On the weak pigeonhole principle

Jan Krajíček*

Mathematical Institute, Academy of Sciences, Prague

Abstract

We investigate the proof complexity, in (extensions of) resolution and in bounded arithmetic, of the weak pigeonhole principle and of Ramsey theorem.

In particular, we link the proof complexity of these two principles. Further we give lower bounds to the width of resolution proofs and to the size of (extensions of) tree-like resolution proofs of Ramsey theorem.

We establish a connection between provability of WPHP in fragments of bounded arithmetic and cryptographic assumptions (the existence of one-way functions).

In particular, we show that functions violating WPHP_n^{2n} are one-way and, on the other hand, that one-way permutations give rise to functions violating PHP_n^{n+1}, and that strongly collision-free families of hash functions give rise to functions violating WPHP_n^{2n} (all in suitable models of bounded arithmetic).

Further we formulate few problems and conjectures; in particular, on the structured PHP (introduced here) and on the unrelativised WPHP.

The symbol WPHP_n^m (with any $n < m \leq \infty$) will denote both propositional and arithmetic formalizations of the weak pigeonhole principle; in the latter case I write $\mathrm{WPHP}_n^m(R)$, where R is a binary relation symbol. The qualification *weak* means $m \geq 2n$ and that is the case studied here. The propositional formalization is a set of clauses in atoms $p_{i,j}$ for $i < m$ and $j < n$:

$$\{p_{i,0}, \ldots, p_{i,n-1}\} \tag{1}$$

for each $i < m$, and

$$\{\neg p_{i,k}, \neg p_{j,k}\} \tag{2}$$

for each $i < j < m$ and $k < n$, and

$$\{\neg p_{i,\ell}, \neg p_{i,k}\} \tag{3}$$

*Partially supported by cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic), by the grant #$A1019901$ of the Academy of Sciences of the Czech Republic, and by the EPSRC fellowship number R/L01176.

for each $i < m$ and $\ell < k < n$. If $m = \infty$ we take infinitely many such clauses for $i, j < \omega$. The arithmetic version $\mathrm{WPHP}^m_n(R)$ is the formula

$$(\exists i < j < m \exists k < n; R(i,k) \wedge R(j,k)) \vee (\exists i < m \forall j < n; \neg R(i,j)) \vee$$

$$(\exists i < m \exists \ell < k < n; R(i,\ell) \wedge R(i,k))$$

(The parameter m is omitted in the formula when $m = \infty$.)

Haken [7] proved that any resolution refutation of PHP^{n+1}_n requires at least $\exp(\Omega(n))$ steps. His method was adapted by Buss and Turán [3] to a lower bound $\exp(\Omega(\frac{n^2}{m}))$ for WPHP^m_n. When $m \geq n^2$ this yields no lower bound at all, and it remains open what are the lengths of resolution proofs for these m.

Another line of research concerns systems of bounded arithmetic introduced by Buss [1]. In particular, it is known that the systems $T^i_2(\alpha)$ are different and there are some non-conservativity results (see Chiari and Krajíček [4] for an overview). The simplest open conservativity relation is whether $T_2(\alpha)$ (or $T^3_2(\alpha)$, in particular) is $\Sigma^b_2(\alpha)$-conservative over $T^2_2(\alpha)$, and various bounded formulas that could witness the conjectured non-conservativity were put forward in Chiari and Krajíček [4, 5], $\mathrm{WPHP}^{2n}_n(R)$ and Ramsey theorem among them.

The proof of the weak pigeonhole principle in theory $T_2(R)$ by Paris, Wilkie and Woods [19] formalizes in $T^3_2(R)$ (see Krajíček [10, Thm.11.2.4] for this calculation[1]) while it is shown in [4] that $\mathrm{WPHP}^{2n}_n(R)$ is not provable in $T^1_2(R)$. Hence the provability of $\mathrm{WPHP}^{2n}_n(R)$ in $T^2_2(R)$ is the only open question (see footnote to L.6.4.). Moreover, the proof from [19] also shows that either all or none of $\mathrm{WPHP}^{2n}_n(R)$, $\mathrm{WPHP}^{n^2}_n(R)$, $\mathrm{WPHP}^{\infty}_n(R)$ are provable in $T^2_2(R)$.

It has been little noticed that these two open problems are, in fact, quite related. This is because in the well known correspondence between propositional proof systems and bounded arithmetic theories (in the translation of Paris and Wilkie [18], see [10, Sec.9.1] for details) the resolution proof system corresponds to a theory strictly stronger than $T^1_2(R)$ but included in $T^2_2(R)$, and $T^2_2(R)$ itself corresponds to an extension $R(\log)$ of R (see Section 1 for the definition).

The present paper gives several results on resolution and bounded arithmetic, on proof complexity of the WPHP and of Ramsey theorem. In particular, we link the proof complexity of these two principles. Further we give lower bounds to the width of resolution proofs and to the size of (extensions of) tree-like resolution proofs of Ramsey theorem.

Although these results are new they are, in my view, in near vicinity of results and methods that are (or ought to be) known. To remedy this I also present several known results and methods, specialized to resolution and $T^2_2(\alpha)$. For example, I give an infinitary criterion for $R^*(\log)$ lower bounds - an extension of tree-like R - that is an immediate corollary of a known statement about search trees from Krajíček [10].

[1]Note that $\mathrm{PHP}(R)$ is defined as the onto-version in that calculation.

I also show that functions violating WPHP_n^{2n} are one-way and, on the other hand, that one-way permutations give rise to functions violating PHP_n^{n+1}, and that strongly collision-free families of hash functions give rise to functions violating WPHP_n^{2n} (all in suitable models of bounded arithmetic). These results are not difficult but they are perhaps a part of the paper pointing most towards new directions promising for further research.

I also formulate few problems and conjectures; in particular, on the structured PHP (introduced here) and on the unrelativised WPHP.

For background I refer the reader to monograph [10]; I often accompany original references by a reference to a place in [10]. The conservativity problem was previously studied in Chiari - Krajíček [4, 5], and I use few facts from there.

A convention: The phrase *exponential size* means size $\exp(n^{\Omega(1)})$.

1 Resolution and its extensions

Resolution R is naturally a subsystem of sequent calculus LK, allowing no connectives except the negation. The following definition augments R so as to correspond to LK-proofs of the Σ-depth 0 (as defined in [8] or [10, Def. 12.2.3]). (We sometimes use the union and disjunction signs interchangeably.)

Definition 1.1 *(a) R^+ is a refutation proof system working with clauses C formed by conjunctions D_i of literals $\ell_{i,j}$:*

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

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 $f : \mathbf{N} \rightarrow \mathbf{N}$ 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 abuse the terminology and use a phrase *$R(f)$-proofs of size S* rather than R^+-proofs of $R(f)$-size S.

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

As on various previous occasions I shall denote by the superscript star the tree-like versions of proof systems: R^*, $R(f)^*$.

2 Bounded formulas and sets of clauses

The first-order formulation of $\mathrm{WPHP}_n^m(R)$ is a $\bigvee \exists \bigwedge \forall$ - formula. In general, negations of formulas that are built from basic formulas (atomic or their negations) in a relational language L by first applying $\bigwedge$'s and $\forall$'s and then $\bigvee$'s and $\exists$'s will translate, as $\neg\mathrm{WPHP}_n^m(R)$ does, to a CNF-formula, a set of clauses. Let us call such formulas shortly DNF_1**-formulas**.

Other DNF-like formulas can be obtained from particular second order formalizations of combinatorial properties. To illustrate this I recall definitions of two principles, Ramsey theorem and Tournament principle (cf. [10, p.233]).

Definition 2.1 *(a)* $RAM_n(\alpha)$ *is a* $\Sigma_1^b(\alpha)$ *- formula*

$$[\exists i < j < n;\ \alpha(i,j) \not\equiv \alpha(j,i)] \ \vee\ \exists X \subseteq \{0,\dots,n-1\};\ |X| = \lfloor \frac{\log n}{2} \rfloor$$

$$\wedge\ [(\forall x, y \in X; x \neq y \rightarrow \alpha(x,y))\ \vee\ (\forall x, y \in X; x \neq y \rightarrow \neg\alpha(x,y))]$$

formalizing Ramsey's statement $n \longrightarrow (\lfloor \frac{\log n}{2} \rfloor)^2_2$*, i.e. that the undirected graph with vertices* $n = \{0, 1, \dots, n-1\}$ *and edges* $\{\{i,j\} \mid \alpha(i,j)\}$ *has a homogeneous subset* X *(a clique or an independent set) of size at least* $\lfloor \frac{\log n}{2} \rfloor$.

The propositional version RAM_n *has variables* x_e *for all possible edges* $e \in [n]^2$*, and the clauses*

$$\bigvee_{e \in [X]^2} x_e \quad \textit{and} \quad \bigvee_{e \in [X]^2} \neg x_e$$

for all possible $X \subseteq n$ *of size* $\lfloor \frac{\log n}{2} \rfloor$.

(b) $TOUR_n(\alpha)$ *is a* $\Sigma_1^b(\alpha)$ *- formula*

$$[\forall i < j < n;\ \alpha(i,j) \not\equiv \alpha(j,i)] \ \longrightarrow$$

$$\exists X \subseteq \{0,\dots,n-1\};\ |X| = 2\log n\ \wedge\ [(\forall x \in n \setminus X \exists y \in X; \alpha(y,x))$$

formalizing Tournament principle: a tournament of size n *has a dominating set of size* $\leq 2\log(n)$.

The propositional version $TOUR_n$ *has variables* $x_{i,j}$ *for all possible directed* (i,j)*,* $i \neq j$*, and the clauses*

$$x_{i,j} \vee x_{j,i} \quad \textit{and} \quad \neg x_{i,j} \vee \neg x_{j,i}$$

for all $i \neq j$*, and*

$$\bigvee_{i \in n \setminus X} \bigwedge_{j \in X} \neg x_{j,i}$$

for all possible $X \subseteq n$ *of size* $2\log n$.

The $2\log n$ bound in TOUR_n is somewhat arbitrary and obviously not optimal. However, it is unknown even if TOUR_n is provable in full bounded arithmetic $T_2(\alpha)$, even with $\log n$ replaced by $(\log n)^{O(1)}$ (such a change may be important for provability).

Both these formulas have a form extending the DNF_1-form by allowing also second order existential quantifier $\exists^{(2)}X(|X| \leq f(n))$ ranging over subsets X of the universe of size $\leq f(n)$ (usually $f(n) = (\log n)^{O(1)}$), and universal quantification $\forall i \in X$ bounded to elements of X's. We shall call them **DNF_2-formulas** for short.

The propositional versions consist, in general (like for TOUR_n), of $R(\log)$-clauses, i.e. clauses formed by conjunctions of literals, the conjunctions having size $\leq f(n)$. The size of the set of associated clauses is $n^{O(f(n))}$, if the second order quantifier is restricted to sets of size $\leq f(n)$. In case of RAM_n and TOUR_n this is $O(\log n)$. Note that the relation $A \models \Phi$, for Φ a DNF_1- or a DNF_2- formula in a general language L, is definable by a $\Sigma^b_2(L)$-formula, provided $f(n) = \log(n)^{O(1)}$.

3 Resolution and arithmetic

There are several relations between subsystems of bounded arithmetic and extensions of resolution. I shall formulate these facts for theories with the smash function #, relating them to quasi-polynomial size propositional proofs. This is because the theories with the smash function are the ones most commonly used. However, similar relations hold with theories without the smash function and polynomial size propositional proofs.

Theorem 3.1 (Krajíček [8, 1.2 and 2.2], [11, Cor.6.2]) *Let a DNF_1- or a DNF_2- formula Φ in a relational language L disjoint from the language of T_2 be provable in (a) $T^1_2(L)$, or (b) $T^2_2(L)$, respectively.*

Then the associated sets of clauses Φ_n have quasi-polynomial size refutations in systems (a) in $R^*(\log)$ and in R, or (b) in $R(\log)$, respectively.

Proof :

Case (b) was proved in [8, 1.2 and 2.2] (or see [10, L. 12.2.1]). Case (a) is a corollary of that proof and was given in [11, Cor.6.2]. To explain this let me recall now the main steps of the proof of (b).

An arithmetic proof in $T^2_2(L)$ translates (after suitable cut-elimination) into an LK-proof that is tree-like, the number of formulas per sequent is bounded by a constant, it has quasi-polynomial size, and every formula has depth ≤ 3 with the depth 3 formulas being conjunctions of disjunctions of poly-logarithmic size conjunctions.

First, the first two properties are used to eliminate the depth 3 connectives; the resulting proof is polynomially longer and still tree-like. The tree-likeness is then used to reduce the next level of connectives, again with a polynomial increase only, resulting in an LK-proof in which all formulas are poly-logarithmic size conjunctions. That is the required $R(\log)$ proof.

In case (a), starting with a $T^1_2(L)$ proof, everything has one less depth. In particular, the first step yields a quasi-polynomial size $R^*(\log)$ proof. Applying the reduction of the depth via tree-likeness once more yields an R-proof (see [11, Cor.6.2]).

q.e.d.

The link between arithmetic and proof systems also allows to lift independence results to lower bounds and, more importantly, methods of independence proofs to lower bound proofs. As an example, I shall state a criterion for lower bounds for $R^*(\log)$. The first one is a weaker version of [10, L.9.5.2] (that lemma talks about search trees[2]).

Theorem 3.2 (Krajíček [10, L.9.5.2]) *Let Φ be a DNF_1-formula in a relational language L that can be violated in an infinite structure.*

Then the corresponding sets of clauses Φ_n require exponential size $R^*(\log)$-proofs.

Similarly as [10, L. 9.5.2] generalized (by a different proof) Riis's independence criterion for $S^2_2(\alpha)$ (cf. Riis [21] or [10, Sec.11.3]) the following fact extends analogously his [21, Thm.11] (or see [10, Thm.11.3.4]

Theorem 3.3 *Let $\Phi = \exists X(|X| = \log^k(n)), \phi(X, n)$ be a DNF_2-formula in a relational language L. Assume that there is an infinite structure in which $\exists X, \phi$ is not witnessed by a finite X.*

Then Φ_n require exponential size $R^*(\log)$-proofs.

While Theorem 3.2 is, in fact, a criterion valid in the iff-form (if $\neg\Phi$ has no infinite model then Φ is provable in the predicate logic alone from the assumption that the universe has $\geq c$ points some $c \geq 1$ - and use Theorem 3.1) Theorem 3.3 is not. An example is given by Ramsey theorem; Theorem 5.2 yields exponential lower bound for $R^*(\log)$-proofs of RAM_n while the hypothesis of the theorem obviously fails.

Let us remark that another proof of Theorems 3.2 and 3.3 is possible: reduce the statements directly to related statements about bounded arithmetic $S^2_2(\alpha)$. Namely, it is sufficient to prove in the theory the soundness of $R^*(\log)$-proofs. For this one needs to augment the data defining the proof by a log-depth tree structure simulating a Spira-type search through the tree.

It would be very interesting if an infinitary criterion like these existed also for R. The only other proof system for which something analogous is known is

[2]S. Riis informed me that he is preparing a manuscript on Theorem 3.2 and related issues.

the constant-degree polynomial calculus (or Nullstellensatz); the role of infinite structures is played by Euler structures (see Krajíček [12]).

Remark: A recent paper by Kullmann [16] contains extensive information on R^*.

4 Non-standard models and lower bounds

Let M be an arbitrary countable model of true arithmetic in the language of T_2, and $n \in M$ any non-standard element. Denote by M_n the structure with the universe

$$\bigcap_{\epsilon} \{u \in M \mid u < 2^{n^\epsilon}\} = \bigcup_{\iota} \{u \in M \mid u < 2^{n^\iota}\}$$

with ϵ's ranging over all positive standard rationals and ι's over infinitesimal rationals. The structure of M_n consists of the reduct of M to the universe, together with a unary predicate symbol R_X for every bounded subset $X \subseteq M_n$ that is coded in M. (Instead of $R_X(u)$ I write $u \in X$.)

Let L_n denotes the language of M_n. Note that M_n satisfies induction for all bounded L_n-formulas.

Let $\forall_1^{\leq b} \bigwedge$ denote the set of $L_n \cup L$-formulas built from basic formulas by conjunctions and bounded universal quantification. $L - \forall_1^{\leq b} \bigwedge$ is the least number principle for such formulas.

Theorem 4.1 *Let T, P be one of the following pairs of a theory and a proof system: $T_2^2(L_n, L)$ and $R(\log)$, $T_2^1(L_n, L) + L - \forall_1^{\leq b} \bigwedge$ and R.*

For arbitrary structure M_n of the form as above the following two statements are equivalent:

1. *There is an expansion of M_n to a model (M_n, L) of T in which Φ_n fails.*
2. *Φ_n requires exponential-size P-proofs.*

Proof :

This is a standard argument (going back to Paris and Wilkie) that I repeat here for reader's benefit; the novel part is the exact correspondence for the pairs T, P. We also use non-standard models in Section 5.

Assume that the lower bound is not true. By compactness there is a non-standard model of true arithmetic, non-standard $n \in M$, and a P-proof represented by a bounded coded subset π of M_n, such that π is a P-refutation of Φ_n in M (and hence in M_n).

Take some expansion (M_n, L) provided by the first statement. This defines an evaluation of atoms of Φ_n that satisfies all initial clauses in π. However, π is sound in M_n as the soundness is provable in T. That is a contradiction.

The opposite implication follows by a model theoretic argument. Let Cl be the set of all clauses in M formed from literals occurring in the set of clauses Φ_n corresponding to Φ. Let $H := Cl \cup \{\neg C \mid C \in Cl\}$. We shall construct set $G \subseteq H$ such that

1. All clauses of Φ_n are in G.
2. C or $\neg C$ is in G, for any $C \in Cl$.
3. If $C \in G$ then $\{\ell\} \in G$ for some $\ell \in C$.
4. If $\neg C \in G$, $\{\neg \ell\} \in G$ for all $\ell \in C$.
5. If the sequence of clauses $\langle C_0, \ldots, C_t \rangle$ from Cl is defined by an L_n-relation symbol, $t \in M_n$, then either there is minimal $i_0 \leq t$ such that $\neg C_{i_0} \in G$, or $\{C_0, \ldots, C_t\} \subseteq G$.
6. There are no π and X in L_n such that $X \subseteq G$ and π is an P-refutation of X.

(We use the name G as, in fact, it is a generic set in an appropriately defined forcing - see [9] or [10, Sec.12.7].)

G is built in countable many steps, arranging in M consecutively the conditions for all C and all sequences $\langle C_0, \ldots, C_t \rangle$ from M_n. The inductive process can start as the set of clauses of Φ_n has no P-refutation in M_n, by the hypothesis. The details are as in the case of V_1^1 and EF in [9]; or see [10, Sec.9.4]. Note that we could not arrange the last but one condition with tree-like proofs.

G defines, by conditions 2. - 4., an interpretation of L in M_n. Φ_n fails by the first condition, while the last but one condition implies that the expansion is a model of the least number principle for $\forall_1^{\leq b} \bigwedge$ formulas.

This proves the statement for $T_2^1(L) + L - \forall_1^{\leq b} \bigwedge$ and R; the case of $T_2^2(L)$ and $R(\log)$ is analogous.

q.e.d.

Remark: The forcing method used for constructions of model of $L\exists_1$ and T_2^1 cannot be used to construct suitable expansions. Namely, let $\mathbf{P}$ be the set of all injective maps $p : dom(p) \longrightarrow n$ coded in M, partially ordered by inclusion. One uses as forcing notions suitable subclasses $\mathbf{Q} \subseteq \mathbf{P}$. A generic set $G \subseteq \mathbf{Q}$ then defines a generic map $f := \bigcup G$.

If one forces with the subclass consisting of p's of standard size then the generic map f is a bijection between M_n and n, and (M_n, f) satisfies the minimization principle for the existential $L_n(f)$-formulas. This was proved by Paris and Wilkie [18], or see [10, Thm.12.7.1]. It is noticed in [10, Sec.12.7,pp.273-4] that taking instead maps p of size bounded above by some n^ι, ι positive infinitesimal rational, yields a bijection $f : M_n \longleftrightarrow n$ satisfying the minimization principle for $\Sigma_1^b(L_n, f)$-formulas (and hence $T_2^1(L_n, f)$). On the other hand, such generic f will never satisfy $T_2^2(f)$ as, for example, the formula

$$\exists u_1 < u_2 < n; u_1 + x = u_2 \ \wedge \ (\forall u_1 \leq v_1 < v_2 \leq u_2; f(v_1) \equiv f(v_2) \pmod 2)$$

will be satisfied in the generic extension by any x smaller than some n^ι, ι positive infinitesimal rational, but not by any bigger one, and hence $\Sigma_2^b(f)$- induction fails.

5 Ramsey theorem

Pudlák [20] showed that $\mathrm{RAM}_n(\alpha)$ is provable in $T_2(\alpha)$ (in fact, in $T_2^5(\alpha)$ as computed in [10, Thm. 12.1.3]) by reducing it to the weak pigeonhole principle for a map definable from α. On the other hand, Chiari - Krajíček [5] proved that $\mathrm{RAM}_n(\alpha)$ is independent of $T_2^1(\alpha)$ and they put it forward as a candidate for a formula independent from $T_2^2(\alpha)$ as well. We derive this conjecture from a hypothesis about the lengths of proofs of $\mathrm{WPHP}_n^{n^4}$.

Theorem 5.1 *Let $g : \mathbf{N} \to \mathbf{N} \setminus \{0\}$ be a function. Assume that $WPHP_n^{n^4}$ requires exponential size $R(2g)$-proofs.*

Then RAM_n requires exponential size $R(g)$-proofs.

Proof :

First consider the case $g = \log(n)$, so that we can use Theorem 4.1; the general case is explained at the end of the proof.

Let M be, as before, a nonstandard model of true arithmetic, and let $n \in M$ be a non-standard number of the form 2^s. Take M_n of the form as earlier, and (M_n, f) the expansion provided by Theorem 4.1, assuming the hypothesis of the theorem. That is, (M_n, f) is a model of $T_2^2(L_n, f)$ in which f maps injectively n^4 into n.

By Erdös [6] there is a graph $G \in M$, $G = (n, E)$ containing no homogeneous set of size $2s = 2\log n$. We shall use E also as the name for the predicate for E in L_n.

Define in (M_n, f) graph $G' = (n^4, E')$ by

$$xE'y \ \equiv_{\mathrm{def}} \ f(x)Ef(y)$$

E' is $\Delta_1^b(R, E)$ - definable, so (M_n, f) satisfies $T_2^2(E')$. If $\mathrm{RAM}_n(\alpha)$ were provable in $T_2^2(\alpha)$, or even just RAM_n had an $R(\log)$-proof in M_n, there would be $X' \subseteq n^4$, $X' \in M_n$, of size $2\log n$ and homogeneous in G'.

Clearly then $X := f(X')$ is homogeneous in G. Moreover, as X' as well as f restricted to X' are coded in M_n so is X and we have $|X'| = |X| = 2\log n$. All sets of $O(\log n)$ size are coded in a model of $S_2^1(L_n, f)$, so X is definable without f. This contradicts, in M, the choice of G without a homogeneous set so large.

Finally, note that the argument works equally well for $R(g)$ in place of $R(\log)$, as the (non-)edge $\{x,y\}$ in G' is defined as $\bigvee(f(x)=i \wedge f(y)=j)$ with the disjunction over all (non-)edges $\{i,j\}$ in G, i.e. an $R(g)$-proof of RAM_n translates into $R(2g)$-proof of $\mathrm{WPHP}_n^{n^4}$.

q.e.d.

The proof of the following statement is a non-uniform version of the proof that $T_2^1(R)$ does not prove $\mathrm{RAM}_n(R)$ from Chiari-Krajíček [5]. I shall give it explicitly as we shall use a variant of the argument later on. (It also gives a hint to a reader not familiar with [10] how Theorems 3.2 and 3.3 are proved following [10, Sec. 11.3].)

Theorem 5.2 *Any $R^*(\log)$-proof of RAM_n requires exponential size.*

Proof :

Let the $R^*(\log)$-proof has size 2^t and all conjunctions in it size $\leq t$. Turning the proof upside down we can use it as a search tree. Namely, given a graph H we walk in the tree from the root (the empty clause) down to a leaf (an axiom) on clauses false for H. This finds a set of size at least $\frac{\log n}{2}$ homogeneous in H. Moreover, we walk through the proof tree in the Spira-type fashion: from a node determining a subtree T_0 we go to its node determining a subtree T_1 of T_0 of size $\frac{|T_0|}{3} \leq |T_1| \leq \frac{2|T_0|}{3}$. Hence the resulting search tree has depth $O(t)$ only.

Let G be the Erdös graph (as in the proof of Thm. 5.1) but on $n^{1/4}$ vertices. I.e., it has no homogeneous set of size $\geq \frac{\log n}{2}$. Walking through the search tree we shall define a part of graph H on n vertices. After k steps we will have a partial isomorphism ψ_k between $\leq k2t$ vertices of H and G. In the $(k+1)$st step, querying an $R(\log)$-clause $C = \bigvee_i D_i$, $D_i = \bigwedge_j \ell_{i,j}$,consider two cases.

Either ψ_k can be extended to make one of D_i true, or not. In the former case answer the query YES and let ψ_{k+1} be a minimal such extension of ψ_k. Note that $|\psi_{k+1} \setminus \psi_k| \leq 2|D_i| \leq 2t$.

In the latter case answer NO and take $\psi_{k+1} := \psi_k$.

We may continue with this strategy as long as there is a room for the extensions, i.e. as long as $|\psi_k| \leq n^{1/4}$, for all k.

At the end (i.e. at the leaf) we have a partial isomorphism ψ in whose domain is a homogeneous set X of size $\geq \frac{\log n}{2}$. That is impossible as its image in ψ would be a homogeneous set in G but G has no so large homogeneous sets.

Hence $t > (1/2)n^{1/4}$.

q.e.d.

Theorem 5.2 demonstrates that Theorem 3.3 is not a criterion but only a sufficient condition, as we cannot use it to prove Theorem 5.2. On the other hand, there obviously exists an infinite tournament without a finite dominating set, hence Theorem 3.3 implies

Theorem 5.3 *Any* $R^*(\log)$*-proof of* $TOUR_n$ *requires exponential size.*

Perhaps I may remind the reader here of an

Open problem: *Does* $TOUR_n$ *have polynomial-size (or even sub-exponential size) constant-depth Frege proofs?*

The clauses of RAM_n have size $\leq (\log n)^2$. The following result shows that the width of any R-proof, i.e. the maximum size of a clause in a proof, must be $n^{1/4}$.

Theorem 5.4 *Any* R*-proof of* RAM_n *must have width at least* $(1/2)n^{1/4}$.

Proof :

The proof is similar to the proof of Theorem 5.2 but with some differences. Let π be an R-refutation of RAM_n. Assume that the width is w. Turning π upside down determines a branching program solving the same search problem as in the proof of Theorem 5.2.

As before, we construct in steps partial isomorphisms ψ_k from the n vertices of H into vertices of Erdös graph G on $n^{1/4}$ vertices. They are constructed differently, however.

Let $C_0 = \emptyset, C_1, \ldots, C_k$ be the path in π that we walked through so far in k steps. Let $supp(C)$ be the set of all vertices occurring in edges corresponding to literals in C. Put $\psi_0 := \emptyset$. It holds that $dom(\psi_i) = supp(C_i)$.

Assume that $C_k = C' \cup C''$ was inferred in π by the inference:

$$\frac{C' \cup \{p_e\} \quad C'' \cup \{\neg p_e\}}{C_k}$$

with $e = \{i, j\}$. Put $\phi := \psi_k \downarrow (supp(C'))$. If ϕ can be extended to i, j so that p_e is false in G, take for ψ_{k+1} one such extension. Otherwise take for ψ_{k+1} any extension of $\psi_k \downarrow (supp(C''))$ to i, j making p_e true. In the former case $C_{k+1} := C' \cup \{p_e\}$, in the latter $C_{k+1} := C'' \cup \{\neg p_e\}$.

As $|\psi_k| \leq 2|C' \cup C''| \leq 2w$, this can be done as long as $2w \leq n^{1/4}$.

q.e.d.

Remark: Krishnamurthy and Moll [15] consider critical Ramsey formulas: For a given $r \geq 3$ take minimal m satisfying the Ramsey relation $m \to (r)^2_2$, and let α_r be the Ramsey formula like RAM_m but with X's ranging over sets of vertices of size r. They proved ([15, Cor.4.1.9]) that the width of R-proofs of α_r must be at least $m/2 - 1$. They also proved an exponential lower bound for Davis-Putnam Procedure (essentially R^*) proofs of the formulas.

The minimal m satisfies $2^{r/2} \leq m \leq 2^{2r}$ and for $r := \frac{\log n}{2}$ it may be that $m << n$. Hence our lower bounds for RAM_n are stronger statements.

6 WPHP in $T^2_2(R)$

Let us denote by $ontoPHP$ the onto version of PHP speaking about bijections rather than injections. The following is well known.

Theorem 6.1 (Paris, Wilkie and Woods [19]) *Let $m = 2n$ or n^2 or ∞.*

1. *$T^3_2(R)$ proves any $WPHP^m_n(R)$.*
2. *$T^2_2(R)$ proves any $onto WPHP^m_n(R)$.*
3. *There are g and h, $\Delta^b_1(R)$-definable in $S^1_2(R)$ such that $S^1_2(R)$ proves the implications*
$$\neg\, WPHP^{2n}_n(R) \longrightarrow \neg\, WPHP^{n^2}_n(g)$$
and
$$\neg\, WPHP^{n^2}_n(R) \longrightarrow \neg\, WPHP^{\infty}_n(h)$$
Same statements hold for the onto version.

By Theorem 3.1 we get

Corollary 6.2 *The $onto WPHP^m_n$, for $m = 2n, n^2, \infty$, has quasi-polynomial $R(\log)$-proofs.*

In fact, as the proof in [8] shows, the conjunctions in the $R(\log)$-proofs have size only $O(\log n)$ rather than generic $(\log n)^{O(1)}$.

An immediate corollary of Theorems 6.1 and 3.1 points to a possible approach to proving resolution lower bounds for $\mathrm{WPHP}^{n^2}_n$ and WPHP^{∞}_n. Namely, instead of trying to improve the current methods to $m = n^2$, improve the lower bound for $m = 2n$ from R to $R(\log)$.

Corollary 6.3 *Assume that $WPHP^{2n}_n$ requires exponential size $R(\log)$-proofs. Then both $WPHP^{n^2}_n$ and $WPHP^{\infty}_n$ require exponential size $R(\log)$-proofs as well.*

By Chiari - Krajíček [4] $S^2_2(f)$ does not prove $onto\mathrm{WPHP}^m_n(f)$. Thus the remaining open problem is whether $T^2_2(f)$ proves (the non-onto) $\mathrm{WPHP}^m_n(f)$. In this connection it is perhaps interesting to note that Buss - Pitassi [2] proved that minimum sizes of R-proofs of WPHP^m_n and $onto\mathrm{WPHP}^m_n$ are polynomially related.

Analysing what makes the increase of quantifier complexity in the proofs of the non-onto version we observe that a function in a model of $T^2_2(f)$ violating the principle $\mathrm{WPHP}^{n^2}_n(f)$ must be one-way.[3]

[3]After this paper circulated for some time, [17] showed that $T^2_2(f)$ proves $\mathrm{WPHP}^{n^2}_n(f)$ (see `http://www.math.cas.cz/~krajicek/mpw.ps` for a short presentation of their proof via bounded arithmetic). I keep L.6.4 as the same construction works for subtheories of $T^2_2(f)$ corresponding to weaker subsystems of $R(\log n)$.

Lemma 6.4 *Let M be a model of $T^2_2(f) + \neg WPHP^m_n(f)$, for $m = 2n, n^2, \infty$.*

Then f is one-way in the following sense: the inverse function $f^{(-1)}$ (defined arbitrarily outside $rng(f)$) is not $\Delta^b_1(f)$ definable in the model, i.e. it is not computable by a polynomial-time Turing machine with oracle f even with a polynomial advice. In particular, $rng(f)$ is also not $\Delta^b_1(f)$ definable.

To explain this I shall refer to the proof of Theorem 6.1 as given in [10, Thm.11.2.3,pp.213-4].

The formula $A_g(r)$ is Π^b_3; however, if the map violating the WPHP were not onto, then the same construction gives only Π^b_4-formula as the function $\ell(i,x)$ is not $\Delta^b_1(f)$ anymore (because one needs to condition upon whether or not $\ell(i,x)$ is in the range of the map). But assuming that the inverse map $f^{(-1)}$ is $\Delta^b_1(f)$ definable, the function $\ell(i,x)$ is also $\Delta^b_1(f)$ definable as the numbers v, w in the second clause of the definition of $\ell(i,x)$ (on [10, p.214]) are just projections of $f^{(-1)}(u)$. Hence the assumption that f is not one-way implies that the proof goes through in $S^3_2(f)$ and hence also in $T^2_2(f)$, contradicting the hypothesis that f violates $\mathrm{WPHP}^{n^2}_n(f)$ in a model of $T^2_2(f)$.

A simple example of this situation (for a reader not familiar with [10]) is this: Let $f : n \times n \to n$. Consider the property $\phi(u) := \exists j < n; f(0,j) = u$. Then ϕ is $\Sigma^b_1(f)$ for all f, but when f is onto n it is, in fact, $\Delta^b_1(f)$ as it is equivalent also to $\forall i, j < n; f(i,j) = u \to i = 0$.

We can complement Lemma 6.4 in a sense.

Theorem 6.5 *Let f be a length preserving, injective polynomial-time function. Assume that f is one-way in the sense of Lemma 6.4, i.e. $f^{(-1)}$ is not computable by polynomial size circuits.*

Then there is a model M of S^1_2 and an infinite n in it such that f is an injective map from n into a proper subset of n. In particular, adding one value to f, f violates PHP^{n+1}_n.

In fact, if the hypothesis is satisfied only in a model N of S^1_2 then M can be a Σ^b_1-elementary extension of N.

Proof :

If no such model exists S^1_2 proves for some $k \geq 1$:

$$a \geq \underline{k} \to \ [(\exists x < a; |f(x)| \neq |x|) \ \vee \ (\exists x < y < a; f(x) = f(y)) \vee$$

$$(\forall y < a \exists x < a; f(x) = y)]$$

By Buss's witnessing theorem (see [1] or [10, Chpt.7]) there is a polynomial-time function $g(a,y)$ that on input $(a,y) \in \mathbf{N} \times \mathbf{N}$, $a \geq k$ and $y < a$, witnesses the above implication. As the first two disjunctions in the succedent are false in $\mathbf{N}$, it actually always finds $f^{(-1)}(y)$. That is a contradiction with the assumption that f is one way.

The last part follows after applying the witnessing theorem to $S^1_2 + Th_{\Pi^b_1}(N)$.

q.e.d.

A family $h_y(x)$ of functions from $\{0,1\}^{\ell(|y|)}$ into $\{0,1\}^{\ell(|y|)-1}$ is a *strongly collision-free family of hash functions* if there is no polynomial-time function f that on y computes $x_1 < x_2 \in \{0,1\}^{\ell(|y|)}$ with $h_y(x_1) = h_y(x_2)$ (cf. [22]).

Theorem 6.6 *Let $h_y(x)$ be a strongly collision-free family of hash functions.*

Then there is a model M of S^1_2 and an infinite $n = 2^{\ell-1}$ in it such that for some $a \in M$, $h_a : \{0,1\}^{\ell} \to \{0,1\}^{\ell-1}$ violates $WPHP^{2n}_n$.

In fact, if the hypothesis is satisfied only in a model N of S^1_2 then M can be a Σ^b_1-elementary extension of N.

Proof :

The non-existence of such M implies that S^1_2 (or $S^1_2 + Th_{\Pi^b_1}(N)$ respectively) proves

$$\forall y \exists x_1, x_2; x_1 < x_2 \wedge h_y(x_1) = h_y(x_2)$$

Buss's witnessing theorem gives a function f finding in polynomial time from y a collision $x_1 < x_2$ for h_y.

q.e.d.

An example of a family of functions conjectured to be strongly collision-free (unless the discrete logarithm is tractable) is the Cham - van Heijst - Pfitzman family, see [22, Chpt.7].

7 Open problems

Surely there are theorems analogous to Theorem 5.1 for other combinatorial principles. For example, the ontoPHP similarly relates to Tournament principle: a small dominating set is pulled back by the bijection from a smaller tournament to a bigger one where no such small dominating set exists. One may also turn the argument around and try to prove WPHP by proving (without WPHP) a suitable combinatorial principle, or by reducing general WPHP to the ontoWPHP in this way. I shall try now to formalize this type of potential new proof of WPHP by the informal notion of *structured PHP*.

For the rest of the discussion let L be a relational language disjoint from the language of T_2. We shall need a suitable class of formulas. Class $\mathcal{A}$ consists of all 2nd order formulas $\Phi(n)$ that have the form:

$$\Phi(n) \ := \ \exists X; |X| \geq F(n) \wedge \phi(X)$$

where ϕ is a DNF_2-formula (see Section 2) with 2nd order quantifiers ranging over sets of size $(\log n)^{O(1)}$, with all $\forall$ restricted to 2nd order variables, and such that:

1. $F(n) = (\log n)^{O(1)}$ and $F(n)$ is definable in S^1_2.

2. There is $k \geq 1$ such that for arbitrarily large n there is an L-structure A with n points such that $A \not\models \Phi(n^k)$.

The proof of the following lemma is analogous to the proof of Theorem 5.1.

Lemma 7.1 *Let a theory T: $S^1_2(L) \subseteq T \subseteq T_2(L)$ and a proof system P be a pair for which Theorem 4.1 holds.*

Assume that T proves that all L-structures A satisfy $\Phi(|A|)$. Then P admits subexponential size proofs of $WPHP^{n^k}_n$.

If, moreover, T proves condition 2. above, it proves also $WPHP^{n^k}_n(f)$.

In the version of the lemma for *onto*WPHP^m_n the formula Φ can be more general: ϕ can be any 2nd order formula (with 2nd order quantifiers still ranging over sets of size $(\log n)^{O(1)}$), subformula $|X| \geq F(n)$ can be replaced by $|X| \leq F(n)$, and condition 2. can be changed to

2'. There is $k \geq 1$ such that for arbitrarily large n there is an L-structure A with n^k points such that $A \not\models \Phi(n)$.

A more generally aimed question is: Is it easier to prove that $f : m \to n$ cannot be injective assuming that n (or m) is equipped with a structure having some particular property? Even more generally, let $\varphi(x, y)$ be a bounded formula in the language of $T_2(L)$. Denote by $S_\varphi PHP^m_n(f)$ the *structured PHP*: If $\varphi(m, n)$ holds then $f : m \to n$ cannot be injective.

Problem 7.2 *Is there $\varphi(x, y)$ such that*

1. *There are arbitrarily large n and $m \geq 2n$ satisfying $\varphi(m, n)$.*

2. *$S_\varphi PHP^m_n(f)$ is provable in $T^2_2(L, f)$?*

Known methods give negative answer for $m = n + 1$ and $T_2(L, f)$, and for $S^2_2(L, f)$.

There are few more problems that I find interesting and stimulating for further work. The first one is aimed towards the remark before Corollary 6.3.

Problem 7.3 *Prove an exponential lower bound on the size of $R(2)$-proofs of $WPHP^{2n}_n$.*

Mentioning $R(2)$ gives me an opportunity to state a conjecture about the system. For the definition of *(monotone) effective interpolation* see [11]. The only constant-depth subsystem of LK for which is the status of monotone effective interpolation unknown is the depth 1 subsystem (depth 0 is resolution that admits monotone effective interpolation, while depth ≥ 2 subsystems do not - see [11, Thms. 6.1 and 9.3]).

Conjecture 7.4 *$R(2)$ has no (monotone) effective interpolation.*

This is related to our main theme by

Theorem 7.5 ([11, Thm.9.4]) *Either $R(id)$ (i.e. depth 1 LK) does not admit monotone effective interpolation or, for any k, $WPHP_n^{n^k}$ requires exponential size R-proofs.*

To conclude the paper I turn for a moment to unrelativised WPHP. A very important open problem (next to the finite axiomatisability) about (unrelativised) bounded arithmetic, formulated by A. Macintyre some twenty years ago, concerns the provability of (various version of) PHP for functions definable in the theory by bounded formulas. Few conditional results are known: $\mathrm{PHP}_n^{n+1}(f)$ is not provable in any one T_2^i for all such f unless the polynomial-time hierarchy collapses (by [14], as it would hold that $T_2^i = T_2$), and further $\mathrm{WPHP}_n^{2n}(f)$ is not provable in S_2^1 for some polynomial-time functions (e.g. exponentiation in finite fields) unless the RSA cryptosystem is not secure (cf. [13]). However, no unconditional results are known.

Definition 7.6 *Denote by $WPHP_{2n}^n$ the statement that $f : n \to 2n$ cannot be onto.*

BT is the theory S_2^1 extended by instances of $WPHP_{2n}^n$ for all polynomial-time functions f.

BT, a subtheory of T_2, is a suitable theory in our context. For example, $T_2^2(f)$ can be replaced by $BT(f)$ in Lemma 6.4.

Problem 7.7 *Is the theory BT $\forall\Sigma_1^b$-conservative over S_2^1?*

By a theorem of A. Wilkie (proved in [10, Thm. 7.3.7][4]) the functions Σ_1^b-definable in BT are computable in random polynomial time . Thus, assuming the existence of strong pseudo-random number generators, they are all polynomial-time. Hence witnessing will not distinguish the theories. So, in effect, the question asks if there are $\forall\Pi_1^b$-consequences of BT unprovable in S_2^1.

In this connection it may be interesting to

Problem 7.8 *Find a natural extension of EF that would correspond to BT.*

The witnessing theorem for BT also implies that a possible reduction of general WPHP to ontoWPHP (looked for via structured PHP) cannot be entirely trivial. This is an observation pointed out to me by N. Thapen. It was proved in [13] that S_2^1 does not prove WPHP_n^{2n} for a particular polynomial-time function (modular exponentiation) unless the cryptosystem RSA is not secure.

[4] See `http://www.math.cas.cz/~krajicek/upravy.html` for a correction relevant to this citation.

The same proof combined with the witnessing theorem for BT shows that even BT does not prove it, using the average case complexity definition of security of RSA. Hence, assuming such security of RSA, one cannot reduce WPHP_n^{2n} to WPHP_{2n}^n, and hence to *onto*WPHP_n^{2n}, in S_2^1.

The following conjecture suggests how a model not satisfying BT may occur. Let $G : \{0,1\}^* \rightarrow \{0,1\}^*$ be a pseudo-random number generator that stretches the inputs by one bit and has exponential hardness. Denote by G_ℓ the restriction of G to inputs of length ℓ (and similarly f_ℓ for any function f).

Conjecture 7.9 *Any model M_n of the form as earlier, $n = 2^\ell$ in M, has a Δ_1^b-elementary extension to a model N of S_2^1 in which there is a map $f : \{0,1\}^\ell \rightarrow \{0,1\}^{\ell+1}$ that is Δ_1^b-definable from G_ℓ and that violates $WPHP_{2n}^n(f)$.*

In particular, if strong pseudo-random number generators exists then $S_2^1 \neq BT$.

As G is a polynomial-time function and hence itself Δ_1^b-definable, the condition on f just means that f is also Δ_1^b-definable. A reference to G thus seems redundant. However, I believe that there is a construction of f from G uniform in G and that there are even G for which one can take $f := G$.

Note that the conjecture has also implication for the Extended Frege system EF. In particular, none of the formulas $\|y \notin Rng(f)\|^{\ell+1}(b)$, $b \in \{0,1\}^{\ell+1}$, has an EF-proof in the model M_n and hence a standard compactness argument yields the next corollary.

Corollary 7.10 *Assume that G is a strong pseudo-random generator and f is a function with properties guaranteed by the conjecture.*

Then tautologies $\|y \notin Rng(f_n)\|^{n+1}(b)$ for $b \in \{0,1\}^{n+1} \setminus Rng(f_n)$, $n = 1, 2, \ldots$, require superpolynomial EF-proofs.

Acknowledgements:

A large part of this work was done while I was a member of the Mathematical Institute of the Oxford University. I am grateful to N. Thapen and A. Wilkie (both Oxford) for many discussions on the topic, and to N. Thapen in particular for valuable comments on the draft of the paper. I thank O. Kullmann (Toronto) for pointing out to me the references [15, 16] and for comments on the preliminary version.

References

[1] Buss, S. R.: *Bounded arithmetic.* Bibliopolis, Naples. (1986).

[2] Buss, S. R., and Pitassi, P.: Resolution and the weak pigeonhole principle, preprint, in: *Computer Science Logic*, (1997) 149-156.

[3] Buss, S. R., Turán, G.: Resolution proofs of generalised pigeonhole principles. *Theoretical Computer Science*, **62** (1988) 311-317.

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

[5] Chiari, M., Krajíček, J.: Lifting independence results in bounded arithmetic. *Archive for Mathematical Logic*, **38(2)** (1999) 123-138.

[6] Erdös, P.: Some remarks on the theory of graphs. *Bulletin of the A.M.S.*, **53** (1947) 292-294.

[7] Haken, A.: The intractability of resolution. *Theoretical Computer Science*, **39** (1985) 297–308.

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

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

[10] ——— : *Bounded arithmetic, propositional logic, and complexity theory.* Encyclopedia of Mathematics and Its Applications, Vol. **60**, *Cambridge University Press*, Cambridge - New York - Melbourne, (1995)

[11] ——— : Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *J. of Symbolic Logic*, **62(2)** (1997) 47-486.

[12] ——— : 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.

[13] Krajíček, J., and Pudlák, P.: Some consequences of cryptographical conjectures for S^1_2 and EF, in: *Logic and Computational Complexity* (Proc. of the meeting held in Indianapolis, October 1994), Ed. D. Leivant, Springer-Verlag, Lecture Notes in Computer Science, Vol. **960** (1995) 200-220.

Revised version in: *Information and Computation*, Vol. **140 (1)** (January 10, 1998) 82-94.

[14] Krajíček, J., Pudlák, P., and Takeuti, G.: Bounded Arithmetic and the Polynomial Hierarchy, *Annals of Pure and Applied Logic*, **52** (1991) 143-153.

[15] Krishnamurthy, B., and Moll, R. N.: Examples of hard tautologies in the propositional calculus. 13th ACM Symposium on Th. of Computing, (1981) 28-37.

[16] Kullmann, O.: Investigating a general hierarchy of polynomially decidable classes of CNF's based on short tree-like resolution proofs. A preprint available in ECCC, TR99-041, (1999).

[17] Maciel, A., Pitassi, T., and Woods, A.: A new proof of the weak pigeonhole principle. Preprint (2000).

[18] Paris, J., and Wilkie, A. J.: Counting problems in bounded arithmetic. In: *Methods in Mathematical Logic*, LNM **1130** (1985) 317–340. Springer.

[19] Paris, J. B., Wilkie, A. J., and Woods, A. R.: Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, **53** (1988) 1235–1244.

[20] Pudlák, P.: Ramsey's theorem in bounded arithmetic, in :*Proc. Computer Science Logic*, Eds. Boerger E, et. al., Springer LN in Comp. Sci., **553** (1992) 308-312.

[21] Riis, S.: 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.

[22] Stinson, D.R.: *Cryptography: theory and practise*, CRC Press LLC, (1995).

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