Combinatorics of first order structures and propositional proof systems

Jan Krajíček*

Mathematical Institute†
Academy of Sciences, Prague

Abstract

We define the notion of a *combinatorics* of a first order structure, and a relation of *covering* between first order structures and propositional proof systems. Namely, a first order structure M *combinatorially satisfies* an L-sentence Φ iff Φ holds in all L-structures definable in M. The combinatorics $\mathrm{Comb}(M)$ of M is the set of all sentences combinatorially satisfied in M. Structure M *covers* a propositional proof system P iff M combinatorially satisfies all Φ for which the associated sequence of propositional formulas $\langle\Phi\rangle_n$, encoding that Φ holds in L-structures of size n, have polynomial size P-proofs. That is, $\mathrm{Comb}(M)$ contains all Φ feasibly verifiable in P. Finding M that covers P but does not combinatorially satisfy Φ thus gives a super polynomial lower bound for the size of P-proofs of $\langle\Phi\rangle_n$.

We show that any proof system admits a class of structures covering it; these structures are expansions of models of bounded arithmetic. We also give, using structures covering proof systems $R^*(\log n)$ and PC, new lower bounds for these systems that are not apparently amenable to other known methods. We define new type of propositional proof systems based on a combinatorics of (a class of) structures.

We continue here research into what could be called infinite limits of polynomially bounded propositional proof systems. Although this is best explained on examples and formal definitions, the reader deserves a quick

*Partially supported by grant # A 101 99 01of the Academy of Sciences of the Czech Republic and by project LN00A056 of The Ministry of Education of the Czech Republic.

†Also member of the Institute for Theoretical Computer Science of the Charles University. A part of this work was done while visiting the Mathematical Institute, Oxford.

explanation for this somewhat bizarre statement. A propositional proof system in a general sense is simply a non-deterministic algorithm accepting exactly the set of propositional tautologies in DeMorgan language. The main problem is the NP vs. coNP problem, a question whether some proof system can run in polynomial time. For a few particular proof systems based on logic or algebraic calculi (e.g. resolution or Nullstellensatz) super-polynomial lower bounds are known. All these lower bounds can be proved for a very uniformly given sequences of tautologies: For $n \geq 1$, the n-th tautology asserts the validity of a combinatorial principle on structures of size n (e.g. the pigeonhole principle). The principle can be formulated by a sentence in a first-order language (or in a simple 2nd order extension allowing for natural formulation of Ramsey theorem and alike).The sentence then makes sense over arbitrary structure in the language, even infinite. The general theory of limits of proof systems we are after says that given a proof system P, if instances of a principle Φ for $n \geq 1$ are valid and proved by P in length polynomial in n then Φ holds true (in the definable sense - see Definition 1.1) in a class of first-order structures associated with P. Such a class of structures is informally called a covering theory of P.

In fact, any P admits a covering theory and one can take for the class a class of suitable generic expansions of models of bounded arithmetic. However, we look for model-theoretically natural classes as this then yields an insight into lower bounds for P. There are two prominent examples known at present. The tree-like resolution proof system R^* (in fact, its extension $R^*(\log)$) corresponds to the class of all infinite structures (and the relation is actually an equivalence), [11, 14]. The second example is Nullstellensatz and polynomial calculus over a finite prime field $\mathbf{F}_p$, corresponding to the so called Euler structures with a suitable Grothendieck ring ([13]).

In this paper we first define the notion of the combinatorics of a first order structure M and give few examples. Then we recall the translation of first-order principles into propositional formulas; we consider a particular translation that produces a set of clauses (or a set of polynomial equations).

In the third section we define the covering relation between first order structures and propositional proof systems, formalizing a relation that exists between all structures and (an extension) of tree-like resolution, and between Euler structures and Nullstellensatz and polynomial calculus over a finite prime field. Structure M *covers* a propositional proof system P iff M combinatorially satisfies all Φ for which the associated sequence of propositional formulas $\langle\Phi\rangle_n$, encoding that Φ holds in L-structures of size n, have polynomial size P-proofs. Finding M that covers P but does not combinatorially satisfy Φ thus gives a super polynomial lower bound for the size of P-proofs of $\langle\Phi\rangle_n$.

We use the covering theories for (an extension of) tree-like resolution [11, 14], and for Nullstellensatz and polynomial calculus systems over a finite prime field [13] to give new lower bounds for these systems, for principles that are not apparently amenable to other known methods. This is in Section 4.

In Section 5 we give a general description of a covering theory of any P as expansions of models of bounded arithmetic.

Finally, in the last section, we show that (classes of) structures with r.e. combinatorics can be seen as propositional proof systems in a natural way.

Definitions of undefined notions in model theory and proof complexity can be found in [7] and [11] respectively.

1 Combinatorics of a structure

Let L be any first order relational language with constants and with equality. The prohibition of general function symbols is not essential but it simplifies some definitions. A suitable general language is the language of directed graphs: a binary relation symbol and constants; any theory is interpretable in a theory in this language (see e.g. [8]).

Let M be a first order structure with at least two different elements. To avoid any confusion we shall assume that L is disjoint from the language of M. The qualification definable means definable with parameters, unless it is specified otherwise. An L-structure is definable in M if its universe is a definable subset of some M^k, and all L-relations are definable too.

Let Φ be an L-sentence.

Definition 1.1 *M* combinatorially satisfies *Φ, $M\models_c\Phi$ in symbols, iff Φ holds in all L-structures definable in M. The* combinatorics of *M is the set*

$$Comb(M) := \{\Phi \mid M\models_c\Phi\}$$

It would be, perhaps, equally natural to consider L-structures interpretable in M (e.g. in the sense of being definable in M^{eq}) rather than only definable. But for our purposes the given definition suffices.

As all finite structures are definable in all M of size at least 2, Comb(M) is a subset of sentences valid in finite structures (hence the name *combinatorics* of M). It is clearly deductively closed. Moreover, it can be non-trivial, i.e. bigger than just predicate logic but smaller than the set of all sentences valid in finite structures.

Example 1.2 *Comb*($\mathbf{R}$) *violates the pigeonhole principle (PHP) but still upholds that there is no map between a set and the set minus one point (the ontoPHP), and that there is no injective map of A^2 into A (the weak pigeonhole principle WPHP).*

The PHP is violated by many maps in $\mathbf{R}$; for example, map $x > 0$ to $x + 1$ and leave $x \leq 0$ in place. The *ontoPHP* holds as semi-algebraic bijections preserve Euler characteristic and the characteristics of a set and the set minus one point differ, cf. [5]. The WPHP holds for dimension reasons.

Example 1.3 *Comb*($\mathbf{C}$) *contains Comb*($\mathbf{R}$)*, as* $\mathbf{C}$ *is definable in* $\mathbf{R}$*, but it is different.* $\mathbf{C}$ *fulfills PHP; this is a theorem of Ax [1]. However, the dual statement:*

Any $f : A \to A$ that is onto must be one-to-one

is clearly not in Comb($\mathbf{C}$) *(e.g. $x \to x^2$).*

The Ax's proof works equally well in a bigger generality and gives the following statement: Any $\forall\exists$ L-sentence Φ that is valid in all finite L-structures is also combinatorially valid in all structures that are elementarily equivalent to ultraproducts of locally finite structures (in the case of $\mathbf{C}$ it is the ultraproduct of algebraic closures of finite fields).

Example 1.4 *If M is pseudo-finite (i.e., elementarily equivalent to an ultraproduct of finite structures) then Comb(M) consists exactly of Φ's valid in all finite structures.*

As the theory of M gets stronger, Comb(M) gets weaker.

Example 1.5 *If M is a model of PA (or even its subtheory $I\Sigma^0_1$) that is Σ^0_1-sound (all Σ^0_1 sentences true in M are true also in* $\mathbf{N}$*) then Comb(M) consists exactly of Φ provable in predicate logic.*

This follows straightforwardly from the completeness theorem which can be formalized in $I\Sigma^0_1$, cf. [6].

We mention two problems whose motivation will be clear later.

Problem 1.6 *Characterize structures M whose combinatorics Comb(M) contains the following principle of finite combinatorics:* Every linear ordering has the least element.

The qualification *characterize* means that we look for a property of such structures of a natural model-theoretic character. For example, structures combinatorially satisfying PHP are those admitting ordered weak Euler characteristic on definable sets, cf. [16].

Problem 1.7 *When is $Comb(M)$ recursively enumerable? Are there some mathematically interesting structures with non-trivial but recursively enumerable combinatorics? Are $Comb(\mathbf{C})$ and $Comb(\mathbf{R})$ r.e.?*

2 First order principles and propositional formulas

A sentence Φ gives raise to an infinite sequence of propositional formulas.

Definition 2.1 *The propositional language $\langle L \rangle$ consists of connectives 1 (true), 0 (false), $\neg$, of $\vee$ and $\wedge$ of unbounded arity, and of infinitely many atoms*

$$p^R_{i_1,\ldots,i_k}$$

one for every relation symbol $R(x_1, \ldots, x_k) \in L$ and every choice of natural numbers $i_1, \ldots, i_k$

The next definition recalls a standard notation [11].

Definition 2.2 *Let Φ be an L-sentence and $n \geq 1$ a natural number. Define propositional formula $\langle \Phi \rangle_n$ in language $\langle L \rangle$ by induction on the logical complexity of Φ:*

1. $\langle i = j \rangle_n$ *is* 1 *iff* $i = j$*, otherwise it is* 0*, for any* $i, j < n$.
2. $\langle R(i_1, \ldots, i_k) \rangle_n := p^R_{i_1,\ldots,i_k}$*, for any* $i_1, \ldots, i_k < n$
3. $\langle \neg\Phi \rangle_n := \neg\langle \Phi \rangle_n$
4. $\langle \Phi \circ \Psi \rangle_n := \langle \Phi \rangle_n \circ \langle \Psi \rangle_n$*, for* $\circ = \vee, \wedge$
5. $\langle \exists x, \Phi(x) \rangle_n := \bigvee_{i<n} \langle \Phi(i) \rangle_n$
6. $\langle \forall x, \Phi(x) \rangle_n := \bigwedge_{i<n} \langle \Phi(i) \rangle_n$

The formula $\langle\Phi\rangle_n$ is, in general, a constant depth formula while some proof systems operate with only restricted class of formulas (like resolution with clauses) or even with formulas that are not DeMorgan (like algebraic proof systems), or even do not operate with formulas at all (like a general NP algorithms). Strictly speaking, this does not need to concern us as, by definition, a proof system proves all tautologies in DeMorgan language. For example, a general formula is encoded for resolution by limited extension.

However, the tautologies we consider are of special form and there is a better way of reaching CNF form of formulas. Sentence Φ is valid in all finite structures iff its Herbrandization Φ_H is; Φ_H is an $\forall\exists$ formula and $\neg\Phi_H$ has the CNF form.

The Herbrandization of a prenex formula Φ:

$$\exists x_1 \forall y_1 \ldots \exists x_k \forall y_k; \phi(\overline{x}, \overline{y})$$

ϕ open formula in DNF form, is

$$\exists x_1 \ldots \exists x_k; \phi(\overline{x}, y_1/h_1(x_1), y_2/h_2(x_1, x_2), \ldots, y_k/h_k(\overline{x})))$$

where h_i are new function symbols. As we do not allow function symbols, each h_i is replaced by $(i+1)$-ary relation symbol $H_i(x_1, \ldots, x_i, z)$, and Φ_H is defined to be the disjunction of the formula

$$\exists x_1 \ldots \exists x_k \exists y_1 \ldots \exists y_k; H_1(x_1, y_1) \wedge H_2(x_1, x_2, y_2) \wedge \ldots$$

$$\wedge\ H_k(\overline{x}, y_k) \wedge \phi(\overline{x}, y_1, \ldots, y_k)$$

together with the formula

$$\exists x_1 \forall y_1 \neg H_1(x_1, y_1) \vee \ldots \vee \exists x_1, \ldots, x_k \forall y_k \neg H_k(x_1, \ldots, x_k, y_k)$$

Hence $\langle\Phi_H\rangle_n$ is a DNF formula and so, possibly always replacing Φ by Φ_H, we may assume henceforth without loss of generality that all Φ translate to a sequence of DNF formulas $\langle\Phi\rangle_n$.

3 Covering theories for proof systems

Let M be a structure and P a proof system.

Definition 3.1 *The symbol $P \vdash_* \langle\Phi\rangle_n$ denotes the existence of P-proofs of $\langle\Phi\rangle_n$ of size $n^{O(1)}$, for all $n \geq 1$.*

M covers *P iff $\Phi \in Comb(M)$ whenever $P \vdash_* \langle\Phi\rangle_n$.*

Our main goal in this research is to find, given P, a rich class of structures M defined by some combinatorial, model-theoretic or geometric property, and covering P. We use the informal term *covering theory* of P for any such class. The point is that one can then use structures in the covering theory for proving lower bounds for P: to prove super-polynomial lower bound for $\langle\Phi\rangle_n$ it is sufficient to find M in the class such that $M \not\models_{\mathrm{C}} \Phi$.

3.1 First example: an extension of tree-like resolution

Resolution R is naturally a subsystem of sequent calculus LK, allowing no connectives except the negation. The following definition augments R as to correspond to LK-proofs of the Σ-depth 0 (as defined in [9] or [11, Def. 12.2.3]).

Definition 3.2 ([14]) *(a) R^+ is a refutation proof system that works with clauses C formed by conjunctions D_i of literals $\ell_{i,j}$:*

$$C = \bigcup_i \{D_i\} \ , \ D_i = \bigwedge_j \ell_{i,j}$$

The inference rules are:

$$\frac{C_1 \cup \{\bigwedge_j \ell_j\} \qquad C_2 \cup \{\neg\ell'_1, \ldots, \neg\ell'_k\}}{C_1 \cup C_2}$$

provided $\ell'_1, \ldots, \ell'_k$ are among ℓ_j's and $k \geq 1$, and

$$\frac{C_1 \cup \{\bigwedge_{j<u} \ell_j\} \qquad C_2 \cup \{\bigwedge_{j<v} \ell_{u+j}\}}{C_1 \cup C_2 \cup \{\bigwedge_{j<u+v} \ell_j\}}$$

(b) Let $f : \mathbf{N} \to \mathbf{N}$ be a function. The $R(f)$-size *of an R^+-proof is the minimum S such that the proof has at most S clauses and each conjunction of literals occurring in clauses has size at most $f(S)$.*

We shall use a phrase $R(f)$-proofs of size S *rather than R^+-proofs of $R(f)$-size S.*

(c) Tree-like versions of proof systems are denoted by star: R^*, $R(f)^*$.

Obviously, $R(1)$ is just R, while $R(\log)$ is the Σ-depth 0 subsystem of LK.

Theorem 3.3 ([11, L.9.5.2]) *Any structure covers* $R^*(\log)$.

The theorem is valid in a stronger sense than it is captured by the notion of covering. Namely, a principle has polynomial size $R^*(\log)$ proofs iff it is provable in predicate logic and, if it is not, then it requires exponential size $R^*(\log)$ proofs.[1] This first example of a covering theory is from [11], where it is a special case of a more general statement about search trees. The upper bound (principles provable in predicate logic have polynomial size $R^*(\log)$ proofs) follows from simulation of bounded arithmetic by $R^*(\log)$ and is already in [9]. See [14] for further discussion.

Theorem 3.3 (and its more general version in [11]) is a non-uniform version of a theorem of S. Riis about provability in bounded arithmetic (the so called finitisation theorem [17]). This non-uniform version for R^* was recently reproved in [18]; there Riis improved the upper bound from $R^*(\log)$ to R^*.

The idea to use pure model theory for lower bounds in proof complexity (via the relation formalized here as covering) is from [13] where our second example is proved.

3.2 Second example: algebraic proof systems

An algebraic proof system seeks to prove that $f_0 \in \langle f_1, \ldots, f_k \rangle$, given polynomials $f_i \in F[\overline{x}]$ over a field F. A proof of the ideal membership in the so called *Nullstellensatz proof system* NS (cf.[2]), is a k-tuple $g_1, \ldots, g_k$ of polynomials from $F[\overline{x}]$ such that $\sum_{i \geq 1} g_i \cdot f_i = f_0$. The degree of the NS proof is $\max_{i \geq 1} \deg(g_i f_i)$.

A proof of the ideal membership in *polynomial calculus* PC is a sequence of polynomials $h_1, \ldots, h_t$ such that $h_t = f_0$, and such that every h_j is either one of $f_1, \ldots, f_k$, or is derived from earlier $h_1, \ldots, h_{j-1}$ by one of the two rules: g_1, g_2 entail any F-linear combination of g_1, g_2, and g entails any $x_i \cdot g$. The degree of the PC proof is $\max_i \deg(h_i)$. We shall denote the systems NS/F and PC/F respectively when we want to stress the particular underlying field F.

Polynomials are encoded using the dense notation, i.e. by listing all coefficients, even zero, of all monomials up to the degree of the polynomial.

[1] Riis [18, Sect.7] mentions that similar gap in proof complexity occurs also for particular second order Σ_1^1 formulas Φ; an example of such a formula is Ramsey theorem RAM formalizing the Ramsey relation $n \to (1/2\log(n))_2^2$ (see [11] or DNF_2 formulas in [14, Sect.3]). If so, it must be proved differently as the criterion [14, 3.3] generalizing his independence criterion for DNF_2 formulas (see [17, Thm.11] or [11, 11.3.4]) analogously to Theorem 3.3 is no longer valid in the iff form - see [14, Sect.3] for an example.

For F finite the size of the code of f is thus proportional to $n^{\deg(f)}$, n the number of variables. Hence polynomial size NS- or PC- proofs over finite fields are exactly proofs of bounded degree.

Given propositional formula ψ with binary $\vee$ and $\wedge$ define polynomial ψ^* by: for atom p, $p^* := p$. Further, $(\psi \vee \phi)^* := \psi^* \cdot \phi^*$ and $(\neg\psi)^* := 1 - \psi^*$ (the truth values TRUE and FALSE are represented by 0 and 1 respectively). Note that $\deg(\psi^*)$ depends on the logical depth of ψ only.

Now take a first order sentence Φ, and we assume that it is in the Herbrand form. Assign to Φ the following set of polynomials:

- $\sum_{j\in[n]} p^{H_t}_{i_1,\ldots,i_t,j} = 1$, one for each $t = 1, \ldots, k$, and $i_1, \ldots, i_t, j \in [n]$
- $p^{H_t}_{i_1,\ldots,i_t,j_1} \cdot p^{H_t}_{i_1,\ldots,i_t,j_2} = 0$, one for each $t = 1, \ldots, k$, and $i_1, \ldots, i_t, j_1, j_2 \in [n]$
- $[H_1(i_1, j_1) \wedge \ldots H_k(i_1, \ldots, i_k, j) \wedge \neg\phi(\bar{i}, \bar{j})]^* = 0$, one for each choice of i's and j's in $[n]$
- $p^2 - p = 0$, any atom p.

Solutions to the polynomial system are in one-to-one correspondence with satisfying assignments of $\neg\langle\Phi\rangle_n$. Hence $\langle\Phi\rangle_n$ is a tautology iff the polynomial system has no solution iff the polynomials generate the trivial ideal (the last set of polynomial allows to look only on solutions in F rather than in F^{alg} in order to apply Nullstellensatz). Hence, whenever we work with algebraic systems we shall work with the polynomial system as the propositional translation of Φ, and we shall denote the systems also $\langle\Phi\rangle_n$.

Theorem 3.4 ([12, Thm.5.5]) *For NS and PC over a finite prime field $\mathbf{F}_p$ and any Φ it holds:*

$$NS/\mathbf{F}_p \vdash_* \langle\Phi\rangle_n \quad \text{iff} \quad PC/\mathbf{F}_p \vdash_* \langle\Phi\rangle_n$$

That is, a structure covers $NS/\mathbf{F}_p$ iff it covers $PC/\mathbf{F}_p$.

Definition 3.5 ([13, Def.2.1]) *Let M be a first-order structure. $Def^k(M)$ is the class of subsets of M^k definable in M (with parameters) and $Def^\infty(M)$ is the union $\bigcup_k Def^k(M)$.*

Let R be a commutative ring with unity. A function

$$\chi : Def^\infty(M) \longrightarrow R$$

is an abstract Euler characteristic on M over R *iff it satisfies the following conditions:*

1. $\chi(\{a\}) = 1$, *any* $a \in M^k$.

2. $\chi(A \cup B) = \chi(A) + \chi(B)$, *whenever* $A, B, A \cup B \in Def^\infty(M)$ *and* A, B *are disjoint.*

3. $\chi(A \times B) = \chi(A) \cdot \chi(B)$, *whenever* $A, B, A \times B \in Def^\infty(M)$.

4. $\chi(A) = \chi(B)$, *whenever* $A, B \in Def^\infty(M)$ *and there is a definable bijection between* A *and* B.

5. $\chi(A) = c \cdot \chi(B)$, *whenever* $c \in R$, $A, B \in Def^\infty(M)$ *and there is a definable map* f *with domain* A *and range* B *such that each its fiber* $f^{(-1)}(b)$, $b \in B$, *has Euler characteristic* $\chi(f^{(-1)}(b)) = c$.

A pair $(M, \chi/R)$ *satisfying this conditions is called* Euler structure.

Theorem 3.6 ([13, Thm.6.1]) *Let* $\mathbf{F}_p$ *be a finite prime field.*

Then any structure M *admitting Euler characteristic over all* $\mathbf{Z}/(p^\nu)$, $\nu \geq 1$, *covers* $NS/\mathbf{F}_p$, *and hence also* $PC/\mathbf{F}_p$.

4 Examples of new lower bounds

In this section we give examples of applications of the covering theories and we derive lower bounds for principles of a type that does not seem to be easily amenable to other known methods.

Let T be the theory of fields in the usual language of rings except that $+$ and $\cdot$ are represented by relations, and let T_q be T together with the axiom that the characteristic is some $q > 0$. Consider the following statements obviously valid for finite fields:

Φ_1 A field of characteristic q is perfect:

$$\bigwedge T_q \ \rightarrow \ \forall y \exists x, x^q = y$$

Φ_2 A field is commutative:

$$\bigwedge T \ \rightarrow \ \forall x, y; x \cdot y = y \cdot x$$

Φ_3 A field is not algebraically closed (a special case):

$$\bigwedge T \ \rightarrow \ \exists y_1, y_2 \forall x; x^2 + y_1 x + y_2 \neq 0$$

Φ_4 A field cannot be ordered:

$$\bigwedge T \;\to\; \neg A$$

where A is a sentence in the language of T augmented by $<$ and expressing that $<$ is a linear ordering respecting the field operations.

Φ_5 Two fields of different characteristic cannot share a common universe:

$$\bigwedge T'_{q'} \;\to\; \neg \bigwedge T''_{q''}$$

where q', q'' are two different primes and T', T'' two copies of theory T in disjoint languages.

Theorem 4.1 *All principles* $\Phi_1, \ldots, \Phi_5$ *require proofs of size* $\exp(n^{\Omega(1)})$ *in* $R^*(\log)$.

Proof :

We apply Theorem 3.3. It is enough to find infinite models (fields) in which the respective principles fail.
Φ_1: There is an infinite imperfect field of characteristic q.
Φ_2: Quaternions.
Φ_3: $\mathbf{C}$.
Φ_4: $\mathbf{R}$.
Φ_5: Two countable fields of different characteristic can sit on $\mathbf{N}$.

q.e.d.

Theorem 4.2 *Let* $p > 0$ *be prime. Then principles* Φ_i, $i = 2, 3, 4$, *require proofs of superpolynomial size (i.e., of non-constant degree) in both NS/*$\mathbf{F}_p$ *and PC/*$\mathbf{F}_p$.

Proof :

The real field $\mathbf{R}$ admits Euler characteristic in $\mathbf{Z}$ (see [13] or [5]) and hence also in all $\mathbf{Z}/(p^\nu)$. Quaternions and complex numbers are interpretable in $\mathbf{R}$ and so admit such Euler characteristic too. Thus examples in cases Φ_i, $i = 2, 3, 4$, from the proof of Theorem 4.1 work here equally well (via Theorem 3.6).

q.e.d.

To prove a similar lower bound for Φ_1 it would be enough to construct an imperfect field of characteristic q that admits Euler characteristic in all $\mathbf{Z}/(p^\nu)$, $\nu \geq 1$. To prove a lower bound for Φ_5 one needs to amalgamate two countable fields of different characteristic admitting the Euler characteristic into one structure admitting it too.

5 A generic construction

In this section we describe a class of structures covering a given proof system P. It is a class of certain expansion of models of bounded arithmetic and its definition explicitly refers to P. Thus it is not a good covering theory in the sense that it does not bring new insight about the system. However, it was one of the original motivations for covering theories to understand combinatorics behind constructions of the expansions via model theoretic forcing and it offers some intuition how to search for a useful covering theory for any P.

Let M be an arbitrary countable model of true arithmetic in the usual language, and let $n \in M$ be any non-standard element. Denote by M_n the structure with the universe $\{u \in M \mid u < n\}$ in language L_n: L_n is the language with a relation symbol R_X for every subset $X \subseteq (M_n)^k$, all $k \geq 1$, that is definable in M. Note that M_n satisfies induction for all L_n-formulas.

Let P be a proof system. Proofs, formulas and evaluations are encoded by relations on M_n. Let $Prf_P(a, \alpha, \sigma, \gamma)$ be a first order L_n-formula such that for some $\ell \in \mathbf{N}$ the Σ^1_1 formula $\exists U \subseteq m^\ell; Prf_P(m, \alpha, \sigma, U)$ defines the relation "α is a P-proof of size $\leq m$ of σ".

Similarly let $Sat(a, \beta, \sigma, \delta)$ be a first order formula such that for some ℓ the Π^1_1 formula $\forall V \subseteq m^\ell; Sat(m, \beta, \sigma, V)$ defines the relation "$\beta \subseteq m$ is a truth evaluation satisfying formula $\sigma \subseteq m$".

Such formulas exist by Fagin's theorem (or by a direct construction, cf. [10, 11]).

Consider formula Rfn_P with set variables $\alpha, \beta, \gamma, \delta, \sigma$:

$$\forall x; [Prf_P(x, \alpha, \sigma, \gamma) \wedge \gamma \subseteq x^\ell] \;\rightarrow\; (\delta \subseteq x^\ell \rightarrow Sat(x, \beta, \sigma, \delta))$$

Note that Rfn_P is valid in M_n.

Let L' be any language extending L_n. Define a class $\mathcal{C}_P$ consisting of L'-structures that are expansions of M_n and that satisfy Rfn_P for all instances obtained by substituting for $\alpha, \beta, \gamma, \delta, \sigma$ definable relations. Class $\mathcal{C}_P$ is non-empty; for example, it contains all expansions of M_n in which the new L'-

relations are definable already in M_n. Such structure satisfies Rfn_P because M_n does.

We assume that P is strong enough in the next theorem. If a particular proof system does not satisfy the hypothesis we can replace it by a stronger proof system that does; a covering theory of the stronger system is also a covering theory of the original weaker one.

Theorem 5.1 *Let P be a proof system that contains a Frege system F, and let $\mathcal{C}_P$ be the associated class of structures. Then any structure from $\mathcal{C}_P$ covers P.*

Proof :

Assume that some $N \in \mathcal{C}_P$ does not cover P. That means that there is Φ such that

(i) all $\langle \Phi \rangle_k$, $k \in \mathbf{N}$, have polynomial size P-proofs

(ii) but $\Phi \notin \text{Comb}(N)$.

We use the assumption $P \supseteq F$ to strengthen (i). Let D be a new unary predicate symbol not in L', and let Φ^D be the relativization of Φ to D. Then we have

(i') all $\langle \Phi^D \rangle_k$, $k \in \mathbf{N}$, have polynomial size P-proofs.

This is because there are, given k, polynomial size (DeMorgan) formulas β_{ij} $(i, j < k)$ with atoms for statements $u \in D$ $(u < k)$ such that Frege system F proves in polynomial size that β_{ij} define a graph of a bijection between D and some initial segment $\{0, 1, \ldots, w-1\}$ of k. This is because F can count (see [3] or [11]).

Property (ii) means that there is an L-structure $K \subseteq M_n^t$ definable in N that violates Φ. Structure K defines an evaluation for atoms of $\langle \Phi^D \rangle_k$, $k = n^t$, that does not satisfy the formula; in particular, predicate D is interpreted by the universe of K. On the other hand, as M is a model of true arithmetic, there is $\pi \in L_n$ that is a P proof of $\langle \Phi \rangle_k$. This gives an instance of Rfn_P that is not true, violating the definition of the class $\mathcal{C}_P$.

q.e.d.

Problem 5.2 *For which proof systems P it holds that if $P \vdash_* \langle \Phi \rangle_n$ then also $P \vdash_* \langle \Phi^D \rangle_n$? In particular, does this hold for resolution?*

The simplest case is when L' extends L_n by L, and $N \in \mathcal{C}_P$ expands M_n by an L-structure on M_n with a suitable property. Such expansions can be constructed, in principle, by forcing (see [10], [11]).

We remark that for many proof systems the axiom scheme Rfn_P is actually equivalent to an induction scheme for formulas of particular form (depending on the system) or, equivalently, to a principle that any linear ordering definable by formulas of a particular type has the least element (this motivates Problem 1.6). See [14] for description of this for resolution and its extension, and [11] for a more general information.

One would like to further replace Rfn_P or the equivalent induction axiom by a transparent combinatorial principle, as it is done for $R^*(\log)$ and $NS/\mathbf{F}_p$, $PC/\mathbf{F}_p$ by their covering theories. However, for these proof systems the combinatorial characterization of polynomial provability is valid only for proofs of $\langle\Phi\rangle_n$ and not for proofs of arbitrary sequences of tautologies. One might not be able to replace Rfn_P by a transparent combinatorial principle without the restriction to uniform sequences $\langle\Phi\rangle_n$. No such general characterization is known for any proof system at present. On the other hand, the restriction to $\langle\Phi\rangle_n$ may allow such combinatorial description of polynomial provability for stronger systems. Particularly interesting would be the cases of resolution R and cutting planes proof system CP.

6 Structures as proof systems

If Comb(M) is r.e., then it defines a proof system. Little bit more generally we define

Definition 6.1 *Let $\mathcal{C}$ be a class of structures such that $\bigcap_{M\in\mathcal{C}} Comb(M)$ is recursively enumerable, and let $\mathcal{M}$ be a Turing machine that enumerates the set.*

Define a proof system $A_\mathcal{C}$ as follows: a string π is a proof of formula σ in the system iff

- *π is a quadruple $\langle\Phi, n, w_1, w_2\rangle$ where $\Phi \in \bigcap_{M\in\mathcal{C}} Comb(M)$, w_1 is a computation of $\mathcal{M}$ certifying this membership, and w_2 is an $R^*(\log)$-proof of σ from $\langle\Phi\rangle_n$.*

We shall denote the proof system A_M when $\mathcal{C}$ consists of just a single structure M.

Recall that a proof system P polynomially simulates a proof system Q iff there is a polynomial time algorithm translating any Q-proof π of σ into a P-proof π' of the same formula, and that P simulates Q iff such π' exists polynomially bounded in the length of π (but is not necessarily construable by a polynomial time algorithm).

Lemma 6.2 *Let $\mathcal{C}$ be a class of structures such that $\bigcap_{M \in \mathcal{C}} Comb(M)$ is recursively enumerable. Then*

1. $A_{\mathcal{C}} \vdash_* \langle \Phi \rangle_n$ *iff* $\Phi \in \bigcap_{M \in \mathcal{C}} Comb(M)$.
2. $A_{\mathcal{C}}$ *polynomially simulates* $R^*(\log)$.
3. *Assume* $P \vdash_* \langle Rfn_P \rangle_n$, *all* $n \in \mathbf{N}$. *If all structures in* $\mathcal{C}$ *cover a proof system* P *then* $A_{\mathcal{C}}$ *simulates* P.

Proof :

Parts 1. and 2. of the lemma are direct consequences of the definition and Theorem 3.3. We shall use bounded arithmetic for Part 3..

By the hypothesis the proof system P polynomially proves formulas $\langle Rfn_P \rangle_n$. Hence $Rfn_P \in \mathrm{Comb}(\mathcal{C})$. Further, $R^*(\log)$ augmented by instances of $\langle Rfn_P \rangle_n$ simulates P; this follows from the fact that $R^*(\log)$ simulates theory $S^2_2(\alpha)$ ([9], [14]) and this theory proves that Rfn_P implies that all σ's with a P-proof are tautologies. In particular, $S^2_2(\alpha)$ proves the implication

$$(\delta \subseteq x^\ell \wedge Sat(x, \beta, \sigma', \delta)) \ \rightarrow \ \sigma$$

where β is the assignment consisting of $\overline{p}$, atoms of σ, and σ' in the antecedent is the set coding the formula σ.

q.e.d.

Note that the hypothesis of part 3. is satisfied by many proof systems, e.g. by $R(\log)$ or F (cf. [15, 11]). In fact, with a more sophisticated formulation of Rfn_P one can show that $R^*(\log)$ also satisfies the hypothesis.

The first example restates the observation after Definition 1.1.

Example 6.3 *M is a sound model of $I\Sigma^0_1$ then A_M is defined (i.e., Comb(M) is recursively enumerable) and $A_M = R^*(\log)$.*

Recall that M is pseudo-finite iff it is elementarily equivalent to an ultraproduct of finite structures.

Example 6.4 *If M is pseudo-finite then Comb(M) is a complete Π^0_1 set and hence A_M is not defined.*

This is because $\text{Comb}(M)$ is then exactly the set of sentences true in finite structures and Trachtenbrot's theorem applies.

Example 6.5 *Weak Euler characteristic is a function satisfying properties 1.-4. of Definition 3.5. The class of structures admitting weak Euler characteristic has recursively enumerable combinatorics.*

The combinatorics of the class is axiomatized by instances of the *ontoPHP* principle, as by [13] this principle characterizes weak Euler structures.

Note that examples from Problem 1.7 would also give examples of these new "structure based" proof systems.

References

[1] J. Ax, The elementary theory of finite fields, *Annals of Mathematics*, **88**, (1968), pp.239-271.

[2] 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.

[3] S. R. Buss, The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic*, **52**, (1987), pp.916-927.

[4] M. Clegg, J. Edmonds, and R. Impagliazzo, Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proceedings of the 28th ACM Symposium on Theory of Computing*, ACM Press. (1996), pp.174-183.

[5] L. van den Dries, *Tame topology and o-minimal structures*, London Math. Soc. Lecture Note Series, Vol. **248**, (1998), Cambridge University Press.

[6] P. Hájek and P. Pudlák, *Metamathematics of first-order arithmetic*, Perspectives in Mathematical Logic, (1993), 460 p. Springer-Verlag.

[7] Hodges, W., *Model Theory*, Cambridge University press, (1993).

[8] J. Krajíček, Some Theorems on the Lattice of Local Interpretability Types, *Zeitschr. f. Mathematikal Logik u. Grundlagen d. Mathematik*, **31**, (1985), pp. 449-460.

[9] J. Krajíček, Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, **59(1)** (1994) 73-86.

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

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

[12] 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.

[13] J. Krajíček, Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets, *Proc. London Mathematical Society*, **(3)81**, (2000), pp.257-284.

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

[15] J. Krajíček, 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.

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

[17] S. Riis, Making infinite structures finite in models of second order bounded arithmetic, in: *Arithmetic,Proof Theory and Computational Complexity*, eds. P. Clote and J. Krajíček, (1993) pp.289-319. Oxford University Press.

[18] S. Riis, A complexity gap for tree-resolution, preprint, BRICS Report Series nb. RS-99-29, (September 1999).

Mailing address:
Mathematical Institute
Academy of Sciences
Žitná 25
Prague 1, CZ - 115 67
The Czech Republic
krajicek@math.cas.cz