Akademie věd
České republiky

Teze disertace
k získání vědeckého titulu „doktor věd“
ve skupině věd fyzikálně-matematických

BOUNDED ARITHMETIC AND COMPLEXITY

Komise pro obhajoby doktorských disertací
v oboru Matematické struktury

Jméno uchazeče: Emil Jeřábek

Pracoviště uchazeče: Matematický ústav AV ČR

Místo a datum: Praha, 2021

Contents

Summary

In the field of *bounded arithmetic*, we study weak formal theories of arithmetic with close connections to *propositional proof complexity* and *computational complexity.*

Syntactic classes of bounded formulas define languages that comprise computational complexity classes such as levels of the polynomial-time hierarchy; we may loosely associate arithmetical theories T with complexity classes C such that T is capable of reasoning with concepts of complexity C (it includes induction, comprehension, ... for formulas corresponding to C), and on the other hand, the provably total computable functions of T have complexity C. We may also associate theories of arithmetic with propositional proof systems P: this generally means that universal statements provable in T translate to sequences of tautologies that have polynomial-size P-proofs, and that T proves suitable reflection principles for P. Thus, provability in T serves as a uniform version of P.

This dissertation presents the author's contribution to several topics in bounded arithmetic.

The first part (Chapters I and II) develops a framework for formalization of *approximate counting* (i.e., determination of cardinalities of definable bounded sets of low complexity, up to a small error, either additive or multiplicative) in theories of bounded arithmetic, using the *surjective weak pigeonhole principle.* (In contrast, *exact* counting is not possible in bounded arithmetic because of its large computational complexity.) Applications include formalization of randomized complexity classes, and proofs of combinatorial statements (such as the tournament principle) employing counting or probabilistic arguments.

In Chapter III, we investigate the provability of several interconnected algebraic and number-theoretic problems in suitable theories of arithmetic: the fundamental theorem of finite abelian groups, Fermat's little theorem, Euler's criterion, multiplicativity of the Legendre symbol, and last but not least, the *quadratic reciprocity theorem* (including the supplementary laws). In particular, our proof of quadratic reciprocity in a theory includ-

ing a certain counting principle modulo 2 yields a purely computational consequence: a randomized reduction of *integer factoring* (as a search problem) to a problem in the complexity class PPA. This, as well as a reduction of factoring to a class corresponding to WPHP, and similar results about computation of square roots modulo composites, form the content of Chapter IV.

In the next part (Chapters V and VI), we formalize a variant of the Ajtai–Komlós–Szemerédi sorting network in a certain theory VNC^1_*—developed for this purpose—that corresponds to slightly nonuniform NC^1. As a consequence, we obtain the polynomial equivalence of the *monotone sequent calculus MLK* with the usual sequent calculus *LK* (or Frege systems), modulo an assumption on the provability of existence of expanders in VNC^1_*.

The last part of the dissertation investigates the power of the theory VTC^0 corresponding to the class TC^0, which can be thought of as the complexity of *elementary arithmetic operations*; specifically, we ask if VTC^0 proves any nontrivial induction schemata for binary integers, such as *open induction* (*IOpen*). This is closely related to the computational problem of *root finding for constant-degree polynomials.* We establish that the latter can be done in TC^0 in Chapter VII, using complex-analytic methods. In Chapter VIII, we prove *IOpen*, and even induction and minimization for Σ^b_0 formulas in Buss's language, in VTC^0 augmented with the *iterated multiplication* axiom *IMUL*.

1 Introduction

This dissertation comprises eight published papers of the author, each constituting one chapter (see p. 25). They have been lightly edited to unify the formatting, but otherwise left identical to the versions that were accepted for publication.

The central subject of this dissertation—bounded arithmetic—arose from the confluence of two seemingly disparate fields: first-order theories of arithmetic, and complexity theory (propositional proof complexity and computational complexity).

The best-known first-order theory of arithmetic is the *Peano arithmetic* (*PA*), an elegant and powerful axiomatic system conceived as a first-order approximation to the original second-order axioms of Peano [52]. The most important axiom of *PA* is the schema of *induction* for all formulas. In theories of bounded arithmetic, induction is restricted to smaller classes of formulas, typically only allowing *bounded quantifiers.*

The prototypical theory of bounded arithmetic, now called $I\Delta_0$, was introduced by Parikh [47]: it includes induction for all bounded formulas in the basic language of arithmetic $\{0, S, +, \cdot, \leq\}$. Paris and Wilkie [48, 49] introduced its extension $I\Delta_0 + \Omega_1$ with an axiom postulating that the function $x^{\log x}$ is total; Buss [12] reformulated it as the theory T_2 in a richer language, which allowed him to define its subtheories T^i_2 and S^i_2 with induction restricted even more. These form one of the two most commonly used frameworks for bounded arithmetical theories; the other framework are the two-sorted ("second-order") theories, originally also introduced by Buss [12], but now usually presented in a considerably simpler formalism due to Zambella [63].

Bounded formulas in the language of Buss's theories define exactly the predicates computable in the polynomial-time hierarchy (PH). Better, we can stratify the class of bounded formulas into the Σ^b_i hierarchy based on the number of alternations of bounded quantifiers, and then Σ^b_i-definable predicates coincide with the level Σ^{P}_i of PH; in particular, NP predicates are exactly those definable by Σ^b_1 formulas. Going to first-order theories, *Parikh's theorem* [47] ensures that in any reasonable bounded arithmetical theory, the provably total Σ_1-definable functions (search problems) are bounded by a term of the language, i.e., a poly-time function in the case of Buss's theories. More precisely, *Buss's witnessing theorem* shows that the provably total NP search problems (i.e., $\forall\Sigma^b_1$ or $\forall\exists\Sigma^b_1$ consequences) of S^1_2 are poly-time computable (FP), and more generally, the $\forall\exists\Sigma^b_i$ consequences of S^i_2 are witnessed by $\mathrm{FP}^{\Sigma^{\mathrm{P}}_{i-1}}$ functions.

This leads to close connections between bounded arithmetic and computational complexity theory. Various questions about bounded arithmetical theories are related to questions in complexity theory (often, the former are "more constructive versions" of the latter). One of the most fundamental examples is the problem of finite axiomatizability of Buss's theory T_2 (or equivalently, the collapse of the T^i_2 hierarchy), which implies collapse of the polynomial hierarchy PH, and is in fact equivalent to *provability* of the collapse of PH in T_2 (Krajíček, Pudlák, and Takeuti [39] and follow-up results, including II.4.6–8 in the present dissertation). Witnessing theorems reduce questions about provability in theories of bounded arithmetic to questions about the complexity of search problems, with some loss of information. For this reason, a lot of ongoing research is invested in characterization of provably total NP search problems of various fragments of bounded arithmetic, which determine their $\forall\Sigma^b_1$ consequences modulo true universal statements.

Viewed from another angle (going back to Parikh [47] and Cook [22]), we may interpret the fact that theories of bounded arithmetic include induction and related schemata (comprehension, minimization, . . .) only for formulas expressing computable predicates of moderate complexity by considering them as modelling *feasible reasoning*: we ask what we can prove while referring only to efficiently computable properties and objects. In particular, when discussing formalization of complexity classes in arithmetic, or specific low-complexity predicates or functions, it is a fundamental question which of their properties can be proved using only reasoning with entities not exceeding their own complexity. One way of making this notion precise is to equate it with provability in an arithmetical theory corresponding to the relevant complexity class.

In propositional proof complexity, we study proof systems for (usually) classical propositional logic, which are specified by a poly-time verifiable notion of proofs such that formulas that have proofs are exactly the tautologies. The list of common proof systems includes Frege (Hilbert) calculi, sequent calculi, resolution, or algebraic proof systems such as the polynomial calculus. We are interested in the complexity of proofs according to various complexity measures, the most basic being the length of proofs.

The connection of bounded arithmetic to propositional proof complexity, originating in Cook [22] and Paris and Wilkie [49], is based on the idea that a bounded formula (of suitable complexity) can be translated into a sequence of propositional formulas that express its truth when restricted to inputs of a given length; if the original formula is universally valid, its translations are tautologies, and if it is provable in a bounded arithmetical theory T, then its translations have polynomial-time constructible proofs in a propositional proof system P depending on the theory (e.g., Cook [22] shows this with $T = PV$ and P being extended resolution, or equivalently, extended Frege). If the pairing of T with P is right, the connection goes both ways: T proves the soundness of P (in the form of reflection principles), and in particular, it proves "if propositional translations of ϕ have P-proofs, then ϕ". Moreover, any proof system whose soundness is provable in T is p-simulated by P.

This correspondence is sometimes expressed by saying that theories of bounded arithmetic are uniform versions of propositional proof systems. It is an important tool for showing consistency (unprovability) results for arithmetical theories by proving superpolynomial lower bounds on the corresponding propositional proof systems; in the other direction, it can be used to construct transparent short proofs of combinatorial tautologies.

2 Our contribution

The present dissertation investigates several themes in the subject of bounded arithmetic and related complexity theory. While each chapter was published as a separate paper, they are connected in various ways. We will now give brief introductions of the individual topics.

2.1 Approximate counting

The first two chapters (originally published as [D1, D2]) are devoted to *approximate counting* in bounded arithmetic. Here, counting refers to determination of the cardinality of a finite set. We consider definable sets $X \subseteq [0, a)$ for some a, and we would like to define the cardinality $|X|$ such that we can manipulate it in the theory; this can be useful for formalization of counting arguments or probabilistic arguments in combinatorics, complexity theory, number theory, etc., and for presentation of randomized algorithms.

Weak fragments of bounded arithmetic (PV_1, or even VTC^0) have a well-behaved definition of counting for sets explicitly encoded by sequences of elements. Strong fragments of arithmetic prove comprehension principles ensuring that a bounded definable set of suitable complexity can be arranged into a sequence, and therefore counted: e.g., $I\Delta_0 + EXP$ proves this for $\Delta_0(\exp)$ sets. However, this set-up essentially requires the presence of exponentiation, as subsets of $[0, a)$ need more than a bits to encode. In fact, Toda's theorem [60] implies that exact counting of polynomial-time bounded sets is not possible to define in bounded arithmetic in *any* reasonable way, unless the polynomial-time hierarchy PH (and even the whole counting hierarchy CH) collapses, which is quite unlikely, and it is outright *disprovable* for "relativized" variants of bounded arithmetic with an uninterpreted new predicate. Similar arguments apply also to *modular counting*, i.e., determination of $|X|$ modulo a fixed constant m.

This leaves open the possibility of defining an *approximation* of $|X|$, up to a polynomially small error ε. Here, we may consider either additive error, i.e., we want to compute s such that $|X| - \varepsilon a \leq s \leq |X| + \varepsilon a$, where $X \subseteq [0, a)$, or multiplicative error, in which case we want s such that $|X|(1 - \varepsilon) \leq s \leq |X|(1 + \varepsilon)$. (Counting with multiplicative error is more precise than with additive error, especially when X is rather sparse.) This can be accomplished within the polynomial-time hierarchy, hence there is no complexity obstacle to formalization in bounded arithmetic.

The *pigeonhole principle* $\mathit{PHP}^b_a(f)$ for $b > a$ asserts that a function $f \colon [0, b) \to [0, a)$ cannot be injective; this amounts to a "passive" form of counting. We speak of the *weak pigeonhole principle* when b is "much" larger than a (the exact meaning depends on the context, such as $b = a^2$ or $b = 2a$; below, we will take $b = a(1 + 1/|a|)$, which corresponds to counting with polynomially small error $\varepsilon \approx 1/|a|$). It turns out that the *surjective* (or *dual*) weak pigeonhole principle is more useful for formalization of counting arguments than the usual (injective) principle: for $a < b$, $\mathit{sPHP}^a_b(f)$ says that $f \colon [0, a) \to [0, b)$ cannot be onto, and $\mathit{sWPHP}(\Phi)$ denotes $\forall a \, \mathit{sPHP}^a_{a(1+1/|a|)}$ for each $f \in \Phi$ (e.g., Φ might be the set of all PV-functions). For clarity, we will denote the original form of the weak pigeonhole principle as iWPHP rather than WPHP to distinguish it from sWPHP.

In bounded arithmetic, PHP is as intractable as other forms of exact counting; in particular, the relativized theory $T_2(\alpha)$ does not prove $\mathit{PHP}(\alpha)$ [1, 8]. But crucially, it *does* prove the weak pigeonhole principle, as shown by Paris, Wilkie, and Woods [50]; more precisely, for $i \geq 1$, $T^{i+1}_2(\alpha)$ proves $\mathit{iWPHP}(\Sigma^b_i(\alpha))$ and $\mathit{sWPHP}(\Sigma^b_i(\alpha))$ by Maciel, Pitassi, and Woods [41]. Besides being an interesting counting principle in its own right, WPHP can be used to simulate certain counting arguments in T_2: the very reason it was introduced in [50] was to prove the unboundedness of primes, and for another important example, Pudlák [54] used it to prove Ramsey's theorem.

A close connection of sWPHP to counting or probabilistic arguments is suggested by *Wilkie's witnessing theorem* (first published in Krajíček [37]): the NP-search problems provably total in $S^1_2 + \mathit{sWPHP}(\mathit{PV})$ are included among TFZPP. In contrast, witnessing $iWPHP(PV)$ is computationally hard: e.g., it is at least as hard as integer factoring [31]. Strictly speaking, $sWPHP(PV)$ and $iWPHP(PV)$ are (presumably) incomparable; nevertheless, $sWPHP(PV)$ is weaker than $iWPHP(PV)$ in that $S^1_2 + sWPHP(PV)$ is $\forall\Sigma^b_1$-conservative over $S^1_2 + iWPHP(PV)$.

As we already mentioned, some counting arguments were formalized in bounded arithmetic using variants of *WPHP* for example in [50, 54], but these papers rely on ingenious ad hoc constructions of counting functions; they do not give any hint how to turn this into a general method. As a case in point, the *tournament principle* (due to Erdős [27]) has a simple counting proof analogous to a counting proof of Ramsey's theorem, but it stood open for a long time whether it can be proved in a bounded arithmetic (this problem originated in Krajíček, Pudlák, and Takeuti [39]; it was stated explicitly in Clote and Krajíček [20]).

The main goal of Chapters I and II is to develop a systematic framework for formalization of approximate counting and probabilistic arguments in bounded arithmetic using *sWPHP*, including a toolbox of basic facts.

Chapter I (originally [D1]) is devoted to approximate counting with *additive error*, working in the theory $PV_1 + sWPHP(PV)$, also called APC_1 in [15]. (It partially builds on [30], not included in this dissertation.) The basic idea is that if $X, Y \subseteq [0, 2^n)$ are sets defined by Boolean circuits, we witness that $|X| \le |Y|$ by the existence of a circuit that computes a surjection $Y \twoheadrightarrow X$, but we weaken it in two ways to make construction of such circuits feasible: first, we actually consider surjections $Y \times [0, v) \twoheadrightarrow X \times [0, v)$ for some $v > 0$, and second, instead of Y, we take its disjoint union with $[0, \varepsilon 2^n)$ for some rational $\varepsilon > 0$. We denote the resulting concept by $X \preceq_\varepsilon Y$, spelled out as *the size of X is approximately less than the size of Y with error ε*. We also write $X \approx_\varepsilon Y$ if $X \preceq_\varepsilon Y$ and $Y \preceq_\varepsilon X$.

The crucial result that makes this definition well behaved is that APC_1 proves that any set "has a size": that is, given $X \subseteq [0, 2^n)$ as above, and

ε at least inverse polynomial in n, there exists $s \le 2^n$ such that $X \approx_\varepsilon [0, s)$; this result comes out from formalization of the Nisan–Wigderson pseudorandom generator [45].

Besides basic consequences of the definition (such as monotonicity), we show that it behaves in the expected way with respect to disjoint unions and Cartesian products (the latter generalizes to a form of the averaging principle). For more advanced counting arguments, we prove a form of the inclusion–exclusion principle and a Chernoff–Hoeffding bound.

In the second half of Chapter I, we apply this machinery to develop the theory of various *randomized complexity classes* in APC_1: specifically, we look at the classes of FRP and TFRP search problems, BPP languages and promise problems, APP real-valued functions (introduced by Kabanets, Rackoff, and Cook [35]), MA languages and promise problems, and—upgrading the theory by one level of the hierarchy to APC_2—the classes of AM languages and promise problems. For each class, we indicate how to formally define algorithms from the class in bounded arithmetic using the approximate counting framework, and we prove basic properties of the class in the theory, such as amplification of the success probability, simulation of randomness by nonuniformity, and standard inclusions between the classes. (Along the way, we solve an open problem from [35] on the recursive enumerability of APP, and find a proof of success amplification for APP which is much simpler than the original one as given in [35].)

Chapter II (originally published as [D2]) is devoted to approximate counting with *multiplicative error.* We work in $T^1_2 + sWPHP(PV_2)$, called APC_2 in [15]. The basic idea is taken from Sipser's coding lemma [59], which employs a universal family of linear hashing functions to distinguish sets X of size $\le s$ from sets of size $\Omega(s \log s)$. We consider here bounded sets X definable by Σ^b_1-formulas (i.e., NP/ poly). In order to get the error down to εs for a polynomially small ε, we apply Sipser's definition to a suitable Cartesian power X^c in place of X itself; we write $X \precsim_\varepsilon s$ for the resulting notion (note the difference from $\preceq_\varepsilon$). The key result is that, up to relative error ε, $X \precsim_\varepsilon s$ is equivalent to the existence of PV_2-surjections $s^c \twoheadrightarrow X^c$ for some c: we prove this in APC_2 by formalization of Sipser's lemma, using the machinery from Chapter I for probabilistic reasoning.

Again, we provide a toolbox showing that the definition of $X \precsim_\varepsilon s$ interacts in the expected way with finite unions, Cartesian products, and more generally, unions of parameterized families, i.e., averaging principles. We also prove that any bounded Σ^b_1-definable X has an "almost bijective" increasing enumeration by a PV_2-function, in a suitable sense.

As applications, we show how the general framework can be used to formalize various counting arguments in combinatorics and complexity theory. We prove Ramsey's theorem (using a much simpler proof than Pudlák [54]) and the tournament principle (solving the open problem from [20]). In fact, we prove a multi-dimensional generalization of the tournament principle with several applications: first, we use it to directly formalize in bounded arithmetic the argument from [39] relating collapse of the T_2 hierarchy to collapse of PH, which improves the previously known results in this area [39, 13, 63, 23]; second, we use it to formalize in APC_2 the result $\mathrm{S}^P_2 \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ due to Cai [17]. We also prove that any interval in a model of T_2 admits a nontrivial approximate Euler characteristic in the sense of Krajíček [38], and we prove in APC_2 that graph isomorphism is in coAM.

Let us mention follow-up work. Buss, Kołodziejczyk, and Thapen [15], besides introducing the names APC_1 and APC_2, prove $\forall\Sigma^b_1$-separations of several fragments of APC_2 from APC_2 itself and from T^2_2 in the relativized setting. (See also Atserias and Thapen [7].) The separations are based on the fact that (using the approximate counting machinery and the tournament principle) APC_2 proves the *ordering principle*, which states that any partial order on a nonempty bounded domain has a minimal element.

Using our approximate counting, Buss, Kołodziejczyk, and Zdanowski [16] formalize Toda's theorem on the collapse of $\mathrm{Mod}_p\,\mathrm{PH}$ to $\mathrm{BP} \cdot \oplus_p\mathrm{P}$ in bounded arithmetic relativized with a $\oplus_p\mathrm{P}$ oracle, specifically showing that $APC_2^{\oplus_p\mathrm{P}} = T_2(\oplus_p\mathrm{P})$. Using the Paris–Wilkie translation, they obtain a collapse for propositional proof systems: the constant-depth Frege system with $\oplus_p$ gates is quasipolynomially simulated by its depth 3 fragment (using $\bigwedge$ of $\oplus_p$ of polylogarithmic $\bigwedge$ of literals). We recall that proving superpolynomial lower bounds for constant-depth Frege with $\oplus_p$ gates is one of the longest-standing open problems in proof complexity.

Pich [53] formalizes the exponential PCP theorem in APC_1 using our approximate counting, and proceeds to prove the full PCP theorem (scaled logarithmically down, whence the weaker theory) in PV_1. Müller and Pich [43] employ approximate counting to formalize in APC_1 several prominent super-polynomial circuit lower bounds: AC^0 lower bounds for Parity, $\mathrm{AC}^0[p]$ lower bounds for Mod_q, and monotone lower bounds for Clique. They also formalize the Razborov–Rudich [56] theorem on natural proofs.

2.2 Abelian groups, quadratic residues, and factoring

Chapter III (originally published as [D3]) is devoted to formalization of several inter-related problems from modular arithmetic, elementary number theory, and algebra in suitable fragments of bounded arithmetic. As a follow-up, some of these results are used in Chapter IV (originally published as [D4]) to draw consequences in pure computational complexity that are not a priori connected to bounded arithmetic, specifically about the complexity of integer factoring.

One motivating problem (still unresolved) for Chapter III is whether the bounded arithmetic T_2 proves *Fermat's little theorem* (*FLT*): $a^p \equiv a \pmod{p}$ for all a and prime p. This basic fact admits a number of elementary proofs, but all seem to require exact counting or exponential-size sums or objects, unavailable in bounded arithmetic. On the other hand, there is no evidence that it is really hard. More generally, we may ask about the structure of the multiplicative groups $\mathbb{F}_p^\times$ for prime p. FLT asserts that these groups have exponent $p-1$; another important property whose provability in T_2 is open is that these groups are *cyclic*. Cyclicity and FLT together are equivalent over $S^1_2 + iWPHP(PV)$ to the statement that primes have Pratt's primality certificates, making primality Σ^b_1.

Another elementary principle related to FLT is *Euler's criterion*, stating that the *Legendre symbol*, defined for integers a and odd primes p by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \mid a, \end{cases}$$

equals $a^{(p-1)/2} \pmod{p}$. Euler's criterion implies FLT, and we may ask how much stronger it is.

This brings us to properties of the Legendre symbol $(a|p)$. The most fundamental are its *multiplicativity* (implied by Euler's criterion), and the celebrated *quadratic reciprocity theorem* (*QRT*)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

for odd primes $p \neq q$, along with the *supplementary laws* $(-1|p) = (-1)^{(p-1)/2}$, $(2|p) = (-1)^{(p^2-1)/8}$. These properties also imply the corresponding statements for the *Jacobi symbol* $(a|n)$, extending the Legendre symbol to all odd $n > 0$ by completely multiplicativity; one consequence is that it leads to simple polynomial-time algorithms for the Jacobi, and therefore Legendre, symbol.

QRT was originally proved by Gauss, and until today, well over 300 proofs (not all essentially different) were published; cf. Lemmermeyer [40]. In the context of weak theories of arithmetic, Cornaros [24] proved QRT in $I\mathcal{E}^2_*$, and Berarducci and Intrigila [10] proved the supplementary laws in $I\Delta_0$ extended with certain modular counting principles. D'Aquino and Macintyre [25, 26] developed the basic theory of quadratic forms in $I\Delta_0 + \Omega_1$ with a vision of eventually formalizing a proof of QRT along the lines of Gauss's second proof, but so far this did not materialize.

We tackle the problems above in Chapter III as follows. As a first step towards clarifying the structure of $\mathbb{F}_p^\times$, we look at the structure of *arbitrary* finite abelian groups (more precisely, Σ^b_1-definable groups with a bounded domain): we prove the fundamental theorem that any such group is a direct sum of cyclic groups in the theory $S^2_2 + iWPHP(\Sigma^b_1)$.

Returning to Fermat's little theorem, if p is a prime, then $\mathbb{F}_p^\times$ is a group with domain $[1, p)$; by the structure theorem, there is an isomorphism $f\colon \mathbb{F}_p^\times \to G = \bigoplus_{i<k} C(p_i^{e_i})$ (defined by a PV-function) for some sequence $\langle p_i^{e_i} : i < k\rangle$ of prime powers. Here, G is a group with domain $[0, a)$ where $a = \prod_i p_i^{e_i}$, and it has exponent a, thus so does $\mathbb{F}_p^\times$. The FLT would follow if $a = p-1$. The weak pigeonhole principle applied to f ensures that $a \approx p$, and we know that a is even, but other than that, it seems quite difficult to rule out that, say, $a = p + 1$, in which case the FLT spectacularly fails. Thus, we only obtain a proof of FLT if we add to $S^2_2 + iWPHP(PV)$ the *strong* pigeonhole principle $PHP(PV)$, which is likely not provable in T_2. All in all, this argument seems to suggest that FLT is *not* provable in T_2, but the evidence is very weak.

Concerning the cyclicity of $\mathbb{F}_p^\times$, the structure theorem implies (over $S^2_2 + iWPHP(PV)$) that it is equivalent to there not being too many qth roots of unity in $\mathbb{F}_p$ for any prime $q \neq p$. More precisely, we obtain an interesting dichotomy: either $\mathbb{F}_p^\times$ is cyclic, and for any prime $q \neq p$, $[0, q)$ PV-surjects onto $\{x \in \mathbb{F}_p : x^q = 1\}$; or $\mathbb{F}_p^\times$ is not cyclic, and there exists a prime $q \neq p$ such that $[0, q^2)$ PV-injects into $\{x \in \mathbb{F}_p : x^q = 1\}$. Thus, one way to prove the cyclicity of $\mathbb{F}_p^\times$ in bounded arithmetic might be to formalize the principle that a degree-q sparse polynomial (here, $x^q - 1$) may only have at most q roots in a finite field, in the sense of approximate counting. Usual proofs of this fact require the existence of exponentially large objects.

Next, we look at Euler's criterion. We first show that the Legendre symbol $(-|p)$ is multiplicative whenever $\mathbb{F}_p^\times$ is a torsion group (this improves the result of Berarducci and Intrigila [10] on its being provable from $iWPHP(PV)$). We use this to show that Euler's criterion is equivalent over S^1_2 to the conjunction of FLT with the statement $\exists a\, a^{(p-1)/2} \equiv -1 \pmod{p}$. In particular, Euler's criterion is provable in $S^2_2 + iWPHP(PV) +$

$PHP(PV)$. Observe that, assuming FLT, the assertion $\exists a\, a^{(p-1)/2} \equiv -1 \pmod{p}$ amounts to the sparse polynomial $x^{(p-1)/2} - 1$ having less than $p-1$ roots, hence we are in a similar situation as with the cyclicity of $\mathbb{F}_p^\times$.

The last section of Chapter III is devoted to quadratic reciprocity. Our starting point is the observation that elementary proofs of QRT often distinctly involve some form of counting modulo 2; cf. also Berarducci and Intrigila's above-mentioned proof of the supplementary laws using counting modulo 4 and 8. This suggests that we should look at bounded arithmetic extended with some form of counting mod 2. The weakest modular counting principle we thought of expresses that we cannot partition $[0, 2a+1)$ into a disjoint union of two-element sets, where the partition is represented by a PV-function f that maps each element to its partner. In other words, f is a fixpoint-free involution. Thus, our counting principle $\mathit{Count}_2(PV)$ states that every involution on $[0, 2a+1)$ defined by a PV-function has a fixpoint. Interestingly, this principle was used outside bounded arithmetic in slick proofs of Fermat's theorem on sums of two squares (related to the first supplementary law of QRT) by Heath-Brown [28] and Zagier [62].

We find a short proof of QRT (as well as the supplementary laws, and multiplicativity of the Legendre symbol) using only simple manipulations of involutions, which can be formalized in $PV_1 + \mathit{Count}_2(PV)$ or $I\Delta_0 + \mathit{Count}_2(\Delta_0)$. The proof is loosely based on Gauss's third proof, but we replace the key Gauss's lemma by a formulation with explicit involutions. Strengthening the base theory from PV_1 to S^1_2, we can also prove the corresponding statements about the Jacobi symbol, leading to its being polynomial-time computable.

This brings us to Chapter IV, which is devoted to the computational complexity of integer factoring, and the closely related problem of computing modular square roots. Factoring is one of the most fundamental problems in mathematical computation, going back to classical antiquity. In modern times, it has significant applications in cryptography: various protocols rely on the computational hardness of factoring.

Factoring is closely related to the problem of computing square roots modulo a given integer. There are randomized poly-time algorithms for computation of square roots modulo primes; using Hensel's lifting and the Chinese remainder theorem, this gives a randomized reduction of square roots with general moduli to factoring. One can also give randomized reductions in the opposite direction.

We study the complexity of factoring as a *total* NP*-search problem*, which is arguably a more natural setting than as a decision problem. Papadimitriou [46] introduced several classes of NP-search problems that are based on "combinatorial proofs" of totality: in particular, a class PPP corresponding to the pigeonhole principle, and several classes based on "parity arguments"—we are interested here in PPA, whose defining complete problem is, given a circuit representing an undirected graph of degree 2, and a vertex of degree 1, find another such vertex. Papadimitriou posed the question whether Factoring belongs to some of his classes. The first progress on this problem was made by Buresh-Oppenheim [11], who proved that factoring of integers of a certain special form is in PPA, and has a randomized reduction to a PPP problem.

We prove in Chapter IV that the general Factoring problem has a randomized reduction to a PPA problem, and to a problem in the subclass PWPP of PPP corresponding to $iWPHP$. We can derandomize the reductions under the assumption of the Riemann hypothesis for quadratic Dirichlet L-functions. Moreover, PPA unconditionally contains the problems of computing modular square roots, and finding square nonresidues.

Our basic strategy is to apply a witnessing theorem to the results of Chapter III on provability of QRT. It is easy to show that the provably total NP-search problems of $S^1_2 + Count_2(PV)$ are in PPA. Since the theory proves that the Jacobi symbol $(a|n)$ is computable by a PV-function, say $J(a,n)$, it also proves the $\forall\Sigma^b_1$ sentence "if $J(a,n) = 1$, then a is a quadratic residue mod n, unless n is composite". Thus, PPA contains the problem FacRoot: given a, n such that $(a|n) = 1$, find a square root of a modulo n, or a proper divisor of n.

We obtain an easy randomized reduction of Factoring to FacRoot by choosing a at random. We also show that FacRoot can be used (deterministically) to compute square roots mod n. While our reduction of general factoring to PPA is randomized, we exhibit special cases that are in PPA deterministically, generalizing the original result of [11].

In order to make the original paper self-contained and accessible to a wider audience, we include a direct combinatorial proof of FacRoot $\in$ PPA, based on a rather complicated dynamic programming algorithm. We believe the bounded arithmetic proof is much more transparent; this seems to be a not-so-common case where witnessing applied to a bounded arithmetic proof yields a genuinely new algorithm.

We also present a randomized reduction of Factoring to PWPP based on the proof of multiplicativity of the Legendre symbol in $PV_1 + iWPHP(PV)$.

2.3 Sorting networks and monotone sequent calculus

The material in Chapters V and VI (originally published as [D5, D6]) is motivated by a problem from propositional proof complexity. The *Frege system* is one of the most fundamental proof systems; it is quite robust in that it can be presented in a variety of ways which turn out all to be p-equivalent: as a system operating with formulas using a finite set of schematic axioms and rules, as a natural deduction system, or as a Gentzen-style *sequent calculus LK*.

An interesting variant of the sequent calculus is the *monotone sequent calculus MLK* (introduced by Pudlák [55]): it operates with two-sided sequents that only use monotone formulas, i.e., formulas using the connectives $\wedge$, $\vee$, $\bot$, and $\top$; the calculus includes the usual derivation rules of *LK* (including the cut rule) pertaining to the restricted language. A natural question to ask (dubbed the *Think Positively Conjecture* by Atserias [4]) is whether *MLK* is p-equivalent to *LK*, in the sense that given an *LK* proof of a monotone sequent, we can construct its *MLK* proof in polynomial time. *MLK* is also included in the intuitionistic sequent calculus LJ, and we can similarly ask if LJ p-simulates LK for monotone sequents.

Atserias, Galesi, and Gavaldà [5] proved that MLK has quasipolynomial proofs of the pigeonhole principle, and then Atserias, Galesi, and Pudlák [6] proved that in general, MLK (and therefore LJ) quasipolynomially simulates LK for all monotone sequents. A question remained whether we can improve this simulation to polynomial. For LJ, the question was resolved by Jeřábek [32], who presented a simple p-simulation of LK-proofs of monotone sequents in LJ.

For MLK itself, the basic idea of [6] was to use the monotone *threshold* (*slice*) *functions*

$$\theta^n_k(x_0,\dots,x_{n-1}) = \begin{cases} 1 & \text{if } \bigl|\{i<n : x_i = 1\}\bigr| \ge k, \\ 0 & \text{otherwise.} \end{cases}$$

If we assume that exactly k of the variables $x_0,\dots,x_{n-1}$ are true, we can express $\neg x_i$ by the monotone function $\theta^n_k(x_0,\dots,x_{i-1},\bot,x_{i+1},\dots,x_{n-1})$, which can be used to make formulas in a proof monotone. There is a straightforward construction of quasipolynomial-size monotone formulas for θ^n_k, and this allowed [6] to prove a quasipolynomial simulation of LK by MLK. They observed that if we could find a *polynomial* construction of monotone formulas for θ^n_k such that certain basic properties of these formulas have polynomial MLK proofs, we would obtain a polynomial simulation of LK by MLK. But surprisingly, they also showed that the same conclusion holds if we only assume that the properties of θ^n_k have polynomial *LK proofs*, using a sort of boot-strapping argument.

Polynomial-size monotone formulas for θ^n_k do, in fact, exist: first, Ajtai, Komlós, and Szemerédi [3, 2] proved that there are *sorting networks* of depth $O(\log n)$, which also gives monotone formulas of depth $O(\log n)$ for θ^n_k, and second, Valiant [61] gave a simple probabilistic construction of such formulas. However, in both cases it's quite unclear how to prove properties of the formulas efficiently in LK: Valiant's construction is randomized, hence it does not even give a uniformly constructible sequence of θ^n_k formulas; the Ajtai–Komlós–Szemerédi (AKS) sorting network is explicit, but it is immensely complicated, and it relies on an expander graph construction, whose formalization is a separate difficult issue on its own.

The goal of Chapters V and VI is to formalize the AKS sorting network proper (i.e., minus the expander construction) in a suitable theory of bounded arithmetic, which then yields monotone θ^n_k formulas whose defining properties have polytime-constructible *LK* proofs by means of propositional translation, modulo an assumption that the theory can prove the existence of the necessary expanders.

The most natural theory that translates to *LK* (Frege) is VNC^1 of Cook and Morioka [21], which corresponds to fully uniform NC^1 (i.e., ALOGTIME $= U_E$-uniform NC^1). As such, the theory can prove that we can evaluate $O(\log n)$-depth (bounded fan-in) Boolean circuits that are presented by their *extended connection language* (*ecl*), as defined by Ruzzo [57]. Unfortunately, the intricate construction of the AKS network does not seem to lend itself to an efficient description of the ecl; we only have the direct connection language (dcl) available, precluding formalization in VNC^1.

In order to solve this problem, we have to find a suitable theory extending VNC^1 where the formalization can go through, but such that it still translates to polynomial-size Frege proofs. This is the purpose of Chapter V. We introduce a theory VNC^1_*, axiomatized using a derivation rule that ensures that we can evaluate any $O(\log n)$-depth circuit whose dcl is definable by a formula without second-order parameters which is VNC^1_*-provably Δ^B_1. We also consider its universal conservative extension $\overline{\mathit{VNC}}^1_*$, whose terms correspond to the Σ^B_1-definable functions of VNC^1_*. We develop both theories and establish their basic properties. In particular, we show that the provably total computable functions of VNC^1_* form a class that includes fully uniform NC^1 functions, and is included among L-uniform NC^1 functions, and crucially, we establish that propositional translations of $\forall\Sigma^b_0$ theorems of VNC^1_* (even in the richer language of $\overline{\mathit{VNC}}^1_*$) have L-uniform polynomial-size *LK* proofs.

In Chapter VI, we proceed to formalize the AKS sorting network (or rather, the somewhat simplified network by Paterson [51]) in VNC^1_*. We modified some inessential details of the construction to facilitate the formalization, and we stream-lined the presentation. The formalization is done under an assumption that VNC^1_* can prove the existence of suitable expander graphs.

We then apply translation of bounded arithmetic to propositional logic: the $\overline{VNC}^1_*$-function that defines the AKS network translates to an L-uniform sequence of monotone $O(\log n)$-depth formulas for the θ^n_k functions, and our VNC^1_* proof that the network correctly sorts translates to L-uniform *LK* proofs establishing the defining properties of the θ^n_k formulas. Thus, all in all, we obtain a proof that *MLK* polynomially simulates *LK* on monotone sequents (the Think Positively Conjecture), modulo our assumption on the existence of expanders in VNC^1_*.

This assumption was subsequently proved (even in VNC^1) by Buss, Kabanets, Kolokolova, and Koucký [14], hence the p-simulation of *LK* by *MLK* is now fully settled. (A rudimentary form of some of their results [36] circulated already before our work.) By results of Jeřábek [33], this also extends to a p-simulation of *LK* (on arbitrary sequents) by the proof system *MCLK* which allows arbitrary sequents in the proof, but restricts the *cut rule* to monotone cut formulas.

It remains an open problem if *tree-like MLK* p-simulates *MLK* (or equivalently, if tree-like *MCLK* p-simulates *LK*).

2.4 Induction in TC^0 theories and root finding

The last two chapters of this dissertation investigate the power of theories corresponding to (DLOGTIME-uniform) TC^0. The class TC^0 has fundamental significance in that it describes the complexity of *elementary arithmetic operations*: the basic integer operations $+$, $-$, $\cdot$, $/$, and the $<$ relation, are computable in TC^0; while $+$, $-$, and $<$ are even in $\mathrm{AC}^0 \subseteq \mathrm{TC}^0$, the operations $\cdot$ and $/$ are TC^0-*complete* under AC^0 Turing reductions. We can also compute in TC^0 iterated addition $\sum_{i<n} X_i$

and iterated multiplication $\prod_{i<n} X_i$. Apart from $\mathbb{Z}$, we can also do the corresponding operations in $\mathbb{Q}$, $\mathbb{Q}(i)$, or other number fields, as well as structures such as polynomial rings. Using iterated addition and multiplication, we can compute approximations of analytic functions given by sufficiently nice power series, such as sin, arctan, exp, or log.

We stress that the TC^0-computability of integer division and iterated multiplication (and other above-mentioned functions that depend on these) is a quite nontrivial result of Hesse, Allender, and Barrington [29] (building on Beame, Cook, and Hoover [9], and Chiu, Davida, and Litow [18]).

The basic theory of bounded arithmetic corresponding to TC^0 is the two-sorted theory VTC^0 introduced by Nguyen and Cook [44]. We may interpret provability in VTC^0 as a formalization of *feasible reasoning about elementary arithmetic operations* $+, \cdot, <$: what can we prove about them while only referring to concepts that do not exceed their complexity? (Note that we are concerned here with operations on *binary* integers, i.e., the second sort of VTC^0; operations on unary integers have much lower complexity.) More precisely, we ask what sentences in the basic language of arithmetic $\{+, \cdot, <\}$ are provable in VTC^0 if we interpret them over the binary integer sort. (This is a particular case of the $RSUV$ isomorphism.)

We are particularly interested if VTC^0 proves any nontrivial instances of induction for binary integers: specifically, let us ask whether VTC^0 (or some extension thereof that still corresponds to TC^0) proves *open* (i.e., *quantifier-free*) *induction*, that is, the $RSUV$-translation of the theory *IOpen* introduced by Shepherdson [58].

The provability of *IOpen* in VTC^0, even extended with true universal (i.e., $\forall\Sigma^B_0$) sentences, has nontrivial computational consequences: if $f(X)$ is any polynomial (with integer coefficients given by second-sort parameters), induction for the formula $f(X) < 0$ is a $\forall\Sigma^B_1$ statement, where the witness to the existential quantifier solves the following search problem: given a (fixed-degree) polynomial f and an integer $X > 0$ such that $f(0) < 0 \leq f(X)$, find an integer $Y < X$ such that $f(Y) < 0 \leq f(Y+1)$.

If this instance of induction is provable in $VTC^0 + \mathrm{Th}_{\forall\Sigma^B_0}(\mathbb{N})$, the search problem is computable by a TC^0 function, which we can easily manipulate to obtain, for each constant d, a TC^0 *root approximation algorithm* for degree-d univariate polynomials: given such a polynomial f and $\varepsilon > 0$, compute rational approximations within additive error ε of all real roots of f, or even $\mathbb{Q}(i)$ approximations of all complex roots of f. (This is, in fact, *equivalent* to provability of *IOpen* in $VTC^0 + \mathrm{Th}_{\forall\Sigma^B_0}(\mathbb{N})$.)

We tackle this computational complexity problem first: in Chapter VII (originally published as [D7]), we prove that TC^0 degree-d root approximation algorithms exist for any constant d. The argument uses tools from complex analysis. The basic idea is that if a is "close" to a root α of a polynomial f, then f has an analytic inverse function g on a neighbourhood of $f(a)$ including 0, and $g(0) = \alpha$. The coefficients of the power series of g can be determined by the *Lagrange inversion formula* (*LIF*), which makes them TC^0-computable, and then $g(0)$ can be approximated in TC^0 by computing a partial sum of the power series.

The exact meaning of a being "close" to α can be quantified using the Cauchy integral formula. Using this, we can set up a polynomial-size set of sample points a such that each root of f is close enough to some a; thus, locally inverting f (as explained above) near all sample points in parallel, we obtain a TC^0 algorithm that computes approximations of all roots of f.

The provability of *IOpen* (and more) in a mild extension of VTC^0 is demonstrated in Chapter VIII (originally published as [D8]). The reason it does not go through in VTC^0 itself is that we need iterated multiplication (and division) all over the place, but formalization of the Hesse, Allender, and Barrington algorithm is a serious problem on its own that's mostly tangential to the question of constant-degree root finding. Thus, we work in the theory $VTC^0 + IMUL$, where the *IMUL* axiom is a suitable formalization of the totality of iterated integer multiplication.

Again, one idea we use is to locally invert polynomials by power series whose coefficients are given by LIF. We can prove a suitable version of

LIF in $VTC^0 + IMUL$ by direct manipulation of multinomial coefficients; in absence of other complex-analytic tools, this allows us to formalize root approximation for polynomials f such that, roughly speaking, the constant coefficient of f is very small w.r.t. the remaining coefficients.

We complement this with a model-theoretic argument based on properties of *valued fields*. Any ordered field F, such as the fraction field of a model M of arithmetic, carries a natural valuation; the completion $\hat{F}$ of F as a valued field coincides with the *Scott completion* of F, which is the largest ordered field extension of F in which F is dense. Exploiting a criterion of Shepherdson [58], we have that $M \vDash IOpen$ iff $\hat{F}$ is a real-closed field. By basic properties of valued fields, one can show that F has a real-closed completion iff its value group is divisible, its residue field is real-closed, and F is *almost henselian*. In the case of F induced from a model of $VTC^0 + IMUL$, the last condition follows from root approximation of polynomials with small constant coefficients that we proved earlier using LIF.

In this way, we prove *IOpen* in $VTC^0 + IMUL$. Leveraging the argument more, we can formalize in $VTC^0 + IMUL$ a suitable version of a result of Mantzivis [42] on the structure of sets defined by sharply bounded (Σ^b_0) formulas, using root approximation for constant-degree polynomials for the base case of atomic formulas; thus, $VTC^0 + IMUL$ proves the $RSUV$ translation of induction and minimization for Σ^b_0 formulas in Buss's language (and even in certain extensions of the language).

We add that Jeřábek [34] recently succeeded to formalize a suitable version of the Hesse–Allender–Barrington algorithm in the base TC^0-theory VTC^0, showing that VTC^0 proves *IMUL*. Thus, by the results of Chapter VIII, the $RSUV$ translation of Σ^b_0-MIN (including *IOpen*) is provable in VTC^0.

Publications constituting the dissertation

[D1] Emil Jeřábek, *Approximate counting in bounded arithmetic*, Journal of Symbolic Logic 72 (2007), no. 3, pp. 959–993.

[D2] ———, *Approximate counting by hashing in bounded arithmetic*, Journal of Symbolic Logic 74 (2009), no. 3, pp. 829–860.

[D3] ———, *Abelian groups and quadratic residues in weak arithmetic*, Mathematical Logic Quarterly 56 (2010), no. 3, pp. 262–278.

[D4] ———, *Integer factoring and modular square roots*, Journal of Computer and System Sciences 82 (2016), no. 2, pp. 380–394.

[D5] ———, *On theories of bounded arithmetic for* NC^1, Annals of Pure and Applied Logic 162 (2011), no. 4, pp. 322–340.

[D6] ———, *A sorting network in bounded arithmetic*, Annals of Pure and Applied Logic 162 (2011), no. 4, pp. 341–355.

[D7] ———, *Root finding with threshold circuits*, Theoretical Computer Science 462 (2012), pp. 59–69.

[D8] ———, *Open induction in a bounded arithmetic for* TC^0, Archive for Mathematical Logic 54 (2015), no. 3–4, pp. 359–394.

References

[1] Miklós Ajtai, *The complexity of the Pigeonhole Principle*, Combinatorica 14 (1994), pp. 417–433.

[2] Miklós Ajtai, János Komlós, and Endre Szemerédi, *Sorting in $c \log n$ parallel steps*, Combinatorica 3 (1983), no. 1, pp. 1–19.

[3] ———, *An $O(n \log n)$ sorting network*, in: Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 1983, pp. 1–9.

[4] Albert Atserias, *The complexity of resource-bounded propositional proofs*, Ph.D. thesis, Universitat Politècnica de Catalunya, Barcelona, 2002.

[5] Albert Atserias, Nicola Galesi, and Ricard Gavaldà, *Monotone proofs of the Pigeon Hole Principle*, Mathematical Logic Quarterly 47 (2001), no. 4, pp. 461–474.

[6] Albert Atserias, Nicola Galesi, and Pavel Pudlák, *Monotone simulations of non-monotone proofs*, Journal of Computer and System Sciences 65 (2002), no. 4, pp. 626–638.

[7] Albert Atserias and Neil Thapen, *The ordering principle in a fragment of approximate counting*, ACM Transactions on Computational Logic 15 (2014), no. 4, article no. 29.

[8] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, Pavel Pudlák, and Alan Woods, *Exponential lower bounds for the pigeonhole principle*, in: Proceedings of the 24th Annual ACM Symposium on Theory of Computing, 1992, pp. 200–220.

[9] Paul W. Beame, Stephen A. Cook, and H. James Hoover, *Log depth circuits for division and related problems*, SIAM Journal on Computing 15 (1986), no. 4, pp. 994–1003.

[10] Alessandro Berarducci and Benedetto Intrigila, *Combinatorial principles in elementary number theory*, Annals of Pure and Applied Logic 55 (1991), no. 1, pp. 35–50.

[11] Joshua Buresh-Oppenheim, *On the* **TFNP** *complexity of factoring*, unpublished note, `http://www.cs.toronto.edu/~bureshop/factor.pdf`, 2006.

[12] Samuel R. Buss, *Bounded arithmetic*, Bibliopolis, Naples, 1986, revision of 1985 Princeton University Ph.D. thesis.

[13] __________, *Relating the bounded arithmetic and polynomial time hierarchies*, Annals of Pure and Applied Logic 75 (1995), no. 1–2, pp. 67–77.

[14] Samuel R. Buss, Valentine Kabanets, Antonina Kolokolova, and Michal Koucký, *Expander construction in* VNC^1, Annals of Pure and Applied Logic 171 (2020), no. 7, article no. 102796, 40 pp.

[15] Samuel R. Buss, Leszek A. Kołodziejczyk, and Neil Thapen, *Fragments of approximate counting*, Journal of Symbolic Logic 79 (2014), no. 2, pp. 496–525.

[16] Samuel R. Buss, Leszek A. Kołodziejczyk, and Konrad Zdanowski, *Collapsing modular counting in bounded arithmetic and constant depth propositional proofs*, Transactions of the American Mathematical Society 367 (2015), no. 11, pp. 7517–7563.

[17] Jin-Yi Cai, $\mathrm{S}_2^p \subseteq \mathrm{ZPP}^{\mathrm{NP}}$, Journal of Computer and System Sciences 73 (2007), no. 1, pp. 25–35.

[18] Andrew Y. Chiu, George I. Davida, and Bruce E. Litow, *Division in logspace-uniform* NC^1, RAIRO – Theoretical Informatics and Applications 35 (2001), no. 3, pp. 259–275.

[19] Peter Clote and Jan Krajíček (eds.), *Arithmetic, proof theory, and computational complexity*, Oxford Logic Guides vol. 23, Oxford University Press, 1993.

[20] __________, *Open problems*, in *Arithmetic, proof theory, and computational complexity* [19], pp. 1–19.

[21] Stephen Cook and Tsuyoshi Morioka, *Quantified propositional calculus and a second-order theory for* $\mathbf{NC}^1$, Archive for Mathematical Logic 44 (2005), no. 6, pp. 711–749.

[22] Stephen A. Cook, *Feasibly constructive proofs and the propositional calculus*, in: Proceedings of the 7th Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[23] Stephen A. Cook and Jan Krajíček, *Consequences of the provability of* $\mathbf{NP} \subseteq \mathbf{P/poly}$, Journal of Symbolic Logic 72 (2007), no. 4, pp. 1353–1371.

[24] Charalambos Cornaros, *On Grzegorczyk induction*, Annals of Pure and Applied Logic 74 (1995), no. 1, pp. 1–21.

[25] Paola D'Aquino and Angus Macintyre, *Quadratic forms in models of* $I\Delta_0 + \Omega_1$*. I*, Annals of Pure and Applied Logic 148 (2007), pp. 31–48.

[26] __________, *Quadratic forms in models of* $I\Delta_0 + \Omega_1$*, Part II: Local equivalence*, Annals of Pure and Applied Logic 162 (2011), no. 6, pp. 447–456.

[27] Paul Erdős, *On a problem in graph theory*, Mathematical Gazette 47 (1963), no. 361, pp. 220–223.

[28] Roger Heath-Brown, *Fermat's two squares theorem*, Invariant 11 (1984), pp. 3–5, Oxford University Invariant Society.

[29] William Hesse, Eric Allender, and David A. Mix Barrington, *Uniform constant-depth threshold circuits for division and iterated multiplication*, Journal of Computer and System Sciences 65 (2002), no. 4, pp. 695–716.

[30] Emil Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, Annals of Pure and Applied Logic 129 (2004), pp. 1–37.

[31] __________, *On independence of variants of the weak pigeonhole principle*, Journal of Logic and Computation 17 (2007), no. 3, pp. 587–604.

[32] __________, *Substitution Frege and extended Frege proof systems in non-classical logics*, Annals of Pure and Applied Logic 159 (2009), no. 1–2, pp. 1–48.

[33] __________, *Proofs with monotone cuts*, Mathematical Logic Quarterly 58 (2012), no. 3, pp. 177–187.

[34] __________, *Iterated multiplication in VTC^0*, arXiv:2011.03095 [cs.LO], 2020, `https://arxiv.org/abs/2011.03095`. Accepted to Archive for Mathematical Logic.

[35] Valentine Kabanets, Charles Rackoff, and Stephen A. Cook, *Efficiently approximable real-valued functions*, Technical Report TR00-034, Electronic Colloquium on Computational Complexity, 2000.

[36] Michal Koucký, Valentine Kabanets, and Antonina Kolokolova, *Expanders made easy: The combinatorial analysis of an expander construction*, unpublished manuscript, 2007.

[37] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications vol. 60, Cambridge University Press, 1995.

[38] ——————, *Approximate Euler characteristic, dimension, and weak pigeonhole principles*, Journal of Symbolic Logic 69 (2004), no. 1, pp. 201–214.

[39] Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti, *Bounded arithmetic and the polynomial hierarchy*, Annals of Pure and Applied Logic 52 (1991), no. 1–2, pp. 143–153.

[40] Franz Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer, 2000, see also `https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html`.

[41] Alexis Maciel, Toniann Pitassi, and Alan R. Woods, *A new proof of the weak pigeonhole principle*, Journal of Computer and System Sciences 64 (2002), no. 4, pp. 843–872.

[42] Spyro-Giorgio Mantzivis, *Circuits in bounded arithmetic part I*, Annals of Mathematics and Artificial Intelligence 6 (1991), no. 1–3, pp. 127–156.

[43] Moritz Müller and Ján Pich, *Feasibly constructive proofs of succinct weak circuit lower bounds*, Annals of Pure and Applied Logic 171 (2020), no. 2, article no. 102735, 45 pp.

[44] Phuong Nguyen and Stephen A. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science 2 (2006), no. 1, article no. 3, 39 pp.

[45] Noam Nisan and Avi Wigderson, *Hardness vs. randomness*, Journal of Computer and System Sciences 49 (1994), no. 2, pp. 149–167.

[46] Christos H. Papadimitriou, *On the complexity of the parity argument and other inefficient proofs of existence*, Journal of Computer and System Sciences 48 (1994), no. 3, pp. 498–532.

[47] Rohit Parikh, *Existence and feasibility in arithmetic*, Journal of Symbolic Logic 36 (1971), no. 3, pp. 494–508.

[48] Jeff B. Paris and Alex J. Wilkie, Δ_0 *sets and induction*, in: Open days in model theory and set theory. Proceedings of a conference held in September 1981 at Jadwisin, near Warsaw, Poland (W. Guzicki, W. Marek, A. Pelc, and C. Rauszer, eds.), Leeds University Press, 1983, pp. 237–248.

[49] __________, *Counting problems in bounded arithmetic*, in: Methods in Mathematical Logic (C. A. Di Prisco, ed.), Lecture Notes in Mathematics vol. 1130, Springer, 1985, pp. 317–340.

[50] Jeff B. Paris, Alex J. Wilkie, and Alan R. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, Journal of Symbolic Logic 53 (1988), no. 4, pp. 1235–1244.

[51] Michael S. Paterson, *Improved sorting networks with* $O(\log N)$ *depth*, Algorithmica 5 (1990), no. 1, pp. 75–92.

[52] Ioseph [Giuseppe] Peano, *Arithmetices principia, nova methodo exposita*, Fratelli Bocca, Torino, 1889 (in Latin).

[53] Ján Pich, *Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic*, Logical Methods in Computer Science 11 (2015), no. 2, article no. 8, 38 pp.

[54] Pavel Pudlák, *Ramsey's theorem in bounded arithmetic*, in: Proceedings of Computer Science Logic '90 (E. Börger, H. K. Büning, M. M. Richter, and W. Schönfeld, eds.), Lecture Notes in Computer Science vol. 533, Springer, 1991, pp. 308–317.

[55] __________, *On the complexity of propositional calculus*, in: Sets and proofs: Invited papers from Logic Colloquium '97 (S. B. Cooper and J. K. Truss, eds.), Cambridge University Press, 1999, pp. 197–218.

[56] Alexander A. Razborov and Steven Rudich, *Natural proofs*, Journal of Computer and System Sciences 55 (1997), no. 1, pp. 24–35.

[57] Walter L. Ruzzo, *On uniform circuit complexity*, Journal of Computer and System Sciences 22 (1981), no. 3, pp. 365–383.

[58] John C. Shepherdson, *A nonstandard model for a free variable fragment of number theory*, Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques 12 (1964), no. 2, pp. 79–86.

[59] Michael Sipser, *A complexity theoretic approach to randomness*, in: Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 1983, pp. 330–335.

[60] Seinosuke Toda, *On the computational power of PP and $\oplus P$*, in: Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science, 1989, pp. 514–519.

[61] Leslie G. Valiant, *Short monotone formulae for the majority function*, Journal of Algorithms 5 (1984), no. 3, pp. 363–366.

[62] Don Zagier, *A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares*, American Mathematical Monthly 97 (1990), no. 2, p. 144.

[63] Domenico Zambella, *Notes on polynomially bounded arithmetic*, Journal of Symbolic Logic 61 (1996), no. 3, pp. 942–966.