Understanding the Hardness of Theorem Proving

Berichterstattung

Projektinformationen

UTHOTP

ID Finanzhilfevereinbarung: 279611

Projekt abgeschlossen

Startdatum
1 Juli 2012

Enddatum
30 Juni 2018

Finanziert unter
Specific programme: "Ideas" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Gesamtkosten
€ 1 460 000,00

EU-Beitrag
€ 1 460 000,00

Koordiniert durch
KUNGLIGA TEKNISKA HOEGSKOLAN
Sweden

Dieses Projekt findet Erwähnung in ...

Final Report Summary - UTHOTP (Understanding the Hardness of Theorem Proving)

In an age of ubiquitous computing, complexity theory is the science of studying what problems can be efficiently solved by computers. Research since the 1970s has zoomed in on so-called NP-complete problems, which can be defined in terms of simple logic formulas but turn out to be exactly the right notion to capture literally thousands of important applied problems in science and industry. Although NP-complete problems are widely believed to be impossible to solve efficiently in the worst case, the last couple of decades have seen the emergence of algorithms that perform surprisingly well for many problems encountered in practice. There has been a very limited understanding of why these algorithms can be so efficient, however, and why they sometimes miserably fail on seemingly very simple problems. This state of affairs is what our ERC project set out to address.

Briefly stated, the goal of the project was twofold: (1) to study mathematical methods of reasoning about logic formulas, connected to the NP-complete Boolean satisfiability (SAT) problem, and prove rigorous theorems about their power and limitations; (2) to exploit these methods constructively to build satisfiability algorithms (SAT solvers) that have the potential to go significantly beyond the state of the art. Although these are two quite different lines of research, throughout the project there have been strong synergies between our theoretical and applied work, even beyond what one could have dared to hope for at the outset. In the rest of this summary we try to outline the main contributions of the project.

On the theoretical side, we have studied the resolution proof system underlying state-of-the-art SAT solvers based on so-called conflict-driven clause learning (CDCL). We have also attacked much stronger algebraic and geometric proof systems based on Gröbner bases and cutting planes (the latter also known as pseudo-Boolean reasoning or 0-1 integer linear programming). Our focus has been on investigating proof size and space, which correspond to running time and memory usage for algorithms using these methods of reasoning. We have published a number of papers in leading international conferences and journals, in several works resolving problems that had been open for well over a decade.

As often happens in theoretical computer science, many of the new mathematical tools and techniques we developed to obtain our results came from unexpected connections with other areas such as information theory, communication complexity, finite model theory, and graph theory. This has been a two-way process

in that some of these connections also led to the solution of fairly long-standing open problems in other areas that were not a priori related to our research project, for instance regarding bounded variable fragments of first-order logic and combinatorial pebble games on graphs.

In our work on applied SAT solving, which has also been published in world-leading venues, we have built new mathematical models to make possible a deeper theoretical analysis of CDCL solvers, and have complemented this with large-scale empirical studies. In particular, we have performed extensive experiments on combinatorial benchmark formulas, carefully chosen drawing on our in-depth knowledge of the theory literature, to study and explain the behaviour of sophisticated heuristics in modern SAT solvers that are currently not amenable to a rigorous mathematical analysis.

Furthermore, we have performed a detailed study of so-called pseudo-Boolean solvers. Such solvers have the potential to be exponentially more efficient than CDCL solvers in theory, but in practice they are often significantly slower! We have modelled the reasoning used in pseudo-Boolean solvers as formal proof systems, which has allowed us to identify some of the reasons for their shortcomings. Armed with these insights, we have then constructed a new pseudo-Boolean solver RoundingSat, where even our first, proof-of-concept, version turns out to be competitive with previous, highly optimized, state-of-the-art solvers, and sometimes outperforms them dramatically.

Letzte Aktualisierung: 11 Dezember 2018

Permalink: https://cordis.europa.eu/project/id/279611/reporting/de