Journal of Automata, Languages and Combinatorics **16** (2011) 1, 37–48
© Otto-von-Guericke-Universität Magdeburg

FEASIBLE PROOFS OF SZPILRAJN'S THEOREM – A PROOF-COMPLEXITY FRAMEWORK FOR CONCURRENT AUTOMATA

Michael Soltys

Department of Computing & Software, McMaster University
1280 Main St. West, Hamilton, Ontario, Canada L8S 4K1
e-mail: soltys@mcmaster.ca

ABSTRACT

The aim of this paper is to propose a proof-complexity framework for concurrent automata. Since the behavior of concurrent processes can be described with partial orders, we start by formalizing proofs of Szpilrajn's Theorem. This theorem says that any partial order may be extended to a total order. We give two feasible proofs of the finite case of Szpilrajn's Theorem. The first proof is formalized in the logical theory **LA** extended to ordered rings; this yields a TC^0 Frege derivation. The second proof is formalized in the logical theory $\exists$**LA** and yields a $\mathsf{P/poly}$ Frege derivation. Although TC^0 is a much smaller complexity class than $\mathsf{P/poly}$, the trade-off is that the $\mathsf{P/poly}$ proof is algebraically simpler – it requires the algebraic theory **LA** over the simplest of rings: $\mathbb{Z}_2$.

Keywords: Proof complexity, concurrency, partial orders

1. Introduction

The purpose of proof complexity is to study logical systems which use restricted reasoning based on concepts from computational complexity; see [1] for an introduction to the subject.

In this paper we propose to investigate the proof complexity of standard reasoning associated with finite orders. The aim is to establish a proof complexity framework for concurrent automata – a framework capable of formalizing, for example, the reasoning in [3] and [5]. See [4] for background related to the fundamentals of concurrency, such as order structures and traces, where Szpilrajn's Theorem finds its important applications.

In particular, [3] deals with the foundations of concurrency theory, and the author shows how structurally complex concurrent behaviors can be modeled by relational structures. We propose a proof-complexity framework (i. e., a logical theory) able to formalize this kind of reasoning. We start at the very beginning, and propose the logical theory **LA** (introduced in [8]) as an appropriate theory for formalizing reasoning about that most basic of relations: orders.