Forcing with random variables in bounded arithmetic and proof complexity

Jan Krajíček

Academy of Sciences and Charles University, Prague

Abstract

We develop a new construction of models of bounded arithmetic. The models are Boolean-valued and are based on random variables. We apply them to independence results and witnessing theorems in bounded arithmetic. We also study possible applications to lower bounds in propositional proof complexity.

This is a draft of Part 1 of long lecture notes to be available during '08.

Acknowledgements

I thank to S. A. Cook (Toronto), E. Jeřábek (Prague), P. Pudlák (Prague), N. Thapen (Prague) and S. Todorcevic (Paris/Toronto) for discussions of related topics and for comments on the draft of (parts) of the notes.

I lectured about parts of this paper at seminars in Oxford in May and November '04, in the IAS in Princeton in February'05, in the Isaac Newton Institute in Cambridge in April'06, and at the meeting Computability in Europe in Swansea in July'06. I also gave a semester long exposition of parts of the paper at the Charles University in Prague in Fall'04. I thank participants of all these events for a number of comments.

Support acknowledgments:

I started to work on the present paper while I was a member of the Institute for Advanced Study in Princeton in Spring'04, supported by the NSF grant DMS-0111298. Parts of this work were done while visiting the Mathematical Institute in Oxford supported by the EPSRC grant GR/S16997/01, the Institute for Advanced Study in Princeton supported by the NSF grant DMS-0111298, and the Isaac Newton Institute in Cambridge (program Logic and Algorithms) supported by an EPSRC grant N09176. Also partially supported by various Czech grant agencies: grants A1019401 and AV0Z10190503 (AS CR), by MSM0021620839, and by grant LC505 (Eduard Čech Center).

Contents

Introduction

Proof complexity studies the time complexity of non-deterministic algorithms. The main problem is the $\mathcal{NP}$ *versus co*$\mathcal{NP}$ problem, a question whether the computational complexity class $\mathcal{NP}$ is closed under the complementation. Central objects studied are propositional proof systems (non-deterministic algorithms for accepting the set of propositional tautologies). Time lower bounds correspond then to lengths-of-proofs lower bounds.

Bounded arithmetic is a generic name for a collection of first-order theories of arithmetic linked to propositional proof systems (and to a variety of other computational complexity topics). The qualification *bounded* refers to the fact that the induction axiom is typically restricted to a subclass of bounded formulas.

The links between propositional proof systems and bounded arithmetic theories have many facets but informally one can view them as two sides of the same thing: The former is a non-uniform version of the latter. In particular, it is known that proving lengths-of-proofs lower bounds for propositional proof systems is very much related to proving independence results in bounded arithmetic. In fact, proving such lower bounds is *equivalent* to constructing non-elementary extensions of particular models of bounded arithmetic. This offers a very clean and coherent framework for thinking about lengths-of-proofs lower bounds, a one that has been quite successful in the past (let us mention just Ajtai's [2] lower bound for the pigeonhole principle in constant-depth Frege systems).

In this paper we introduce a new method for constructing (extensions of) bounded arithmetic models, and hence for proving independence results and lengths-of-proofs lower bounds. Its brief description could be *forcing with random variables* but it has actually also features of non-standard analysis and of definable ultraproducts. The novelty lies neither in using forcing in bounded arithmetic or proof complexity (see Remark on the literature below) nor in forcing with random variables (that is well-established in set theory, cf.[56, 26]), but rather in finding a way how to do this meaningfully in arithmetic, and further in using families of random variables samplable by algorithms restricted in a particular way (different from one application to another) rather than using the family of all random variables with a given sample space and range.

The models are built from random variables defined on a sample space Ω which is a non-standard finite set (often parameterized by a subset of $\{0,1\}^n$ with non-standard n), and samplable by functions of some restricted complexity. This is considered inside an $\aleph_1$-saturated non-standard model of true arithmetic. One could equivalently work with sequences of bigger and bigger sample spaces and random variables defined on them, and consider their limit behavior using a suitable ultrafilter on $\mathbf{N}$, simulating indirectly the ultraproduct construction. However, the use of a non-standard model from the beginning simplifies things considerably. This is analogous to the situation in non-standard analysis: While proofs using infinitesimals (or other features of non-standard analysis) can be translated into the $\epsilon - \delta$ formalization, the intuition or clarity of the original argument may be lost in the translation.

Random variables define distributions and determine probabilities of events. In particular, two random variables may be neither equal nor non-equal; rather they may be equal with some probability. However, there is a fundamental problem: Probabilities cannot be used as truth-values should classical logic be preserved. The (almost) right choice for the truth-value is the subset of the sample space consisting of those samples for which the two random variables are equal. At the heart of our construction is the realization that we can employ a bit of non-standard analysis (namely Loeb's measure [45]) at this point: If one identifies two such truth-values (subsets of the sample space) if their symmetric difference has an infinitesimal measure one gets a *complete* Boolean algebra - this is the single most important feature of our method. Evaluation of first-order formulas in complete Boolean algebras is very natural and faithful (as it is well-known from Boole [6] for propositional logic and from Rasiowa-Sikorski [51] for predicate logic).

The models we get are not classical but are Boolean-valued[1]. But that is

---

[1]One can get classical models by applying a bit of logic: First apply Löwenheim-Skolem theorem to the whole situation (i.e. not only the model but also the Boolean algebra and the truth valuation) to replace it by a countable one, and then apply the Rasiowa-Sikorski theorem [52] to collapse the Boolean algebra to the two-element Boolean algebra while preserving joins and meets used for defining the truth values, and hence collapsing the

perfectly sufficient for the purpose of independence results (and lengths-of-proofs lower bounds): In order to demonstrate that a sentence is not provable from a set of axioms it is enough to show that its truth value in some model is smaller than the truth value of any finite conjunction of the axioms.

Although some of the models appear interesting in their own right we interpret the construction as

- **a method that reduces an independence result or a lengths-of-proofs lower bound to a combinatorial/complexity-theoretic statement about random variables**.

The statement we refer to here expresses that the truth-value of a particular sentence (in a particular model) is some particular value, typically $1_{\mathcal{B}}$ or $0_{\mathcal{B}}$. The validity of such a statement is a property of the particular family of random variables forming the model. For the families we consider it can be often formulated as a statement that an algorithm of a certain type can (or cannot) perform some computational task successfully for a high fraction of inputs.

Remark on the literature. A form of forcing has been applied in bounded arithmetic earlier. Paris-Wilkie [48] and later Ajtai [2, 3, 4] and Riis [55] used simple variant of Robinson's model-theoretic forcing (although combined with an involved combinatorial reduction in [2, 3, 4]). Then Wilkie[2] described a construction of Boolean valued models of theory S^1_2 and reproved using it a relation - known previously from Cook [16] and Buss [7] - between S^1_2 and Extended Frege proof system. This has been further extended by Krajíček [29, 31, 34, 30] to a wider context. With a slight simplification one can describe the Boolean algebras involved in these constructions as Lindenbaum algebras based not on provable equivalence of formulas (or circuits) as they are defined classically but based on *feasibly provable* (i.e. with somehow bounded length) equivalence. This works well in the sense that any valid lower bound can be proved, in principle, by such a forcing. But on the other hand the algebras are defined using the notion of a feasible proof about which we are supposed to say something by the construction in the first place, and so it is in a sense a vicious circle. Takeuti and Yasumoto [60, 61, 59] changed the feasibly provable equivalence to simply "true equivalence" - breaking this

model to a classical one.

[2]Unpublished lecture at the *Int. Congress on Logic, Methodology and Philosophy of Science* in Moscow, 1987.

vicious circle - but it apparently did not help much as we know very little about the power of Boolean circuits of feasible size. Most importantly the algebras used in all these constructions were not complete but were closed only under some definable unions. That makes it very hard to use them.

Background. This is a research in bounded arithmetic and proof complexity and we expect that the reader is familiar with established basic definitions, facts, methods and aims of the field. A relevant background can be found in Krajíček [30] but some reader may find useful shorter explanations of some basic points in [27, 31, 35, 36]. We also always briefly review the relevant theories and propositional proof systems before they are studied. Recently Cook and Nguyen [17] offered an exposition of basic theories and their relations to proof systems.

Despite the natural character and simplicity of Boolean-valued models they were discovered only in late 1960s by Vopěnka and by Scott-Solovay as their version of Cohen's forcing; paper by Scott [56] is a beautiful exposition of the basic ideas aimed at non-logicians, best to this date (it also contains detailed bibliographical/historical comments[3]). Paper [56] as well as virtually all later expositions (e.g. in [62, 26]) consider only Boolean-valued models of set theory. Mansfield [47] attempts a general theory but concentrates on model-theoretic properties of the class of such models as oppose to properties of particular models and gives a version that yields only elementary extensions and hence is unsuitable for independence results.

[3]Takeuti reports in [60] that Gödel recognized in Boolean-valued models a model-theoretic version of a reinterpretation of logical operations he developed earlier but never used for independence results as it was too complicated.

Part I

Basics

Chapter 1

The definition of the models

1.1 The ambient model of arithmetic

Let L_{all} be the language containing symbols for every relation and function on the natural numbers $\mathbf{N}$; each symbol from L_{all} has a canonical attached interpretation in $\mathbf{N}$. Let $\mathcal{M}$ be an $\aleph_1$-saturated model of the true arithmetic in the language L_{all}. Such a model exists by general model-theoretic constructions, cf. [23]. Definable sets mean definable with parameters, unless specified otherwise.

The $\aleph_1$-saturation implies the following:

- If a_k, $k \in \mathbf{N}$, is a countable family of elements of $\mathcal{M}$ then there exists a non-standard $t \in \mathcal{M}$ and a definable sequence $(b_i)_{i<t} \in \mathcal{M}$ such that $b_k = a_k$ for all $k \in \mathbf{N}$.

  We shall often denote the non-standard sequence simply $(a_i)_{i<t}$.

For example, if all elements $\{a_k\}_{k\in\mathbf{N}}$ obey some definable property P then - by induction in $\mathcal{M}$ - also some b_s with a non-standard index $s \leq t$ will obey P. Such element b_s will serve well as "a limit" of the sequence $\{a_k\}_{k\in\mathbf{N}}$.

Another property implied by the $\aleph_1$-saturation (and equal to it if we used a countable language) is the following:

- If A_k, $k \in \mathbf{N}$, is a countable family of definable subsets of $\mathcal{M}$ such that $\bigcap_{i<k} A_i \neq \emptyset$ for all $k \geq 1$, then $\bigcap_k A_k \neq \emptyset$.

  However, the intersection $\bigcap_k A_k$ need not to be definable.

The ambient model $\mathcal{M}$ will suffice for our purposes everywhere in this paper. However, in general we could take for $\mathcal{M}$ an $\aleph_1$-saturated elementary extension of $\mathbf{N}$ in a many sorted language having names not only for all elements of $\mathbf{N}$ and relations and functions on $\mathbf{N}$ as L_{all} has, but also names for all families of sets, families of families of sets, etc., for the whole so called *superstructure* (this is commonly done in non-standard analysis and this terminology is used there). In such a rich model the properties above would hold also for sequences of sets, families, etc..

1.2 The Boolean algebras

Let $\Omega \in \mathcal{M}$ be an arbitrary infinite set. It will be called a *sample space*. As it is an element of $\mathcal{M}$, it is $\mathcal{M}$-finite. Let $N = |\Omega|$ be the size of Ω in the sense of $\mathcal{M}$.

Let $\mathcal{A} := \{A \in \mathcal{M} \mid A \subseteq \Omega\}$. This is a Boolean algebra but not a σ-algebra as the class of definable sets is not closed under all countable unions (for example, while it contains all singletons it does not contain the countable set of those elements of Ω having only standardly many predecessors in Ω). The counting measure (i.e. the uniform probability) on $\mathcal{A}$ is defined by:

$$A \in \mathcal{A} \rightarrow \ |A|/N \ .$$

Its values are in the $\mathcal{M}$-rationals.

Define an ideal $\mathcal{I} \subseteq \mathcal{A}$ by:

$$A \in \mathcal{I} \ \text{ iff } \ |A|/N \ \text{ is infinitesimal} \ .$$

I is not definable in $\mathcal{M}$ (otherwise the set of natuarl numbers $\mathbf{N}$ would be definable, violating the induction in $\mathcal{M}$). Using $\mathcal{I}$ define Boolean algebra $\mathcal{B} := \mathcal{A}/\mathcal{I}$.

The induced measure on $\mathcal{B}$ (the Loeb's measure) will be denoted μ. Hence $\mu(b)$ for $b \in \mathcal{B}$ is the standard part of $|B|/N$ for any $B \in \mathcal{A}$ such that $B/\mathcal{I} = b$. It is a measure in the ordinary sense: The values of μ lie in the standard reals $\mathbf{R}$. It is σ-additive and a strict measure: $\mu(b) > 0$ if $b \neq 0_{\mathcal{B}}$.

The following lemma is a combination of two well-known facts, one from non-standard analysis and one from measure theory.

Lemma 1.2.1 *$\mathcal{B}$ is a complete Boolean algebra.*

Proof :

First, as in the construction of Loeb's measure [45], we use the $\aleph_1$-saturation to show that

Claim 1: *$\mathcal{B}$ is a σ-algebra and the measure μ is σ-additive.*

To establish the claim let $\{b_k\}_{k\in\mathbf{N}}$ be a countable subset of $\mathcal{B}$. Assume $b_k = B_k/\mathcal{I}$ for B_k's from $\mathcal{A}$. We may assume, without a loss of generality, that $B_0 \subseteq B_1 \subseteq \ldots$. It is enough to find $C \in \mathcal{A}$ such that $B_k \subseteq C$ for all $k \in \mathbf{N}$ and $\mu(C) = \lim_{k\to\infty} \mu(B_k)$. It holds that for any $k \geq 1$ there is $n_k \geq 1$ such that for all $m > \ell \geq n_k$

$$\frac{|B_\ell|}{N} \leq \frac{|B_m|}{N} \leq \frac{|B_\ell|}{N} + \frac{1}{k} \ .$$

We may assume, by taking subsequence $\{B_{n_k}\}_{k\in\mathbf{N}}$, that $n_k = k$.

Take a non-standard extension $\{B_i\}_{i<t}$ of $\{B_k\}_{k\in\mathbf{N}}$ guaranteed to exists by the $\aleph_1$-saturation (each B_k is an element of $\mathcal{M}$). Consider the following property P parameterized by s:

$$B_s \in \mathcal{A} \ \wedge \ \forall i \leq s; B_i \subseteq B_s \wedge \frac{|B_i|}{N} \leq \frac{|B_s|}{N} \leq \frac{|B_i|}{N} + \frac{1}{i} \ .$$

Property P is obeyed by all standard s and hence, by induction in $\mathcal{M}$, also by some non-standard $s_0 < t$.

It is easy to verify that $C := B_{s_0}$ has the required properties.

Claim 2: *$\mathcal{B}$ satisfies the ccc condition: Any antichain is at most countable.*

This holds because the measure is strictly positive, i.e. $\mu(b) > 0$ for $b \neq O_{\mathcal{B}}$: Any antichain can contain only finitely many (non-zero) elements with measure in each interval $(1/(n+1), 1/n]$, $n \geq 1$.

As a consequence we get

Claim 3: *Any family of elements of $\mathcal{B}$ has the same set of upper bounds as one of its countable subfamilies.*

To see this note that a family has the same set of upper bounds as the ideal it generates which in turn has the same set of upper bounds as any maximal antichain it contains - such antichains are countable by ccc (Claim 2), and each element of the antichain is majorized by a union of a finite number of elements of the family).

We can conclude the proof that $\mathcal{B}$ is complete: The union of any family can be defined as the union of a countable subfamily (Claim 3), and any countable family has a union by the σ-additivity (Claim 1).

q.e.d.

We conclude this subsection by pointing out two facts that are generally *not true* in $\mathcal{B}$. The first observation is that the quotient operation $\dots/\mathcal{I}$ that defines $\mathcal{B}$ from $\mathcal{A}$ does not commute with infinite unions: It is not true that it would generally hold that $(\bigcup_i A_i)/\mathcal{I} = \bigvee_i (A_i/\mathcal{I})$. In fact, the left-hand side may not be defined (i.e. in $\mathcal{A}$), and even when it is the equality may not hold (e.g. if A_i' run over all singleton subsets of Ω then the left-hand side is $\Omega/\mathcal{I} = 1_{\mathcal{B}}$ while the right-hand is $\bigvee_i 0_{\mathcal{B}} = 0_{\mathcal{B}}$).

The second failure is well-know: Infinite distributive law

$$\bigwedge_{i \in I} \bigvee_{j \in J} b_{ij} = \bigvee_f \bigwedge_{i \in I} b_{i,f(i)} \ ,$$

where f range over all functions from I to J, may not hold (the left-hand side always majorizes the right-hand side though). However, it holds when I is finite.

Furthermore, for measure algebras (and hence for $\mathcal{B}$, see Section 2) *weak* distributive law

$$\bigwedge_{i \in I} \bigvee_{j \in J} b_{ij} = \bigvee_g \bigwedge_{i \in I} \bigvee_{j \in g(i)} b_{i,j} \ ,$$

holds, where g is a map assigning to elements of I finite subsets of J.

See [62, 26] for details.

1.3 The models $K(F)$

Let Ω, $\mathcal{A}$, $\mathcal{I}$ and $\mathcal{B}$ be as in the previous section.

Let $L \subseteq L_{all}$ and let F be a non-empty set of functions such that:

1. $F \subseteq \mathcal{M}$.
2. The domain of any function $\alpha \in F$ is Ω (hence $\alpha : \Omega \to M$).
3. F is closed under L-functions and contains all L-constants.

Any such F will be called an L**-closed family** of random variables. Note, in particular, that F itself need not to be $\mathcal{M}$-definable; in fact, it almost never will be in our applications.

Definition 1.3.1 *Assume that F is an L-closed family of random variables.*

$K(F)$ is a Boolean-valued L-structure with universe F. The L-functions are interpreted by composition: $f(\alpha) := f \circ \alpha$, any L-function f.

The Boolean valuation of L-sentences with parameters from $K(F)$ has values in $\mathcal{B}$ and is given by the following inductive conditions:

- $[\![\alpha = \beta]\!] := \{\omega \in \Omega \mid \alpha(\omega) = \beta(\omega)\}/\mathcal{I}$.
- $[\![R(\alpha_1, \ldots, \alpha_k)]\!] := \{\omega \in \Omega \mid R(\alpha_1(\omega), \ldots, \alpha_k(\omega))\}/\mathcal{I}$, *any L-relation R.*
- $[\![\ldots]\!]$ *commutes with* $\neg, \vee, \wedge$.
- $[\![\exists x A(x)]\!] := \bigvee_{\alpha \in F} [\![A(\alpha]\!]$.
- $[\![\forall x A(x)]\!] := \bigwedge_{\alpha \in F} [\![A(\alpha]\!]$.

Note that the values of $[\![\exists x A(x)]\!]$ and $[\![\forall x A(x)]\!]$ are well-defined as $\mathcal{B}$ is complete by Lemma 1.2.1. The notation $K(F)$ is sound as Ω is determined by F and $\mathcal{A}$, I and $\mathcal{B}$ are determined by Ω.

1.4 Valid sentences

We say that a sentence A is **valid** in $K(F)$ iff its Boolean value is $1_{\mathcal{B}}$. It is straightforward to verify that all axioms of first order predicate calculus in any particular formalization, including axioms of equality, are valid in any $K(F)$, and that the value $1_{\mathcal{B}}$ is preserved by inference rules. Further, an implication is valid iff the truth value of the succedent majorizes the truth value of the antecedent. Hence we have the following.

Lemma 1.4.1 *Let T be a set of L-sentences and A an L-sentence (parameters from $K(F)$ are allowed). If A is provable from T in predicate calculus with equality then*

$$\bigwedge_{B \in T_0} [\![B]\!] \leq [\![A]\!]$$

for some finite $T_0 \subseteq T$.

In particular, if A is logically valid then $[\![A]\!] = 1_{\mathcal{B}}$ (as $\bigwedge \emptyset = 1_{\mathcal{B}}$), i.e. A is valid in $K(F)$.

Although we are primarily interested in models of bounded arithmetic theories and functions in the families F will typically have a small computational complexity, note that $K(F)$ can be a model of a very strong theory. For example, taking for F all function (in $\mathcal{M}$) with domain Ω yields a model where $Th(\mathbf{N})$ is valid.

For Γ a prefix class of formulas and $L \subseteq L_{all}$ let $Th_\Gamma(L)$ denote the set of true Γ-sentences valid in the canonical L-structure on $\mathbf{N}$. The following lemma is obvious.

Lemma 1.4.2 *Let F be an L-closed family. Then $Th_\forall(L)$ is $K(F)$-valid. If F contains (constant functions) $\mathbf{N}$ then $Th_{\exists\forall}(L)$ is $K(F)$-valid.*

This seems to block a priori constructions of non-Π^b_1-elementary extensions which are needed for lengths-of-proofs lower bounds. However, there is a simple way out: A statement that can be expressed by a Π^b_1-formula or even an atomic formula in one language need not to be so expressible in another language. For example, if we have a function symbol for an algorithm checking that a truth assignment satisfies a set of clauses then such a statement is expressible by an atomic formula. But without such a symbol we may need a Π^b_2-formula to express it (every clauses contains a satisfied literal).

Lemma 1.4.2 will be also used in Section 4 in a crucial way to foster a link between the truth in $\mathbf{N}$ and the validity in $K(F)$.

1.5 Possible generalizations

We could have started the construction of $\mathcal{B}$ from any probability space $(\Omega, \mathcal{A}, \nu)$ that is definable in $\mathcal{M}$. In particular, both sets Ω and $\mathcal{A}$ have to be definable in $\mathcal{M}$ (the definability of the whole $\mathcal{A}$ - the definability of each element of $\mathcal{A}$ is not enough - is needed for Loeb's construction) and ν must be a definable finitely additive measure on $\mathcal{A}$ (with values in $\mathcal{M}$-rationals). One also needs to add a condition on α's from F: Each $\alpha^{(-1)}(a)$ for $a \in \mathcal{M}$ has to be measurable, i.e. in $\mathcal{A}$.

An example of this more general space is a probability space on an $\mathcal{M}$-finite Ω with a non-uniform distribution. An example of a space with an $\mathcal{M}$-infinite Ω is $\Omega := \{w \in \mathcal{M} \mid |w| \geq n\}$, $\mathcal{A}$ consisting of all $\mathcal{M}$-finite Boolean combinations of r.e. subsets of Ω (defined using a code for the

Boolean combination and a universal Σ^0_1-formula) and measure ν giving to a string w the weight $2^{n-1-2|w|}$.

However, we have no application for these more general constructions here and we restrict to the counting measure on $\mathcal{M}$-finite Ω.

Two random variables α, β on $\{0,1\}^n$ are "almost equal" (i.e. the formula $\alpha = \beta$ is $K(F)$-valid) if they differ for an infinitesimal fraction of samples $\omega \in \{0,1\}^n$. In complexity theory however, a stronger condition would be used: The random variables should differ in a negligible fraction, i.e. less than n^{-k}, any $k \in \mathbf{N}$. Whenever necessary (not in this paper though) this can be remedied analogously to complexity theory: Build the model from the same random variables but computed on a tuple of independent samples.

More precisely, let F be an L-closed family on Ω, and let $t \geq 1$, $t \in \mathcal{M}$, be arbitrary. For $\alpha \in F$ define $\alpha^{(t)} : \Omega^t \to M^t$ by:

$$\alpha^{(t)}(\omega_1, \ldots, \omega_t) := (\alpha(\omega_1), \ldots, \alpha(\omega_t)) \ .$$

Denote by $F^{(t)}$ the collection of all $\alpha^{(t)}$; it is also an L-closed family.

Interpret an L-relation R on elements $a^i = (a^i_1, \ldots, a^i_t) \in \mathcal{M}^t$, $i \leq k$, as

$$R(a^1, \ldots, a^k) := \bigwedge_{j \leq t} R(a^1_j, \ldots, a^k_j) \ ,$$

i.e. we assign the Boolean-value by the equation:

$$[\![R((\alpha^1)^{(t)}, \ldots, (\alpha^k)^{(t)})]\!] := \{(\omega_1, \ldots, \omega_t) \in \Omega^t \mid \bigwedge_{j \leq t} R(\alpha^1(\omega_j), \ldots, \alpha^k(\omega_j))\}/\mathcal{I} \ .$$

Let $\mathcal{A}^t$ be the t-product of $\mathcal{A}$, a probability space on Ω^t, and let $\mathcal{B}^{(t)}$ be the complete Boolean algebra resulting from the construction in Subsection 1.2. (It is not the t-product of $\mathcal{B}$; in fact, $\mathcal{B}^t$ is not even defined when t is non-standard.) The $F^{(t)}$-formulas are evaluated in $\mathcal{B}^{(t)}$.

Then for $\alpha^{(t)} = \beta^{(t)}$ to be valid in $K(F^{(t)})$ it is not sufficient that $p := Prob_{\omega \in \Omega}[\alpha(\omega) \neq \beta(\omega)]$ is infinitesimal: It must be that $p \cdot t$ is infinitesimal.

Chapter 2

Measure on $\mathcal{B}$

Boolean algebra $\mathcal{B}$ carries a strict probabilistic measure μ. We shall interpret it in this section as a metric and also link it with probability.

2.1 A metric on $\mathcal{B}$

The map

$$A \longrightarrow \mu([\![A]\!])$$

assigns real numbers to L-sentences, and satisfies

- $0 \leq \mu([\![A]\!]) \leq 1$,
- $\mu([\![\neg A]\!]) = 1 - \mu([\![A]\!])$
- $\mu([\![A \vee B]\!]) + \mu([\![A \wedge B]\!]) = \mu([\![A]\!]) + \mu([\![B]\!])$

and with suitable F (see Section 3) also

- $\mu([\![\exists x A(x)]\!]) = \sup_{\alpha \in F} \mu([\![A(\alpha)]\!])$ and $\mu([\![\forall x A(x)]\!]) = \inf_{\alpha \in F} \mu([\![A(\alpha)]\!]))$.

Further it satisfies the all-important inequality

- $\mu([\![A]\!]) \leq \mu([\![B]\!])$ if A logically implies B.

However, the number $\mu([\![A]\!])$ cannot be interpreted as the probability of A. The passage from the Boolean-value to probability is more subtle (Subsection

2.2). The right interpretation of this number seems to be in terms of a metric on $\mathcal{B}$. Define for $a, b \in \mathcal{B}$:

$$d(a,b) := \mu(a \triangle b)$$

where $a \triangle b$ is the symmetric difference $(a \wedge \neg b) \vee (\neg a \wedge b)$.

The following lemma is verified by looking at the Venn diagram.

Lemma 2.1.1 *Function d is a metric on $\mathcal{B}$. Further, the following equality and two inequalities hold for any $a, a', b, b' \in \mathcal{B}$:*

1. $d(a,b) = d(\neg a, \neg b)$.
2. $d(a \wedge b, a' \wedge b') \leq d(a,a') + d(b,b')$.
3. $d(a \vee b, a' \vee b') \leq d(a,a') + d(b,b')$.

2.2 From Boolean value to probability

In this subsection we investigate a relation between the probability of a sentence in $\mathcal{M}$ and the μ-measure of its Boolean value in $K(F)$.

The following lemma follows from Definition 1.3.1 and from the fact that the quotient operation $A \in \mathcal{A} \to A/\mathcal{I} \in \mathcal{B}$ commutes with $\neg, \vee, \wedge$ (binary).

Lemma 2.2.1 *Let F be an L-closed family, $A(x)$ an open L-formula, and $\alpha \in F$.*

Then for all standard $\epsilon > 0$:

$$\Pr_{\omega \in \Omega}[A(\alpha(\omega))] \geq \mu([\![A(\alpha)]\!]) - \epsilon \ .$$

(The probability expression is defined in $\mathcal{M}$.)

In order to be able to apply Lemma 3.3.3 we need some extension of Lemma 2.2.1 to universal formulas. However, in general it is not true that $\Pr_{\omega \in \Omega}[\forall z A(\alpha(\omega), z)]$ can be bounded from below by a term in $\mu([\![\forall z A(\alpha, z)]\!])$. For example, it can be that $\forall x \exists! z \neg A(x,z)$ but that no $\gamma \in F$ finds such z for more than a negligible fraction of x's. Then $[\![\forall z A(\mathrm{id}_\Omega, z)]\!] = 1_{\mathcal{B}}$ while $\Pr_{\omega \in \Omega}[\forall z A(\omega, z)] = 0$.

The way out is to choose suitable families F. Call any function ξ satisfying:

$$\forall x \ [\exists z \neg A(x,z) \to \neg A(x, \xi(x))]$$

a counter-example function for $\forall z A(x,z)$.

Lemma 2.2.2 *Assume that $A(x,z)$ is an open L-formula, ξ is a counter-example function for $\forall z A(x,z)$, and F is an L-closed family closed under ξ.*

Then for any $\alpha \in F$ and any $\epsilon > 0$:

$$\Pr_{\omega \in \Omega}[\forall z A(\alpha(\omega), z)] \;\geq\; \mu([\![\forall z A(\alpha, z)]\!]) - \epsilon \ .$$

Proof :

Let $[\![\forall z A(\alpha, z)]\!] = b$. For all $\gamma \in F$ we have $[\![A(\alpha,\gamma)]\!] \geq b$, so

$$\Pr_{\omega \in \Omega}[A(\alpha(\omega), \gamma(\omega))] \;\geq\; \mu(b) - \epsilon \ ,$$

any $\epsilon > 0$ by Lemma 2.2.1.

For a particular $\gamma(\omega) := \xi(\alpha(\omega))$ we also have

$$(\forall z A(\alpha(\omega), z)) \equiv A(\alpha(\omega), \gamma(\omega)) \ ,$$

so:

$$\Pr_{\omega \in \Omega}[\forall z A(\alpha(\omega), z)] \;=\; \Pr_{\omega \in \Omega}[A(\alpha(\omega), \gamma(\omega))]$$

and the lemma follows.

q.e.d.

Chapter 3

Witnessing quantifiers

Consider an L-sentence A of the form

$$\exists x_1 \forall y_1 \dots \exists x_k \forall y_k B(x_1, y_1, \dots, x_k, y_k)$$

with B open. Let K be an L-structure. Two players, $\exists$-player and $\forall$-player, pick sequentially witnesses $\alpha_1, \beta_1, \dots, \alpha_k, \beta_k \in F$ to the quantifiers. The $\exists$-player wants to make the truth value $[\![B(\alpha_1, \beta_1, \dots, \alpha_k, \beta_k)]\!]$ as large as possible by selecting $\alpha_1, \dots, \alpha_k$ suitably, while the $\forall$-player's objective is the opposite, to make it as small as possible by picking $\beta_1, \dots, \beta_k$ well.

If K were a classical structure (i.e. $\mathcal{B}$ were the 2-element algebra) the situation would be simple: If A is true then the $\exists$-player has a strategy to achieve value $1_{\mathcal{B}}$, and if A is false the $\forall$-player has a strategy to reach value $0_{\mathcal{B}}$. However, if K is a Boolean-valued structure there may not be optimal moves $\alpha_1, \beta_1, \dots$ that would ensure that

$$[\![B(\alpha_1, \beta_1, \dots, \alpha_k, \beta_k)]\!] = [\![\exists x_1 \forall y_1 \dots \exists x_k \forall y_k B(x_1, y_1, \dots, x_k, y_k)]\!]$$

and, in general, the players need to collaborate to get as close (in terms of the metric on $\mathcal{B}$) to

$$[\![\exists x_1 \forall y_1 \dots \exists x_k \forall y_k B(x_1, y_1, \dots, x_k, y_k)]\!]$$

as possible.

In this Section we will study under which conditions posed on F we can guarantee the existence of suitable moves (called often "witnesses") $\alpha_1, \beta_1, \dots, \alpha_k, \beta_k$. Let us mention two reasons why we are interested in it.

Consider a sentence A of the form $\forall x \exists y B(x, y)$, B open. Assume that $\mathrm{id}_\Omega \in F$, where $\Omega = \{0,1\}^n$. If $[\![A]\!] = b$ then $[\![\exists y B(\mathrm{id}_\Omega, y)]\!] \geq b$. Assume that we can witness y by some $\alpha \in F$ such that:

$$[\![\exists y B(\mathrm{id}_\Omega, y)]\!] = [\![B(\mathrm{id}_\Omega, \alpha)]\!]$$

By Lemma 2.2.1 then:

$$Prob_{\omega \in \Omega}[B(\omega, \alpha(\omega)] \geq \mu(b) - \epsilon \ ,$$

for all standard $\epsilon > 0$. Hence we have reduced the question of approximating $[\![A]\!]$ (in $\mathcal{B}$ as a metric space) to a question about the witnessing power of F-functions in the ambient model $\mathcal{M}$, and consequently also in $\mathbf{N}$.

For the second example assume that we can find witnesses $\alpha_1, \ldots, \beta_k$ to quantifiers in $A(\gamma) := \exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k, \gamma)$ such that

$$[\![B(\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k, \gamma)]\!] = [\![\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k, \gamma)]\!]$$

(B is again open and has a parameter $\gamma \in F$). The left-hand side value can be computed explicitly:

$$\{\omega \mid B(\alpha_1(\omega), \beta_1(\omega), \ldots, \alpha_k(\omega), \beta_k(\omega), \gamma(\omega))\}/\mathcal{I} \ .$$

So in this case we are able to represent the truth value of an arbitrarily complex formula by a set defined by an open formula. Such computation of the truth values of a complex formula by the truth value of a simpler one is, in principle, possible because the value $[\![A(\gamma)]\!]$ has, in general, nothing to do with

$$\{\omega \mid \exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k, \gamma(\omega))\}/\mathcal{I} \ .$$

When we shall quantify in statements over $\epsilon > 0$ it is tacitly meant over *standard* ϵ's.

3.1 Propositional approximation of truth values

Let A be a sentence (possibly with parameters) of the form $\exists x B(x)$; B needs not to be open here. The first statement we used already in the proof of Lemma 1.2.1 and we state it here for completeness. It is a consequence of the ccc property of $\mathcal{B}$ (the second part is a consequence of the σ-additivity of μ).

Lemma 3.1.1 *There are countably many $\alpha_k \in F$, $k \in \mathbf{N}$, such that*

$$[\![\exists x B(x)]\!] = \bigvee_{k \in \mathbf{N}} [\![B(\alpha_k)]\!] \ .$$

In particular, for any $\epsilon > 0$ there are finitely many $\alpha_1, \ldots, \alpha_\ell \in F$ such that

$$d([\![\exists x B(x)]\!], \bigvee_{k \le \ell} [\![B(\alpha_k)]\!]) < \epsilon \ .$$

Iterating Lemma 3.1.1 yields the following statement.

Lemma 3.1.2 *Let A be an L-sentence of the form*

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k)$$

with B open (parameters are allowed). Let $\epsilon > 0$ be arbitrary.

Then there are $\ell \in \mathbf{N}$ and elements of F:

$$\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \alpha_2^{i_1,j_1,i_2}, \ldots, \beta_k^{i_1,\ldots,j_k}$$

with $i_1, \ldots, j_k < \ell$, such that the distance between $[\![A]\!]$ and

$$\bigvee_{i_1} \bigwedge_{j_1} \cdots \bigvee_{i_k} \bigwedge_{j_k} [\![B(\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \ldots, \beta_k^{i_1,\ldots,j_k})]\!]$$

is less than ϵ.

In particular, the distance between $[\![A]\!]$ and

$$\{\omega \in \Omega \mid \bigvee_{i_1} \bigwedge_{j_1} \ldots \bigvee_{i_k} \bigwedge_{j_k} B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega))\}/\mathcal{I}$$

is less than ϵ.

Proof :

Fix small enough $\delta > 0$ (how small we be clear at the end of the proof), a standard rational. Denote:

$$C(x_1) := \forall y_1 \exists x_2 \forall y_2 \ldots B(x_1, y_1, \ldots) \ .$$

By Lemma 3.1.1 there are $\alpha_1^0, \ldots, \alpha_1^{u-1} \in F$, $u \in \mathbf{N}$, such that

$$d([\![A]\!], \bigvee_{i<u} [\![C(\alpha_1^i)]\!]) \ \le \ \delta \ .$$

Next denote for $i < u$:

$$D_i(y_1) := \exists x_2 \forall y_2 \ldots B(\alpha_1^i, y_1, x_2, y_2, \ldots) \ .$$

By Lemma 3.1.1 again there are $\beta_1^{i,j} \in F$, $j < v$ some standard v, such that:

$$d([\![C(\alpha_1^i)]\!], \bigwedge_{j<v} [\![D_i(\beta_1^{i,j})]\!]) \ \leq \ \delta/u$$

for all $i < u$. By Lemma 2.1.1 then:

$$d([\![A]\!], \bigvee_{i<u} \bigwedge_{j<v} [\![\exists x_2 \forall y_2 \ldots B(\alpha_1^i, \beta_1^{i,j}, x_2, y_2, \ldots)]\!]) \ \leq \ 2\delta \ .$$

Proceeding analogously for $\exists x_2, \forall y_2, \ldots$ we find in F elements

$$\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \alpha_2^{i_1,j_1,i_2}, \ldots, \beta_k^{i_1,\ldots,j_k}$$

with all $i_1, \ldots, j_k$ ranging over some standard finite domain such that the distance of $[\![A]\!]$ from

$$\bigvee_{i_1} \bigwedge_{j_1} \ldots [\![B(\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \ldots, \beta_k^{i_1,\ldots,j_k})]\!]$$

is at most $2k\delta$. However, this truth value equals, modulo the ideal I, to the set of all $\omega \in \Omega$ satisfying (as evaluated in $\mathcal{M}$) the Boolean formula formed from formulas $B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega))$:

$$\bigvee_{i_1} \bigwedge_{j_1} \ldots B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega)) \ .$$

By picking $\delta > 0$ less than $\epsilon/2k$ we get the lemma.

q.e.d.

3.2 Witnessing in definable families

Our next lemma gives a sample statement and a proof whose variants will be used repeatedly. The construction shows that the $\aleph_1$-saturation can be used in a place where in set theory we could have used a straightforward induction on $k \in \mathbf{N}$.[1]

[1] Paradoxically there is "no arithmetic in arithmetic", meaning that in arithmetic we do not have the set of natural numbers: PA is equivalent to ZFC with the Axiom of Infinity replaced by its negation. This blocks a transplantation of Cohen's forcing to arithmetic.

Lemma 3.2.1 *Assume that F is definable in $\mathcal{M}$. Let $b_k := B_k/\mathcal{I}$ for some $B_k \in \mathcal{A}$ and $\alpha_k \in F$, for all $k \in \mathbf{N}$. Assume that $b_k \wedge b_\ell = 0_\mathcal{B}$ for all $k \neq \ell \in \mathbf{N}$ (i.e. b_ks form an antichain).*

Further assume that for all $k \in \mathbf{N}$ there is $\beta \in F$ such that for all $\ell = 1, \ldots, k$:

$$(1) \qquad \beta(\omega) = \alpha_\ell(\omega) \ \ \textit{for} \ \ \omega \in B_\ell \setminus \bigcup_{i<\ell} B_i \ .$$

Then there exists $\beta \in F$ such that for all $k \in \mathbf{N}$:

$$(2) \qquad [\![\beta = \alpha_k]\!] \ \geq b_k \ .$$

Proof :

Let $S = \{(B_i, \alpha_i)\}_{i<t}$ be a non-standard extension of $\{(B_k, \alpha_k)\}_{k\in\mathbf{N}}$ provided by the $\aleph_1$-saturation. Using S, and the fact that F is definable, we can define for all $k \in \mathbf{N}$ the set C_k of all $\beta \in F$ satisfying condition (1).

Clearly $C_0 \supseteq C_1 \supseteq \ldots$ and each $C_k \neq \emptyset$ (by the hypothesis of the lemma). Hence, again by the $\aleph_1$-saturation, $\bigcap_{k\in\mathbf{N}} C_k \neq \emptyset$, and any β from the intersection satisfies condition (2).

q.e.d.

We derive a simple corollary about witnessing of quantifiers for particular families F. First a definition.

Definition 3.2.2 *Family F is* **closed under definitions by cases** *if for any $\alpha_0, \alpha_1 \in F$ and any $B \in \mathcal{A}$ there is $\beta \in F$ such that:*

$$\beta(\omega) = \begin{cases} \alpha_0(\omega) & \textit{if } \omega \in B \\ \alpha_1(\omega) & \textit{otherwise.} \end{cases}$$

Clearly the hypothesis (1) of Lemma 3.2.1 is satisfied for families closed under definitions by cases.

Lemma 3.2.3 *Assume that F is definable in $\mathcal{M}$ and that it is closed under definitions by cases.*

Then for each sentence $\exists x C(x)$ there is an $\alpha \in F$ such that

$$[\![\exists x C(x)]\!] = [\![C(\alpha)]\!]$$

(C needs not to be open).

In fact, for each sentence A of the form

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k)$$

(B arbitrary, possibly with parameters), there are $\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k \in F$ such that:

$$\begin{aligned} & [\![A]\!] \ = \\ & [\![\forall y_1 \exists x_2 \forall y_2 \ldots \exists x_k \forall y_k B(\alpha_1, y_1, \ldots, x_k, y_k)]\!] \ = \\ & [\![\exists x_2 \forall y_2 \ldots \exists x_k \forall y_k B(\alpha_1, \beta_1, \ldots, x_k, y_k)]\!] \ = \\ & \ldots \\ & [\![\forall y_k B(\alpha_1, \beta_1, \ldots, \alpha_k, y_k)]\!] \ = \\ & [\![B(\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k)]\!] \ . \end{aligned}$$

Proof :

The second part of the lemma is proved by induction on the number of quantifiers in A using the first part.

By Lemma 3.1.1 there are α_k, $k \in \mathbf{N}$, such that $[\![\exists x C(x)]\!] = \bigvee_{k \in \mathbf{N}} [\![C(\alpha_k)]\!]$. Define $b_0 := [\![C(\alpha_0)]\!]$ and for $k > 0$ put:

$$b_k \ := \ [\![C(\alpha_k)]\!] \setminus \bigvee_{\ell < k} b_\ell \ .$$

By induction one can verify that for all k:

$$\bigvee_{i \leq k} [\![C(\alpha_i)]\!] = \bigvee_{i \leq k} b_i$$

and, in particular,

$$\bigvee_{\alpha \in F} [\![C(\alpha)]\!] = \bigvee_{k} b_k \ .$$

Clearly any two different b_k's are incompatible. By Lemma 3.2.1 there is $\beta \in F$ such that

$$[\![\beta = \alpha_k]\!] \geq b_k \ , \quad \text{for all } k \in \mathbf{N} \ .$$

But then clearly

$$[\![C(\beta)]\!] \leq [\![\exists x C(x)]\!] = \bigvee_{\alpha \in F} [\![C(\alpha)]\!] = \bigvee_{k \in \mathbf{N}} b_k \leq [\![C(\beta)]\!] \ .$$

The last inequality uses $b_k \leq [\![C(\alpha_k)]\!] \wedge [\![\beta = \alpha_k]\!]$ and hence $b_k \leq [\![C(\beta)]\!]$, for all $k \in \mathbf{N}$.

q.e.d.

Note that having witnesses $\alpha_1, \ldots, \beta_k$ such that

$$[\![A]\!] = [\![B(\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k)]\!]$$

does not, in general, imply that the witnesses also obey the remaining equations stated in the lemma.

The problem with the witnessing statement 3.2.3 is that families F we encounter never meet the two requirements:

1. F is closed under definition by cases.

2. F is definable.

An example of F to keep in mind is a family F_{PV} consisting of polynomial time functions (i.e. p-time samplable random variables on $\{0,1\}^n$). F_{PV} satisfies neither of the two conditions.

We shall see in the next two subsections that it is possible to relax the conditions so that Lemma 3.2.3 still holds but interesting families will satisfy the new conditions.

3.3 Definition by cases by open formulas

Definition 3.3.1 *We shall say that F is* **closed under definitions by cases by open L-formulas** *iff whenever $\alpha, \beta \in F$ and $B(x)$ is an open L-formula with free variable x then there is $\gamma \in F$ such that:*

$$\gamma(\omega) = \begin{cases} \alpha(\omega) & \textit{if } B(\alpha(\omega)) \textit{ holds} \\ \beta(\omega) & \textit{otherwise.} \end{cases}$$

Note that the example family F_{PV} of polynomial time functions is closed under definitions by cases by open L-formulas, as long as all relations and functions in L are computable by polynomial time algorithms.

Lemma 3.3.2 *Let F be an L-closed family closed under definition by cases by open $L(F)$-formulas. Let $B(x)$ be an open L-formula (possibly with parameters).*

Then for every $\epsilon > 0$ there is $\alpha \in F$ such that

$$d([\![\exists x B(x)]\!], [\![B(\alpha)]\!]) < \epsilon \ .$$

In particular, if $\exists x B(x)$ is $K(F)$-valid then for every $\epsilon > 0$ there is $\alpha \in F$ such that

$$\mu([\![B(\alpha)]\!]) > 1 - \epsilon \ .$$

Proof :

For any two $\beta_1, \beta_2 \in F$ there is (by the hypothesis that F is closed under definitions by cases by open L-formulas) $\beta_3 \in F$ such that $\beta_3(\omega) = \beta_1(\omega)$ if $B(\beta_1(\omega))$ holds, and $\beta_3(\omega) = \beta_2(\omega)$ otherwise. Then it follows rather easily from the definition of β_3 that:

$$[\![B(\beta_3)]\!] = [\![B(\beta_1)]\!] \vee [\![B(\beta_2)]\!] \ .$$

Combining this with Lemma 3.1.1 we get a countable sequence $\beta_0, \beta_1, \ldots \in F$ such that

$$[\![B(\beta_0)]\!] \leq [\![B(\beta_1)]\!] \leq \ldots$$

and such that $\lim_{k\to\infty} \mu([\![B(\beta_k)]\!]) = \mu([\![\exists x B(x)]\!])$. The lemma follows.

q.e.d.

Now we extend Lemma 3.3.2 to more complex formulas.

Lemma 3.3.3 *Let F be an L-closed family closed under definition by cases by open $L(F)$-formulas (L-formulas with parameters from F).*

Let $\exists x C(x)$ be an L-sentence, C an arbitrary formula with parameters. Then for any $\epsilon > 0$ there is an $\alpha \in F$ such that

$$d([\![\exists x C(x)]\!], [\![C(\alpha)]\!]) < \epsilon \ .$$

In particular, if $\exists x C(x)$ is $K(F)$-valid then

$$\mu(C(\alpha)) > 1 - \epsilon \ .$$

In fact, for each sentence A of the form

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k)$$

(B open, possibly with parameters), there are $\alpha_1, \beta_1, \dots, \alpha_k, \beta_k \in F$ *such that:*

$$d([\![A]\!], [\![\forall y_1 \exists x_2 \forall y_2 \dots \exists x_k \forall y_k B(\alpha_1, y_1, \dots, x_k, y_k)]\!]) < \epsilon$$

$$d([\![\forall y_1 \dots \forall y_k B(\alpha_1, y_1, \dots, y_k)]\!], [\![\exists x_2 \dots \forall y_k B(\alpha_1, \beta_1, x_2, \dots, y_k)]\!]) < \epsilon$$

$$\dots$$

$$d([\![\forall y_k B(\alpha_1, \beta_1, \dots, \alpha_k, y_k)]\!], [\![B(\alpha_1, \beta_1, \dots, \alpha_k, \beta_k)]\!]) < \epsilon \ .$$

Proof :

The lemma appears similar to Lemma 3.2.3 where the second part followed from the first part. However, here it is the other way around; we need to prove the second part while the first one is a special case of it.

We shall describe the construction for $k = 1$, i.e. for A of the form

$$\exists x \forall y B(x, y) \ ,$$

B open. This will display the key idea; the general case $k \geq 1$ is proved analogously by induction on the quantifier complexity of the formula.

The following claim follows from Lemma 3.3.2: Apply it to $\exists y \neg B(\alpha, y)$ (here we use the hypothesis that F is closed under definitions by cases by open $L(F)$-formulas).

Claim 1: *For any* $\alpha \in F$ *and* $\delta > 0$ *there is* $\beta \in F$ *such that*

$$d([\![\forall y B(\alpha, y)]\!], [\![B(\alpha, \beta)]\!]) < \delta \ .$$

The next claim is a bit subtler.

Claim 2: *For any* $\alpha_1, \alpha_2 \in F$ *and* $\xi > 0$ *there is* $\alpha_3 \in F$ *such that*

$$d([\![\forall y B(\alpha_3, y)]\!], [\![\forall y B(\alpha_1, y)]\!] \vee [\![\forall y B(\alpha_2, y)]\!]) < \xi \ .$$

To prove the claim we first apply Claim 1 to α_1, α_2 and $\delta > 0$ (to be specified later) to get $\beta_1, \beta_2 \in F$ such that

$$(1) \qquad d([\![B(\alpha_i, \beta_i)]\!], [\![\forall y B(\alpha_i, y)]\!] < \delta \quad \text{, for } i = 1, 2.$$

Define pair α_3, β_3:

$$\alpha_3(\omega), \beta_3(\omega) = \begin{cases} \alpha_1(\omega), \beta_1(\omega) & \text{if } B(\alpha_1(\omega), \beta_1(\omega)) \text{ holds} \\ \alpha_2(\omega), \beta_2(\omega) & \text{otherwise.} \end{cases}$$

Clearly $[\![B(\alpha_3,\beta_3)]\!] = [\![B(\alpha_1,\beta_1)]\!] \vee [\![B(\alpha_2,\beta_2)]\!]$. Observe that:

$$(2) \qquad d([\![\forall y B(\alpha_3,y)]\!],[\![B(\alpha_3,\beta_3)]\!]) < 3\delta \ .$$

This is because otherwise we could find (via Claim 1) $\gamma \in F$ such that

$$d([\![\forall y B(\alpha_3,y)]\!],[\![B(\alpha_3,\gamma)]\!]) < \delta$$

and use it to modify β_i, $i = 1$ or $i = 2$, to decrease the measure of $[\![B(\alpha_i,\beta_i)]\!]$ by more than δ, which is impossible by the choice of β_i's.

Putting (1) and (2) together, and using Lemma 2.1.1 we get:

$$(3) \qquad d([\![\forall y B(\alpha_3,y)]\!],[\![\forall y B(\alpha_1,y)]\!] \vee [\![\forall y B(\alpha_2,y)]\!]) < 5\delta \ ,$$

and taking $\delta := \xi/5$ yields the claim.

To conclude the proof of the lemma let $\alpha_1, \alpha_2, \ldots$ be a countable family such that $\bigvee_k [\![\forall y B(\alpha_k,y)]\!] = [\![\exists x \forall y BA(x,y)]\!]$. Put $\hat{\alpha}_1 := \alpha_1$ and apply Claim 2 to pairs $\hat{\alpha}_k, \alpha_{k+1}$ and parameters $\xi_k := \epsilon/2^{k+1}$ to get $\hat{\alpha}_{k+1}$ for $k = 1, 2, \ldots$. Then

$$d([\![\forall y B(\hat{\alpha}_k,y)]\!], \bigvee_{j \le k} [\![\forall y B(\alpha_j,y)]\!]) < \epsilon/2(\frac{2^k-1}{2^k}) \ .$$

Hence for k so large that

$$d(\bigvee_{j \le k} [\![\forall y B(\alpha_j,y)]\!],[\![\exists x \forall y B(x,y)]\!]) < \epsilon/2$$

$\hat{\alpha}_k$ is the wanted element.

q.e.d.

3.4 Compact families

The following concept will substitute in Subsection 3.5 the definability of F used in Lemma 3.2.3.

Definition 3.4.1 *Let $F \subseteq \mathcal{M}$ be a family. F is* **compact** *iff there exists an L_{all}-formula $H(x,y)$ such that for*

$$F_a := \{b \in \mathcal{M} \mid M \models H(a,b)\}$$

the following two properties hold:

1. $\bigcap_{k \in \mathbf{N}} F_k = F$.

2. $F_k \supseteq F_{k+1}$, *for all* $k \in \mathbf{N}$.

The second property is only technical: If $H(x,y)$ satisfies the first one then $H'(x,y) := \forall z \leq x; H(z,y)$ will satisfy both (and, in fact, the second one will be satisfied for all $a \in \mathcal{M}$).

Our example family F_{PV} of polynomial time computable functions is not compact. However, in many applications we can replace it by a bigger family F that is compact: The family of functions computable by circuits of subexponential size (here we take $\Omega = \{0,1\}^n$ and the qualification "subexponential" means less than 2^{n^ξ}, some infinitesimal ξ, i.e. size $2^{n^{o(1)}}$). Definable sets F_k witnessing that F is compact consists of functions computable by circuits of size less than $2^{n^{1/k}}$. Note that we switched to non-uniform algorithms in order to gain the definability of F_k's. Of course, we could have produced a tighter compact envelope F' of F_{PV} by taking for F'_k, for example, the set of functions computable by circuits of size less than $n^{\log^{(k)}(n)}$ ($\log^{(k)}$ is k-times iterated logarithm). However, the subexponential family yields stronger independence results and lower bounds.

The following lemma justifies the name **compact**: If we think of non-standard extensions of sequences as their "limits", then it says that any sequence of elements of a compact family F has a limit in F.

Lemma 3.4.2 *Let F be a compact family. Assume C_k, $k \in \mathbf{N}$, are definable sets such that*

$$F \cap \bigcap_{\ell < k} C_\ell \neq \emptyset \ ,$$

for all $k \geq 1$. Then:

$$F \cap \bigcap_{k \in \mathbf{N}} C_k \neq \emptyset \ .$$

Further, if $\{\alpha_k\}_{k \in \mathbf{N}}$ is a countable sequence of elements of F and $(\alpha_i)_{i<t}$ its arbitrary non-standard extension then there is non-standard $s < t$ such that

$$\alpha_i \in F, \quad \textit{for all } i \leq s \ .$$

Proof :

Let $H(x,y)$ be the formula certifying that F is compact. Put:

$$F_a := \{b \in \mathcal{M} \mid H(a,b)\} \ .$$

Define sets

$$D_k := C_k \cap F_k \ .$$

These are definable (as F_k's are) and satisfy

$$\bigcap_{\ell<k} D_\ell \neq \emptyset$$

as

$$\bigcap_{\ell<k} D_\ell \supseteq \bigcap_{\ell<k} C_\ell \cap F \neq \emptyset \ .$$

Here we use $F_k \supseteq F$.

By the $\aleph_1$-saturation we have:

$$\bigcap_{k\in\mathbf{N}} D_k \neq \emptyset \ .$$

But any $\alpha \in \bigcap_{k\in\mathbf{N}} D_k$ is, in particular, an element of $\bigcap_{k\in\mathbf{N}} F_k = F$.

For the second part and any non-standard extension $(\alpha_i)_{i<t}$ of $\{\alpha_k\}_{k\in\mathbf{N}}$ consider the definable property $P(i)$:

$$\alpha_i \in F_i \wedge F_0 \supseteq F_1 \supseteq \ldots \supseteq F_i \ .$$

$P(k)$ holds for all $k \in \mathbf{N}$ and so by induction in $\mathcal{M}$ it hold sup to some non-standard $s < t$. By $P(i)$ it holds that $\alpha_i \in F_i \subseteq \bigcap_{k\in\mathbf{N}} F_k = F$, for all $i \leq s$.

q.e.d.

3.5 Propositional computation of truth values

We shall strengthen Lemmas 3.1.2 and 3.3.3 in this subsection for the case of compact families. The strengthening lies in the elimination of the error term ϵ.

Theorem 3.5.1 *Let F be an L-closed compact family. Let $s \in \mathcal{M}$ be arbitrary non-standard number.*

Let A be an L-sentence, possibly with parameters from F, and assume that A has the form:

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k)$$

with B open.

Then there are elements of F

$$\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \alpha_2^{i_1,j_1,i_2}, \ldots, \beta_k^{i_1,\ldots,j_k}$$

with $i_1, \ldots, j_k < s$ such that $[\![A]\!]$ equals modulo the ideal I to the set - defined in $\mathcal{M}$ - of all $\omega \in \Omega$ satisfying:

$$\bigvee_{i_1} \bigwedge_{j_1} \cdots \bigvee_{i_k} \bigwedge_{j_k} B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega)) \ .$$

Proof :

Fix arbitrary $\epsilon > 0$, a standard rational. By Lemma 3.1.2 there are $r \in \mathbf{N}$ and elements of F:

$$\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \alpha_2^{i_1,j_1,i_2}, \ldots, \beta_k^{i_1,\ldots,j_k}$$

with all $i_1, \ldots, j_k < r$ such that the distance of $[\![A]\!]$ from

$$\bigvee_{i_1} \bigwedge_{j_1} \cdots [\![B(\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \ldots, \beta_k^{i_1,\ldots,j_k})]\!]$$

is at most ϵ. However, this $[\![\ldots]\!]$-value equals, modulo the ideal I, to the set of all $\omega \in \Omega$ satisfying (as evaluated in $\mathcal{M}$) the Boolean formula formed from formulas $B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega))$:

$$\bigvee_{i_1} \bigwedge_{j_1} \cdots B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega)) \ .$$

Applying this for $\epsilon := 1/2\ell$ yields the following claim.

Claim: *For any $\ell \in \mathbf{N}$ there are $r_\ell \in \mathbf{N}$ and $\alpha_1^{i_1}, \beta_1^{i_1,j_1}, \ldots, \beta_k^{i_1,\ldots,j_k} \in F$ with $i_1, \ldots, j_k < r_\ell$ such that the distance of $[\![A]\!]$ and of $V_\ell/\mathcal{I}$, where V_ℓ is the set of all $\omega \in \Omega$ satisfying the formula U_ℓ:*

$$\bigvee_{i_1 < r_\ell} \bigwedge_{j_1 < r_\ell} \cdots B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega))$$

is at most $1/2\ell$.

Let $(U_w)_{w<t}$ be a non-standard extension of $(U_\ell)_{\ell \in \mathbf{N}}$ provided by the $\aleph_1$-saturation. Let $V \in \mathcal{A}$ be a set such that $[\![A]\!] = V/\mathcal{I}$.

By the hypothesis that F is compact, $F = \bigcap_{k \in \mathbf{N}} F_k$ for some definable family $(F_a)_a$ (defined by an L_{all} formula H - cf.Definition 3.4.1), and $F_k \supseteq F_{k+1}$ for all $k \in \mathbf{N}$.

Consider the following three properties parameterized by w:

1. U_w is a formula of the form
$$\bigvee_{i_1<r}\bigwedge_{j_1<r}\ldots B(\alpha_1^{i_1}(\omega),\beta_1^{i_1,j_1}(\omega),\ldots,\beta_k^{i_1,\ldots,j_k}(\omega))$$
for some $r<s$, and with $\alpha_1^{i_1},\beta_1^{i_1,j_1},\ldots,\beta_k^{i_1,\ldots,j_k}$ from F_w.
2. The symmetric difference $V\triangle V_w$ has the counting measure at most $1/w$.
3. $F_1\supseteq F_2\supseteq\ldots\supseteq F_w$.

For any standard w all three properties are met: The arity r_w is standard and so $r_w<s$, and αs and βs occurring in U_w are even from $F\subseteq F_w$. The second property as also satisfied: The counting measure of the symmetric difference $V\triangle V_w$ differs from the distance of $[\![A]\!]$ and $V_w/\mathcal{I}$ by at most an infinitesimal amount (in particular, by less than $1/2w$) and the distance itself is at most $1/2w$. The third property holds by the definition of compact families.

The properties are all definable in $\mathcal{M}$ (using formula H and V and $(U_w)_{w<t}$ as parameters) and hence by overspill must hold up to some non-standard $p<t$.

The αs and βs occurring in U_p are from F_p which is contained in all F_k for $k\in\mathbf{N}$, hence in F. The counting measure of $V\triangle V_p$ is $<1/p$. This is infinitesimal, so
$$[\![A]\!]=V/\mathcal{I}=V_p/\mathcal{I}\ .$$

q.e.d.

Consider the simplest case when $A(\beta)$ has the form $\exists xB(x,\beta)$, B open and β the only parameter from F. Then (for compact F):
$$[\![A(\beta)]\!]\ =\ \{\omega\in\Omega\mid\bigvee_{i<s}B(\alpha^i(\omega),\beta(\omega)\}/\mathcal{I}$$
for some αs from F. This does not mean that A is equal in $\mathcal{M}$ to $\bigvee_{i<s}B(\alpha^i,\beta)$, as $[\![A(\beta)]\!]$ generally does not equal (modulo I) to the set of ωs satisfying $A(\beta(\omega))$. Also, the right-hand side is not equal to $\bigvee_{i<s}[\![B(\alpha^i,\beta)]\!]$ as taking the quotient by I does not commute with infinite disjunctions. Hence we should be careful in interpreting the theorem.

It is now clear that we can analogously strengthen Lemma 3.3.3.

Theorem 3.5.2 *Let F be an L-closed family that is*

1. *closed under definition by cases by open L-formulas, and*
2. *compact.*

Let A be an L-sentence of the form

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k B(x_1, y_1, \ldots, x_k, y_k)$$

with B open (and with parameters).

Then there are $\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k \in F$ such that for all $i = 1, \ldots, k$:

$$[\![\forall y_i \exists x_{i+1} \forall y_{i+1} \ldots \exists x_k \forall y_k B(\alpha_1, \beta_1, \ldots, \alpha_i, y_i, x_{i+1}, y_{i+1}, \ldots, x_k, y_k)]\!] = [\![A]\!]$$

and

$$[\![\exists x_{i+1} \forall y_{i+1} \ldots \exists x_k \forall y_k B(\alpha_1, \beta_1, \ldots, \alpha_i, \beta_i, x_{i+1}, y_{i+1}, \ldots, x_k, y_k)]\!] = [\![A]\!] \ .$$

For compact families we shall consider in Part **??**, based on various types of decision trees, Theorem 3.5.2 actually follows from Theorem 3.5.1 (formulas $B(\alpha_1^{i_1}(\omega), \beta_1^{i_1,j_1}(\omega), \ldots, \beta_k^{i_1,\ldots,j_k}(\omega))$ are then computed by decision trees and hence the whole formula too).

Chapter 4

The truth in N and the validity in $K(F)$

In this section we apply a particular Skolemization to a formula in order to link its truth-values in **N** and $K(F)$.

Consider an L-formula of the form $\exists y C(\overline{x}, y)$, with $\overline{x}$ a k-tuple of free variables, C open (with parameters from F). Let $f(\overline{x})$ be a new k-ary function symbol, and let

$$Sk[\exists y C(\overline{x}, y); f]$$

be the universal closure of the formula

$$C(\overline{x}, y) \to C(\overline{x}, f(\overline{x})) \ .$$

Clearly $Sk[\exists y C(\overline{x}, y); f]$ implies (in predicate calculus) the equivalence

$$\exists y C(\overline{x}, y) \equiv C(\overline{x}, f(\overline{x})) \ .$$

For an L-formula of the form $\forall y C(\overline{x}, y)$, again C open with parameters from F, we define

$$Sk[\forall y C(\overline{x}, y); f]$$

to be

$$Sk[\exists y \neg C(\overline{x}, y); f] \ .$$

This axiom then implies

$$\forall y C(\overline{x}, y) \equiv C(\overline{x}, f(\overline{x})) \ .$$

This reduction can be iterated. Let A be an L-sentence of the form

$$Q_1 x_1 \dots Q_k x_k B(x_1, \dots, x_k) \ ,$$

B open and possibly with parameters. Introduce $(k-1)$-ary function symbol f_k and axiom $Sk[Q_k x_k B(x_1, \dots, x_k); f_k]$. Then A is equivalent, modulo this axiom, to

$$Q_1 x_1 \dots Q_{k-1} x_{k-1} B(x_1, \dots, x_{k-1}, f_k(x_1, \dots, x_{k-1})) \ .$$

Analogously introduce $(i-1)$-ary function symbols f_i and corresponding axioms, for $i = k-1, k-2, \dots 1$ to successively reduce the quantifier complexity of the formula, the last formula

$$B(f_1, f_2(f_1), \dots, f_k(f_1, f_2(f_1), \dots, f_{k-1}(f_1, f_2(f_1), \dots)))$$

(any occurrence of f_i is substituted for an occurrence of x_i - we do not show it explicitly) being a quantifier-free sentence (f_1 is a constant).

Definition 4.0.3 *For a sentence A of the form as above denote by*

$$Sk[A; f_1, \dots, f_k]$$

the conjunction of the k universal axioms introduced in the reduction process, and by A_{Sk} the quantifier-free sentence obtained at the end.

Any k-tuple of functions $f_1, \dots, f_k$ (of the appropriate arity) defined on $\mathbf{N}$ *and satisfying $Sk[A; f_1, \dots, f_k]$ will be called a* **Skolem tuple** *for A.*

The next lemma follows from the construction.

Lemma 4.0.4 *For a sentence A of the form as above the axiom $Sk[A; f_1, \dots, f_k]$ implies in predicate logic alone the equivalence*

$$A \equiv A_{Sk} \ .$$

We aim at the following statement.

Lemma 4.0.5 *Assume that A is an L-sentence of the form as above. Assume also that L contains (symbols from L_{all} for) a Skolem tuple for A, and constants for all elements of* $\mathbf{N}$*.*

Then for any L-closed family F it holds that:

$$\mathbf{N} \models A \ \ \textit{iff} \ \ [\![A]\!] = 1_{\mathcal{B}} \ .$$

Proof :

Let $f_1, \ldots, f_k$ be a Skolem tuple for A that is in L. By Lemma 1.4.2 the axiom $Sk[A; f_1, \ldots, f_k]$ is $K(F)$-valid. By Lemma 4.0.4 then A is equivalent to A_{Sk} in both $\mathbf{N}$ and $K(F)$.

But by Lemma 1.4.2 again $\mathbf{N} \models A_{Sk}$ holds if and only if $[\![A_{Sk}]\!] = 1_{\mathcal{B}}$.

q.e.d.

We shall use this lemma to our advantage in both directions, to pull facts from $\mathbf{N}$ to $K(F)$ and vice versa.

Chapter 5

A summary of notations and conventions

Let us summarize here notation for some basic objects introduced in earlier sections, as well as some standard notation.

- $\mathbf{N}$ is the standard structure of natural numbers, its language is L_{all} having a symbol for all functions and relations on $\mathbf{N}$.
- $\mathcal{M}$ is an $\aleph_1$-saturated model of the theory of $\mathbf{N}$ in the language L_{all}.
- $\Omega \in \mathcal{M}$ is a sample space, $\mathcal{A} \in \mathcal{M}$ the Boolean algebra of its subsets, $\mathcal{I} \subseteq \mathcal{A}$ is the ideal of sets having infinitesimal counting measure.
- $\mathcal{B}$ is the quotient algebra $\mathcal{A}/\mathcal{I}$ (it is complete) and μ is the induced measure on it with values in standard reals $\mathbf{R}$.
- $[n] := \{1, \dots, n\}$ while we identify n with $\{0, \dots, n-1\}$.

We have made a useful convention that will remain valid throughout the whole paper:

- Letters ϵ and δ always stand for a **positive standard** rational.

When we will want to talk about positive infinitesimals we shall always denote them $1/t$ or similarly, for t a nonstandard element of $\mathcal{M}$.

Below we remark few facts that do follow from the definitions but that cannot harm to mention explicitly:

- Probabilities $Pr_{\omega \in \Omega}[\ldots]$ are evaluated in $\mathcal{M}$ and hence their values are $\mathcal{M}$-rationals.
- If $\mu(b) = 1$ for $b = X/\mathcal{I}$, $X \in \mathcal{A}$, then it follows that the counting measure of X is infinitesimally close to 1 and so bounded from below by any $1 - \epsilon$ ($\epsilon > 0$ is standard by the convention above).

Part II

Second order structures

Part III

AC^0 world: witnessing and independence

Part IV

AC^0-world: constant depth Frege systems

Part V

$AC^0(2)$ world

Part VI

Polynomial-time and higher worlds

Part VII

Logical auxilliaries

Bibliography

[1] M. Ajtai, Σ_1^1 - formulae on finite structures, *Annals of Pure and Applied Logic*, **24**, (1983), pp.1-48.

[2] M. Ajtai, The complexity of the pigeonhole principle, in: *Proc. IEEE 29^{th} Annual Symp. on Foundation of Computer Science*, (1988), pp. 346-355.

[3] M. Ajtai, Parity and the pigeonhole principle, in: *Feasible Mathematics*, Eds. S.R.Buss and P.J.Scott, (1990), pp.1-24. Birkhauser.

[4] M. Ajtai, The independence of the modulo p counting principles, in: *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, (1994), pp.402-411. ACM Press.

[5] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák: Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proceedings of the London Mathematical Society*, **(3) 73**, (1996), pp.1-26.

[6] G. Boole, *The mathematical analysis of logic*, Barclay and Macmillan, Cambridge, (1847).

[7] S. R. Buss, *Bounded Arithmetic.* Naples, Bibliopolis, (1986).

[8] S. R. Buss, Axiomatizations and conservation results for fragments of bounded arithmetic, in: *Logic and Computation*, Contemporary Mathematics **106**, (1990), pp.57-84. Providence, American Mathematical Society.

[9] S. R. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi, Linear gaps between degrees for the polynomial calculus modulo distinct primes, *Journal of Computer and System Sciences*, **62**, (2001), pp.267-289.

[10] S. R. Buss, and L. Hay, On truth-table reducibility to SAT and the difference hierarchy over NP, *Proc. Structure in Complexity*, IEEE, (1988), pp.224-233.

[11] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall: Proof complexity in algebraic systems and bounded depth Frege systems with modular counting, *Computational Complexity*, **6(3)**, (1996/1997), pp.256-298.

[12] S. R. Buss, and J. Krajíček, An application of boolean complexity to separation problems in bounded arithmetic, *Proceedings of the London Mathematical Society*, **69(3)**, (1994), pp. 1-21.

[13] S. R. Buss, J. Krajíček, and G. Takeuti, On provably total functions in bounded arithmetic theories R_3^i, U_2^i and V_2^i, in: *Arithmetic, Proof Theory and Computational Complexity*, eds.P. Clote and J. Krajíček, (1993), pp.116-161, Oxford Press.

[14] C. C. Chang, and J. Keisler, *Model theory*, Ser. Studies in Logic, North-Holland, (1977).

[15] M. Chiari, and J. Krajíček, Witnessing functions in bounded arithmetic and search problems, *J. of Symbolic Logic*, **63(3)**, (1998), pp. 1095-1115.

[16] S. A.Cook, Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, (1975), pp. 83-97. ACM Press.

[17] S. A. Cook, and P. Nguyen, *Foundations of proof complexity*, draft of a book, (2006).

[18] S. A. Cook, and Reckhow, The relative efficiency of propositional proof systems, *J. Symbolic Logic*,**44(1)**, (1979), pp.36-50.

[19] S. A. Cook, and N. Thapen, The strength of replacement in weak arithmetic, preprint, (2004).

[20] M. Furst, J. B. Saxe, and M. Sipser, M. Parity, circuits and the polynomial-time hierarchy, *Math. Systems Theory*, (1984), **17**: 13–27.

[21] J. Hanika, *Search Problems and Bounded Arithmetic*, PhD.Thesis, Charles University, Prague, (2004).

[22] J. Hastad, Almost optimal lower bounds for small depth circuits. in: *Randomness and Computation*, ed. S.Micali, Ser.Adv.Comp.Res., (1989), **5**: 143-170. JAI Pres.

[23] W. Hodges, *Model theory*, Encyclopedia of Mathematics and Its Applications, Vol. **42**, Cambridge University Press, (1993).

[24] R. Impagliazzo, P. Pudlak, and J. Sgall, Lower bounds for the polynomial calculus and the Groebner basis algorithm, *Comput. Complexity*, **8(2)**, (1999), pp.127-144.

[25] R. Impagliazzo, and N. Segerlind, Counting axioms do not polynomially simulate counting gates, in: *Proc. IEEE 42^{nd} Annual Symp. on Foundation of Computer Science*, (2001), pp. 200-209.

[26] T. Jech, *Set theory*, (2003). Springer.

[27] J. Krajíček, A fundamental problem of mathematical logic, *Annals of the Kurt Gödel Society*, Springer-Verlag, *Collegium Logicum*, Vol.**2**, (1996), pp.56-64.

[28] J. Krajíček, Fragments of bounded arithmetic and bounded query classes, *Transactions of the A.M.S.*, **338(2)**, (1993), pp.587-598.

[29] J. Krajíček, On Frege and Extended Frege Proof Systems. in: "Feasible Mathematics II", eds. P. Clote and J. Remmel, Birkhauser, (1995), pp. 284-319.

[30] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[31] J. Krajíček, On methods for proving lower bounds in propositional logic, in: *Logic and Scientific Methods* Eds. M. L. Dalla Chiara et al., (Vol. 1 of Proc. of the Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence (August 19-25, 1995)), Synthese Library, Vol.259, Kluwer Academic Publ., Dordrecht, (1997), pp.69-83.

[32] J. Krajíček, Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus, in:

Eds. I.Prívara, P. Růžička, 22nd Inter. Symp. *Mathematical Foundations of Computer Science* (Bratislava, August '97), Lecture Notes in Computer Science 1295, Springer-Verlag, (1997), pp.85-90.

[33] J. Krajíček, On the degree of ideal membership proofs from uniform families of polynomials over a finite field, *Illinois J. of Mathematics*, **45(1)**, (2001), pp.41-73.

[34] J. Krajíček, Extensions of models of PV, in: Logic Colloquium'95, Eds. J.A.Makowsky and E.V.Ravve, ASL/Springer Series *Lecture Notes in Logic*, Vol. **11**, (1998), pp.104-114.

[35] J. Krajíček, On the weak pigeonhole principle, *Fundamenta Mathematicae*, Vol.**170(1-3)**, (2001), pp.123-140.

[36] J. Krajíček, Tautologies from pseudo-random generators, *Bulletin of Symbolic Logic*, **7(2)**, (2001), pp.197-212.

[37] J. Krajíček, Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds", *J. of Symbolic Logic*, **69(1)**, (2004), pp.265-286.

[38] J. Krajíček, Hardness assumptions in the foundations of theoretical computer science, *Archive for Mathematical Logic*, to app.

[39] J. Krajíček and P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, *J. Symbolic Logic*, **54(3)**, (1989), pp.1063-1079.

[40] J. Krajíček and P. Pudlák, Propositional provability in models of weak arithmetic, in: *Computer Science Logic (Kaiserlautern, Oct. '89)*, eds. E. Boerger, H. Kleine-Bunning and M.M. Richter, Lecture Notes in Computer Science **440**, (1990), pp. 193-210. Springer-Verlag.

[41] J. Krajíček and P. Pudlák, Some consequences of cryptographical conjectures for S^1_2 and EF", *Information and Computation*, Vol. **140 (1)**, (January 10, 1998), pp.82-94.

[42] J. Krajíček, P. Pudlák and G. Takeuti, Bounded arithmetic and the polynomial hierarchy, *Annals of Pure and Applied Logic*, **52**, (1991), pp.143–153.

[43] J. Krajíček, P. Pudlák,and A. Woods, An Exponential Lower Bound to the Size of Bounded Depth Frege Proofs of the Pigeonhole principle", *Random Structures and Algorithms*, **7(1)**, (1995), pp.15-39.

[44] J. Krajíček, and T. Scanlon, Combinatorics with definable sets: Euler characteristics and Grothendieck rings", *Bulletin of Symbolic Logic*, **3(3)**, (2000), pp.311-330.

[45] P. A. Loeb, Conversion from nonstandard to standard measure spaces and applications in probability theory, *Trans. Am. Math. Soc.*, Vol.**211**, (1975), pp.113-122.

[46] A. Maciel and T. Pitassi, Towards lower bounds for bounded-depth Frege proofs with modular connectives, in: *Proof Complexity and Feasible Arithmetics*, P. Beame and S. Buss, eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. **39**, pp. 195-227, American Mathematical Society, (1998).

[47] R. Mansfield, The theory of boolean ultrapowers, *Annals of Mathematical Logic*, **2(3)**, (1971), pp.297-323.

[48] J. Paris and A. J. Wilkie, Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic*, LNM 1130, (1985), pp. 317-340. Springer-Verlag.

[49] T. Pitassi, P. Beame, and R. Impagliazzo, Exponential lower bounds for the pigeonhole principle, *Computational complexity*, **3**, (1993), pp.97-308.

[50] A. A. Razborov, Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution, preprint, (Dec.'02).

[51] H. Rasiowa and R. Sikorski, Algebraic treatment of the notion of satisfiability, *Fundamenta Mathematicae*, **40**, (1953), pp.62-65.

[52] H. Rasiowa and R. Sikorski, *The mathematics of metamathematics*, Panstwowe Wydaw. Naukowe, Warsaw, (1963).

[53] A. A. Razborov, Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, (1987), 598-607.

[54] A. A. Razborov, Lower Bounds for the Polynomial Calculus, *Computational Complexity*, **7(4)**, (1998), pp.291-324.

[55] S. Riis, *Independence in bounded arithmetic*, DPhil. Thesis, (1993), Oxford University.

[56] D. Scott, A proof of the independence of the continuum hypothesis, *Mathematical Systems Theory*, **1**, (1967), pp.89-111.

[57] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in: *Proc. 19th Ann. ACM Symp. on Th. of Computing*, (1987), pp. 77-82.

[58] G. Takeuti, *Two applications of logic to mathematics*, (1978). Princeton Univ. Press.

[59] G. Takeuti, Cuts and forcing of bounded arithmetic, *Annals of Pure and Applied Logic*, aa

[60] G. Takeuti and M. Yasumoto, Forcing in bounded arithmetic, in: Gódel'96, Ed. P. Hájek, LN in Logic **6**, (1996), pp.120-138.

[61] G. Takeuti and M. Yasumoto, Forcing in bounded arithmetic II., *J.Symbolic Logic*, **63**, (1998), pp.860-868.

[62] G. Takeuti and W. Zaring, *Axiomatic set theory*, Grad. Texts in Math. **8**, (1973). Springer.

[63] K. W. Wagner, Bounded query classes, *SIAM J. Computing*, **19(5)**, (1990), pp.833-846.

[64] A. Yao, Separating the polynomial-time hierarchy by oracles, in: *Proc. 26th Ann. IEEE Symp. on Found. of Comp. Sci.*, (1985), pp. 1-10.

Mailing address:

Mathematical Institute
Academy of Sciences
Žitná 25, Prague, CZ-115 67
The Czech Republic
`krajicek@math.cas.cz`