HOKKAIDO UNIVERSITY

| | |
|---|---|
| Title | Practical Techniques and Applications of Binary Decision Diagrams in Property Verification Problems [an abstract of dissertation and a summary of dissertation review] |
| Author(s) | 岩下, 洋哲 |
| Degree Grantor | 北海道大学 |
| Degree Name | 博士(情報科学) |
| Dissertation Number | 甲第11291号 |
| Issue Date | 2014-03-25 |
| Doc URL | https://hdl.handle.net/2115/55446 |
| Rights(URL) | https://creativecommons.org/licenses/by-nc-sa/2.1/jp/ |
| Type | doctoral thesis |
| File Information | Hiroaki_Iwashita_abstract.pdf, 論文内容の要旨 |

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

# 学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称　博士（情報科学）　氏名　岩下　洋哲

## 学 位 論 文 題 名

Practical Techniques and Applications of Binary Decision Diagrams in Property Verification Problems

（プロパティ検証問題における二分決定グラフの実用的な技術と応用）

コンピュータによる LSI などの設計支援技術の中でも、検証はその初期から現在まで続いている重要課題の一つである。検証のコストは設計対象の規模に対して指数的に増大するため、同じ検証技術のままでは設計を大規模化していくことができない。そのため検証規模の限界が設計規模の限界を支配していると言っても過言ではなく、産業界からは常に検証技術の革新が求められてきた。一方、二分決定グラフ (BDD) は論理関数の表現形式として優れているため、LSI 設計支援における中心的な基本技術の一つとして発展してきた。BDD は離散的な対象をコンピュータ上で効率良く列挙索引化することができるため、LSI に限らず様々な検証の分野に応用することができる。本研究では特に、対象においてある性質 (プロパティ) が常に成立するかを確認するプロパティ検証を対象とした。その基本はプロパティに該当する全ての場合を列挙することであり、BDD 技術はそのための強力な手段となる。

本研究ではまず、LSI 検証における代表的な検証手法である論理シミュレーションと記号モデル検査について、産業界における課題の解決に取り組んだ。論理シミュレーションでは、機能テストパターンの品質改善が最も重要な課題の一つである。一般には人手に頼ることが中心となる機能テストパターン作成に対して、その品質改善の鍵は、テストするプロパティの明確化を含む問題全体のモデル化と、そのモデルに基づく機能テストパターン作成の自動化である。本研究では FSM によるモデル化と BDD を用いた状態空間探索の技術を応用することで、その課題を解決した。具体的には、現実のマイクロプロセッサ設計におけるパイプライン制御機能のテストに関する問題に取り組み、これまでに無かった枠組み — (1) 人手で容易に記述できるパイプライン仕様記述、(2) (1) を入力としたパイプラインハザード発生パターンの列挙、(3) (1) と (2) の結果からのパイプライン制御 FSM の自動生成、(4) (3) の FSM 上での状態空間探索による網羅的な機能テストパターンの自動生成 — を開発した。さらに、FSM がパイプライン制御を表現しているという特性を利用して (4) の状態探索順序に工夫を施すことによって、アルゴリズムの空間使用量を大幅に削減することに成功した。実験により、本手法は実設計規模のパイプライン仕様に対しても適用可能であることが示された。

記号モデル検査では、現実の検証対象の設計規模が検証アルゴリズムの処理限界を超える場合が多いことが課題である。そこで本研究では、現実問題に合わせたプロパティの限定と検証アルゴリズムの最適化を実現した。BDD を用いた記号モデル検査では、検証対象を FSM でモデル化し、その上の状態集合と状態遷移関係を共に BDD で表現する。与えられた状態集合に含まれる一つ以上の状態から遷移可能な全ての次状態の集合を求める論理関数処理は「像計算」、反対に与えられた状態集合に含まれる一つ以上の状態へ遷移可能な全ての前状態の集合を求める論理関数処理は「逆像計算」と呼ばれる。一般的な記号モデル検査では、プロパティ記述言語 CTL の自然な解釈と一

致する逆像計算が主に使われていた。これに対して本研究では、ハードウェアの実設計を検証対象とする場合には像計算のコストに対して逆像計算のコストが非常に大きくなるケースが多いことに着目し、記号モデル検査の基本演算を逆像計算から像計算に置き換える Forward model checking の手法を新しく提案した。そして、実設計に対して使用頻度の高い CTL プロパティの多くは像計算のみで検証可能であることを示すとともに、像計算のみで検証可能なプロパティクラスに限定する場合の仕様記述言語としてω正規表現が適していることを提案した。さらに、グラフ表現したプロパティを深さ優先で処理することにより、バグ検出までの計算時間を大幅に短縮する検証アルゴリズムも提案した。実験では、実設計に対する本手法の適用効果を計算時間とメモリ使用量の両面で確認することができた。

本研究では次に、LSI に限らずより広い意味でのプロパティ検証問題に対する BDD 技術の応用に取り組んだ。フロンティア法は、意味のある複雑な BDD を演算の繰り返しではなく一度のトップダウン操作で構築する新しい枠組みである。これにより、与えられたグラフ上のパスや木などの高速な列挙索引化が可能になった。グラフは様々な離散構造を表現する汎用的なモデルであるため、それらは検証技術としても広い応用が期待される。その実用化を推進するため、個別の事例毎に発生する問題や制約条件の変化に柔軟に対応できるような、フロンティア法やそれに類似した手法に関する共通の枠組みを開発した。提案したインタフェースを用いれば、フロンティア法において列挙対象のプロパティ毎に異なるような実装部分を容易に切り分けることができる。本研究では、共通部分の実装に改良を加えることにより、実行効率の改善と機能の拡張を実現する処理系 (C++ ライブラリ) を開発した。またその一方で、フロンティア法における列挙対象を限定してそのプロパティ固有の制約をより積極的に利用することによる、さらなる最適化の可能性についても考察を深めた。本研究では格子グラフ上のパス (自己回避歩行) の数え上げを例に、フロンティア法の汎用的な処理系に対してどれだけの性能改善が可能であるかを試行した。その結果、対象の限定によってフロンティア法における全ての状態遷移パターンや到達可能状態 (BDD の幅) を事前に分析できる場合には、BDD ノード情報の管理や並列処理などにおいて大幅な効率化の可能性があることが明らかになった。最適化された実装は汎用的な実装に対して 5 倍のメモリ使用効率向上と 2 桁の実行速度改善を達成し、世界でもこれまで解かれていなかった規模の問題を解くこと (オンライン整数列大辞典 A007764 および A140517 の更新) にも成功した。

本研究を通して、プロパティ検証問題に対する BDD 関連技術の有効性を再確認するとともに、その多岐にわたる実用化技術を開発した。検証技術開発の本質はその枠組み作り、すなわち人に何を入力させコンピュータに何を解かせるかという問題設定である。本研究の成果が今後の技術発展に必要な知見の蓄積としても貢献することを願う。