The Book Review Column[1]

by Frederic Green

Departments of Mathematics and Computer Science
Clark University
Worcester, MA 01610
email: fgreen@clarku.edu

Sadly, I never had a chance to really get to know Juris Hartmanis. However, at the time that I was still wondering what avenues to pursue in computer science, his work was one of my principle motivations. His talks, several of which I remember attending back in the 1980s, were crystal clear, entertaining, and inspiring. As much as he will be missed, he lives on through his legacy, as manifested in his work as well as his many eminent students.

Hence we set aside the usual format of the Book Review Column, and present a review of one of his books, published in 1978. As far as I have been able to tell, it was never reviewed in SIGACT News. It should have been, is notably of current interest, and at last here it is.

As promised in my previous column, the next column will be the work of my successor, Nicholas Tran.

Review of[2]
Feasible Computations and Provable Complexity Properties
by Juris Hartmanis
SIAM, 1978
62 pages, Paperback

Review by
Frederic Green (fgreen@clarku.edu)
Departments of Mathematics and Computer Science
Clark University, Worcester, MA

"It may only be a slight exaggeration to claim that in the 1930s we started to understand what is and is not *effectively* computable and that in the 1970s we started to understand what is and is not *practically* or *feasibly* computable. There is no doubt that the results about what can and cannot be effectively computed or formalized in mathematics have had a profound influence on mathematics, and, even more broadly, they have influenced our view of our scientific methods. We believe that the results about what can and cannot be practically computed will also have a major influence on computer science, mathematics, and even though more slowly, will affect other research areas and influence how we think about scientific theories."
– *Juris Hartmanis* (from the Introduction)

1 Introduction

Although this book was written a very long time ago by the standards of our field, its content continues to be investigated and provide motivation for further research. The overarching themes encompass some of the most important aspects of the theory that Hartmanis studied, and in many cases originated, and which led to countless contributions by the research community over the years. Notably, this includes gems such as the isomorphism conjecture, the closely related question of whether NP-complete problems can reduce to sparse sets, and the possible independence of questions such as $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$. It is striking (or depressing, depending on your frame of mind) how many of the open problems mentioned are still open.

2 Summary of Contents

In the brief Introduction (Chapter 1), Hartmanis states that the goal of the book is to give an overview of "recent developments in the structure of feasible computations," including a focus on properties of feasible computations that are or are not formally provable. This is followed by a summary of the topics to be covered.

Chapter 2, "Reductions and Complete Sets," sets down the basic definitions of reductions, complexity classes, completeness. Here and throughout the rest of the book the emphasis is on *logspace* many-one reductions ("L-reductions") and the corresponding completeness notions. The principle complexity classes investigated include $\mathsf{L}, \mathsf{NL}, \mathsf{DCSL}, \mathsf{CSL}, \mathsf{P}, \mathsf{NP}, \mathsf{PSPACE}, \mathsf{EXP}$, and $\mathsf{EXPSPACE}$[3]. A few NL and NP-complete problems are listed, and basic information about what is known (including some easier proofs) or

[3] Here I am using the currently more common notations for the latter three, called in the book, $\mathsf{PTAPE}, \mathsf{EXPTIME}$, and $\mathsf{EXPTAPE}$, respectively.

unknown regarding relations among these classes are also summarized. The unknown results (e.g., $\mathsf{DCSL} \overset{?}{\subseteq} \mathsf{P}$ or vice vera, and, of course famous ones such as $\mathsf{P} \overset{?}{=} \mathsf{NP}$) remain unknown to this day.

Chapter 3, "L-Isomorphisms of Complete Sets," treats the isomorphism conjecture, which asserts that NL-complete and NP-complete sets are, respectively, logspace isomorphic. This is a hard thing to prove since it immediately implies that $\mathsf{L} \neq \mathsf{NL}$ and $\mathsf{P} \neq \mathsf{NP}$. (The same implication holds for $\mathsf{P} \neq \mathsf{NP}$ under polynomial-time reductions.) The route to this conjecture starts with the development of a criterion for determining if a set is isomorphic to the "known" complete sets. That criterion is similar to the "p-paddable" set for classes like NP and PSPACE, here re-worked to accommodate logspace reductions. The universal complete sets for the classes considered here have that property, and furthermore any complete set has the property iff it is L-isomorphic to the corresponding universal complete set (this is a vague statement of Theorem 3.7). A large number of known complete sets have been checked to have that property. Thus this reasoning culminates in the concluding claim of the chapter, namely that the "known" complete sets for $\mathsf{NL}, \mathsf{CSL}, \mathsf{P}, \mathsf{NP}, \mathsf{PSPACE}$, etc., are all, respectively, L-isomorphic. The sticking point, of course, is that we can't be sure we have covered all complete sets by just checking the known ones. To this date, it is unknown if the "known" complete sets are or are not representative of the "unknown" ones.

It is immediate, assuming the isomorphism conjecture is true, that NP-complete sets cannot be sparse (i.e., have polynomial density). Berman and Hartmanis's conjecture [BH], repeated here, stated that indeed NP-complete sets cannot be sparse (resolved in 1982 by Mahaney [Ma], who showed that the existence of sparse complete sets sets for NP is *equivalent* to $\mathsf{P} = \mathsf{NP}$). One then is also quickly led to the question of whether NP-complete sets *reduce* to sparse sets, irrespective of membership in NP. That is one of the main topics of Chapter 4, "Structure of Complete Sets." (For an extensive summary of subsequent research, see [CO].) The other is whether complete sets in certain classes have easily computable infinite subsets. E.g., an important question is whether NP-complete sets have infinite subsets in P (as the current terminology would say, that NP-complete sets are not p-immune). However, as this would imply that NP-complete sets are infinite, and hence $\mathsf{P} \neq \mathsf{NP}$, this problem remains open. Regarding sparse sets, the chapter proves that no L-complete language for $\mathsf{CSL}, \mathsf{PSPACE}, \mathsf{EXP}$, or $\mathsf{EXPSPACE}$ can be sparse. Whether results of this kind hold for NP remains open, although there has been much work in the intervening years concerning the existence of sparse NP-hard sets, given some commonly held complexity theoretic assumptions (e.g., Karp/Lipton's theorem [KL] that the existence of sparse hard sets for NP implies the collapse of the polynomial hierarchy to the second level, or Mahaney's theorem mentioned above). Regarding non-L-immunity, the chapter shows that every L-complete set for DCSL contains infinite logspace recognizable subsets, a technique that generalizes (e.g.) to CSL and PSPACE.

Hartmanis draws on the techniques of Chapter 4 to prove that, in any formal proof system, there exist infinite sets of "trivially true" theorems whose proofs must, of necessity, be as long as the proofs of the "hardest" theorems. Furthermore, these infinitely many sets can be found effectively. Hartmanis summarizes the significance of these results as follows:

> These results show very clearly that we pay a price for formalizing mathematics. In every formalization, infinite sets of trivial theorems will require very long proofs. Thus we have a very dramatic and quantitative explanation why we should not and in practice do not freeze a formation when discussing or doing mathematics. They also give a warning that a necessarily long proof in a formal system does not certify that the result is nontrivial.

These results are the content of Chapter 5, "Long Proofs of Trivial Theorems." It begins by examining the phenomenon in the realm of computability. There it is shown that, given an enumeration of Turing machines, for any creative set B, one can effectively find an infinite recursive subset of B which is easily recognized in space $L(n)$, but which, for any TM in the enumeration recognizing B, requires at least $f \circ L(n)$ space for *any* recursive function f. In the complexity setting, the analog of the infinite recursive subset is regular, but any machine recognizing the analog of B (which we may call here A), requires an amount of space growing with the same rate as that recognizing A.

It was well-known, long before the publication of this book (indeed, by a result of Hartmanis in 1968 [Ha]) that it is not as easy to prove separations between time-complexity classes as it is for space-complexity classes. A standard way to prove the former type of separation is to carry along a "clock" in simulating a single-tape Turing machine, which introduces an overhead that is not necessary in space separations, resulting in separations that are not as sharp. Chapter 6, "What Can and Cannot be Proved About Computational Complexity," takes a different approach, in which the "clock" is replaced by the existence of a formal proof that a TM (against which we are diagonalizing) does not take too much time. Hartmanis defines a F-$TIME[T(n)]$ in which it is formally provable that TMs recognizing the languages in the class take time at most $T(n)$. Even for any recursive function $g(n) \geq 1$, it is proved here that $TIME[T(n) \cdot g(n)] \not\subseteq F$-$TIME[T(n)]$. Thus, assuming F-$TIME[T(n)] = TIME[T(n)]$, one would obtain much sharper bounds for time-bounded classes. Hartmanis conjectures that this equality holds for $T(n)$ with certain honesty conditions (i.e., reasonable functions such as n^2, 2^n, etc.). Later in the chapter he proves that an analogous equality indeed does hold for space classes. On the other hand, there are recursive $T(n)$ for which the equality does *not* hold for time classes, also proved here.

The theme is continued in the final chapter, "Relativized $\mathsf{P} = \mathsf{NP}$ Problem." The famous non-relativizing nature of that question, established by Baker, Gill, and Solovay [BGS], is used as a springboard towards determining if the problem is undecidable. Hartmanis proves that for any formal system F, one may effectively construct a Turing Machine M_i such that $L(M_i) = \varnothing$, and neither $\mathsf{P}^{L(M_i)} = \mathsf{NP}^{L(M_i)}$ nor $\mathsf{P}^{L(M_i)} \neq \mathsf{NP}^{L(M_i)}$ are provable in F. This is one of the results in the book that gave me a bit of a start, since $\mathsf{P}^{L(M_i)} = \mathsf{P}$ and $\mathsf{NP}^{L(M_i)} = \mathsf{NP}$. But, as he points out, it is only the particular formulation of the problem in terms of $\mathsf{P}^{L(M_i)}$ and $\mathsf{NP}^{L(M_i)}$ that is not provable! (A nice relatively recent review of this line of research can be found, e.g., in [Aa].)

3 Opinion

This book provides a brief but definitive overview of some of Hartmanis's central and most influential work. For example, the isomophorphism conjecture with respect to poly-time reducibilities, known as the Berman-Hartmanis Conjecture, gave rise to much fruitful research over the decades, both for and against its possible validity, which still remains open. The final three chapters help lay the foundation of a now long-standing and ongoing technique in the field: If you can't prove something in computational complexity, use computational complexity to explain why it's hard to prove! Examples (since the work of Baker, Gill and Solovay) include such "barrier" ideas as natural proofs and algebrization. These barriers, in turn, have on occasion led the way to techniques that avoid them. No doubt, new barriers, and new techniques to get around them (if possible) will come into view as we learn more.

Hartmanis, one of the founders of computational complexity theory, teaches lessons here that will continue to resonate over many years. This book is eminently worth a carful reading.

References

[Aa] S. AARONSON, "Is P versus NP formally independent?" in *Bulletin of the EATCS* **81**, pp. 109–

136 (2003).
Also `http://people.cs.uchicago.edu/~fortnow/beatcs/column81.pdf`.

[BGS] T. P. BAKER, J. GILL, AND R. SOLOVAY, “Relativizations of the P=?NP question,” in *SIAM Journal on Computing,* **4**(4), pp. 431–442 (1975).

[BH] L. BERMAN AND J. HARTMANIS, *On isomorphisms and density of NP and other complete sets,* in*SIAM Journal on Computing*, **6**(2), pp. 305–322 (1977).

[CO] J.-Y. CAI AND M. OGIHARA, “Sparse Sets versus Complexity Classes,” in *Complexity Theory Retrospective II,* Lane A. Hemaspaandra and Alan L. Selman, eds., Springer 1997, pp. 53–80.]

[Ha] J. HARTMANIS, “Computational complexity of one-tape Turing machine computations,” in *Journal of the ACM*, **15**, pp. 339–352 (1968).

[KL] R. KARP AND R. LIPTON, “Turing machines that take advice,” in *L’enseignement Mathématique*, **28**(3/4), pp. 191–209 (1982).

[Ma] S. MAHANEY, “Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis,” *Journal of Computer and System Sciences*, **25**(2) pp. 130–143 (1982).