

学 位 論 文 の 要 旨

Algorithms and Lower Bounds for Threshold Circuits

しきい値回路に対するアルゴリズムと下界の研究

氏 名 齋藤 惇 印

A fundamental purpose of theory of computation is to understand differences between uniform computation and nonuniform one. In particular, Boolean circuit has been studied in an area of nonuniform computation models, because Boolean circuits are natural formalization of computer architecture and hardware. Boolean circuit is compared with uniform computation expressed as fixed size programs which run for an arbitrary input length. In the computational complexity theory, cost of nonuniform computation is measured through infinite family of Boolean circuits. Proving computational limitations of Boolean circuits is an extremely important and challenging task in the theoretical computer science.

A remarkable recent result about satisfiability algorithms is a nontrivial algorithm for testing satisfiability of depth two sparse threshold circuits which have linear number of wires by Impagliazzo et. al. In this thesis, we construct a nontrivial algorithm for a larger class of circuits. We give a nontrivial circuit satisfiability algorithm for a class of circuits which may not be sparse in gates with dependency. Two gates in a circuit are dependent, if the output of the one is always greater than or equal to the other one. An independent gate set is a set of gates in which two arbitrary gates are not dependent. In our setting, the number of restrictions to bottom level gates is bounded above because of dependency of bottom gates. We first define some partial order on the set of bottom gates. Next, we define a problem: for given a pair of a circuit and a Hasse diagram relating with the circuit, output YES if and only if the circuit is satisfiable. Because of an upper bound on the expected number of restrictions to bottom level gates, the running time of the randomized algorithm is faster than the complexity of the trivial exhaustive search.

Recently, Williams proved a separation between $NEXP$ and $ACC \circ THR$, where an $ACC \circ THR$ circuit has a single layer of threshold gates at the bottom and an ACC circuit at the top. Two main ideas of his strategy are a closure property of circuit class and an algorithm for counting satisfying assignments of circuits. In this thesis, we show that this general scheme based on these two ideas can be applied for a certain class of circuits with multilayer of threshold gates. The circuit class we give has the symmetric gate at the top and poly-log layers of threshold gates to which an extra condition on the dependency is imposed. We show that, if the size of a

maximum independent gate set of each layer of threshold gates is at most n^γ for sufficiently small $\gamma > 0$, then two key ingredients needed to apply his strategy can be established. We also give a result about lower bounds against NEXP, extending the results by Williams.

計算の理論の基本的な目的として、一様計算と非一様計算の違いを理解することがあげられる。論理回路は、計算機ハードウェアの自然な形式化であることから、非一様計算モデルの研究において研究されてきた。論理回路は、入力サイズによらない固定サイズのプログラムとして表現される一様な計算と比較される。計算量理論においては、非一様な計算の手間は、論理回路の族によって測定される。理論計算機科学において、論理回路の計算の限界を示すことは、非常に重要であり困難な課題といえる。

注目すべきことに最近、Impagliazzo らは、ワイヤの本数が線形である疎な 2 段のしきい値回路に対して、非自明な充足可能性のアルゴリズムを与えた。本論文においては、依存性によって制約された必ずしも疎であるとは限らない 2 段回路のクラスに対して充足可能性手続きを構成した。二つのゲートが依存するとは、片方のゲートの出力値が、常にもう一方のゲートの出力値以上であることをいう。独立なゲート集合とは、その集合のどんな 2 個のゲートについて依存性が成立しないことをいう。本論文の設定においては、ボトム位置のゲートへの出力の固定の仕方の個数が依存性により限定される。最初に、ボトムゲートの集合の上の順序集合を定める。次に、入力として 2 段の依存性のある回路と、この順序集合にともなうハッセ図が与えられて、回路が充足可能であるか否かを判定する問題を定義する。出力ゲートの固定の仕方の期待値を上から押さえることにより、自明な手続きより高速なもの構成する。

近年、Williams は NEXP と ACC ◦ THR という 2 つの計算量クラスを分離した。ただし、ACC ◦ THR は ACC 回路をトップの位置に、ボトムの位置に単層のしきい値ゲートを並べた回路である。主要な考えが、2 つあり、一つは回路クラスの閉包性質、二つ目は充足解の数え上げアルゴリズムである。本論文においては、この一般的な枠組みを適用可能であるような多層のしきい値ゲートを含む論理回路のクラスを与えた。与えた回路クラスは、出力に対称ゲートを有する、かつ、依存性という条件の付けられたしきい値ゲートの層が対数多項式個だけある。本論文においては、もし独立なゲート集合のサイズが十分小さな $\gamma > 0$ に対して n^γ 以下であるなら、これらの 2 つの手法が適用可能であることを示した。さらに、Williams の結果自体を含むような下界を与えた。