

The ultra-weak Ash conjecture and some particular cases

Annie Chateau* and Malika More**

Laboratoire Logique, Algorithmique et Informatique de Clermont,
Institut Universitaire de Technologie de Clermont-Ferrand,
Campus des Cézeaux, B.P. 86, F-63172 Aubière Cedex, France

Received 26 May 2005, revised 8 August 2005, accepted 19 August 2005
Published online 2 January 2006

Key words Finite models, descriptive complexity, spectrum conjecture, Ash's conjecture.

MSC (2000) 03C13, 68Q15, 68Q19

Ash's functions $N_{\sigma,k}$ count the number of k -equivalence classes of σ -structures of size n . Some conditions on their asymptotic behavior imply the long standing spectrum conjecture. We present a new condition which is equivalent to this conjecture and we discriminate some easy and difficult particular cases.

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

1 Introduction

The development of finite model theory is mainly due to the interest of the theoretical computer science community for this subject. For instance, in complexity theory, following the well known Fagin theorem [12] which states that existential second-order logic ESO exactly captures the complexity class NP, most complexity classes have been proved to have a logical characterization, see for instance the textbook [19].

However, among the tools developed by logicians to prove theorems in model theory, very few subsist when finite models are involved. A notable exception is Fraïssé's back-and-forth method, and its game description, due to Ehrenfeucht (see [15, 9, 18, 8]). The main interest of this method, or of its many variants, is that it can be used to prove non-expressibility results (i. e. lower bounds for complexity problems), the research for such results being one of the major aims of theoretical computer science.

On the other hand, counting is also a key notion in complexity theory. Counting classes such as #P have been widely studied (see for instance [26, 24, 25, 27]), and (non-)closure under counting of very small complexity classes is known to provide significant information about their expressive power (see [1, 7, 14]).

In 1994, the Australian logician Christopher J. Ash puts these two frameworks together: he publishes a short original paper [2] in which he proposes to count the number of non k -equivalent structures of the same finite size. He shows a surprising result: the asymptotic behavior of these counting functions is closely connected to closure under complement of the complexity class NE, more precisely, of its logical counterpart, the class SPEC of all spectra of first-order sentences, a well-known open problem in complexity theory. As far as we know, these ideas of Ash's have not been exploited afterwards, and his paper has remained somehow isolated.

In this paper we propose a new version of Ash's conjecture which we prove to be equivalent to the assertion $NE = \text{co-NE}$, and we classify many particular cases of this conjecture. We show that some cases are easy, i. e. we prove the conjecture, whereas others are difficult, i. e. solving them implies solving the full conjecture.

2 Background and definitions

We assume the reader to be familiar with basic notions of first-order logic and complexity theory, see for instance the textbooks [11, 22]. Unless otherwise stated, all signatures in this paper are finite, purely relational, i. e. they

* Corresponding author: e-mail: chateau@llaic.u-clermont1.fr

** e-mail: more@llaic.u-clermont1.fr

contain no function and no constant, and contain equality. We say that a signature is k -ary if it contains only relations with arities $\leq k$ (except equality, if $k = 1$). We denote by \mathbb{N}^+ the set of positive integers.

Scholz [23] defines in 1952 the spectrum of a first-order sentence as the set of cardinalities of its finite models and calls for a characterization of the class SPEC of all spectra. It is interesting to note that this very first question of finite model theory was originally raised without any reference to theoretical computer science. In 1955, Asser [3] states a conjecture which remains unproved.

Conjecture 1 (The spectrum conjecture) *The complement of a spectrum is a spectrum, i. e.*

$$\text{SPEC} = \text{co-SPEC}.$$

More formally, for a given sentence φ on a finite relational signature σ and its spectrum $\text{Sp}(\varphi) \subseteq \mathbb{N}^+$, the spectrum conjecture states that there exist a finite relational signature τ and a first-order τ -sentence ψ such that $\text{Sp}(\psi) = \mathbb{N}^+ \setminus \text{Sp}(\varphi)$.

Let us recall the complexity theory characterization of SPEC. We denote by $\text{NTIME}(2^{c \cdot n})$ (respectively $\text{DTIME}(2^{c \cdot n})$) the class of all sets of integers recognizable by a non-deterministic (respectively deterministic) RAM in exponential time $\mathcal{O}(2^{c \cdot n})$, where n is the size of the binary notation of the input integer and c is a constant. Define $\text{NE} = \bigcup_{c \geq 1} \text{NTIME}(2^{c \cdot n})$ (respectively $\text{E} = \bigcup_{c \geq 1} \text{DTIME}(2^{c \cdot n})$). Scholz' question is answered by Jones and Selman [20] in 1974: they show that $\text{SPEC} = \text{NE}$. Note that the correspondence between the complexity class NE and the logical class SPEC is similar to Fagin's characterization of NP via ESO in [12]. The main difference lies in the nature of the considered sets: spectra are sets of integers, whereas ESO is composed of sets of finite structures.

Consequently, the spectrum conjecture is equivalent to the assertion $\text{NE} = \text{co-NE}$. Since $\text{NE} \neq \text{co-NE}$ would imply $\text{P} \neq \text{NP}$, it is not surprising that the spectrum conjecture has remained open for some fifty years.

Now let us turn to Ash's contribution. The so-called k -equivalence between structures is introduced by Fraïssé [15] in 1954 and the game presentation is due to Ehrenfeucht [9] in 1961. In the two following definitions, signatures may contain constants.

Definition 2.1 Let σ be a signature, let \mathcal{A} and \mathcal{B} be σ -structures and let k be an integer. The two structures \mathcal{A} and \mathcal{B} are k -equivalent if and only if they satisfy the same σ -sentences with quantifier depth $\leq k$.

For a detailed presentation of k -equivalence, we refer the reader to [8, 18]. For our purpose, the two most important features of the above notion are the following:

1. For each finite signature σ and for each quantifier depth k , the number of k -equivalence classes of σ -structures is finite and we denote it by $M_{\sigma,k}$.
2. For each finite signature σ , for each quantifier depth k and for each k -equivalence class of σ -structures \mathcal{C} , there exists a σ -sentence $\psi_{\mathcal{C}}$ of quantifier depth k such that, for all σ -structures \mathcal{A} , we have $\mathcal{A} \in \mathcal{C}$ if and only if $\mathcal{A} \models \psi_{\mathcal{C}}$.

In Subsection 4.1, we also use the notion of k -equivalent tuples of elements of a structure.

Definition 2.2 Let σ be a signature, let \mathcal{A} be a σ -structure of domain A , let (a_1, \dots, a_p) and (b_1, \dots, b_p) be two p -tuples of elements of A , and let k be an integer. The tuples (a_1, \dots, a_p) and (b_1, \dots, b_p) are k -equivalent if and only if the two structures $\langle \mathcal{A}, a_1, \dots, a_p \rangle$ and $\langle \mathcal{A}, b_1, \dots, b_p \rangle$ are k -equivalent.

In 1994, Ash [2] introduces a counting function relative to the k -equivalence classes.

Definition 2.3 Let σ be a finite relational signature, and let k be a positive integer. Ash's function $N_{\sigma,k}$ counts, for each positive integer n , the number of k -equivalence classes of σ -structures of size n .

This function is obviously bounded by the total number of classes, $M_{\sigma,k}$, and Ash's conjecture deals with its asymptotic behavior.

Conjecture 2 (Ash's constant conjecture) *For any finite relational signature σ and any positive integer k , the Ash function $N_{\sigma,k}$ is eventually constant.*

A weaker version of his conjecture is also proposed.

Conjecture 3 (Ash's periodic conjecture) *For any finite relational signature σ and any positive integer k , the Ash function $N_{\sigma,k}$ is eventually periodic.*

Ash [2] shows by a very neat proof that both conjectures imply the spectrum conjecture.

In this paper, we first propose in Section 3 a third version of Ash's conjecture, the so-called *ultra-weak Ash conjecture*, which we prove to be equivalent to the spectrum conjecture.

In Section 4, we show that, for any signature σ , Ash's functions $N_{\sigma,2}$ are eventually constant, i. e. the number of non-2-equivalent σ -structures of size n eventually does not depend on n . Then we show that, by contrast, the eventual behavior of Ash's functions for quantifier depth 3 is as difficult to analyze as the general case. Similarly, we prove that the case when the signature is reduced to one single binary relation is also a difficult one.

In Section 5, we turn to the Ash functions for theories, i. e. we impose a fixed semantical interpretation to the signature. In this framework, we first present a sufficient condition for a function to be the Ash function for some theory. Then we prove that the asymptotic behavior of the Ash functions for a theory is connected to the closure under complement of the spectra of the sentences which imply this theory. Finally, we also present some difficult theories, according to Ash's previously mentioned criterion.

3 The ultra-weak Ash conjecture

Let φ and ψ be two sentences, we denote $\psi \models_f \varphi$ if φ holds in all finite models of ψ . We say that ψ *decides* φ if $\psi \models_f \varphi$ or $\psi \models_f \neg\varphi$.

Let σ be a finite relational signature and k be a positive integer. The function N depends on σ and k , but in order to make the proofs more readable, we let it implicit.

For all $i \in \mathbb{N}^+$, we note as usual $N_{\sigma,k}^{-1}(i) = \{n \in \mathbb{N}^+ \mid N_{\sigma,k}(n) = i\}$, the inverse image of the positive integer i under the function $N_{\sigma,k}$. Remark that the sets $N_{\sigma,k}^{-1}(i)$ partition \mathbb{N}^+ , and that they are empty for $i > M_{\sigma,k}$, i. e. $\mathbb{N}^+ = \dot{\bigcup}_{i=1}^{M_{\sigma,k}} N_{\sigma,k}^{-1}(i)$.

Note that Ash's constant conjecture can be restated using the sets $N_{\sigma,k}^{-1}(i)$ as follows: All non-empty sets $N_{\sigma,k}^{-1}(i)$ but one are finite sets (the infinite one being consequently co-finite). Similarly, Ash's periodic conjecture can be rephrased in terms of the sets $N_{\sigma,k}^{-1}(i)$, now also using periodic sets. Both conjectures are subsumed under the following condition.

Conjecture 4 (The ultra-weak Ash conjecture) *For any finite relational signature σ , for any positive integer k and for all $i \in \mathbb{N}^+$, the set $N_{\sigma,k}^{-1}(i)$ is a spectrum.*

Since most spectra are much more complicated than finite, cofinite or periodic sets, this conjecture is clearly weaker than Ash's original conjectures. We call it "ultra-weak", because it cannot be weakened any more, as it is proved just below. Indeed, the main result of this section is that the above condition is necessary and sufficient for the complement of a spectrum to be a spectrum.

Theorem 3.1 *Let σ be a finite relational signature, and let k be a positive integer. For all $i \in \mathbb{N}^+$, the set $N_{\sigma,k}^{-1}(i)$ is a spectrum if and only if for every σ -sentence φ of quantifier depth $\leq k$, the set $\mathbb{N}^+ \setminus \text{Sp}(\varphi)$ is a spectrum.*

Proof. This proof is similar to Ash's proof in [2].

(\Rightarrow) We fix a finite relational signature σ , a quantifier depth $k \geq 1$ and a σ -sentence φ with quantifier depth k . Let us consider the set Ψ of all σ -sentences with quantifier depth k which characterize the k -equivalence classes of σ -structures. Observe that Ψ contains exactly $M_{\sigma,k}$ sentences. Since φ has quantifier depth k , all (finite or infinite) structures in a given class satisfy or do not satisfy φ together. Hence, in particular, a sentence $\psi \in \Psi$ decides φ .

For all $\psi \in \Psi$, we denote by ψ' the sentence built from ψ by duplicating the original signature σ into $M_{\sigma,k}$ new pairwise disjoint copies (equality is not duplicated).

We can now define, for all $j \in \{1, \dots, M_{\sigma,k}\}$, the sentence $\theta_j^\varphi = \bigvee \{ \bigwedge_{\psi \in \Theta} \psi' \mid \Theta \subseteq \Psi, |\Theta| = j, \Theta \models_f \neg\varphi \}$, meaning that there exists a set of j distinct k -equivalence classes of structures not satisfying φ .

Using the fact that $N_{\sigma,k}(n) = j$ means that there are exactly j different k -equivalence classes that have a representative of size n , it is now easy to check that $\mathbb{N}^+ \setminus \text{Sp}(\varphi) = \bigcup_{j=1}^{M_{\sigma,k}} (\text{Sp}(\theta_j^\varphi) \cap N_{\sigma,k}^{-1}(j))$.

It is well known that spectra are closed under finite union and intersection. Consequently, if all sets $N_{\sigma,k}^{-1}(i)$ are spectra, the set $\mathbb{N}^+ \setminus \text{Sp}(\varphi)$ is also a spectrum.

(\Leftarrow) We fix a finite relational signature σ and an integer $k \geq 1$. Let φ_0 be an always false sentence with quantifier depth k . For all $j \in \{1, \dots, M_{\sigma,k}\}$, we consider the sentences $\theta_j^{\varphi_0}$ as above. For all $j \in \mathbb{N}^+$, we have $\text{Sp}(\theta_j^{\varphi_0}) = \{n \in \mathbb{N}^+ \mid N_{\sigma,k}(n) \geq j\}$, and of course $N_{\sigma,k}^{-1}(j) = \text{Sp}(\theta_j^{\varphi_0}) \setminus \text{Sp}(\theta_{j+1}^{\varphi_0})$, which can be also written $N_{\sigma,k}^{-1}(j) = \text{Sp}(\theta_j^{\varphi_0}) \cap (\mathbb{N}^+ \setminus \text{Sp}(\theta_{j+1}^{\varphi_0}))$.

Now observe that $\text{Sp}(\theta_j^{\varphi}) = \bigcup \{ \bigcap_{\psi \in \Theta} \text{Sp}(\psi') \mid \Theta \subseteq \Psi, |\Theta| = j, \Theta \models_f \neg \varphi \}$, because the signatures of the sentences ψ' are pairwise disjoint. Consequently

$$\mathbb{N}^+ \setminus \text{Sp}(\theta_{j+1}^{\varphi_0}) = \bigcup \{ \bigcap_{\psi \in \Theta} (\mathbb{N}^+ \setminus \text{Sp}(\psi')) \mid \Theta \subseteq \Psi, |\Theta| = j, \Theta \models_f \neg \varphi \}.$$

Since ψ' can also be seen as a σ -sentence of quantifier depth k , then by assumption $\mathbb{N}^+ \setminus \text{Sp}(\psi')$ is a spectrum. Finally, $N_{\sigma,k}^{-1}(j)$ is also a spectrum. \square

Remark that the core of the proof of Theorem 3.1 is contained in the following more general proposition, which may prove to be useful in quite different scenarios.

Proposition 3.2 *Let Ψ be a finite set of sentences such that $\models_f \bigvee_{\psi \in \Psi} \psi$ and for distinct $\psi, \psi' \in \Psi$, $\models_f \neg(\psi \wedge \psi')$. Let $N^{-1}(i) = \{n \in \mathbb{N}^+ \mid |\{\psi \in \Psi \mid \psi \text{ has a model of size } n\}| = i\}$.*

1. *If for all $\psi \in \Psi$, $\mathbb{N}^+ \setminus \text{Sp}(\psi)$ is a spectrum, then for all $i \in \mathbb{N}^+$, $N^{-1}(i)$ is a spectrum.*
2. *If for all $i \in \mathbb{N}^+$, $N^{-1}(i)$ is a spectrum, and φ is decided by each $\psi \in \Psi$, then the set $\mathbb{N}^+ \setminus \text{Sp}(\varphi)$ is a spectrum.*

All in all, we obtain

Corollary 3.3 *The spectrum conjecture is true if and only if the ultra-weak Ash conjecture is true.*

Finally, note that in the particular case when, for given σ and k , the Ash function $N_{\sigma,k}$ is eventually constant, a closer look at the logical proof of Theorem 3.1 given above provides interesting additional information about complements of spectra that would not be obtained from a purely complexity theoretical proof using NE instead of SPEC. Indeed, let us denote by r the eventual value of $N_{\sigma,k}$. Let φ be a σ -sentence of quantifier depth $\leq k$. From the restatement of Ash's constant conjecture in terms of the sets $N_{\sigma,k}^{-1}(j)$ and from the equality $\mathbb{N}^+ \setminus \text{Sp}(\varphi) = \bigcup_{j=1}^{M_{\sigma,k}} (\text{Sp}(\theta_j^{\varphi}) \cap N_{\sigma,k}^{-1}(j))$ it follows that, up to a finite set, we have $\mathbb{N}^+ \setminus \text{Sp}(\varphi) = \text{Sp}(\theta_r^{\varphi})$. Thus, we obtain the following corollary.

Corollary 3.4 *Let σ be a finite relational signature, and let k be a positive integer. If the Ash function $N_{\sigma,k}$ is eventually constant, then for every σ -sentence φ of quantifier depth $\leq k$, the set $\mathbb{N}^+ \setminus \text{Sp}(\varphi)$ is the spectrum of a sentence of the same quantifier depth as φ over a signature with the same arities as σ .*

A similar remark holds whenever, for given σ and k , the sets $N_{\sigma,k}^{-1}(i)$ are spectra of sentences of quantifier depth $\leq k$ over a signature with arities not higher than the arities in σ .

4 Some particular cases

The spectrum conjecture being a very difficult question, it is also the case of Ash conjectures. In order to make some progress, we consider in this section particular cases of Ash conjectures, i. e. we limit the range of the couples (σ, k) .

Let us recall first that Ash [2] already considers particular cases of his conjectures. For instance, he shows

Proposition 4.1 *If σ_1 is a unary signature, then for all $k \geq 1$, Ash's function $N_{\sigma_1,k}$ is eventually constant.*

Thus, one deduces from Theorem 3.1 that the complement of the spectrum of a unary sentence is also a spectrum (of a unary sentence of the same quantifier depth). However, this is not a new result, because it is well-known that the expressive power of unary signatures is very weak: only finite and cofinite spectra are definable.

In Subsection 4.1, we prove that if $k = 2$, then for any relational signature σ , Ash's function $N_{\sigma,2}$ is also eventually constant. Note that, once again, sentences of quantifier depth 2 define only finite and cofinite spectra (see [21]).

Conversely, we show in Subsection 4.2 that the cases of the signature $\text{BIN} = \{=, B\}$, where B is a binary relation, and of $k = 3$ are as difficult as the full ultra-weak conjecture. More precisely, if for all $k \geq 1$ and for all $i \in \mathbb{N}^+$, the set $N_{\text{BIN},k}^{-1}(i)$ is a spectrum, then the spectrum conjecture holds. Similarly if for all σ and for all $i \in \mathbb{N}^+$, the set $N_{\sigma,3}^{-1}(i)$ is a spectrum, then the spectrum conjecture holds.

4.1 Quantifier depth 2

First we consider the case when the signature contains only unary and binary relation symbols.

Proposition 4.2 *Let σ_2 be a finite binary relational signature. Then $N_{\sigma_2,2}$ is eventually constant.*

Proof. If σ_2 contains t unary relation symbols U_1, \dots, U_t and s binary relation symbols B_1, \dots, B_s , then the number of non-1-equivalent elements of a σ_2 -structure is bounded by some (big) integer n_0 . Now let $n > n_0$, and let \mathcal{M} be a σ_2 -structure of size n : at least two elements of \mathcal{M} are 1-equivalent. Let x_1, \dots, x_p be the elements of a 1-equivalence class of elements of \mathcal{M} with at least two elements (i. e. $p \geq 2$). Consider the σ_2 -structure \mathcal{N} of size $n + 1$ obtained from \mathcal{M} by adding a new element x_0 such that

1. for $i = 1, \dots, t$, $U_i(x_0)$ if and only if $U_i(x_1)$;
2. for $i = 1, \dots, s$, $B_i(x_0, x_0)$ if and only if $B_i(x_1, x_1)$;
3. for $i = 1, \dots, s$ and for $x \neq x_1$, $B_i(x_0, x)$ if and only if $B_i(x_1, x)$, and $B_i(x, x_0)$ if and only if $B_i(x, x_1)$;
4. for $i = 1, \dots, s$, $B_i(x_0, x_1)$ if and only if $B_i(x_1, x_2)$, and $B_i(x_1, x_0)$ if and only if $B_i(x_2, x_1)$.

Using an easy game argument, one proves that \mathcal{M} and \mathcal{N} are 2-equivalent.

Thus, if a given 2-equivalence class of σ_2 -structures has a representative of size $n > n_0$, then it has a representative of size $n + 1$, which means that Ash's function $N_{\sigma_2,2}$ is eventually nondecreasing. Remember that for all $n \in \mathbb{N}^+$, we have $N_{\sigma_2,2}(n) \leq M_{\sigma_2,2}$, and conclude that $N_{\sigma_2,2}$, being a nondecreasing and bounded function from \mathbb{N}^+ to \mathbb{N}^+ , is eventually constant. \square

This proof is similar to Ash's proof for unary signatures and does not extend to $k = 3$, even for the very restricted vocabulary $\text{BIN} = \{=, B\}$, where B is a binary relation symbol, because the construction of a 3-equivalent structure with exactly one more element is not always possible.

The above result extends to non-binary signatures, because any structure is 2-equivalent to an essentially binary structure.

Corollary 4.3 *For any finite relational signature σ , Ash's function $N_{\sigma,2}$ is eventually constant.*

Proof. Assume that σ consists of the unary relation symbols U_1, \dots, U_t and the relation symbols R_1, \dots, R_s with respective arities $r_1, \dots, r_s \geq 2$. Let n_1 be the number of 1-equivalence classes of elements in a σ -structure. The argument is similar to the proof of Proposition 4.2: for a given σ -structure \mathcal{M} with $n > n_1$ elements, the construction of a 2-equivalent structure with exactly $n + 1$ elements is possible. Indeed, for the additional element x_0 , we fix similar conditions to those of Proposition 4.2 concerning the tuples with x_0 and at most one other element. We also impose, for instance, that no tuple with at least three distinct elements and containing x_0 belongs to any relation R_1, \dots, R_s (this condition does not interfere with 2-equivalence). \square

4.2 Padding and difficult cases of the ultra-weak Ash conjecture

In this subsection, we prove that unary signatures or quantifier depth 2 are essentially the only "easy" cases of Ash conjectures, because any non trivial enlargement leads to a case that implies the spectrum conjecture.

The results we present here are based on the following observation. Assume that there exist a set \mathcal{G} of one-to-one functions $g : \mathbb{N}^+ \rightarrow \mathbb{N}^+$ and a set $\mathcal{E} \subset \text{SPEC}$ such that

1. for all $S \in \text{SPEC}$, there exists $g \in \mathcal{G}$ such that $g(S) = \{g(n) \mid n \in S\} \in \mathcal{E}$;
2. for all $S \in \mathcal{E}$, the set $\mathbb{N}^+ \setminus S \in \text{SPEC}$;
3. for all $g \in \mathcal{G}$ and for all $S \in \text{SPEC}$, the set $g^{-1}(S) = \{n \mid g(n) \in S\} \in \text{SPEC}$.

Let $S \in \text{SPEC}$, then for some $g \in \mathcal{G}$,

$$\begin{aligned} \mathbb{N}^+ \setminus S &= \{n \mid n \notin S\} \\ &= \{n \mid g(n) \notin g(S)\} && \text{(because } g \text{ is one-to-one)} \\ &= \{n \mid g(n) \in \mathbb{N}^+ \setminus g(S)\} \\ &= g^{-1}(\mathbb{N}^+ \setminus g(S)). \end{aligned}$$

Hence

$$\begin{aligned} S \in \text{SPEC} &\stackrel{1}{\Rightarrow} g(S) \in \mathcal{E} \stackrel{2}{\Rightarrow} \mathbb{N}^+ \setminus g(S) \in \text{SPEC} \stackrel{3}{\Rightarrow} g^{-1}(\mathbb{N}^+ \setminus g(S)) \in \text{SPEC} \\ &\Rightarrow \mathbb{N}^+ \setminus S \in \text{SPEC}, \end{aligned}$$

i. e. the spectrum conjecture holds.

In the literature, several so-called ‘padding results’ exist that exhibit couples $(\mathcal{G}, \mathcal{E})$ satisfying condition 1. above. Usually, condition 3. is also satisfied, because the functions in \mathcal{G} are polynomials, and NE is closed under inverse images of polynomials. Also, in many cases, \mathcal{E} is the set of all spectra defined by a σ -sentence of quantifier depth k , where σ ranges in Σ and k in K . Hence, using Theorem 3.1, condition 2. is equivalent to

‘for all $(\sigma, k) \in \Sigma \times K$, and for all $i \in \mathbb{N}^+$, the set $N_{\sigma, k}^{-1}(i)$ is a spectrum’.

We present below two applications of this observation. The first one restricts the range of the signatures σ , whereas the second one restricts the range of the quantifier depths k .

Let $\text{BIN} = \{=, B\}$, where B is a binary relation symbol. Fagin [13] shows that, up to a polynomial padding, every spectrum is the spectrum of a BIN-sentence.

Theorem 4.4 *For every first-order sentence φ , there exist an integer $l \geq 1$ and a BIN-sentence ψ such that $\text{Sp}(\psi) = \{n^l \mid n \in \text{Sp}(\varphi)\}$.*

Note that the quantifier depths of the BIN-sentences obtained in the proof of this result are unbounded. However, conditions 1. and 3. of the observation above are still fulfilled, with $\mathcal{E} = \{\text{Sp}(\varphi) \mid \varphi \text{ is a BIN-sentence}\}$ and $\mathcal{G} = \{n \mapsto n^l \mid l \geq 1\}$.

Corollary 4.5 *If for all $k \geq 1$ and for all $i \in \mathbb{N}^+$, the set $N_{\text{BIN}, k}^{-1}(i)$ is a spectrum, then the spectrum conjecture holds.*

It can also be proved that, up to a polynomial padding, every spectrum is the spectrum of a quantifier depth 3 sentence over a binary signature. This result is a suggestion of Étienne Grandjean.

Proposition 4.6 *For every first-order sentence φ , there exist an integer $l \geq 1$ and a binary sentence ψ of quantifier depth 3 such that $\text{Sp}(\psi) = \{m^l \mid m \in \text{Sp}(\varphi)\}$.*

Proof. Jones and Selman’s result means that for each sentence φ there exists l such that

$$\text{Sp}(\varphi) \in \text{NTIME}(2^{l \cdot n}),$$

where n is the length of the binary representation of the input integer m . A classical padding argument implies that $\{m^l \mid m \in \text{Sp}(\varphi)\} \in \text{NTIME}(2^n)$. Now Grandjean proves in [17] that $\text{NTIME}(2^n)$ is the set of spectra of prenex universal sentences with one quantifier over a signature consisting of 1-ary functions. Thus, there exists some sentence θ of the above form such that $\{m^l \mid m \in \text{Sp}(\varphi)\} = \text{Sp}(\theta)$.

Finally, without loss of generality, assume that any atomic sub-formula of θ is $f(g(x)) = h(x)$ or $f(g(x)) = x$ (up to an increasing of the number of unary functions in the signature of θ in order to unfold the nested terms). Let ψ be the sentence with quantifier depth 3 over a binary (relational) signature obtained as the conjunction of the following sentences:

1. for every function f in the signature of θ , the sentence

$$\forall x \exists y \forall z (R_f(x, z) \rightarrow z = y),$$

expressing the fact that f is a function;

2. the sentence θ' obtained from θ by replacing each atomic sub-formula of the form $f(g(x)) = h(x)$ by

$$\exists y \exists z (R_g(x, y) \wedge R_f(y, z) \wedge R_h(x, z))$$

and each atomic sub-formula of the form $f(g(x)) = x$ by

$$\exists y (R_g(x, y) \wedge R_f(y, x)).$$

Clearly we have $\text{Sp}(\theta) = \text{Sp}(\psi)$. □

Note that Grandjean's result [17] can be improved to the use of two unary functions, by a result of [6]. However, the unfolding of nested functional terms used in this proof still introduces an unbounded number of new unary functions, and hence an unbounded number of binary relations in the final signature. Once again, the conditions of the observation above hold.

Corollary 4.7 *If for every binary signature σ_2 and for all $i \in \mathbb{N}^+$, the set $N_{\sigma_2,3}^{-1}(i)$ is a spectrum, then the spectrum conjecture holds.*

Finally, let us examine some possible improvements of the results of the present section.

Concerning easy cases, the extensions of Proposition 4.1 to binary signatures, even restricted to one binary relation, or of Corollary 4.3 to quantifier depth 3, even with a signature restricted to be binary, are clearly prevented by Corollaries 4.5 and 4.7. Thus, essentially, it remains to investigate the asymptotic behavior of $N_{\text{BIN},3}$. We have not been able to handle this case by hand.

On the other hand, concerning difficult cases, any significant improvement of Corollaries 4.5 or 4.7 using the same type of proof with a padding argument would lead to restricting both σ and k to range in finite sets, say respectively Σ and K (e. g. $\Sigma = \{\text{BIN}\}$ and $K = \{3\}$). Since the signatures are relational, in such a case the total number of non-equivalent σ -sentences of quantifier depth $\leq k$ for $\sigma \in \Sigma$ and $k \in K$ is finite, and so is the set \mathcal{E} of their spectra.

Let \mathcal{G} be a set of padding functions. If there is some $g \in \mathcal{G}$ which is used for padding an infinite subset S of SPEC, since \mathcal{E} is finite, at least two spectra in S are mapped to the same spectrum in \mathcal{E} . But, since g is one-to-one, $S \neq S'$ implies $g(S) \neq g(S')$, a contradiction. Thus, every function in \mathcal{G} is used for padding only a finite subset of SPEC.

As far as we know, no such padding result exists, so that presently our results seem the best possible.

5 The Ash functions for a theory

5.1 Definition

In order to make further progress in solving particular cases of Ash conjectures, we introduce a new type of restriction, concerning the semantics of the signatures. More precisely, let σ be a finite relational signature, and let \mathcal{T} be a σ -theory, i. e. a (finite or infinite) set of σ -sentences. We denote $\mathcal{T}_k = \{\varphi \in \mathcal{T} \mid \varphi \text{ has quantifier depth } \leq k\}$ for all $k \geq 1$. In order to exclude pathological cases, we require our theories \mathcal{T} to be consistent, i. e. to have some (finite or infinite) model. Under this assumption, for all $k \geq 1$, the sub-theory \mathcal{T}_k is also consistent.

Definition 5.1 *For any positive integer k , the Ash function for the consistent theory \mathcal{T} , denoted by $N_{\mathcal{T},k}$, counts the number ($\leq M_{\sigma,k}$) of non- k -equivalent models of \mathcal{T}_k of size n for all $n \geq 1$.*

For all $i \in \mathbb{N}$, we denote $N_{\mathcal{T},k}^{-1}(i) = \{n \in \mathbb{N}^+ \mid N_{\mathcal{T},k}(n) = i\}$, and we have $\mathbb{N}^+ = \dot{\bigcup}_{i=0}^{M_{\sigma,k}} N_{\mathcal{T},k}^{-1}(i)$.

Let $\text{qd}(\mathcal{T}) = \max\{d \mid \text{some sentence in } \mathcal{T} \text{ has quantifier depth } d\} \in \mathbb{N}^+ \cup \{\infty\}$ be the quantifier depth of \mathcal{T} . Remark that if the quantifier depth of the sentences in \mathcal{T} is bounded (e. g. if \mathcal{T} is finite), say $\text{qd}(\mathcal{T}) = k_0$, then for all $k \geq k_0$, we have $\mathcal{T}_k = \mathcal{T}$. In such a case, the Ash function $N_{\mathcal{T},k}$ counts the number of non- k -equivalent models of \mathcal{T} of size n .

Let \mathcal{B} be the set of the axioms of Boolean algebras. The maximal quantifier depth of these sentences is 3. It is well-known that any finite Boolean algebra has size 2^α for some $\alpha \geq 1$, and that all the Boolean algebras of the same size are isomorphic. Thus, we have $N_{\mathcal{B},3}^{-1}(1) = \{2^\alpha \mid \alpha \geq 2\}$, $N_{\mathcal{B},3}^{-1}(0) = \mathbb{N} \setminus \{2^\alpha \mid \alpha \geq 2\}$ and $N_{\mathcal{B},3}^{-1}(i) = \emptyset$ for $i \notin \{0, 1\}$. From this example it follows that we cannot expect Ash's constant or periodic conjectures to hold for theories, whereas the ultra-weak Ash conjecture for theories makes sense. However, it may happen that for a given theory the Ash functions are eventually constant or periodic, see Section 6.

5.2 A wide variety of Ash's functions

Now a natural question arises: Which functions can be Ash's function for some theory? We propose the following sufficient condition.

Proposition 5.2 *Let $f : \mathbb{N}^+ \rightarrow \mathbb{N}$ be a function bounded by some constant M_f and computable in E. Then there exist a signature σ , a σ -sentence φ and a quantifier depth K such that $f = N_{\varphi,K}$.*

Proof. For all $i \in \mathbb{N}$, let $f^{-1}(i) = \{n \in \mathbb{N}^+ \mid f(n) = i\}$. Note that for all $i > M_f$, we have $f^{-1}(i) = \emptyset$, and that $\mathbb{N}^+ = \bigcup_{i=0}^{M_f} f^{-1}(i)$. Moreover, for all $i \leq M_f$, the set $f^{-1}(i)$ lies in the complexity class E.

Now the key point of the proof is a result of Fagin in [12] showing that any set in E is the spectrum of some categorical sentence, i. e. a sentence with at most one model for each finite size, up to isomorphism. In addition, looking at Fagin's proof, one observes that the models of the considered sentences are ordered structures, i. e. we can assume without loss of generality that their signatures contain a linear ordering.

Applying this result to our sets $f^{-1}(i)$, we obtain that for all $i \leq M_f$, there exist a signature σ_i (containing a common linear ordering symbol $<$) and a categorical σ_i -sentence θ_i of quantifier depth k_i such that $f^{-1}(i) = \text{Sp}(\theta_i)$.

Let U be a new unary relation, and for all $j \in \mathbb{N}^+$, let $\text{Card}(U, j)$ be the $\{U, <\}$ -sentence of quantifier depth $j + 1$ expressing the fact that the j smallest elements of the universe and only them belong to U .

Let $K = \max(\{k_i \mid i \leq M_f\} \cup \{M_f + 1\})$ and $\varphi = \bigvee_{h=1}^{M_f} (\theta_h \wedge \bigvee_{j=1}^h \text{Card}(U, j))$. Now we show that $N_{\varphi, K} = f$. Let $n \in \mathbb{N}^+$ and suppose that $f(n) = i$. Hence we have to verify that $N_{\varphi, K}(n) = i$. Since φ has quantifier depth K , remember that $N_{\varphi, K}(n)$ is the number of non k -equivalent models of φ of size n . Since $f(n) = i$, we have $n \in f^{-1}(i) = \text{Sp}(\theta_i)$, and for all $i' \neq i$ it follows that $n \notin \text{Sp}(\theta_{i'})$. If $i = 0$, then we have $n \notin \bigcup_{h=1}^{M_f} \text{Sp}(\theta_h)$, hence $n \notin \text{Sp}(\varphi)$, i. e. $N_{\varphi, K}(n) = 0$. Else, \mathcal{M} is a model of φ of size n if and only if it is a model of $\theta_i \wedge \bigvee_{j=1}^i \text{Card}(U, j)$ and of no other disjunct. Since θ_i is categorical, it has exactly one model of size n . Now if $i \neq 0$, the unary predicate U can be interpreted exactly in i different ways in order to obtain i non- k -equivalent models of $\theta_i \wedge \bigvee_{j=1}^i \text{Card}(U, j)$, hence of φ . Thus, $N_{\varphi, K}(n) = i$. \square

Note that the theory φ is ad hoc and that we do neither control its signature nor its quantifier depth.

5.3 Connection to the spectrum conjecture

Now let us turn to the ultra-weak Ash conjecture for theories.

Conjecture 5 (The ultra-weak Ash conjecture for theories) *For any finite relational signature σ , for any consistent σ -theory \mathcal{T} , for any positive integer k and for all $i \in \mathbb{N}$, the set $N_{\mathcal{T}, k}^{-1}(i)$ is a spectrum.*

We are interested in somehow expressive theories \mathcal{T} , in particular, we consider as natural to require that for any positive integer h , the sub-theory \mathcal{T}_h has at least one model of size n for any positive integer n (i. e. $N_{\mathcal{T}, h}^{-1}(0) = \emptyset$). We say that *the theory \mathcal{T} has a full spectrum*, which is obviously much stronger than its being consistent. Under such an assumption, we obtain a result similar to Theorem 3.1.

Theorem 5.3 *Let σ be a finite relational signature, let \mathcal{T} be a σ -theory with a full spectrum and let k be a positive integer. For all $i \in \mathbb{N}^+$, the set $N_{\mathcal{T}, k}^{-1}(i)$ is a spectrum if and only if for every σ -sentence φ of quantifier depth $\leq k$ which implies \mathcal{T}_k (i. e. every model of φ is also a model of every sentence in \mathcal{T}_k), the set $\mathbb{N}^+ \setminus \text{Sp}(\varphi)$ is a spectrum.*

Proof. It is very similar to the proof of Theorem 3.1. The only modification is that we demand the k -equivalence classes to satisfy \mathcal{T}_k . For $j \in \{1, \dots, M_{\sigma, k}\}$, let

$$\theta_j^{\mathcal{T}, k} = \bigvee \{ \bigwedge_{\psi \in \Theta} \psi' \mid \Theta \subseteq \Psi, |\Theta| = j, \Theta \models_f \neg \varphi \wedge \mathcal{T}_k \}.$$

Then we have $\mathbb{N}^+ \setminus \text{Sp}(\varphi) = \bigcup_{j=1}^{M_{\sigma, k}} (\text{Sp}(\theta_j^{\mathcal{T}, \varphi}) \cap N_{\mathcal{T}, k}^{-1}(i))$, which in turn is a spectrum.

Conversely, we use an always false sentence φ_0 and show that $N_{\mathcal{T}, k}^{-1}(i) = \text{Sp}(\theta_j^{\mathcal{T}, \varphi_0}) \cap (\mathbb{N}^+ \setminus \text{Sp}(\theta_{j+1}^{\mathcal{T}, \varphi_0}))$ and that $\mathbb{N}^+ \setminus \text{Sp}(\theta_{j+1}^{\mathcal{T}, \varphi_0})$ is a spectrum, so that $N_{\mathcal{T}, k}^{-1}(i)$ is a spectrum. \square

In some particular cases, we obtain more information about complements of spectra. As in the case of Theorem 3.1, if, for given σ , \mathcal{T} and k , Ash's function $N_{\mathcal{T}, k}$ is eventually constant, then for any σ -sentence φ of quantifier depth k which implies \mathcal{T}_k , we can deduce from the proof of Theorem 5.3 that $\mathbb{N}^+ \setminus \text{Sp}(\varphi) = \text{Sp}(\psi)$, where ψ is a sentence of quantifier depth k over a signature τ of the same arities as σ . But in addition, we also know that τ is subject to the same semantical restrictions as σ . For instance, if \mathcal{T} expresses that all binary relations in σ are functional (which can be done using quantifier depth 3 sentences), and if $k \geq 3$, then all binary relations in τ are functional, too.

Notice that if $N_{\mathcal{T},k}^{-1}(0) \neq \emptyset$, i. e. if \mathcal{T} has not a full spectrum, the statement of Theorem 5.3 has to be modified. Indeed, it makes sense to consider $\text{Sp}(\varphi)$ as a subset of $\mathbb{N}^+ \setminus N_{\mathcal{T},k}^{-1}(0)$ rather than \mathbb{N}^+ and to take

$$(\mathbb{N}^+ \setminus N_{\mathcal{T},k}^{-1}(0)) \setminus \text{Sp}(\varphi)$$

as its complement. Up to this restriction, a similar result can be proved.

Let us turn to particular cases of our conjecture for theories. Once again, we assume that our σ -theory \mathcal{T} has a full spectrum. We present below some theories for which the study of Ash's functions is as difficult as the general case. More precisely, let us consider the following theories with quantifier depth 3:

1. over the signature $\text{BIN} = \{B, =\}$, the theory

$$\mathcal{T}_g = \text{“the binary relation } B \text{ is symmetric and irreflexive”};$$

2. over the signature $\{B_1, B_2, =\}$, the theories

$$\mathcal{T}_{2\equiv} = \text{“the binary relations } B_1 \text{ and } B_2 \text{ are equivalence relations”} \quad \text{and}$$

$$\mathcal{T}_{2f} = \text{“the binary relations } B_1 \text{ and } B_2 \text{ are functional relations”}.$$

Proposition 5.4 *Let $\mathcal{T} \in \{\mathcal{T}_g, \mathcal{T}_{2\equiv}, \mathcal{T}_{2f}\}$. If for every positive integer k and for all $i \in \mathbb{N}^+$, the set $N_{\mathcal{T},k}^{-1}(i)$ is a spectrum, then the spectrum conjecture holds.*

The proof of this result is similar to the proofs in Subsection 4.2. The padding results we use are presented below.

Theorem 4.4, due to Fagin [13], is more precisely

Theorem 5.5 *For every first-order sentence φ , there exist an integer $l \geq 1$ and a BIN-sentence ψ which implies \mathcal{T}_g such that $\text{Sp}(\psi) = \{n^l \mid n \in \text{Sp}(\varphi)\}$.*

The following result is proved by Durand, Fagin and Loescher in [6].

Theorem 5.6 *For every first-order sentence φ , there exist two integers $l, d \geq 1$ and a $\{B_1, B_2, =\}$ -sentence ψ which implies \mathcal{T}_{2f} such that $\text{Sp}(\psi) = \{d \cdot n^l \mid n \in \text{Sp}(\varphi)\}$.*

The last result is proved in [4]. Notice that a similar result can also be found in [10].

Theorem 5.7 *For every BIN-sentence φ , there exists a $\{B_1, B_2, =\}$ -sentence ψ which implies $\mathcal{T}_{2\equiv}$ such that $\text{Sp}(\psi) = \{2 \cdot n^2 \mid n \in \text{Sp}(\varphi)\}$.*

6 Conclusion and open problems

Having Proposition 5.4 in mind, it is natural to consider sub-theories of the difficult theories it points out. More precisely, let us consider the following theories of quantifier depth 3 over the signature BIN :

$$\mathcal{T}_b = \text{“the binary relation } B \text{ is bijective”},$$

$$\mathcal{T}_f = \text{“the binary relation } B \text{ is functional”},$$

$$\mathcal{T}_{\equiv} = \text{“the binary relation } B \text{ is an equivalence relation”}.$$

In all these cases, we have been able to determine the asymptotic behavior of Ash's functions. For the proofs of these results, we refer the reader to [4] and [5].

Theorem 6.1 *For all $k \geq 3$, the Ash functions $N_{\mathcal{T}_b,k}$, $N_{\mathcal{T}_f,k}$, and $N_{\mathcal{T}_{\equiv},k}$ are eventually periodic.*

If B is a bijective relation, the above result can be made more precise. As far as we know, it is the first non-trivial negative result concerning Ash's functions.

Theorem 6.2 *For all $k \geq 3$, the Ash functions $N_{\mathcal{T}_b,k}$ are not eventually constant.*

Note that, in all the cases under consideration, the corresponding spectra are known to be unions of sets of the form $\{an + b \mid n \in \mathbb{N}\}$ (see [6]), hence their complements have the same form. Consequently, the corollary of Theorem 6.1 about complements of spectra of these theories is not a new result.

Concerning further work, a wide range of problems concerning Ash's functions is open. For instance, it would be interesting to investigate the asymptotic behavior of Ash's functions for a natural theory which is not finitely axiomatizable in first-order logic (e. g. “the binary relation B is a finite tree”).

From a broader point of view, it can be noticed that every easy case pointed out in this paper corresponds to decidable logics (unary signatures, quantifier depth 2 [21], one function, one bijection, one equivalence relation), whereas difficult cases correspond to undecidable logics (binary signatures, quantifier depth 3 [16], two functions, two bijections, two equivalence relations). Is there a formal connection between undecidability and difficulty of Ash's question?

Acknowledgements The authors are very grateful to Étienne Grandjean for drawing their attention to Ash's paper [2] and for his active interest during the preparation of this paper. They also thank Ronald Fagin for his interest and his advice concerning the possible extensions of this work. Finally, they must thank an anonymous referee who suggested a simplification of the proof of Theorem 3.1 and stated Proposition 3.2.

References

- [1] M. Ajta and M. Ben-Or, A theorem on probabilistic constant depth computations. Proceedings 16th ACM STOC, pp. 471 – 474, 1984.
- [2] C. J. Ash, A conjecture concerning the spectrum of a sentence. *Math. Logic Quarterly* **40**, 393 – 397 (1994).
- [3] G. Asser, Das Repräsentantenproblem im Prädikatenkalkül der ersten Stufe mit Identität. *Z. Math. Logik Grundlagen Mathematik* **1**, 252 – 263 (1955).
- [4] A. Chateau, Utilisation des destinées pour la décision et sa complexité dans le cas de formules à profondeur de quantification bornée sur des structures logiques finies et infinies. Ph. D. thesis, Université d'Auvergne, 2003.
- [5] A. Chateau and M. More, Characterization of Ehrenfeucht-Fraïssé equivalence in two classes of finite graphs and application to Ash's counting functions. Technical report, LLAIC, Université d'Auvergne, 2005.
- [6] A. Durand, R. Fagin, and B. Loescher, Spectra with only unary function symbols. In: *Lecture Notes in Computer Science* 1414, pp. 189 – 202 (Springer, London 1998).
- [7] L. Denenberg, Y. Gurevich, and S. Shelah, Definability by constant-depth polynomial-size circuits. *Information and Control* **70**, 216 – 240 (1986).
- [8] H.-D. Ebbinghaus and J. Flum, *Finite Model Theory* (Springer, Berlin 1999).
- [9] A. Ehrenfeucht, An application of games to the completeness problem for formalized theories. *Fundamenta Mathematicae* **49**, 129 – 141 (1961).
- [10] Y. Ershov, I. Lavrov, A. Taimanov, and M. Taitslin, Elementary theories. *Russian Math. Surveys* **20**, 35 – 105 (1965).
- [11] H. B. Enderton, *A Mathematical Introduction to Logic* (Academic Press, New York 1972).
- [12] R. Fagin, Generalized first-order spectra and polynomial-time recognizable sets. In: *Complexity of Computation* (R. Karp, ed.), SIAM-AMS Proceedings 7, pp. 43 – 73, 1974.
- [13] R. Fagin, A spectrum hierarchy. *Z. Math. Logik Grundlagen Mathematik* **21**, 123 – 134 (1975).
- [14] R. Fagin, M. Klawe, N. Pippenger, and L. Stockmeyer, Bounded-depth, polynomial-size circuits for symmetric functions. *Theoretical Computer Science* **36**, 239 – 250 (1985).
- [15] R. Fraïssé, Sur quelques classifications des systèmes de relations. *Publ. Sci. Univ. Alger, Sér. A*, **1**, 35 – 182 (1954).
- [16] W. D. Goldfarb, The unsolvability of the Gödel class with identity. *J. Symbolic Logic* **49**, 1237 – 1252 (1984).
- [17] E. Grandjean, First-order spectra with one variable. *J. Computer and System Sciences* **40** (2), 136 – 153 (1990).
- [18] W. Hodges, *Model Theory*. *Encyclopedia of Mathematics and its Applications* 42 (Cambridge University Press, Cambridge 1993).
- [19] N. Immerman, *Descriptive Complexity* (Springer, New York 1999).
- [20] N. D. Jones and A. L. Selman, Turing machines and the spectra of first-order formulas. *J. Symbolic Logic* **39**, 139 – 150 (1974).
- [21] M. Mortimer, On languages with two variables. *Z. Math. Logik Grundlagen Mathematik* **21**, 135 – 140 (1975).
- [22] C. H. Papadimitriou, *Computational Complexity* (Addison-Wesley, Reading 1994).
- [23] H. Scholz, Ein ungelöstes Problem in der symbolischen Logik. *J. Symbolic Logic* **17**, 160 (1952).
- [24] S. Toda, On the computational power of pp and $\oplus p$. In: *IEEE Symposium on Foundations of Computer Science*, pp. 514 – 519, 1989.
- [25] J. Torán, Complexity classes defined by counting quantifiers. *J. Association Computing Machinery* **38**, 753 – 774 (1991).
- [26] L. Valiant, The complexity of enumeration and reliability problems. *SIAM Journal of Computing* **8** (3), 410 – 421 (1979).
- [27] K. W. Wagner, The complexity of combinatorial problems with succinct input representation. *Acta Informatica* **23**, 325 – 356 (1986).