

令和 4 年 6 月 13 日現在

機関番号：12612

研究種目：若手研究(B)

研究期間：2017～2021

課題番号：17K17725

研究課題名（和文）大規模制約充足問題の全解探索のための実用的な計算基盤の確立とその応用

研究課題名（英文）Development of Practical Techniques for All Solution Enumeration of Large-scale Constraint Satisfaction Problems

研究代表者

戸田 貴久（Toda, Takahisa）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：50451159

交付決定額（研究期間全体）：（直接経費） 3,300,000円

研究成果の概要（和文）：本研究では、制約充足問題のすべての解を探索する手法を活用して、そのような解探索が求められる高度な問題解決のための効率的な計算基盤の開発を行った。主な成果として、ハードウェアやソフトウェアの不具合の原因解析を支援するための自動化手法を開発した。他の成果として、VLSIの単純配線問題や数独ヒント生成問題の効率的な解法を提案した。また新たな展開として、制約充足問題の解のサンプリング手法の開発とその応用、制約充足問題の最適化を応用したデータベースの匿名化に関する手法の開発など、当初想定していなかったプライバシー・セキュリティ関係の研究成果も得られた。

研究成果の学術的意義や社会的意義

情報システムは現代社会の基盤技術であり、特にセキュリティ、プライバシー、人命などが関わる場面では情報システムの高い品質が求められる。しかし、そのような品質の保証や解析に関わる技術は一般に計算コストが高く、本来的に完全な自動化は見込めないことが多い。本研究の主要な成果として、検証やテスト目的で広く使われている技術（モデル検査）に対してより高度な解析機能を追加した。これにより人手で行われる解析作業を一部自動化することが可能になる。モデル検査以外にもセキュリティ・プライバシーに関わる研究成果も得られ、制約充足に関する最新技術を活用した応用研究の新しい展開につながった。

研究成果の概要（英文）：In this research, we developed an efficient method for computationally hard problems that intrinsically require us to enumerate all solutions of constraint satisfaction problems (CSPs). As a major achievement, we developed a computer-aided method to help us to locate faults in the designs of hardware and software. Model checking is a widely applied method for the verification and debugging of information systems. A counterexample is detected from an erroneous system as a proof of error by executing model checking, however, there is a big gap between computing counterexamples and locating faults. We thus proposed a method for providing information regarding error in a more understandable form than counterexamples by abstracting many counterexamples, which is expected to aid us in moving a trace of failure (i.e., a counterexample) to an understanding of the essence of the failure.

Beside the model checking application, we tackled security/privacy-related researches.

研究分野：知能情報学

キーワード：制約充足問題 SATソルバー モデル検査 反例解析 セキュリティ プライバシ

1. 研究開始当初の背景

人工知能、データマイニング、計算生物学など幅広い分野で、集合、グラフ、論理式などの離散構造に関する計算問題を解くことが求められる。そのような問題の中には、制約を充足する解の網羅的な探索が本質的に必要とされるものが多い。しかし、計算過程において莫大な数の組合せや場合分けが生じ、従来の手法では現実的な時間内に処理を完了させることが困難になる(図1)。一つの解を探索する SAT ソルバーは、近年の急速な発展により、大規模問題でもしばしば現実的な時間内に解くことができるようになった。一方、全ての解を探索する問題(AIISAT)は SAT よりずっと困難である。近年、AIISAT の重要性が様々な研究領域において認識され始めている。

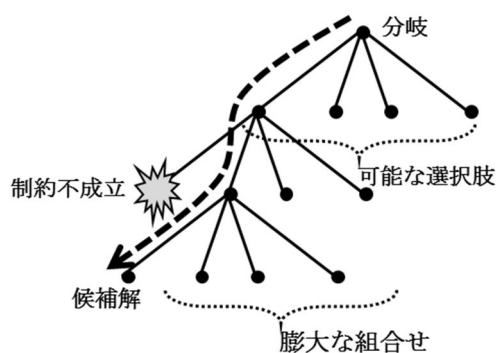


図1. 与えられた制約下での解の探索

2. 研究の目的

現実の問題は数千～数万(あるいはもっと多くの)の変数を持つので、そのような大規模問題を扱うためには現在のソルバーの性能では十分ではない。また、各種の応用では効率の悪い方法が採用されているため、現実規模の問題に歯が立たないことが多く、AIISAT ソルバーを基盤にした問題解法が現実的な選択肢として認識されにくい。そこでこれらの課題の解決に向けて、本研究では、AIISAT ソルバー自体の高速化、および、AIISAT ソルバーを中心技術として活用した問題解決のための計算基盤の開発に取り組む。

3. 研究の方法

(1) AIISAT ソルバーの高速化

変数の個数が増えればそれだけ問題を解くのが困難になる傾向がある。現実規模の問題は数千、数万(あるいはもっと多く)の変数を持つ。そのような問題に立ち向かうため、現実のデータの持つ構造や規則性に着目し、活用する。

(2) AIISAT ソルバーを中心技術として活用した問題解決のための計算基盤の開発

モデル検査の高機能化に取り組む。**モデル検査 (Model Checking)** は、仕様に反する設計の不具合を発見するための強力な手法である。例えば、ネットワークの機能を検証するためには、不具合を引き起こす種類のパケットではなく、サブネットやポート範囲などパケットの集合を知る必要がある。現実規模のネットワークの検証に向けて最新の AIISAT 技法を応用する。さらに、開発したモデル検査手法をネットワーク検証の研究で広く使われている実問題に適用し評価する。

(3) 応用研究の展開

その他にも制約充足分野の最新技術を活用した応用研究について調査・検討を進める。有望な応用があれば研究を進める。

4. 研究成果

(1) AIISAT ソルバーの高速化

AIISAT ソルバーを活用した問題解法では、解決したい計算問題を命題論理式に変換する必要がある。この方式は、どんな問題であれいったん命題論理式に変換できさえすれば、同じ解法(AIISAT ソルバー)を利用できるという利点がある。しかし、変換後の命題論理式からは、変換前の問題がどのようなであったかに関する情報は一般に失われてしまうので、問題ごとの特性を解法の中で活用することができない。しかも、変換により数多くの命題論理式が導入されるため、元の問題に比べて変換後の命題論理式のサイズが大きくなり、AIISAT ソルバーの性能が低下することがある。これらの課題を解決するために、命題論理式への変換過程で導入される論理変数の間において成り立つ機能的な従属関係を自動で抽出する方法を考案した。さらに、この従属関係を AIISAT ソルバーの探索アルゴリズムにおいて活用することで、AIISAT ソルバーの動作を高速化する手法を開発した。

(2) AIISAT ソルバーを中心技術として活用した問題解決のための計算基盤の開発

有界モデル検査はハードウェアやソフトウェアなどの情報システムに含まれる不具合を発見するための実践的な手法の一つとして広く知られている。ここで、有界モデル検査が不具合の証拠として出力するのは、システムの開発者が当然成り立つと期待する仕様違反するシステムの実行例(反例)である。有界モデル検査では、そのような反例を SAT ソルバーで求める方法が取られてきた。しかし、誤りの根本原因が一つであったとしても、ただ一つの実行トレースが反

例として存在することはなく、一般には数多くの反例が存在する。有界モデル検査は1つの反例だけを不具合の証拠として提示するが、その反例を構成する変数の値自体には特段の意味はなく、異なる値をとっても不具合のままであることがある。本研究ではこの点に着目して、反例を構成する特定の変数をピックアップして、その変数の値だけを変動させるとき依然反例のままであるような、取りうる値の最長の区間を計算によって求める手法を開発した。

この一般的な手法をネットワーク検証に対して適用する方法についても与え、通常モデル検査の限界についても議論し、提案手法の効果を計算機実験で評価した。具体的には以下の通りである。まず、ネットワーク検証における反例はネットワークの設計者が策定した仕様に違反するパケットに対応する。通常モデル検査を適用する場合、そのようなパケットを1つ求めるだけであり、それだけではネットワークの設計中に含まれる不具合を特定するのに十分な情報とはならない。一方、本研究を適用する場合、例えば、送信先のアドレスなど特定のフィールドに着目して、その値だけが異なる一連の違反パケット群を求めることが可能になる。提案手法の性能を評価するために、計算機実験ではネットワーク検証の分野で広く使われているネットワークベンチマークを使い、通常モデル検査を適用した場合に対して提案手法を適用した場合の性能を比較評価した。その結果、提案手法は通常モデル検査よりも高度な計算処理をしているにも関わらず、通常モデル検査に比べてそれほど大きな性能差は見られないことが確認された。

(3) 応用研究の展開

制約充足分野における最新の技術を適用することで、さまざまな問題解決への効率的な解法を提案した。主な成果としては、(a) VLSIにおける単純配線問題、(b) 数独ヒント生成問題、(c) 制約充足解のサンプリング技法の改善や応用、(d) 制約充足問題の最適化に基づくデータベースの匿名化、などが挙げられる。

ここでは、新たな展開として得られた研究成果(c)について以下に概要をまとめる。当初の研究計画では制約充足問題の解をすべて列挙する技術を中心にした研究を想定していた。しかし、実用上は必ずしもすべての解が必要とされることはあまりないので、そのような場合も考慮して、制約充足解をサンプリングする技法の研究も同時に進めた。この結果として、最新のサンプリング技法の精度を改善する手法を開発した。さらに、そのようなサンプリング技法を中心にした各種の問題解決についても研究を進めた。その結果として、複合イベント処理システムの開発を行った。すでに国内研究会において本システムの基本的な枠組みについて研究発表を行った。今後さらに内容を洗練させ、国際会議や国際的な学術誌において発表する予定である。

5. 主な発表論文等

〔雑誌論文〕 計4件（うち査読付論文 4件 / うち国際共著 0件 / うちオープンアクセス 1件）

1. 著者名 渡辺 光洋, 戸田 貴久	4. 巻 J104-D
2. 論文標題 交差回避制約を用いた単純配線決定問題のCSP解法	5. 発行年 2021年
3. 雑誌名 電子情報通信学会論文誌 D	6. 最初と最後の頁 434-441
掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transinfj.2020JDP7051	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Kohei Nishikawa, Takahisa Toda	4. 巻 13
2. 論文標題 Exact Method for Generating Strategy-Solvable Sudoku Clues	5. 発行年 2020年
3. 雑誌名 Algorithms	6. 最初と最後の頁 1-17
掲載論文のDOI (デジタルオブジェクト識別子) 10.3390/a13070171	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -
1. 著者名 Takahisa Toda, Takeru Inoue	4. 巻 25
2. 論文標題 Exploiting Functional Dependencies of Variables in All-Solutions SAT Solvers	5. 発行年 2017年
3. 雑誌名 Journal of Information Processing	6. 最初と最後の頁 459-468
掲載論文のDOI (デジタルオブジェクト識別子) 10.2197/ipsjjip.25.459	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Takahisa Toda, Takeru Inoue	4. 巻 29
2. 論文標題 Interval-based Counterexample Analysis for Error Explanation	5. 発行年 2021年
3. 雑誌名 Journal of Information Processing	6. 最初と最後の頁 630-639
掲載論文のDOI (デジタルオブジェクト識別子) 10.2197/ipsjjip.29.630	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計12件（うち招待講演 1件 / うち国際学会 0件）

1. 発表者名 戸田貴久
2. 発表標題 制約言語の観点におけるCP4IMの複雑さ
3. 学会等名 基盤(S) 離散構造処理系プロジェクト 「2019年度 初夏のワークショップ」
4. 発表年 2019年

1. 発表者名 戸田貴久
2. 発表標題 SATフィルターの検討
3. 学会等名 基盤(S) 離散構造処理系プロジェクト 「2019年度 秋のワークショップ」
4. 発表年 2019年

1. 発表者名 戸田貴久
2. 発表標題 モデル検査における反例空間の構造解析
3. 学会等名 人工知能学会 第107回人工知能基本問題研究会
4. 発表年 2018年

1. 発表者名 戸田貴久
2. 発表標題 誤りの効果的な説明のための反例空間解析
3. 学会等名 第170回アルゴリズム研究会
4. 発表年 2018年

1. 発表者名 戸田貴久
2. 発表標題 モデル検査における反例発見から反例列挙への拡張
3. 学会等名 基盤(S) 離散構造処理系プロジェクト「2017年度 初夏のワークショップ」
4. 発表年 2017年

1. 発表者名 戸田貴久
2. 発表標題 命題論理式を充足する変数割当の網羅的探索手法について
3. 学会等名 人工知能学会 第103回人工知能基本問題研究会（招待講演）
4. 発表年 2017年

1. 発表者名 戸田貴久, 宋剛秀
2. 発表標題 効率的なAllSATソルバーの実装と評価
3. 学会等名 第19回プログラミングおよびプログラミング言語ワークショップ
4. 発表年 2017年

1. 発表者名 渡辺光洋, 戸田貴久
2. 発表標題 交差回避制約によるSAT型ナンバーリンクソルバーの高速化
3. 学会等名 人工知能学会 第109回人工知能基本問題研究会(SIG-FPA1)
4. 発表年 2019年

1. 発表者名 中島祐輝, 戸田貴久
2. 発表標題 命題論理式の解の一様サンプリングの改善
3. 学会等名 第20回情報科学技術フォーラム
4. 発表年 2021年

1. 発表者名 戸田 貴久, 伊藤 健洋, 川原 純, 宋 剛秀, 鈴木 顕, 照山 順一
2. 発表標題 有界モデル検査による独立集合遷移問題の解法に関する考察
3. 学会等名 第186回アルゴリズム研究発表会
4. 発表年 2022年

1. 発表者名 夏 滄, 戸田 貴久
2. 発表標題 不確実性下における複合イベント処理に関する考察
3. 学会等名 第186回アルゴリズム研究発表会
4. 発表年 2022年

1. 発表者名 磯田 飛鳥, 戸田 貴久
2. 発表標題 属性間依存度を考慮したデータベースの安全なフラグメント化
3. 学会等名 第14回データ工学と情報マネジメントに関するフォーラム
4. 発表年 2022年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Strategy-Solvable Sudoku Clue Generation
<http://www.disc.lab.uec.ac.jp/toda/code/scg.html>
All Solutions SAT Repository
<http://www.sd.is.uec.ac.jp/toda/code/allsat.html>

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究協力者	井上 武 (Inoue Takeru)	日本電信電話株式会社・NTT未来ねっと研究所・主任研究員	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------