Open problems

In the following sections, we distinguish between *fundamental problems* and *other problems*, the former which currently seem to be beyond existent techniques, but form the motivation for the latter which seem more accessible. This problem list was largely drawn up with the help of all participants during a problem session held during the conference held in Prague. We thank S. Buss and P. Pudlák for extensive comments on preliminary versions of this list. Attributions of problems are given to the best of our knowledge.

Peter Clote
Jan Krajíček

1 Bounded Arithmetic

The study of theories of bounded arithmetic was largely begun by work of R. Parikh [51] and the ground-breaking work of J. Paris and A. Wilkie [54, 73, 58, 57, 72, 25]. Especially with the work of S. Buss [10], proof theoretic problems of weak theories of bounded arithmetic were seen to be connected with problems of computational complexity theory. For instance, a recent result of Krajíček, P. Pudlák and G. Takeuti [47] shows that if the theory S_2 of [10] (or equivalently, the theory $I\Delta_0 + \Omega_1$ of [73]) is finitely axiomatizable then the polynomial time hierarchy collapses. See work of A. Wilkie [72] and A. Woods [75] for discussion of a result related to the question of collapse of the $\Delta_0^{\mathbf{N}}$ hierarchy, or equivalently of the linear time hierarchy.

1.1 Fundamental problems in bounded arithmetic

A. (Paris, Wilkie) Is $I\Delta_0$ or $I\Delta_0 + \Omega_1$ finitely axiomatizable? Buss [10] defined a finite conservative extension S_2 of $I\Delta_0 + \Omega_1$ and its subtheories $S_2^1 \subseteq S_2^2 \subseteq \ldots$ whose union is S_2. Each S_2^i is finitely axiomatizable and hence $I\Delta_0+\Omega_1$ is finitely axiomatizable iff $S_2^i = S_2$ for some i. By the theorem of [47] the answer is negative assuming that the polynomial hierarchy does not collapse.

B. Which theorems of finite combinatorics, number theory and complexity theory can be proved in $I\Delta_0$ and $I\Delta_0 + \Omega_1$? In particular, which counting techniques are available in these theories? Here are four specific questions.
(a) (Wilkie) Does $I\Delta_0$ prove the existence of infinitely many primes? Note that in [55], it is shown that $I\Delta_0 + \Omega_1$ (or equivalently S_2) proves the existence of infinitely many primes.
(b) (Wilkie, Wilmers) Does S^1_2 prove the little Fermat theorem ($a^{p-1} \equiv 1 \bmod p$, for p prime not dividing a) where the latter is formalized as a first order statement by using repeated squaring? A.J. Wilkie and G.M. Wilmers have observed[10] that an affirmative answer to this question implies the existence of a polynomial time integer factorization algorithm, which appears most unlikely. In [69], G. Takeuti introduces second order systems $U^{n,w}_2$ which are essentially equivalent to the S^n_2, and then shows that for all n, $U^{n,w}_2$ does not prove Fermat's little theorem, and $U^{n,w}_2$ does not prove Wilson's theorem $(p-1)! \equiv -1 \bmod p$, for p prime, where both are expressed using a (second order) relation symbol.
(c) (Macintyre) Does $I\Delta_0$ or $I\Delta_0 + \Omega_1$ prove the pigeonhole principle for bounded functions, i.e. that there is no Δ_0 - definable injection of $n+1$ into n? By Paris, Wilkie and Woods [55] $I\Delta_0 + \Omega_1$ proves the weak pigeonhole principle (with $2n$ in place of $n+1$). The answer is negative, if the language is extended by a binary predicate R (a graph of the function) and induction for all $\Delta_0(R)$-formulas is allowed, see [3, 8, 48, 60]. It is also open whether $I\Delta_0$ or $I\Delta_0(R)$ prove the weak pigeonhole principle.
(d) (Paris, Wilkie) Is the Matijasevič theorem for bounded formulas provable in $I\Delta_0$? That is: Is every bounded formula equivalent in $I\Delta_0$ to an existential formula? A.J. Wilkie observed in [72] that an affirmative answer to this question would imply that $NP = co-NP$.

1.2 Other problems in bounded arithmetic

The following problems seem to us to be not intractable and should give information about the above main problems.

1. (Paris, Wilkie) Show that the theory $I\Delta_0 + \Omega_1$ is not Π^0_1-conservative over $I\Delta_0$, possibly assuming some hypothesis from complexity theory (such as whether the linear time hierarchy is properly contained in the polynomial time hierarchy). Show the same result at least for the case where a new predicate symbol has been added to the language. Krajíček and Wilkie (independent, unpublished proofs) showed that the Π^0_1-conservativity of $I\Delta_0 + \Omega_1$ over $I\Delta_0$ would imply that $I\Delta_0$ is not finitely axiomatizable.

2. Characterize the functions which are Σ^b_i-definable in the theory T^i_2. A more difficult problem is to determine those functions which are Σ^b_j-definable in T^i_2, for $j \leq i$. This seems to be related to question whether T^i_2 is somehow conservative over S^i_2. Characterizations of functions Σ^b_{i+1}-definable in S^{i+1}_2, T^i_2 and S^i_2 are known by [10, 16, 39]. Also, Buss and Krajíček [13] showed that $T^i_2(\alpha)$ is not $\forall\Sigma^b_i(\alpha)$-conservative over $S^i_2(\alpha)$, and they characterized functions Σ^b_1-definable in T^1_2 in terms of polynomial local search problems.

3. (Krajíček, Pudlák. Takeuti) If S_2 proves that the polynomial time hierarchy (PH) collapses then S_2 is finitely axiomatizable, and by [47], if S_2 is finitely axiomatizable then PH collapses. In fact, $T^i_2 = S^{i+1}_2$ implies that PH collapses. Buss found recently another proof of this theorem which does formalize in S_2. In particular, he showed that $T^i_2 = S^{i+1}_2$ implies that T^i_2 proves that PH collapses and $T^i_2 = S_2$. Formalize in S_2 the original proof of [47]. In particular, does S_2 prove the "tournament principle", which states that given any tournament of n players (a directed graph $G = (V, E)$ with $|V| = n$, such that for all distinct i, j from V, $(i,j) \in E$ iff $(j,i) \notin E$) there exists a "dominating" set D of size $\log(n)$, where the dominating set D satisfies: For all $i \in V \setminus D$, there exists $j \in D$ such that $(j,i) \in E$. For the formalization one needs a hypergraph version of this principle. Note that Pudlák [63] proved in $I\Delta_0 + \Omega_1$ a related Ramsey theorem.

4. Does $S^i_2 = T^i_2$, some i, imply that PH collapses? Krajíček [39] showed that the assumption implies that $L^{\Sigma^p_i} = \Delta^p_{i+1}$ but it is unknown whether the latter equality imply the collapse of PH. Also, does $S^i_2 = T^i_2$ imply that $S^i_2 = S_2$?

5. (Wilkie) Show that $I\Delta_0$ is not finitely axiomatized, provided that the linear time hierarchy does not collapse. By [47] this is true with the polynomial time hierarchy in place of the linear time hierarchy. Note that it is an open problem whether these two hierarchies coincide.

6. (Ajtai) Show with respect to $I\Delta_0$ and "counting" modulo q, one cannot "count" modulo p, for distinct primes p, q. Specifically, let $\Theta_p(R, S, X)$ say

   (i) $0 \in X$
   (ii) R is a partition of X into classes of size p
   (iii) S is a partition of $X \setminus \{0\}$ into classes of size p.

[0] Unpublished correspondence from spring 1984.

Then show that the theory

$$I\Delta_0(R,S,X)+\Theta_p(R,S,X)+\{\neg\Theta_q(\overline{R},\overline{S},\overline{X})\quad \overline{R},\overline{S},\overline{X}\in\Delta_0(R,S,X)\}$$

is consistent, for p,q distinct primes. Here, $\Delta_0(R,S,X)$ denotes the collection of Δ_0-formulas with parameters R,S,X. Ajtai [4] showed that $I\Delta_0(R,S,X)+\Theta_2(R,S,X)$ is consistent with the pigeonhole principle for $\Delta_0(R,S,X)$ - definable functions.

(Wilkie) Let P^{top} be the theory of Peano arithmetic with a "top" element. Formally, P^{top} has the relational language $0, \max, \overline{S}, \overline{+}, \bar{\cdot}, \leq$, with constant symbols for zero and a maximum element (top), binary predicate symbol $\overline{S}$ for the graph of the successor function, ternary predicate symbols $\overline{+}, \bar{\cdot}$ for the graphs of addition and multiplication and the usual ordering relation. The axioms of P^{top} are the relational variants of the usual recursive axioms for the functions (here understood as partial functions), together with axioms stating that 0 is the least element, that max is the largest element, and that $\leq$ is a total ordering which satisfies $x \leq y \iff (\exists z)(\overline{+}(x,z,y))$, together with the scheme of induction (or equivalently of bounded induction). Is P^{top} finitely axiomatizable?

Pudlák, Krajíček-Takeuti) Form the theory $I\Delta_0^{count}$ from $I\Delta_0$ by he iteration of the following step countably many times:

> For every predicate X, which is Δ_0-definable in previously introduced function symbols, add a new function symbol f_X and an axiom stating that f_X "counts" X; i.e. the following axioms
>
> $0 \in X \rightarrow f_X(0) = 1,$
> $0 \notin X \rightarrow f_X(0) = 0,$
> $(\forall n)((n \in X \rightarrow f_X(n) = 1 + f_X(n-1)) \wedge$
> $(n \notin X \rightarrow f_X(n) = f_X(n-1))).$

and then add induction axioms for all bounded formulas in the language resulting from first step. Characterize the Π_1^0-consequences of the theory $I\Delta_0^{count}$. Note that all Π_1^0 consequences of $I\Delta_0^{count}$ are provable in the theory U_1^1 of [10], a second order extension of S_2, and also in $I\Delta_0 + Exp$, and that $I\Delta_0 + Exp$ is not Π_1^0-conservative over $I\Delta_0^{count}$ (see [41] for related results). It is unknown whether U_1^1 is Π_1^0-conservative over $I\Delta_0^{count}$. Note that by [49] U_2^1 is not Π_1^0-conservative over $I\Delta_0$.

9. (Takeuti) Let $S_2^{-\infty}$ be the equational theory involving equations $s = t$, where s,t are closed terms in the language of S_2,with natural rules based on recursive definitions of the functions symbols. Show that

$$S_2 \nvdash Con(S_2^{-\infty}).$$

Recall the fact that $I\Delta_0 \vdash Con(I\Delta_0^{-\infty})$, since in $I\Delta_0$ one can define values of closed terms in the language $\{0,1,+,\cdot\}$. Values of terms of the language of S_2 are not definable in S_2 since e.g. the value of term $t = 2\#\ldots\#2$ is exponentially large in its Gödel number.

10. (Buss, Krajíček, Takeuti) Within the framework of Gentzen's sequent calculus, let the Δ_i^b-PIND rule be the inference: From the sequent

$$\phi(a) \equiv \neg\psi(a)$$

where ϕ, are Σ_i^b and the sequent

$$\Gamma, \phi(\lfloor x/2 \rfloor) \rightarrow \phi(x), \Delta$$

infer the sequent

$$\Gamma, \phi(0) \rightarrow \phi(t), \Delta.$$

(Note that this is different from the Δ_i^b-PIND axiom, where the equivalence of ϕ and $\neg\psi$ is an antecedent of the formula.) In [14], it was shown by a model theoretic argument that S_2^i proves the Δ_{i+1}^b-PIND rule. Give a proof theoretic proof of this fact.

11. (Buss, Krajíček, Takeuti) Is R_2^{i+1} Σ_{i+1}^b-conservative over S_2^i? Note that in [14], it was shown that R_3^{i+1} is Σ_{i+1}^b-conservative over S_3^i.

12. (Buss, Ressayre) What is the strength of Σ_i^b-replacement relative to T_2^{i-1} and S_2^{i-1}? Note that R_2^i proves Σ_i^b-replacement, see [5] and that Σ_1^b-definable functions in R_2^1 are exactly those computable in the class NC of functions computable in polylogarithmic time with a polynomial number of processers on a parallel random access machine [5, 22].

13. (Buss, Krajíček, Takeuti) Assume that T_2^i proves $(\forall x)(\exists y)\phi(x,y)$, where ϕ is Σ_i^b. Does there exists ψ in Σ_i^b such that T_2^i proves $(\forall x)(\exists! y)$ $\psi(x,y)$ and T_2^i proves $(\forall x,y)(\psi(x,y) \rightarrow \phi(x,y))$? Same question for R_3^i.

14. (Verbrugge) Let ϕ be a Σ_1^0-sentence. Is it necessarily true that

$$S_2 \vdash \phi \rightarrow \ \mathrm{Pr}_{S_2}(\ulcorner\phi\urcorner).$$

Note that Parikh's theorem implies that if this holds for formulas instead of sentences then $NP = coNP$, see [71].

(Krajíček, Pudlák) Show that S^1_2, or a stronger system, does not prove superpolynomial lower bounds for extended Frege system proofs. It is known that the system $\forall\Sigma^b_1(S^1_2)$ does not, see [46].

2 Complexity of Proofs

As mentioned in the preface, in 1956 K. Gödel essentially raised the following k-symbol provability question, which is now known to be equivalent to $P = NP$: Does there exist a polynomial time algorithm to determine, given a first order formula F and integer k, whether there is a proof of F with at most k symbols? In [50], as reported in [62], Gödel as well raised the question of determining, given theories S, T, the length of shortest proof of "finitistic consistency" $Con_T(\underline{n})$ in S. Here $Con_T(\underline{n})$ is the first order statement that there is no proof with at most n symbols of falsehood $0 = 1$. See [62, 61] for some partial results. It is worth remarking that a superpolynomial lower bound to the length of proofs of $Con_T(\underline{n})$ in S implies that S does not prove $NP = coNP$.

From Cook's seminal result that SAT is NP-complete, it follows that $NP = co{-}NP$ iff there exists a polynomially bounded, or in terminology of [23] *super*, proof system for all propositional logic tautologies $TAUT$ [23]. In [45] this problem was shown to be equivalent to Gödel's question about finitistic consistency statements. In order to pinpoint the combinatorial difficulties arising in an attempt to prove $NP \neq co-NP$, to date there has been a focus on proving superpolynomial and exponential lower bounds for proof size (total number of symbols) of combinatorial families of propositional tautologies for *explicit* proof systems. Such superpolynomial bounds are now known for semantic tableaux (folklore), resolution [30, 15], Gentzen without cut [70] and constant-depth Frege systems [3, 4]. It is interesting to note that M. Ajtai's technique for proving a superpolynomial proof size in constant-depth Frege systems uses combinatorics similar to those employed in his lower bound [2] for boolean circuit depth. As well, unpublished work of Beame, Impagliazzo, Pitassi [60] and of Krajíček, Pudlák and Woods [48] (see [8]) uses Yao-Haståd style combinatorics in order to improve Ajtai's work to obtain an exponential lower bound for constant-depth Frege proofs of the pigeonhole principle. Exponential lower bounds for constant-depth systems and superpolynomial speed-up of depth $d + 1$ systems over the depth d systems were proved earlier in [42].

2.1 Fundamental problems in complexity of proofs

In this section, the most important and motivating open problems seem to be the following.

C. Prove superpolynomial (and exponential) lower bounds to the size of proofs of some combinatorial statements in any propositional proof system stronger than bounded-depth Frege systems, in particular for Frege and extended Frege systems. Not even superquadratic lower bounds are known (or superlinear when proof-steps are counted).

D. In predicate calculus, prove lower bounds for the length of proofs of naturally arising statements; in particular, improve lower bounds for the finitistic consistency statements. Specifically, for some S strong enough to meaningfully formalize syntactical notions and some $T \supseteq S$, both axiomatized schemes (e.g. $S = I\Delta_0 + \Omega_1, T = ZF$), show that there are no proofs of $Con_T(\underline{n})$ in S of size polynomial in n. Note that this implies that S does not prove $NP = coNP$.

E. Prove Kreisel's conjecture on "generalizing" proofs; i.e. if there exists an integer k for which $\phi(s^{(n)}(0))$ is provable in Peano arithmetic in k lines, for all $n \in \mathbf{N}$, then $\forall x\phi(x)$ is provable. This conjecture is sensitive to the language chosen for the theory and its form of axiomatization. (The conjecture is formulated for the axiomatization based on induction axioms and the language $\{0, 1, s, +, \cdot, =\}$.) It is true if addition and multiplication are treated as ternary relations [52], for any theory axiomatized by schemes with all function symbols at most unary [43, 26], for any finite theory [44], and for $L\exists_1$ (the least number principle for existential formulas) in the language $\{0, 1, s, +, \cdot, =\}$ [7]. See the survey [40].

2.2 Other problems in complexity of proofs

The following problems seem somewhat accessible.

16. (Razborov) Let $\Phi(\alpha, d, N)$ be a $\Sigma^{0,b}_1$-formula encoding the following statement:

> $d \leq |N|$, *α represents a Boolean circuit of depth at most d in $|N|$ variables* (*along with truth-tables of all Boolean functions appearing as intermediate results*) *and the top node of this circuit outputs* "SATISFIABILITY".

Let $\Sigma^{1,b} \rightleftharpoons \bigcup_{i\geq 0} \Sigma^{1,b}_i$. Does there exist a $\Sigma^{1,b}$-definable function $d(N)$ such that $\mathbf{N} \models \omega(\log|N|) \leq d(N) \leq |N|$ and $V^1_1 \vdash \neg\Phi(\alpha, d(N), N)$?

In another words, can V_1^1 prove superlogarithmic lower bounds on the depth of Boolean circuits (= superpolynomial lower bounds on the formula size) for SATISFIABILITY? Note that by the main result of [68, 67, 65] this is equivalent to the provability of an appropriate formalization of the same statement in S_2^1. Note also that V_1^1 (or S_2^1 if you prefer) is exactly the right theory to formalize proofs of lower bounds known in Boolean complexity so in particular it proves that no monotone circuit and no bounded-depth circuit over $\{\wedge, \vee, MOD_p\}$ of subexponential size can compute SATISFIABILITY.

A reasonable first step toward resolving this might be the following:

Show that $V_1^0 \nvdash \neg\Phi(\alpha, d(N), N)$.

It is an easy corollary of the cut elimination theorem that V_1^0 is $\Sigma_1^{0,b}$-conservative over $I\Delta_0(\alpha)$, so this second question might be accessible with the techniques mentioned in the introduction to this section.

17. (W. Cook et al.) An extension of resolution called cutting planes proof system was investigated in [24]. Give a polynomial size family of propositional logic formulas for which every cutting plane proof family has superpolynomial length.

18. (Goerdt, Clote) A. Goerdt [28] has shown that Frege systems p-simulate cutting planes proofs, and P. Clote [20] has shown that a particular extension of cutting planes p-simulates constant depth Frege proofs. Does cutting planes with limited extension p-simulate constant depth Frege proofs?

19. (Clote) For p a positive integer, let CP_p denote the modification of the cutting planes proof systems, obtained by restricting the division rule to allow only division by p. For p, q relatively prime integers, is it the case that CP_p cannot polynomially simulate CP_q?

20. (Krajíček) Let PA denote the first order theory of Peano arithmetic in the language $\{0, 1, s, +, \cdot, =\}$. Is there a recursive function $f(k, \phi)$ such that

$$PA \vdash_{k \text{ steps}} \phi \Rightarrow PA \vdash_{f(k,\phi) \text{ symbols}} \phi?$$

By [44] this is known for finitely axiomatized theories, and for schematic theories whose language contains finitely many predicate symbols and at most unary function symbols [43, 27].

21. (Baaz) What happens with known results concerning the number of proof lines (Kreisel's conjecture) if Gentzen sequent calculus (or predicate logic) is augmented by the equality scheme, or when it is modified to allow the introduction of an entire block of like quantifiers in one step? See [6] for a partial result.

22. (Pudlák) Assume that $(\forall x)(\exists y)\phi(x, y)$ is provable in predicate logic. Introduce a new function symbol f and an axiom A_ϕ which states

$$(\forall x)\phi(x, f(x)).$$

Does there exist formula ϕ such that the extended system gives a superexponential speed-up over predicate calculus, with respect to number of symbols in proofs?

23. (Krajíček) For the theory RCF of real closed fields, is there a generalization result of the form: If there exists an integer k for which $\phi(1 + \ldots + 1)$ (with n occurrences of 1) is provable in k lines, for all $n \in \mathbf{N}$, then $\forall x \phi(x)$ is provable?

24. (Buss) Let LK_e denote Gentzen's sequent calculus with equality. Assume $LK_e \vdash_{k \text{ steps}} \phi$, where the formula ϕ has no occurrence of the symbol for equality. Does it follow that $LK \vdash_{k \text{ steps}} \phi$?

25. (Montagna) Letting PA denote Peano arithmetic, does $PA \vdash_{k \text{ steps}} \Box\phi \rightarrow \phi$ imply that $PA \vdash_{k \text{ steps}} \phi$, where $\Box\phi$ is the formalized statement that ϕ is provable?

26. (Buss) Let $f(n)$ be a polynomial (e.g. $f(n) = n^2$ or more generally, $f(n) = n^{O(1)}$). Find a sequence $\phi_0, \phi_1, \phi_2, \ldots$ of formulas and integer k such that

    (i) $LK \vdash \phi_i$, for all i,
    (ii) for each i,

$$LK \vdash_{f(k) \text{ steps}} \phi_i \Rightarrow LK \vdash_{k \text{ steps}} \phi_i$$

    (iii) $\{i : LK \vdash_{k \text{ steps}} \phi_i\}$ is not recursive.

This is known for $f(n) = n + 1$ by a construction from [12].

27. (Cook, Reckhow) Give a non-linear (resp. super-quadratic) lower bound to the number of steps (resp. of symbols) for Frege proofs. For instance find a family $\langle \phi_n : n \in \mathbf{N} \rangle$ of propositional tautologies, ϕ_n of length n, and positive rational ϵ, such that for every family

$\langle P_n : n \in \mathrm{N} \rangle$ of Frege proofs of these tautologies, it is the case that the number of steps (resp. of symbols) in P_n is at least $n^{1+\epsilon}$ (resp. $n^{2+\epsilon}$). In [23], the question was posed whether the pigeonhole principle, as a scheme in propositional logic, requires superpolynomial Frege proofs. In [11], S.R. Buss answered this in negative. With the results of [11, 28, 20, 19], it is clear that most combinatorial results proved by rudimentary counting have polynomial size Frege proofs. Apart from somewhat unnatural propositional versions of consistency statements of Peano arithmetic, ZF set theory, etc., there are currently few candidates of combinatorial tautologies requiring superpolynomial size proofs. In [63], P. Pudlák proved that a certain version of the finite Ramsey theorem has polynomial size constant depth Frege proofs. In [20] Clote suggested propositional formulations of the Paris-Harrington theorem [53] and related combinatorial independence results as candidates of tautology families requiring superpolynomial size proofs. For instance, work of A. Kanamori and K. McAloon [33] shows that (roughly) the Ackermann function $ack(m,m)$ is a lower and upper bound for the least N, such that given any integer coloring of increasing pairs i,j with $i<j$ satisfying the property that the color of (i,j) is at most i, there is a size m min-homogeneous set with the property that for all increasing pairs drawn from that set the color only depends on the first coordinate. This can be expressed in propositional logic as follows:

$$\bigwedge_{0 \le i < j \le N} \bigvee_{0 \le k < i} p_i$$

$$\rightarrow$$

$$\bigvee_{0 \le i_1 < \ldots < i_m \le N} \bigvee_{k_1 \le i_1, \ldots, k_m \le i_m} \bigwedge_{1 \le \alpha \le m, \alpha < \beta \le m} p_{i_\alpha, i_\beta, k_\alpha}.$$

Krajíček suggested the following sequence of tautologies based on theorem of Bondy as hard for Frege systems: for n let B_n be the formula with n^2 atoms $p_{ij}(i,j<n)$:

$$B_n = \left(\bigwedge_{i<j<n} \bigvee_{k<n} (p_{ik} \not\equiv p_{jk}) \right) \quad \left(\bigvee_{\ell<n} \bigwedge_{i<j<n} \bigvee_{k<n, k \neq \ell} (p_{ik} \not\equiv p_{jk}) \right)$$

He showed that constant-depth Frege proofs of B_n require exponential size.

28. (Bonet) Assume that $\mathcal{F}$ is a Frege system. Does there exist a constant c (depending on $\mathcal{F}$) such that $\mathcal{F}, \phi \vdash_{k \text{ symbols}} \psi$ implies that $\mathcal{F} \vdash_{c \cdot k \text{ symbols}} \phi \rightarrow \psi$? In other words, if $\mathcal{F}, \phi \vdash_{k \text{ symbols}} \psi$, then does it follow that $\mathcal{F} \vdash_{O(k) \text{ symbols}} \phi \rightarrow \psi$? This is known to be true with $O(k^2)$ in place of $O(k)$, or if there is a tree-like proof with k symbols of ψ from ϕ, see [9].

3 Fragments of Peano arithmetic

3.1 Fundamental problems in fragments

The main problems in the area of Peano arithmetic and its fragments which currently seem to be beyond existent techniques appear to concern a threshold for combinatorial independence results and the construction of model extensions. In [32], C.G. Jockusch asked whether there is a recursive partition of unordered pairs of integers into two classes, such that the r.e. complete set K of the halting problem is recursive in every infinite homogeneous set (this problem is related to the so-called $2-3$ problem in models of arithmetic). Recently, D. Seetapun (unpublished) gave a negative solution to Jockusch's problem, using a new forcing construction. See [37] for related work.

(Paris, Wilkie) Does every countable model M of $I\Delta_0 + B\Sigma_1$ have an end extension to a model of $I\Delta_0$ [59] ? This is the most popular problem in the area but appears to be difficult and several problems below are related to it (and hopefully more tractable).

3.2 Technical problems in fragments

The following technical problems are perhaps accessible and should give information about the above main problems.

29. (Paris, Wilkie) Does $I\Delta_0 + \neg exp \vdash B\Sigma_1$, where exp is the formula expressing $(\forall x)(\exists y)(2^x = y)$. A positive answer is known, if one assumes that the Matijasevič theorem is provable in $I\Delta_0$, cf. Problem B(d). See [59] for partial results and discussion. An affirmative answer to this problem implies a negative answer to the second fundamental problem above.

30. (Krajíček) Is there an interpretation of $I\Delta_0 + \neg B\Sigma_1$ in $I\Delta_0$? An affirmative answer to this problem implies a negative answer to the previous problem, since $I\Delta_0 + exp$ is not interpretable in $I\Delta_0$. (Here $\neg B\Sigma_1$ means the negation of any instance of the Σ_1-collection scheme.)

31. (Kaye) Is there a countable rigid model of $B\Sigma_1 + \neg I\Sigma_1$. Here, rigid means having no nontrivial automorphisms. Or even, is there a countable model of $B\Sigma_1 + \neg I\Sigma_1$ with at most countably many automorphisms, or even having no proper elementary substructure. It is known that countable rigid models of $I\Delta_0 + \neg I\Sigma_1$ exist. See [36, 38] for current results.

32. (Wilmers) Let IE_1 (resp. IE_1^-) denote the theory of arithmetic whose principal axiom scheme is induction for bounded existential formulas (resp. bounded existential formulas without parameters). Is IE_1^- a proper subtheory of IE_1? Does IE_1^- have the Tennenbaum property, meaning that it has no recursive countable non-standard models. See work of G. Wilmers [74], R. Kaye [35, 34], and Z. Adamowicz [1].

33. (Clote) For $n \geq 1$, if M is a countable model of $B\Sigma_{n+1}$ then does there exist an $n+1$-elementary end extension K of M such that $K \models B\Sigma_n$? See [18] for discussion and related results.

34. (Paris) For $n \geq 1$, is it the case that $I\Delta_n$ is equivalent to $B\Sigma_n$? It is known that $B\Sigma_n$ is equivalent to $L\Delta_n$ (Gandy, see [29]).

35. (Clote) Does $I\Delta_0 + exp$ prove $Con(B\Sigma_{n+1}) \equiv Con(I\Sigma_n)$? See [21] for a proof of $1 - Con(B\Sigma_{n+1}) \equiv 1 - Con(I\Sigma_n)$ over $I\Delta_0 + exp$.

36. (Hájek) J. Paris [56] and H. Friedman (unpublished) independently proved that $B\Sigma_{n+1}$ is Π_{n+2}-conservative over $I\Sigma_n$. A proof theoretic proof of this result was given by W. Sieg [66]. Though not explicitly mentioned in [66], for each fixed Π_{n+2} formula ϕ, Sieg's proof can be formalized to show that over $I\Delta_0 + exp$, if $B\Sigma_{n+1} \vdash \phi$ then $I\Sigma_n \vdash \phi$. A newer model theoretic proof due to P. Hájek, easily admits a similar formalization — see [21]. See also work of S. Buss [17] for a proof theoretic proof of this conservation result using the "witness" predicate. Give a sharp bound f such that for all Π_{n+2} formulas Θ, if there is a proof in $B\Sigma_{n+1}$ of Θ consisting of m symbols then there is a proof in $I\Sigma_n$ of Θ consisting of $f(m)$ symbols. Can f be polynomial?

37. (Quinsey) Let $N \rightarrow_* (k)^n_m$ mean that for every partition F of the unordered subsets of $\{0, \ldots, N-1\}$ of size n into m classes, there is a set $Y \subseteq \{0, \ldots, N-1\}$ of cardinality $\max(k, \min(Y))$, all of whose size n subsets are sent to the same class. With this notation, does Peano arithmetic prove

$$(\forall k)(\exists n) n \rightarrow_* (k+1)^k_2 \ ?$$

In [64], the notion of 'fulfillment' is used to sharpen the original Paris-Harrington result [53] to show that if $k+1$ is replaced by $k+2$, or the subscript 2 is replaced by 3, then the resulting combinatorial principle is unprovable in Peano arithmetic.

38. (Kanamori) In [33], the following elegant partition relation is introduced: $N \rightarrow (k)^n_{\mathrm{reg}}$ means that for every regressive partition F of the size n unordered subsets of $\{0, \ldots, N-1\}$ there is a min-homogeneous set of size k. Here the function F is said to be regressive, if

$$F(\{a_1, \ldots, a_n\}) < a_1$$

holds for all $a_1 < \cdots < a_n < N$, and a subset $Y \subseteq \{0, \ldots, N-1\}$ is said to be min-homogeneous if

$$F(\{a_1, a_2, \ldots, a_n\}) = F(\{a_1, b_2, \ldots, b_n\})$$

for all $a_1 < a_2 < \ldots a_n$ and $a_1 < b_2 < \cdots < b_n$ drawn from Y. Does Peano arithmetic prove

$$(\forall k)(\exists n) n \rightarrow (k+2)^k_{\mathrm{reg}}$$

In [33], it is shown that Peano arithmetic does not prove the combinatorial principle resulting from replacing $k+2$ by $2k$.

References

[1] Z. Adamowicz and G. Morales-Luna. A recursive model for arithmetic with weak induction. *Journal of Symbolic Logic*, 50:49–54, 1985.

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

[3] M. Ajtai. The complexity of the pigeon hole principle. In *Proceedings of IEEE 29th Annual Symposium on Foundations of Computer Science*, 1988. pp. 346 - 355.

[4] M. Ajtai. Parity and the pigeonhole principle. In S.R. Buss and P.J. Scott, editors, *Feasible Mathematics*, pages 1–24. Birkhäuser, 1990.

[5] B. Allen. Arithmetizing uniform NC. *Annals of Pure and Applied Logic*, 53(1):1–50, 1991.

[6] M. Baaz. Note on the existence of most general semi-unifiers. In *this volume*.

[7] M. Baaz and P. Pudlák. Kreisel's conjecture for $L\exists_1$. In *this volume*.

[8] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for the pigeonhole principle. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, Victoria*, 1992.

[9] M.L. Bonet. Number of symbols in Frege proofs with and without the deduction rule. In *this volume*.

[10] S. Buss. *Bounded Arithmetic*, volume 3 of *Studies in Proof Theory*. Bibliopolis, 1986. 221 pages.

[11] S. Buss. The propositional pigeonhole principle has polynomial size Frege proofs. *Journal of Symbolic Logic*, 52:916 - 927, 1987.

[12] S. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53:72–102, 1991.

[13] S. Buss and J. Krajíček. An application of boolean complexity to separation problems in bounded arithmetic. Preprint, 1992.

[14] S. Buss, J. Krajíček, and G. Takeuti. Provably total functions in bounded arithmetic theories for R_3^i, U_2^i, and V_2^i. In *this volume*.

[15] S. Buss and G. Turán. Resolution proofs of generalized pigeonhole principles. *Theoretical Computer Science*, 62:311 - 317, 1988.

[16] S.R. Buss. Axiomatizations and conservation results for fragments of bounded arithmetic. In W. Sieg, editor, *Logic and Computation*, pages 57–84. American Mathematical Society, 1990. Contemporary Mathematics 106, Proceedings of a Workshop held at Carnegie Mellon University, June 30 - July-2, 1987.

[17] S.R. Buss. The witness function method and provably recursive fragments of peano arithmetic. In *Proceedings of Logic, Methodology and Philosophy of Science '91.* to appear.

[18] P. Clote. Partition relations in arithmetic. In C.A. DiPrisco, editor, *Methods in Mathematical Logic*. pages 32–68. Springer-Verlag, 1985. Lecture Notes in Mathematics 1130.

[19] P. Clote. ALOGTIME and a conjecture of S.A. Cook. In *Proceedings of IEEE Symposium on Logic in Computer Science*, 1990. Journal version in *Annals of Mathematics and Artificial Intelligence*, **6** (1992) 57–106. See related paper in *this volume*.

[20] P. Clote. Cutting planes and constant depth Frege proofs. In *Proceedings of IEEE Symposium on Logic in Computer Science*, 1992.

[21] P. Clote, P. Hájek, and J. Paris. On some formalized statements in arithmetic. *Archive for Mathematical Logic*, 30(4):201–221, 1991.

[22] P. Clote and G. Takeuti. Bounded arithmetics for NC, $ALOGTIME$, L and NL. *Annals of Pure and Applied Logic*. 56:73–117. 1992.

[23] S.A. Cook and R. Reckhow. On the relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36 - 50, 1977.

[24] W. Cook, C.R. Coullard, and G. Turan. On the complexity of cutting plane proofs. *Discrete Applied Mathematics*, 18:25–38, 1987.

[25] C. Dimitracopoulos and J. Paris. Truth definitions for Δ_0 formulae. *Logic and Algorithmic. An International Symposium Held in Honor of Ernst Specker, Monogr. Enseign. Math. Univ. Geneve*, pages 317–329, 1982.

[26] W. Farmer. The Kreisel length-of-proof problem. Annals of Pure and Applied Logic, 1988.

[27] W. Farmer. A unification algorithm for second-order monadic terms. *Annals of Pure and Applied Logic*, 39:131–174, 1988.

[28] A. Goerdt. Cutting plane versus Frege proof systems. In E. Börger, editor, *Proceedings of Computer Science Logic 1990*, pages 174–194, 1992. Springer Lecture Notes in Computer Science **553**.

[29] P. Hájek and P. Pudlák. *Metamathematics of first order arithmetic.* Springer-Verlag, 1992.

[30] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297 - 305, 1985.

[31] J. Hartmanis. The Structural Complexity Column: Gödel, von Neumann and the $P =?NP$ problem. *EATCS Bulletin*, 38:101–107, June 1989.

[32] C.G. Jockusch. Ramsey's theorem and recursion theory. *Journal of Symbolic Logic*, 37(2), 1972.

[33] A. Kanamori and K. McAloon. On Gödel incompleteness and finite combinatorics. *Annals of Pure and Applied Logic*, 33:23–41, 1987.

[34] R. Kaye. Parameter-free universal induction. *Zeitschrift für Mathematische Logik u. Grundlagenforschung*, 35(5):443–456, 1989.

[35] R. Kaye. Diophantine induction. *Annals of Pure and Applied Logic*, 46(1):1–40, 1990.

[36] R. Kaye. Model-theoretic properties characterizing Peano arithmetic. *Journal of Symbolic Logic*, 56(3):949–963, 1991.

37] L. Kirby. Ultrafilters and types on models of arithmetic. *Annals of Pure and Applied Logic*, 27:215-252, 1984.

38] R. Kossak. On extensions of models of strong fragments of arithmetic. *Proceedings of the American Mathematical Society*, 108:223–232, 1990.

[39] J. Krajíček. Fragments of bounded arithmetic and bounded query classes. *Transactions of the American Mathematical Society*, to appear.

[40] J. Krajíček. Generalization of proofs. In *Proc. 5-th Easter Model Theory Conference*, pages 82–99. Seminarberichte der Humboldt Universität, 1987.

[41] J. Krajíček. Exponentiation and second order bounded arithmetic. *Annals of Pure and Applied Logic*, 48:261–276, 1990.

42] J. Krajíček. Lower bounds to the size of constant-depth propositional proofs. Submitted, 1991.

[43] J. Krajíček. On the number of steps in proofs. *Annals of Pure and Applied Logic*, 52(1-2):143–154, 1991.

44] J. Krajíček and P. Pudlák. The number of proof lines and the size of proofs in first order logic. *Archive for Math. Logic*, 27:69–84, 1988.

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

46] J. Krajíček and P. Pudlák. Propositional provability in models of weak arithmetic. In E. Börger et al., editor, *Computer Science Logic (Kaiserslautern, October 1989)*, pages 193–210. Springer-Verlag, 1989.

47] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52(1-2):143–153, 1991.

48] J. Krajíček, P. Pudlák, and A. Woods. Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. Submitted, 1991.

49] J. Krajíček and G. Takeuti. On bounded Σ^1_1 polynomial induction. In S.R. Buss and P.J. Scott, editors, *Feasible Mathematics*, pages 259–280. Birkhäuser, 1990.

50] G. Kreisel. Mathematical logic: What has it done for the philosophy of mathematics. In R. Schoenemann, editor, *Bertrand Russell: Philosopher of the Century*, pages 201–272. George Allen & Unwin, 1967.

[51] R. J. Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494 - 508, 1971.

[52] R. J. Parikh. Some results on the length of proofs. *Transactions of the American Mathematical Society*, 177:29–36, 1973.

[53] J. Paris and L. Harrington. A mathematical incompleteness in arithmetic. In J. Barwise, editor, *Handbook of Mathematical Logic*, pages 1133 - 1142. North Holland, 1977.

[54] J. B. Paris and A. J. Wilkie. Counting problems in bounded arithmetic. In C. A. di Prisco, editor, *Methods in Mathematical Logic*, pages 317 – 340. Springer Verlag Lecture Notes in Mathematics, 1985. Proceedings of Logic Conference held in Caracas, 1983.

[55] J. B. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53(4):1235 – 1244, 1988.

[56] J.B. Paris. Some conservation results for fragments of arithmetic. In C. Berline, K. McAloon, and J.-P. Ressayre, editors, *Model Theory and Arithmetic*, pages 251–262. Springer-Verlag, 1981. Lecture Notes in Mathematics 890.

[57] J.B. Paris and A.J. Wilkie. Δ_0 sets and induction. In W. Guzicki, W. Marek, A. Pelc, and C. Rauzer, editors, *Open Days in Model Theory and Set Theory*, pages 237–248. Leeds University Press, 1981. Proceedings of a conference held in September 1981 at Jadwisin, near Warsaw, Poland.

[58] J.B. Paris and A.J. Wilkie. Models of arithmetic and rudimentary sets. *Bull. de la Soc. Math. de Belgique*, 33(B):157–169, 1981.

[59] J.B. Paris and A.J. Wilkie. On the existence of end extensions of models of bounded induction. In J.E. Fenstad et al., editor, *Logic, Methodology and Philosophy of Science VIII*. North Holland, 1989.

[60] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. Technical Report 257/91, University of Toronto, October 1991.

[61] P. Pudlák. On the lengths of proofs of finitistic consistency statements in first order theories. In J.B. Paris, A.J. Wilkie, and G.M. Wilmers, editors, *Logic Colloquium '84*, pages 165 – 196. North-Holland, 1986.

[62] P. Pudlák. Improved bounds to the length of proofs of finitistic consistency statements. In S.G. Simpson, editor, *Logic and Combinatorics*, volume 65. Contemporary Mathematics, *American Mathematical Society*, 1987.

[63] P. Pudlák. Ramsey's theorem in bounded arithmetic. In E. Börger, editor, *Proceedings of Computer Science Logic 1990*. 1992. Springer Lecture Notes in Computer Science **553**.

[64] J.E. Quinsey. *Some problems in logic: Applications of Kripke's notion of fulfillment*. PhD thesis, Oxford University, April 1980.

[65] A.A. Razborov. An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic. In *this volume*.

[66] W. Sieg. Fragments of arithmetic. *Annals of Pure and Applied Logic*, 28:33–71, 1985.

[67] G. Takeuti. *RSUV* isomorphism. In *this volume*.

[68] G. Takeuti. S_3^i and $\overset{\circ}{V}{}_2^i(BD)$. *Archive for Math. Logic*, 29:149–169, 1990.

[69] G. Takeuti. A second order version of S_2^1 and U_2^1. *Journal of Symbolic Logic*, 56 (3):1038–1063, 1991.

[70] A. Urquhart. Hard examples for resolution. *Journal of the Association of Computing Machinery*, 34(1):209 – 219, 1987.

[71] R. Verbrugge. Feasible interpretability. In *this volume*.

[72] A.J. Wilkie. Applications of complexity theory to Σ_0-definability problems in arithmetic. In L. Pacholski, J. Wierzejewski, and A.J. Wilkie, editors, *Model Theory of Algebra and Arithmetic*, pages 363–369. Springer-Verlag, 1980.

[73] A.J. Wilkie and J.B. Paris. On the schema of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, 35:261 – 302, 1987.

[74] G. Wilmers. Bounded existential induction. *Journal of Symbolic Logic*, 50:72 – 90, 1985.

[75] A. Woods. Bounded arithmetic formulas and turing machines of constant alternation. In J.B. Paris, A.J. Wilkie, and G.M. Wilmers, editors, *Logic Colloquium 1984*. North Holland, 1986.