

$$(G, f, S) =_{\text{def}} \left(\bigcup_{f(a)=1} T_S(a) \;, \ldots, \; \bigcup_{f(a)=k} T_S(a) \right).$$

2. *The* class of k-partitions defined by the k-poset (G, f) *is given by*

$$\mathcal{K}(G, f) =_{\text{def}} \left\{ \; (G, f, S) \;\middle|\; S \textit{ is } \mathcal{K}\textit{-homomorphism on } G \; \right\}.$$

Proposition 4. *Let (G, f) be a k-poset with $f : G \to \{1, 2, \ldots, k\}$ surjective.*

1. *$(\mathcal{K}, \ldots, \mathcal{K}) \subseteq \mathcal{K}(G, f) \subseteq (\text{BC}(\mathcal{K}), \ldots, \text{BC}(\mathcal{K}))$.*
2. *If $\mathcal{K}$ is closed under complements then $\mathcal{K}(G, f) = (\mathcal{K}, \ldots, \mathcal{K})$.*

Definition 5. *The family $\text{RBH}_k(\mathcal{K}) =_{\text{def}} \{\mathcal{K}(G, f) \mid (G, f)$ is a k-poset$\}$ is the* refined boolean hierarchy of k-partitions over $\mathcal{K}$.

It would be very useful to decide whether $\mathcal{K}(G, f) \subseteq \mathcal{K}(G', f')$ for k-posets (G, f) and (G', f') by only looking at the defining posets. To this end a relation $\leq$ on finite labeled posets has been introduced.

Definition 6. *Let (G, f) and (G', f') be k-posets with $k \geq 2$.*

1. $(G, f) \leq (G', f')$ *if and only if there is a monotonic mapping* $\varphi : G \to G'$ *such that for every* $x \in G$, $f(x) = f'(\varphi(x))$.
2. $(G, f) \equiv (G', f')$ *if and only if* $(G, f) \leq (G', f')$ *and* $(G', f') \leq (G, f)$.

Note that among all equivalent k-posets there is always (up to isomorphy) a unique poset having the minimal number of elements. For the relation $\leq$ we are able to state an Embedding Lemma.

Lemma 7. (Embedding Lemma.) *Let* (G, f) *and* (G', f') *be* k*-posets. Then, if* $(G, f) \leq (G', f')$*, then* $\mathcal{K}(G, f) \subseteq \mathcal{K}(G', f')$.

The possibility to redirect the Embedding Lemma depends on the base class $\mathcal{K}$. For NP several results has been proven. Next theorem is currently the one with widest scope of validity since it holds for all finite labeled posets.

Theorem 8. *Let* (G, f) *and* (G', f') *be* k*-posets. It holds that* $\mathrm{NP}^A(G, f) \subseteq \mathrm{NP}^A(G', f')$ *for all oracles* A *if and only if* $(G, f) \leq (G', f')$.

4 Separability Notions

The notion of separability mentioned in the introductory section always supposes pairs of disjoint sets. In order to make the notion applicable to general pairs we introduce two reasonable extensions.

Definition 9. *Let* $\mathcal{K}$ *be a class of subsets of* M*. Let* A *and* B *be subsets of* M.

1. *The pair* (A, B) *is said to be* $\mathcal{K}$-separable *if and only if there exist sets* $C, D \in \mathcal{K}$ *such that* $A \subseteq C$, $B \subseteq D$, $C \cup D = M$, *and* $A \cap B = C \cap D$.
2. *The pair* (A, B) *is said to be* weakly $\mathcal{K}$-separable *if and only if there exists a set* $C \in \mathcal{K}$ *such that* $A \setminus B \subseteq C$ *and* $B \setminus A \subseteq \overline{C}$.

The definition is of $\mathcal{K}$-separability is motivated by the following correspondence to the refined boolean hierarchy of $\mathcal{K}$-partitions.

Proposition 10. *Let* $\mathcal{K}$ *be a class with* $\emptyset, M \in \mathcal{K}$ *which is closed under intersection and union. Let* $\mathfrak{S}_0$ *and* $\mathfrak{S}_\infty$ *be the* 4*-poset presented in Figure 1.*

1. $\mathcal{K}(\mathfrak{S}_0) = \left\{ \ (A, B, \overline{A \cup B}, A \cap B) \ \middle| \ A, B \in \mathcal{K} \ \right\}$.
2. $\mathcal{K}(\mathfrak{S}_\infty) = \left\{ \ (A, B, \overline{A \cup B}, A \cap B) \ \middle| \ A, B \in \mathcal{K} \text{ and } (A, B) \text{ is } \mathcal{K}\text{-separable} \ \right\}$.
3. *All pairs of* $\mathcal{K}$ *sets are* $\mathcal{K}$*-separable if and only if* $\mathcal{K}(\mathfrak{S}_0) = \mathcal{K}(\mathfrak{S}_\infty)$.

Note that if we only consider pairs of disjoint sets then we have a similar equivalence, namely by the equality of the partition classes generated by the same posets but without the least elements (with label 4.)

The following propositions are easily seen from the definitions.

Proposition 11. *Let* $\mathcal{K}$ *be a class of subsets of* M*. Let* A *and* B *be subsets of* M.

1. (A, B) *is* $\mathcal{K}$*-separable if and only if* (B, A) *is* $\mathcal{K}$*-separable.*
2. *If* (A, B) *is* $\mathcal{K}$*-separable then* (A, B) *is weakly* $\mathcal{K}$*-separable.*

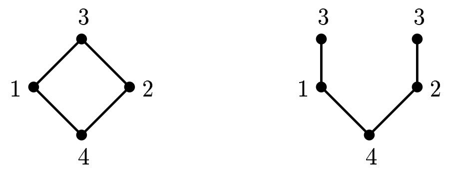

Fig. 1. The 4-posets $\mathfrak{S}_0$ (on the left) and $\mathfrak{S}_\infty$ (on the right)

3. Let $A \cap B = \emptyset$. (A, B) is $\mathcal{K}$-separable if and only if (A, B) is weakly $\mathcal{K}$-separable.

Proposition 12. *Let $\mathcal{K} \subseteq \mathcal{C}$.*

1. All pairs (A, B) of $\mathcal{K}$ sets are $\mathrm{BC}(\mathcal{C})$-separable.
2. All pairs (A, B) of $\mathcal{K}$ sets are weakly $\mathcal{C}$-separable.

Proof. 1. Set $C = A$ and $D = B \cup \overline{A}$ in Definition 9.1.
2. Set $C = A$ in Definition 9.2. ❑

The next result can be obtained by adapting the proof of Theorem 4 from [KW00, p. 165]. A set A is 2-$\{\wedge, \vee\}$-tt-*self-reducible*, if there exists a polynomial-time computable function f computing for every input $x \in \Sigma^*$ a triple $(\circ, x_0, x_1)$ with $x_0, x_1 \in \Sigma^{\leq |x|-1}$ and $\circ \in \{\wedge, \vee\}$ such that $x \in A \Leftrightarrow x_0 \in A \circ x_1 \in A$.

Theorem 13. *Let $\mathcal{K}$ be closed under $\leq_m^p$ and let $\mathcal{K}$ possess a $\leq_m^p$-complete set that is 2-$\{\wedge, \vee\}$-tt-self-reducible. If all pairs of $\mathcal{K}$ sets are weakly $\mathcal{C}$-separable, then $\mathcal{K} \subseteq \mathrm{P}^{\mathcal{C}}$.*

Together with Proposition 12 we conclude the following.

Corollary 14. *Let $\mathcal{K}$ be closed under $\leq_m^p$ and let $\mathcal{K}$ possess a $\leq_m^p$-complete set that is 2-$\{\wedge, \vee\}$-tt-self-reducible. Then, the following statements are equivalent.*

1. All pairs of $\mathcal{K}$ sets are $\mathrm{P}^{\mathcal{C}}$-separable.
2. All pairs of $\mathcal{K}$ sets are weakly $\mathrm{P}^{\mathcal{C}}$-separable.
3. $\mathcal{K} \subseteq \mathrm{P}^{\mathcal{C}}$.

The low and the high hierarchy within NP were introduced by Schöning [Sch83]. Define Low_k to be the class of all NP sets A such that $\Sigma_k^p(A) = \Sigma_k^p$. Let High_k be the class of all sets $A \in \mathrm{NP}$ such that $\Sigma_k^p(A) = \Sigma_{k+1}^p$. The following is well known.

- $\mathrm{Low}_0 = \mathrm{P}$ and $\mathrm{Low}_1 = \mathrm{NP} \cap \mathrm{coNP}$.
- $\mathrm{P}^{\mathrm{Low}_k} = \mathrm{Low}_k$ and $\mathrm{P}^{\mathrm{High}_k} = \mathrm{High}_k$.
- $\mathrm{NP} = \mathrm{Low}_k \Longleftrightarrow \mathrm{PH} = \Sigma_k^p$ and $\mathrm{NP} = \mathrm{High}_k \Longleftrightarrow \mathrm{PH} = \Sigma_k^p$.

So Corollary 15 is immediate since Satisfiability is clearly 2-$\{\wedge, \vee\}$-tt-self-reducible.

Corollary 15. *1. All pairs of NP sets are (weakly) Low_k-separable if and only if $\mathrm{PH} = \Sigma_k^p$.*
2. All pairs of NP sets are (weakly) High_k-separable if and only if $\mathrm{PH} = \Sigma_k^p$.

The similar result can be obtained for pairs of coNP sets since TAUTOLOGY is 2-$\{\wedge, \vee\}$-tt-self-reducible. In particular, we thus have that all pairs of NP sets are P-separable if and only if all pairs of coNP sets are P-separable, and both is equivalent to $\mathrm{P} = \mathrm{NP}$. This symmetry is remarkable since it is not known to hold for pairs of disjoint sets (see [FFNR96,MV96]).

We now turn to separability for disjoint sets. The following theorem generalizes the proof of Grollmann and Selman [GS88] who obtained a similar result for $\mathcal{C} = \mathcal{K} = \mathrm{P}$.

Theorem 16. *Let $\mathcal{K} \subseteq \mathcal{C}$ and let $\mathcal{K}$ be closed under $\leq_m^p$. If all pairs of disjoint $\mathrm{U} \cdot \mathcal{K}$ sets are $\mathcal{C}$-separable, then $\mathrm{U} \cdot \mathcal{K} \subseteq \mathrm{P}^{\mathcal{C}}$.*

Proof. Let $A \in \mathrm{U} \cdot \mathcal{K}$, i.e., there are a set $B \in \mathcal{K}$ and a polynomial p such that

$$\begin{aligned} x \in A &\iff \|\{y \mid |y| = p(|x|) \wedge \langle x, y \rangle \in \mathcal{K}\}\| = 1, \\ x \notin A &\iff \|\{y \mid |y| = p(|x|) \wedge \langle x, y \rangle \in \mathcal{K}\}\| = 0. \end{aligned}$$

Define the following sets:

$$\begin{aligned} S_B &= \{(x, z) \mid (\exists y, |y| = p(|x|))[z \leq y \wedge \langle x, y \rangle \in B]\} \\ T_B &= \{(x, z) \mid (\exists y, |y| = p(|x|))[z > y \wedge \langle x, y \rangle \in B]\} \end{aligned}$$

Obviously, $S_B, T_B \in \mathrm{U} \cdot \mathcal{K}$, $S_B \cap T_B = \varnothing$, and $S_B \cup T_B = A \times \Sigma^*$. Hence, there exists a set $C, D \in \mathcal{C}$ with $D = \overline{C}$ and $S_B \subseteq C \subseteq \overline{T_B}$. Using this set C as an oracle for binary search, one can determine for each $x \in \Sigma^*$ a value $b(x)$ such that $x \in A \iff \langle x, b(x) \rangle \in B$. Hence, $A \in \mathrm{P}^{\mathcal{C}}$. ❑

Corollary 17. *Let $\mathcal{K} \subseteq \mathrm{P}^{\mathcal{C}}$ and let $\mathcal{K}$ be closed under $\leq_m^p$. Then the following statements are equivalent.*

1. *All pairs of $\mathrm{U} \cdot \mathcal{K}$ sets are $\mathrm{P}^{\mathcal{C}}$-separable.*
2. *All pairs of disjoint $\mathrm{U} \cdot \mathcal{K}$ sets are $\mathrm{P}^{\mathcal{C}}$-separable.*
3. $\mathrm{U} \cdot \mathcal{K} \subseteq \mathrm{P}^{\mathcal{C}}$.

Corollary 18. *The following statements are equivalent.*

1. *All pairs of UP sets are P-separable.*
2. *All pairs of disjoint UP sets are P-separable.*
3. $\mathrm{P} = \mathrm{UP}$.

Corollary 19. *1. If all pairs of disjoint NP sets are Low_k-separable then $\mathrm{UP} \subseteq \mathrm{Low}_k$.*
2. If all pairs of disjoint NP sets are High_k-separable then $\mathrm{UP} \subseteq \mathrm{High}_k$.

Sheu and Long [SL96] proved that for all $k \in \mathbb{N}$ there are oracles C and D such that $\mathrm{UP} \not\subseteq \mathrm{Low}_k$ relative to C, and $\mathrm{UP} \not\subseteq \mathrm{High}_k$ relative to D. So we obtain that there exist relativized worlds where all pairs of disjoint NP sets are not Low_k-separable as well as there exist relativized worlds where all pairs of disjoint NP sets are not High_k-separable.

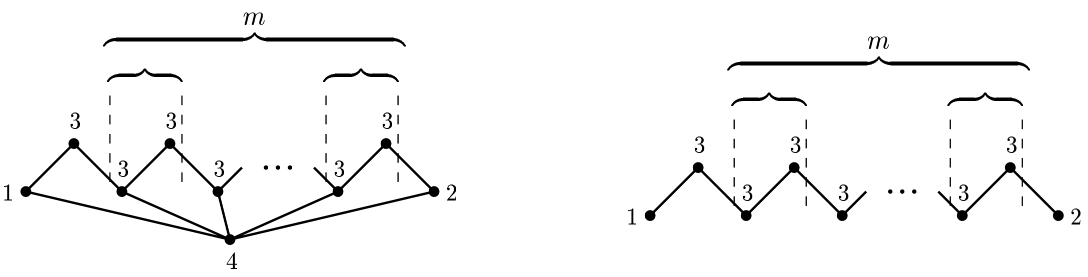

Fig. 2. The labeled posets $\mathfrak{S}_m$ (on the left) and $\mathfrak{S}_m^0$ (on the right) for $m \in \mathbb{N}$

5 A Quantitative Approach to Separability

Proposition 10 shows that the 4-poset $\mathfrak{S}_0$ represents the class of all pairs of $\mathcal{K}$ sets and that the 4-poset $\mathfrak{S}_\infty$ represents the class of $\mathcal{K}$-separable pairs of $\mathcal{K}$ sets. However, there are further 4-posets in between $\mathfrak{S}_0$ and $\mathfrak{S}_\infty$ with respect to our relation $\leq$ on labeled posets, namely, all the 4-posets $\mathfrak{S}_m$ in Figure 2 (in the case that we consider disjoint sets, for all $m \in \mathbb{N} \cup \{\infty\}$, let $\mathfrak{S}_m^0$ be the 3-poset that emerges from $\mathfrak{S}_m$ by deleting the minimum of the poset). This motivates the following definition.

Definition 20. *Let $\mathcal{K}$ be a class of subsets of M. Let A and B be subsets of M. Let $m \in \mathbb{N}$. The pair (A, B) is said to be* m-separable *in $\mathcal{K}$ if and only if there exist sets $C_0, C_1, \ldots, C_m \in \mathcal{K}$ such that the following conditions are satisfied:*

1. $\bigcup_{j=0}^{m} C_j = M$,
2. $A \cap B \subseteq C_j$ *for all* $j \in \{0, 1, \ldots, m\}$,
3. $C_i \cap C_k = A \cap B$ *for all* $i, j \in \{0, 1, \ldots, m\}$ *with* $|i - j| \geq 2$,
4. $A \setminus B \subseteq C_0 \setminus C_1$ *and* $B \setminus A \subseteq C_m \setminus C_{m-1}$.

We say that the sets $C_0, C_1, \ldots, C_m$ m-separate the pair (A, B).

Figure 3 shows an example of a pair of disjoint sets which is 3-separable.

Proposition 21. *Let $\mathcal{K}$ be a class with $\emptyset, M \in \mathcal{K}$ and which is closed under intersection and union. Let $m \in \mathbb{N}$. Let $\mathfrak{S}_m$ and $\mathfrak{S}_m^0$ be the labeled posets presented in Figure 2. then the following is true.*

1. $\mathcal{K}(\mathfrak{S}_m) = \left\{ (A, B, \overline{A \cup B}, A \cap B) \mid A, B \in \mathcal{K} \text{ and } (A, B) \text{ is } m\text{-separable in } \mathcal{K} \right\}$.
2. $\mathcal{K}(\mathfrak{S}_m^0) = \left\{ (A, B, \overline{A \cup B}) \mid A, B \in \mathcal{K}, A \cap B = \emptyset \text{ and } (A, B) \text{ is } m\text{-separable in } \mathcal{K} \right\}$.

The notion of m-separability induces a hierarchy which contains each pair of sets from $\mathcal{K}$.

Proposition 22. *Let $\mathcal{K}$ be such that $\emptyset, M \in \mathcal{K}$ and which is closed under intersection and union. Let A and B subsets of M.*

1. *(A, B) is 0-separable in $\mathcal{K}$.*
2. *For every $m \in \mathbb{N}$, if (A, B) is $(m + 1)$-separable in $\mathcal{K}$ then (A, B) is m-separable in $\mathcal{K}$.*
3. *If (A, B) is $\mathcal{K}$-separable then (A, B) is m-separable in $\mathcal{K}$ for all $m \in \mathbb{N}$.*

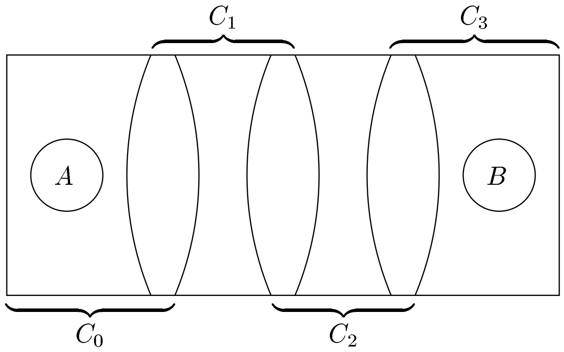

Fig. 3. A 3-separable pair of disjoint sets with its separating sets

Proof. 1. Set $C_0 = M$ in Definition 20.
2. Follows from Proposition 21 and the Embedding Lemma.
3. Follows from Proposition 10 and the Embedding Lemma. ❑

It depends on the properties of the class $\mathcal{K}$ how many levels the hierarchy concretely has. For instance, by Proposition 12, if $\mathcal{K}$ is closed under complements then each pair of $\mathcal{K}$ sets is $\mathcal{K}$-separable. Generally one can prove the following theorem specifying connections in the structure of the hierarchy.

Theorem 23. *Let $\mathcal{K}$ be a class with $\emptyset, M \in \mathcal{K}$ and which is closed under intersection and union. Let $m \in \mathbb{N}$. If all pairs of $\mathcal{K}$ sets that are m-separable in $\mathcal{K}$ are also $(m+1)$-separable in $\mathcal{K}$, then they all are n-separable in $\mathcal{K}$ for all $n \geq m$.*

Proof. Suppose that all pairs of $\mathcal{K}$ sets being m-separable in $\mathcal{K}$ are $(m+1)$-separable in $\mathcal{K}$. It suffices to show that then all pairs of $\mathcal{K}$ sets being $(m+1)$-separable in $\mathcal{K}$ are $(m+2)$-separable in $\mathcal{K}$ as well. The theorem then follows by induction. Let the pair (A, B) of $\mathcal{K}$ sets be $(m+1)$-separable. Let $C_0^{m+1}, C_1^{m+1}, \ldots, C_{m+1}^{m+1}$ be the sets that $(m+1)$-separate (A, B) in $\mathcal{K}$. Then the pair (C_0^{m+1}, B) is m-separable in $\mathcal{K}$ as is easily seen by setting $D_0^m = C_0^{m+1} \cup C_1^{m+1}$ and $D_i^m = C_{i+1}^{m+1}$ for $i \in \{1, 2, \ldots, m\}$. By our supposition, (C_0^{m+1}, B) is also $(m+1)$-separable in $\mathcal{K}$. Let $D_0^{m+1}, D_1^{m+1}, \ldots, D_{m+1}^{m+1}$ be the sets in $\mathcal{K}$ that $(m+1)$-separate (C_0^{m+1}, B). Define the sets E_j^{m+1} for $j \in \{0, 1, \ldots, m+1\}$ as follows:

$$E_j^{m+1} =_{\mathrm{def}} \left(D_j^m \cap \bigcup_{r=0}^{j} D_r^{m+1} \right) \cup \left(D_{j-1}^m \cap \bigcup_{r=j}^{m+1} D_r^{m+1} \right)$$

where we consider both D_{-1}^m and D_{m+1}^m to be the empty set. Clearly, all E_j^{m+1} are in $\mathcal{K}$.

Claim. (C_0^{m+1}, B) is $(m+1)$-separated in $\mathcal{K}$ by $E_0^{m+1}, E_1^{m+1}, \ldots, E_{m+1}^{m+1}$.

Proof of the claim. We have to show that all conditions in Definition 20 are fulfilled.

1. Let $x \in M$. Since $\bigcup_{j=0}^{m} D_j^m = M$ and $\bigcup_{j=0}^{m+1} D_j^{m+1} = M$ there exist indexes i and j with $x \in D_i^m \cap D_j^{m+1}$. For such i and j we clearly have that if $i > j$ then $x \in E_i^{m+1}$ else $x \in E_{i+1}^{m+1}$.

2. That $C_0^{m+1} \cap B \subseteq E_j^{m+1}$ for all $j \in \{0, 1, \dots, m+1\}$ is obvious.
3. We have to show that $E_i^{m+1} \cap E_j^{m+1} \subseteq C_0^{m+1} \cap B$ for all i, j with $|i-j| \geq 2$. Without loss of generality, let $i < j$. Using the distributive law it is enough to conclude that

$$D_i^m \cap D_j^m \cap \bigcup_{r=0}^{i} D_r^{m+1} \subseteq C_0^{m+1} \cap B$$

$$D_{i-1}^m \cap D_j^m \cap \bigcup_{r=0}^{m+1} D_r^{m+1} \subseteq C_0^{m+1} \cap B$$

$$D_i^m \cap D_{j-1}^m \cap \left(\bigcup_{r=0}^{i} D_r^{m+1} \right) \cap \left(\bigcup_{r=j}^{m+1} D_r^{m+1} \right) \subseteq C_0^{m+1} \cap B$$

$$D_{i-1}^m \cap D_{j-1}^m \cap \bigcup_{r=j}^{m+1} D_r^{m+1} \subseteq C_0^{m+1} \cap B$$

4. On the one hand we easily calculate that

$$\begin{aligned} E_0^{m+1} \setminus E_1^{m+1} &= (D_0^m \cap D_0^{m+1}) \setminus (D_1^m \cup D_1^{m+1}) \\ &= (D_0^m \setminus D_1^m) \cap D_0^{m+1} \cap (D_0^{m+1} \setminus D_1^{m+1}) \cap D_0^m \ \supseteq \ C_0^{m+1} \cap B. \end{aligned}$$

On the other hand we conclude

$$E_{m+1}^{m+1} \setminus E_m^{m+1} = (D_m^m \cap D_{m+1}^{m+1}) \setminus D_m^{m+1} = D_m^m \cap (D_{m+1}^{m+1} \setminus D_m^{m+1}) \supseteq C_0^{m+1} \cap B.$$

This shows the claim.

Now we define the sets C_j^{m+2} for all $j \in \{0, 1, \dots, m+2\}$ as follows:

$$C_j^{m+2} =_{\text{def}} \begin{cases} C_0^{m+1} & \text{if } j = 0, \\ E_0^{m+1} \cap C_1^{m+1} & \text{if } j = 1, \\ E_{j-1}^{m+1} & \text{if } j \geq 2. \end{cases}$$

Since $E_0^{m+1} \subseteq D_0^m$ we have that $E_0^{m+1} \subseteq C_0^{m+1} \cup C_1^{m+1}$. So using the claim we obtain that (A, B) is $(m+2)$-separated in $\mathcal{K}$ by the sets $C_0^{m+2}, C_1^{m+2}, \dots, C_{m+2}^{m+2}$. ❑

Theorem 23 is a remarkable result. Literally taken it seems to pose that an equality ("m-separability equals $m+1$-separability") translates upwards ("m-separability equals n-separability for all $n \geq m$"). Actually we have a downward translation of equality. If we consider the corresponding partition classes $\mathcal{K}(\mathfrak{S}_m)$, then it clearly holds

- $\mathcal{K}(\mathfrak{S}_0) \supseteq \mathcal{K}(\mathfrak{S}_1) \supseteq \cdots$,
- $\mathcal{K}(\mathfrak{S}_m) = \mathcal{K}(\mathfrak{S}_{m+1})$ implies for all $n \geq m$, $\mathcal{K}(\mathfrak{S}_m) = \mathcal{K}(\mathfrak{S}_n)$.

Thus, in the refined boolean hierarchy of k-partition for $k \geq 3$ we can observe downward collapses that are usually very rare to find in hierarchies (see discussions in, e.g., [All91,AW90,HJ95,HHH99]).

It arises the issue of how far-reaching the collapse is. More specifically, when do

- $\mathcal{K}(\mathfrak{S}_m) = \mathcal{K}(\mathfrak{S}_{m+1}) \Longrightarrow \mathcal{K}(\mathfrak{S}_m) = \mathcal{K}(\mathfrak{S}_\infty)$ or
- $\bigcap_{m=0}^{\infty} \mathcal{K}(\mathfrak{S}_m) = \mathcal{K}(\mathfrak{S}_\infty)$

hold? The validity of the second statement trivially implies the validity of the first statement. That the issue is reasonable follows from the next theorem.

Theorem 24. *1. $\mathfrak{S}_\infty$ is the greatest 4-poset which is less than $\mathfrak{S}_m$ for all $m \in \mathbb{N}$.*
2. $\mathfrak{S}^0_\infty$ is the greatest 3-poset which is less than $\mathfrak{S}^0_m$ for all $m \in \mathbb{N}$.

Proof. We start with the proof of the second statement.

2. Obviously, $\mathfrak{S}^0_\infty \leq \mathfrak{S}^0_m$ for all $m \geq 0$. So it remains to prove that for all minimal 3-posets $\mathfrak{T} = (T, t)$ with $\mathfrak{T} \leq \mathfrak{S}^0_m$ for all $m \geq 0$, it holds that $\mathfrak{T} \leq \mathfrak{S}^0_\infty$. To do that we adapt some notions from graph theory. For any poset G we say that a subset $E \subseteq G$ is isolated in G if for all $x, y \in G$, $x \leq y$ implies that $x, y \in E$ or $x, y \in G \setminus E$. We say that a poset G is connected if G does not contain any isolated subset. Note that each poset G can be uniquely partitioned into maximal connected subposets. Let $\mathfrak{T}' = (T', t')$ be any k-subposet of $\mathfrak{T}$ such that T' is a maximal connected subposet of T and t' is the restriction of the labeling function t to T'. Note that $\mathfrak{T}'$ is minimal since $\mathfrak{T}$ is minimal. Then clearly, $\mathfrak{T}' \leq \mathfrak{S}^0_m$ for all $m \in \mathbb{N}$. Let $\varphi_m : T' \to S_m$ be a monotonic function witnessing $\mathfrak{T}' \leq \mathfrak{S}^0_m$. Since T' is connected, $\varphi_m(T')$ is a connected subposet of S_m. Hence, for $m > \|T'\|$ there exist no $x, y \in \varphi_m(T')$ with $s_m(x) = 1$ and $s_m(y) = 2$. Thus $\|t'(T')\| \leq 2$. Since T' is connected, $\mathfrak{T}'$ has to be a labeled chain. Hence, represented as words over the alphabet $\{1, 2, 3\}$, $\mathfrak{T}'$ is in $\{1, 2, 3, 13, 23\}$. Consequently, $\mathfrak{T}' \leq \mathfrak{S}^0_\infty$. Since T' was arbitrarily chosen among all maximal connected subposets of T, we obtain $\mathfrak{T} \leq \mathfrak{S}^0_m$.
1. Again it is obvious, that $\mathfrak{S}_\infty \leq \mathfrak{S}_m$ for all $m \geq 0$. If, for any 4-poset $\mathfrak{T} = (T, t)$, $\mathfrak{T} \leq \mathfrak{S}_m$ for all $m \in \mathbb{N}$, then we consider the 4-poset $\mathfrak{R} = (R, t)$ instead of $\mathfrak{T}$ where $R = T \setminus \{a \in T \mid (\exists b \in T)[t(b) = 4 \wedge a \leq b]\}$ and proceed as above. This is correct since each element in T which is labeled by 4 has to be mapped to the least element in $\mathfrak{S}_m$.

❑

From this theorem we easily obtain that between $\mathfrak{S}_0$ and $\mathfrak{S}_\infty$ no further (minimal) labeled posets can occur since all posets must exactly have the maximal chains 413 and 423 represented as words over the alphabet $\{1, 2, 3, 4\}$. But $\mathfrak{S}_m$ for $m \in \mathbb{N} \cup \{\infty\}$ are all minimal labeled posets with this property. The same holds for the posets between $\mathfrak{S}^0_0$ and $\mathfrak{S}^0_\infty$.

Finally, we apply all our notions and results to the class NP obtaining a probably infinite separation hierarchy.

Theorem 25. *Let $m \in \mathbb{N}$.*

1. *All pairs of* NP *sets are $(m+1)$-separable in* NP *if and only if* NP = coNP.
2. *There exists a relativized world such that there is a pair of disjoint* NP *sets that is m-separable in* NP *but not $(m+1)$-separable in* NP.

References

[All91] E. Allender. Limitations of the upward separation technique. *Mathematical Systems Theory*, 24:53–67, 1991.

[AW90] E. Allender and C. Wilson. Downward translations of equality. *Theoretical Computer Science*, 75:335–346, 1990.

[BDG95] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2nd edition, 1995.

[Bei88] R. Beigel. NP-hard sets are P-superterse unless R=NP. Technical Report TR 88-04, Johns Hopkins University, Baltimore, 1988.

[DP90] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order.* Cambridge University Press, Cambridge, 1990.

[FFNR96] S. Fenner, L. Fortnow, A. V. Naik, and J. D. Rogers. Inverting onto functions. In *Proceedings 11th IEEE Conference on Computational Complexity*, pages 213–222. IEEE Computer Society Press, Los Alamitos, 1996.

[FHT97] S. Fischer, L. A. Hemaspaandra, and L. Torenvliet. Witness-isomorphic reductions and local search. In A. Sorbi, editor, *Complexity, Logic, and Recursion Theory*, volume 187 of *Lecture Notes in Pure and Applied Mathematics*, pages 207–223. Marcel Dekker, Inc., New York, 1997.

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

[Grä78] G. Grätzer. *General Lattice Theory.* Akademie-Verlag, Berlin, 1978.

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

[HHH99] E. Hemaspaandra, L. A. Hemaspaandra, and H. Hempel. A downward collapse within the polynomial hierarchy. *SIAM Journal on Computing*, 28(2):383–393, 1999.

[HHN+95] L. A. Hemaspaandra, A. Hoene, A. V. Naik, M. Ogihara, A. L. Selman, T. Thierauf, and J. Wang. Nondeterministically selective sets. *International Journal of Foundations of Computer Science*, 6(4):403–416, 1995.

[HJ95] L. A. Hemaspaandra and S. K. Jha. Defying upward and downward separation. *Information and Computation*, 121(1):1–13, 1995.

[Kec95] A. S. Kechris. *Classical Descriptive Set Theory*, volume 156 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[Kle50] S. K. Kleene. A symmetric form of Gödel's theorem. *Ind. Math.*, 12:244–246, 1950.

[KM98] J. Köbler and J. Messner. Complete problems for promise classes by optimal proof systems for test sets. In *Proceedings 13th IEEE Conference on Computational Complexity*, pages 182–185. IEEE Computer Society Press, Los Alamitos, 1998.

[Kos00] S. Kosub. On NP-partitions over posets with an application of reducing the set of solutions of NP problems. In *Proceedings 25th Symposium on Mathematical Foundations of Computer Science*, volume 1893 of *Lecture Notes in Computer Science*, pages 467–476. Springer-verlag, Berlin, 2000.

[KW99] S. Kosub and K. W. Wagner. The boolean hierarchy of partitions. Technical Report 233, Julius-Maximilians-Universität Würzburg, Institut für Informatik, July 1999. Revised, November 2000.

[KW00] S. Kosub and K. W. Wagner. The boolean hierarchy of NP-partitions. In *Proceedings 17th Symposium on Theoretical Aspects of Computer Science*, volume 1770 of *Lecture Notes in Computer Science*, pages 157–168. Springer-Verlag, Berlin, 2000.

[MS72] A. R. Meyer and L. J. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential time. In *Proceedings 13th Symposium on Switching and Automata Theory*, pages 125–129. IEEE Computer Society Press, Los Alamitos, 1972.

[MV96] A. A. Muchnik and N. K. Vereshchagin. A general method to construct oracles realizing given relationships between complexity classes. *Theoretical Computer Science*, 157(2):227–258, 1996.

[Raz94] A. A. Razborov. On provably disjoint NP pairs. Technical Report RS-94-36, Basic Research in Computer Science Center, Aarhus, 1994.

[Raz95] A. A. Razborov. Bounded arithmetic and lower bounds in boolean complexity. In P. Clote and J. B. Remmel, editors, *Feasible Mathematics II*, volume 13 of *Progress in Computer Science and Applied Logic*, pages 344–387. Birkhäuser, Boston, 1995.

[Sch83] U. Schöning. A low and a high hierarchy within NP. *Journal of Computer and System Sciences*, 27:14–28, 1983.

[Sho58] J. R. Shoenfield. Degrees of formal systems. *Journal of Symbolic Logic*, 23:389–392, 1958.

[SL96] M.-J. Sheu and T. J. Long. UP and the low and high hierarchies: A relativized separation. *Mathematical Systems Theory*, 29:423–449, 1996.

[SP98] U. Schöning and R. Pruim. *Gems of Theoretical Computer Science*. Springer-Verlag, Berlin, 1998.

[Sto77] L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

[Tar49] A. Tarski. On essential undecidability. *Journal of Symbolic Logic*, 14:75–76, 1949.

[Tra53] B. A. Trakhtenbrot. On recursive separability. *Doklady Akademii Nauk SSSR*, 88:953–956, 1953. In Russian.

[Usp53] V. A. Uspenski. Gödel's theorem and the theory of algorithms. *Doklady Akademii Nauk SSSR*, 91:737–740, 1953. In Russian.

[WW86] K. W. Wagner and G. Wechsung. *Computational Complexity*. Deutscher Verlag der Wissenschaften, Berlin, 1986.