Lecture Notes in Computer Science 12050

More information about this series at http://www.springer.com/series/7407

Oded Goldreich et al.

Computational Complexity and Property Testing

On the Interplay Between Randomness and Computation

With Contributions by
Itai Benjamini, Scott Decatur, Maya Leshkowitz, Or Meir, Dana Ron, Guy Rothblum, Avishay Tal, Liav Teichner, Roei Tell, and Avi Wigderson

Springer

Volume Editor
Oded Goldreich
Weizmann Institute of Science
Rehovot, Israel

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-43661-2 ISBN 978-3-030-43662-9 (eBook)
https://doi.org/10.1007/978-3-030-43662-9

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Cover illustration: Artwork by Harel Luz, Tel Aviv, Israel

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains a collection of studies in the areas of complexity theory and property testing. These studies were conducted at different times, mostly during the last decade. Although most of these works have been cited in the literature, none of them were formally published before.

Indeed, this volume is quite unusual, but not without precedence. In fact, in 2011, I published a similar volume, titled *Studies in Complexity Theory and Cryptography* (LNCS, Vol. 6650), and my impression is that it was well received. Still, these volumes raise two opposite questions regarding the publication of the foregoing studies: (1) why were these studies not published (formally) before? and (2) why are they being published now?

I believe that the second question is answered *a posteriori* by the popularity of the first volume. Although many of the works included in it were known before they appeared in that volume, my impression is that their dissemination benefited from this publication. Furthermore, I feel that it is somewhat more appropriate to refer to publication in a volume of the current type rather than to a posting on forums such as ECCC.

The latter assertion is related to the first question; that is, why were these works not published (formally) before, and why not publish them (especially, the more recent ones) in an ordinary venue now? While there are specific reasons in some of the specific cases, I believe that the answer is more general. In a nutshell, I think that the standard mechanism of conferences and journals has become dysfunctional. The source of trouble is over-preoccupation with competition, and neglect of the original goal of providing accessibility and dissemination.

Specifically, the relevant scientific community seems to act as a reviewing panel rather than as an (active) audience; it seems too preoccupied with the question of whether the submission is "competitive" (with respect to the publication venue)[1] and tends to neglect the actual contents of the submission (beyond, of course, whatever is necessary to determine competitiveness). In other words, the energy and resources of the community are devoted to determining competitiveness, and whatever does not serve that goal gets too little attention. Furthermore, under the current mind-frame, having a submission accepted to such a venue merely means "taking the slot" from other submissions.

The point is that I want the works included in this volume to be read, because I think they are interesting. I want them to be read out of interest in their contents, not as means towards ranking them. I do not want to feel that the main effect of submitting a

[1] Originally, "competitive" in the context of these publication venues was understood as fitting some absolute (or relative) standards, but with time "competitive" has evolved to mean worthy of the "award" of being accepted by the venue (as discussed below). I object to the dominance of the question of "competitiveness" even under the former interpretation, let alone under the latter one.

work to a venue is competing against the works of others. I would not feel good about it, regardless of whether I win or lose. I want to contribute to the community, not to compete with its members.

A short detour: On excellence and competitions. Let me stress that I do acknowledge that any realistic struggle for excellence gives rise to a competition, at least implicitly. But this does not mean that struggle and competition are identical; ditto regarding achievement and success. Of course, my issue is not with the semantics of (the colloquial meaning of) these words, but rather with fundamentally different situations that can be identified by referring to these words.

Loosely speaking, by *struggle* I mean both the huge investment of intellectual energy towards *achieving* some goals and the inherent conflict that arises between individuals (or groups) who attempt to achieve the same goals and positions relative to a given setting. That is, the achievements are the goals of the struggle, and the focus of this situation is on the achievements. In contrast, by *competitions* I mean artificial constructs that are defined on top of the basic setting, while not being inherent to it, and *success* typically refers to winning these competitions. That is, success is merely the outcome of the competition, and the focus of this situation is on the competition.

Of course, once these competitions are introduced, the setting changes; that is, a new setting emerges in which these competitions are an inherent part. Still, in some cases—most notably in scientific fields—one can articulate in what sense the original (or basic) setting is better than the modified setting (i.e., the setting modified by competitions). These issues as well as related ones are the topic of my essay *On Struggle and Competition in Scientific Fields*.[2]

Needless to say, in reality we never encounter pure struggles for excellence, devoid of competitional aspects, nor are we likely to encounter—at least in academia—pure competitions devoid of any contents. Reality is always mixed, although it is often useful to analyze it using pure notions. But, currently, the standard publication venues seem extremely biased towards the competition side. Under these circumstances, one may seek alternative vehicles for communicating one's work.

About the contents of this volume. The works included in this collection address a variety of topics in the areas of complexity theory and property testing. Within complexity theory the topics include constant-depth Boolean circuits, explicit construction of expander graphs, interactive proof systems, monotone formulae for majority, probabilistically checkable proofs (PCPs), pseudorandomness, worst-case to average-case reductions, and zero-knowledge proofs. Within property testing the topics include distribution testing, linearity testing, lower bounds on the query complexity (of property testing), testing graph properties, and tolerant testing. A common theme in this collection is *the interplay between randomness and computation*.

About the nature of these works. In the previous volume (LNCS, Vol. 6650), I partitioned the works to three categories labeled 'research contributions', 'surveys', and 'programmatic' papers. The current collection contains a few works for which these

[2] See the web-page http://www.wisdom.weizmann.ac.il/~oded/on-struggle.html as well as *SIGACT News*, Vol. 43, Nr. 1, March 2012.

categories feel too rigid. So I decided to avoid such categories and listed all works in chronological order (of original completion time).

About the revisions. All papers were revised by me in the last few months. In some cases the revision is extremely significant, and in other cases it is very minimal. One benefit of editing this collection is that it provided me with motivation to look back at past works and to reflect on their contents and form in retrospect.

Two outliers. A look at the table of contents reveals two outliers. The first is the work "A Probabilistic Error-Correcting Scheme that Provides Partial Secrecy" (co-authored by Scott Decatur and Dana Ron), which was posted in 1997. This work would have fit better in the previous volume (LNCS, Vol. 6650), and the only reason that it was not included in it is an accidental omission. The second outlier is a (solo) work by Roei Tell, titled "Note on Tolerant Testing with One-Sided Error", which deviates from my original plan of including only works co-authored by me. Still, given that this study grew out of a discussion between us, and that I have supervised its writing (as Roei's PhD adviser), I felt that it was okay to bend the rules a bit.

Acknowledgements. The research underlying the papers included in this volume was partially supported by various Israel Science Foundation (ISF) grants (i.e., Nr. 460/05, 1041/08, 671/13, and 1146/18). The papers were revised and edited while I was enjoying the hospitality of the computer science department of Columbia University.

February 2020 Oded Goldreich

Contents