Review of
Metamathematics of First-Order Arithmetic

by P. Hájek and P. Pudlák

Since its first hardback appearance in 1993 the book under review has become one of the most influential monographs in the area of logic.

The study of systems of formal arithmetic has been at the center of mathematical logic ever since K. Gödel obtained his famous incompleteness theorems in 1930. In the following decades the subject evolved into an extensive discipline with deep roots in model theory, proof theory and computation theory, and with its own remarkable achievements and sophisticated methods. The interest in formal arithmetic shifted from incompleteness and consistency proofs in the 30's and 40's to general questions of arithmetization, reflection principles and interpretability in the 50's and 60's. Another impetus came from a different direction by the solution of Hilbert's 10-th problem by Yu. Matiyasevich preceded by the work of J. Robertson, M. Davis and H. Putnam. In the 70's and 80's the field has been strongly influenced by the contribution of J. Paris and his school to the model theory of arithmetic, which culminated in the discovery of independent combinatorial principles. The most recent upsurge of interest was due to the discovered connections between weak systems of arithmetic and computation complexity theory, the topic to which the second author of the book, among others, made principal contributions.

The monograph provides an encompassing and systematic view of this landscape. From the other books published on the subject [1, 2, 3, 4, 5], the present work is distinguished by the variety of covered topics. It is not the kind of book where one particular method or point of view prevails, but rather an open-ended book, where you see a variety of different methods applied to a number of different areas, difficulties are not hidden and connections are emphasized.

Perhaps, as with many encyclopedic in-depth monographs, there is a price to pay — the loss of some potential readership. The book will probably be too difficult for an average graduate student, it includes some relatively complex material which textbooks would normally leave out. (The books by R. Kaye and C. Smoryński are better suited as graduate texts, but they do not offer comparable breadth.) The presentation is not very polished, there are lots of misprints and little inaccuracies that may annoy the reader a great deal.

However, the book is extremely useful for a specialist. It is rich in ideas. It brings together in a systematic way a vast amount of material, which can otherwise only be found scattered among a large number of papers. It also contains an amazing 43 pages long bibliography, an invaluable source for professionals working in the field and for all those who want to seriously get into this subject. It is the kind of book every working logician should have on his shelf.

The book is divided into three parts: the part on 'positive results' on fragments of arithmetic, the part on 'incompleteness', and the part on bounded arithmetic.

Chapter 1 of the book introduces basic fragments of arithmetic and establishes their main relationships. It also develops the encoding of sets, logical syntax and some recursion theory in suitable fragments. The system $I\Sigma_1$ of induction for Σ_1-definable (r.e.) predicates serves as the basic fragment for the first two parts of the book. An important technical tool is the construction of partial truth definitions in $I\Sigma_1$. On the recursion-theoretic side, the so-called low basis theorem in $I\Sigma_1$ is established. Using the low basis theorem a version of the arithmetized completeness theorem for first order logic is proved. Then one obtains some corollaries on the provability of reflection principles in fragments $I\Sigma_n$. (This is not the most standard way of arriving at reflection principles. One usually proves reflection principles by proof-theoretic cut-elimination techniques. But the present method keeps up with the generally semantic spirit of the book.)

Chapter 2 is devoted to combinatorics in fragments. It gives an extensive discussion of Ramsey-type theorems. The authors consider the classic Paris–Harrington principle as well as some restricted versions of the infinite Ramsey theorem, for which their exact place in the hierarchy of fragments of arithmetic is found. Main result of the chapter is the equivalence of the Paris–Harrington principle (and refinements thereof) with Σ_1-reflection principles over Peano arithmetic and its fragments. This is done by the method of indiscernibles. Finally, α-large sets, transfinite induction and fast growing hierarchy of provably total recursive functions in fragments $I\Sigma_n$ is discussed. This part of the chapter is mainly based on the work of Ketonen and Solovay.

Chapter 3, the first one in the part on incompleteness, presents a modern introduction into Gödel's incompleteness theorems, interpretability and partial conservativity. The main tool is Gödel's method of self-reference, which also provides a name to the chapter. However, some other important techniques are presented here, for example, Solovay's method of shortening cuts. Apart from Gödel's theorems the chapter includes Orey–Feferman–Hájek characterization of interpretability in pure extensions of Peano arithmetic, Lindström's theorem on Π^0_2-completeness of the set of partially conservative sentences and various related results by Solovay, Guaspari and Hájek. It also presents Pudlák's strengthening of Gödel's second incompleteness theorem, though in a somewhat less general form than in the original 1985 paper.

The relatively short Chapter 4 presents model theory of fragments of arithmetic. Some basic constructions in nonstandard models are developed. Theorems concerning the existence of elementary end extensions and Paris–Friedman conservation result for Σ_{n+1}-collection schema over $I\Sigma_n$ are proved. Furthermore, Friedman's theorem stating that every nonstanderd model of $I\Sigma_1$ has a proper initial segment isomorphic to a model of Peano arithmetic is established. In the same chapter the provably total recursive functions of theories $I\Sigma_n$ are studied by the method of indicators. In particular, provably total recursive functions of $I\Sigma_1$ are shown to coincide with primitive recursive functions. (By the way, this result originally proved by C. Parsons [7] is not quite correctly attributed in the book only to G. Mints and G. Takeuti, who obtained it several years later.) Provably total functions of Peano arithmetic are characterized using the fast growing hierarchy and using α-large sets. This is a natural continuation of the theme of Chapter 2.

Chapter 5, identical with Part 3 of the book, deals with bounded arithmetic. It can be read, to a large extent, independently from the previous parts and is a little book in itself. It begins with a very clear survey of basic weak fragments of arithmetic and their relative strength. Parikh's theorem on Δ_0-definable functions provably total in $I\Delta_0$ and its immediate generalizations are presented. Then a brief introduction to the relevant parts of complexity theory is given. This includes, first of all, definitions of the main time and space complexity classes and compexity-theoretic hierarchies. Most of the attention is paid to the linear time and polynomial time hierarchies. It is shown that Δ_0-definable sets coincide with the linear time hierarchy, the proof is based on a theorem of Nepomnyashchij. Some examples of separating complexity classes and hierarchies by diagonal method are also presented.

Section 3 of Chapter 5 is largely technical. It is devoted to the problems of encoding in bounded arithmetic. It presents a detailed construction of a Δ_0-definition of the graph of exponentiation function as well as of the function counting the number of ones in a binary expansion. It also shows how to verify necessary properties of these functions in bounded arithmetic. A general result on how to formalize syntax based on contex-free grammars is presented.

Section 4 develops Buss' important hierarchies of the bounded arithmetic systems S_2^n and T_2^n. Using model-theoretic techinques Buss' results on provably total Σ_n^b-definable functions in S_2^n are proved, including the important characterization of polynomial time computable functions as $\exists\Sigma_1^b$-definable and provably total in S_2^1. In the same section a remarkable theorem due to Krajíček, Pudlák and Takeuti is also established: If the polynomial time hierarchy does not collapse, then neither does Buss' hierarchy of fragments S_2^n.

Section 5 deals with interpretability and consistency in the context of weak arithmetic and presents a very beautiful piece of theory mainly due to A. Wilkie and P. Pudlák. First of all, using shortening of cuts techniques it is shown that rather strong bounded arithmetic theories $I\Delta_0 + \Omega_n$ are interpretable in, and hence provably equiconsistent with, a very weak system Q. Hence, it is impossible to prove in $I\Delta_0 + \Omega_n$ the consistency of Q. Secondly, alternative formalized notions of provability are studied: Herbrand provability, cut-free provability and cut-rank k-provability. Using these notions several characterizations due to Wilkie and Paris of the set of Π_1-sentences provable in $I\Delta_0 + exp$ are obtained. Finally, yet another beautiful strengthening of Gödel's second incompleteness theorem (with respect to k-consistency relativized to a cut) is obtained.

This ends our survey of the material in the book. Despite the very broad scope of the monograph the reader should be warned that not everything important is in there. Some significant material concerning formal arithmetic was left out, for example, the proof of Matiyasevich theorem, the theory of parameter-free induction and collection principles as well as of the fragments of arithmetic axiomatized by inference rules. The model theory chapter of the book is somewhat shorter than one expects, e.g., recursively saturated models are absent. The part on self-reference lacks provability and interpretability logic. However, the authors tried to provide in all such cases sufficient references to the existing literature, including textbooks. Thus, Matiyasevich theorem is presented in detail in [2] and there is a newer book by Matiyasevich [6] on the same topic. Kaye's book [1] provides additional information on recursively saturated models and satisfaction classes. Lindström [5] gives more information on lattices of interpretability and partial conservativity and can be considered as a valuable extension of Chapter 2 of the book under review. There are several good textbooks on provability logic and self-reference.

One should also mention that by now bounded arithmetic has been developed well beyond the material presented in the last part of the book. Most importantly, a lot of research has recently been done on connections between bounded arithmetic and propositional and algebraic proof complexity. These connections are elaborated in Krajíček [4].

Overall, the book is a very important contribution to the logical literature. It has not lost its significance in the past 10 years since its first appearance and predictably will not in many years to come.

References

[1] R. Kaye. *Models of Peano arithmetc*, Oxford University Press, 1991.

[2] C. Smoryński. *Logical number theory I*, Springer–Verlag, 1991.

[3] S. Buss. *Bounded arithmetic*, Bibliopolis, Napoli, 1986.

[4] J. Krajíček. *Bounded arithmetic, propositional logic and complexity theory*, Oxford University Press, 1993.

[5] P. Lindström. *Aspects of incompleteness*, Lecture Notes in Logic, no. 10, Springer–Verlag, 1997.

[6] Yu. V. Matiyasevich. *Hilbert's Tenth Problem*, MIT Press, Cambridge, Massachusetts, 1993.

[7] C. Parsons. *On a number-theoretic choice schema and its relation to induction*, Intuitionism and Proof Theory, A. Kino, J. Myhill and R.E. Vessley, editors, North Holland, Amsterdam, 1970, 459–473.