DISS. ETH NO. 22433

Tradeoffs Between Computational Complexity and Information Content

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES

of

ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

Kfir Shlomo Barhum

M. Sc. in Computer Science and Applied Mathematics,
Weizmann Institute of Science

born June 23, 1980 in Tel-Aviv,
citizen of Israel

accepted on the recommendation of

Prof. Dr. Juraj Hromkovič, examiner
Prof. Dr. Peter Widmayer, co-examiner
Prof. Dr. Stefan Wolf, co-examiner

2015

Abstract

In this dissertation, we study trade-offs between computational complexity and information content of problems arising in different facets of theoretical computer science.

In the first part of the dissertation, we study the information content of online problems. For the online Steiner tree problem, we give matching upper and lower bounds on the advice complexity of the problem for the entire range of advice bits and thus resolve the problem. Then, we continue to study the randomness complexity of the disjoint path allocation problem. Our result shows that, in some cases, it is possible to use random bits instead of advice bits, while maintaining the same performance of the algorithm. In light of previous work on the power of advice bits for this problem, our algorithm is optimal.

The second part of the dissertation is devoted to constructions of cryptographic primitives, focusing on constructions of a universal one-way hash function from a one-way function. First, we relate the regularity assumptions made about the one-way function to the efficiency of the construction, measured by the number of calls it makes to the one-way function. Qualitatively speaking, the stronger the assumptions about the structure of the underlying one-way function are, the better the performance of the construction is. We then study the limits of black-box constructions for this task, which, loosely speaking, are constructions that only use the functionality of the one-way function, but not its description. Since their introduction by Naor and Yung (STOC, 1989) twenty-five years ago, no lower bound on the number of calls to the one-way function such a construction has to make was known other than the trivial one of a single call. We give a first lower bound of an almost-linear number of calls. Moreover, if the function is regular, our bound is tight.

Finally, in the last part of the dissertation, we continue the study of a recently introduced model of communication complexity with advice. We establish that the equality problem admits a protocol of polylogarithmic communication, provided a laconic advice of just one bit. For the divisibility problem, we design a protocol with sublinear communication and advice.

Zusammenfassung

In dieser Dissertation untersuchen wir das Verhältnis zwischen der Berechnungskomplexität und dem Informationsgehalt von Problemen, die in verschiedenen Zusammenhängen innerhalb der theoretischen Informatik auftreten.

Im ersten Teil der Dissertation untersuchen wir den Informationsgehalt von Online-Problemen. Für das Online-Steinerbaum-Problem geben wir übereinstimmende obere und untere Schranken für die Advice-Komplexität an, für das gesamte mögliche Spektrum von verwendeten Advice-Bits. Damit haben wir die Advice-Komplexität dieses Problems abschliessend geklärt. Weiterhin untersuchen wir die Anzahl von Zufallsbits, die notwendig und hinreichend ist, um ein Problem aus dem Bereich der Kommunikationsalgorithmen in Netzwerken, das sogenannte Disjoint-Path-Allocation-Problem, zu lösen. Unsere Ergebnisse zeigen, dass in einigen Fällen Zufallsbits anstelle von Advice-Bits verwendet werden können, ohne die Qualität der berechneten Lösung zu beeinträchtigen. Unter Berücksichtigung vorangegangener Arbeiten über die Ausdrucksstärke von Advice-Bits für dieses Problem ist unser Algorithmus optimal.

Der zweite Teil dieser Dissertation widmet sich Konstruktionen von kryptographischen Grundfunktionen, mit dem Schwerpunkt auf Konstruktionen einer universellen Einweg-Hashfunktion aus einer Einwegfunktion. Zunächst bringen wir die Regularitätsannahmen für die Einwegfunktion in Verbindung zur Effizienz der Konstruktion, gemessen in der Anzahl von Aufrufen der Einwegfunktion. Qualitativ gesprochen wird die Konstruktion umso effizienter, je stärker die Annahmen über die Struktur der zugrundeliegenden Einwegfunktion sind. Wir untersuchen dann die Grenzen von Black-Box-Konstruktionen für diese Aufgabe. Dies sind grob gesagt Konstruktionen, die nur die Funktionalität der Einwegfunktion verwenden, aber nicht deren Beschreibung. Seit der Einführung dieses Konzepts durch Naor und Yung (STOC, 1989) vor 25 Jahren ist keine bessere untere Schranke für die Anzahl der Aufrufe der Einwegfunktion bekannt als die triviale Schranke, dass ein Aufruf nötig ist. Wir geben eine erste nichttriviale untere Schranke an von einer fast linearen Anzahl benötigter Aufrufe. Weiterhin ist unsere Schranke bestmöglich für den Fall regulärer Funktionen.

Abschliessend setzen wir im letzten Teil der Dissertation die Untersuchung eines kürzlich eingeführten Modells der Kommunikationskomplexität mit Advice fort. Wir zeigen, dass für das Gleichheitsproblem ein Protokoll mit polylogarithmischer Kommunikation existiert, das einen lakonischen Advice

von nur einem Bit erhält. Für das Teilbarkeitsproblem entwerfen wir ein Protokoll mit sublinearer Kommunikation und sublinearem Advice.