| | |
|---|---|
| 氏名 | Gu Qian Ping 顧 謙 平 |
| 授与学位 | 工学博士 |
| 学位授与年月日 | 昭和63年11月9日 |
| 学位授与の根拠法規 | 学位規則第5条第1項 |
| 研究科，専攻の名称 | 東北大学大学院工学研究科<br>（博士課程）情報工学専攻 |
| 学位論文題目 | A Study on the Complexity Theory Based on Boolean Algebra<br>（ブール代数に基づいた計算量理論に関する研究） |
| 指導教官 | 東北大学教授 丸岡 章 |
| 論文審査委員 | 東北大学教授 丸岡 章　東北大学教授 木村 正行<br>東北大学教授 斎藤 伸自 |

# 論文内容要旨

In the research of computaional complexity, Turing machine and Boolean circuits are usually used as computation model. The combinational Boolean circuit model addresses both the size and time cost. Circuit depth provides the " time" measure and the size of circuits is clearly a reflection of the hardware costs. The correspondence between Boolean circuits and Turing machines is known as: Turing machine time is polynomially related to circuit size, and likewise Turing machine space to circuit depth. Since circuit model is very simple and easy to understand, it is well used in theoretic research of computation recently. Many computation problems can be reduced to the problem of constructing Boolean circuits and formulae for certain Boolean functions. In this dissertation, we study two important areas of computational complexity based on the Boolean circuit model. These two areas are one about the amplification of Boolean functions and one about learning Boolean functions. The amplification of Boolean functions specifies an important property of Boolean functions. There is a new approach of constructing Boolean circuits and formulae for Boolean functions based on the amplification. Learning Boolean functions is a way to construct Boolean circuits and formulae for Boolean functions

in the absence of explicit definition of those functions. Many important computation problems are expected to be solved in these two areas.

This dissertation is organized as follows. Chapter 1 is the introduction.

Chapter 2 gives a review of the research of the amplification of Boolean functions. The study of the amplification of Boolean functions originates from the reliable design of relay contact networks with unreliable contacts. It is then used in constructing Boolean circuits and formulae for certain Boolean functions. Using the amplification method, L. Valiant shows the best known upper bound of the size of monotone Boolean formulae that compute Boolean majority functions. The amplification of Boolean functions itself is also well studied for its own sake. To describe the results about the amplification of Boolean functions, we need a few of definitions. Let f be a Boolean function. The amplification function $A_f$ of f is defined as

$$A_f(p) = Pr[f(x_1,\ldots,x_n)=1],$$

where $x_1,\ldots,x_n$ are independent random Boolean variables with $Pr[x_i=1]=p$ for $1\leq i\leq n$. f is said to amplify (p, q) to (p', q'), if $Af(p)\leq p'$ and $Af(q)\geq q'$. In the followings, we will often identify a Boolean formula with the Boolean function it computes. L. Valiant obtains monotone Boolean formulae of size $0((m/c)^{3.3})$ that amplify $(p, p+1/m)$ to $(p', p'+1/c)$. R. Boppana proves that Valiant's upper bound is an optimal one. In Valiant's result, there is no restriction on the depth of formulae. M. Ajtai and M. Ben-Or show that $(p, p+1/m)$ can be amplified to $(p', p'+1/c)$ by Boolean circuits of depth d and size $EXP(O(d(m/c)^{2/d}))$.

In Chapter 3, we estimate the amount of the amplification of monotone read once formulae of depth d and alternative layers of AND and OR, which we denote $\Sigma_d$ and $\Pi_d$ depending the type of gate of the top layer. Using the results, we derive an upper bound of size of monotone Boolean formulae that compute Boolean threshold functions. In this chapter, the fan-ins of the gates in the same layer of the formulae are assumed to be the same. We prove that $(p, p+1/m)$ can be amplified to $(p', p'+1/c)$ by formulae in $\Sigma_d \cup \Pi_d$ of size $EXP(O((d-1)(m/c)^{1/(d-1)}))$. We also prove that if the formulae in $\Sigma_d \cup \Pi_d$ amplify $(p, p+1/m)$ to $(p', p'+1/c)$ then the size of the formulae is $EXP(\Omega((d-1)(m/c)^{1/(d-1)}))$. Our upper bound and lower bound are tight to a constant factor in the exponent. As a consequence of these bounds, we obtain that if a formulae in $\Sigma_d \cup \Pi_d$ of size polynomial in $m/c$ amplifies $(p, p+1/m)$ to $(p', p'+1/c)$ then $d=\Theta(\log(m/c))$. Applying the upper bound, we prove that there are monotone formulae of depth d+3 and size polynomial in n that compute Boolean threshold functions $th_t$ for $1\leq t\leq(\log n)^d$. R. Boppana proves that for $t=\Omega(\log n)$ the depth of monotone formulae of size polynomial in n that compute Boolean threshold functions $th_t$ is at least d+1. Our upper bound on the depth of the formulae given above is very closed to the lower bound on the depth given by Boppana. On the other hand, our lower bound of the size of

formulae given above shows the limitation of the amplification method for constructing certain Boolean circuits and formulae.

In Chapter 4, we discuss the complexity for concept learning based on the learning model given by L. Valiant. In this model, the objects to be learned are Boolean functions expressed by Boolean formulae. The learning model consists of learning protocol and learning algorithm. The former specifies the manner in which information about the function to be learned is obtained from outside and the latter is the mechanism by which a formula to approximate the function to be learned is deduced. There are two types of learning protocols. The first type provides information about the function to be learned through examples of the form $(v,f(v))$, $v$ in $\{0, 1\}^n$, generated according to some probability distribution D on $\{0, 1\}^n$. The second type gives the value $f(v)$ when the learning algorithm asks for any $v$ in $\{0, 1\}^n$. A class F of Boolean formulae is said to be $p(\cdot, \cdot, \cdot)$ learning time $q(\cdot, \cdot, \cdot,)$ communication time learnable by a class of Boolean formulae G, if there exists an learning algorithm A such that for *any* f *in* F, *any probability distribution* D on $\{0, 1\}^n$, *and any* $h > 1$ *(error parameter)*, A halts in $p(n, size(f), h)$ time, calls $q(n, size(f), h)$ times for learning protocols, and outputs a formula g in G with probability at least $1 - 1/h$ such that

$$\sum_{v \in f \Delta g} D(V) < 1/h$$

where $f \triangle g$ denotes the symmetric difference of $\{v \mid f(v) = 1\}$ and $\{v, g(v) = 1\}$. It is noted that *the communication time is always less than the learning time.*

In Chapter 5, we give upper bounds and lower bounds of the learning time and the communication time for learning certain classes of Boolean formulae. Blumer and others proved that *the communication time for learning a class of Boolean formulae is bounded below by the* Vapnik−Chervonenkis dimension, a simple combinatorial parameter for classes of Boolean formulae. Let t−DNF and TH denote the class of disjunctive normal form formulae with at most t monomials and the class of the formulae of threshold functions, and let t−MDNF denote the class of monotone formulae in t−DNF. By estimating the Vapnik−Chervonenkis dimensions for these classes, we prove the lower bounds on communication time for learning t−DNF, t−MDNF, and TH are $\Omega(tn)$, $\Omega(tn)$, and $\Omega(n)$, respectively. We also prove that t−MDNF is $O(tn)$ learning time learnable when both two types of learning protocols are used, t−MDNF is $O(n^{t+1})$ learning time $O(n^t)$ communication time learnable when only the second ty pe of learning protocol is used, and TH is $O(n)$ communication time $Poly(n)$ learning time le arnable when the second type of learning protocol is used.

In Chapter 6, we discuss the learnibility of certain classes of Boolean formulae when only the first type of learning protocol can be used. It is proved by L. Valiant and others that some classes of Boolean formulae are polynomial learning time learnable and on the assumption

that RP≠NP the others are not. In the definition of learnibility, it is assumed that examples (v,f(v)) are drawn according to an unknown arbitrary probability distribution. This assumption may be too strong in some practical situations. For classes of Boolean functions for which poly time learing algorithms have not been found, it is reasonable to find feasible algorithms for learning those classes on the assumption that examples are drawn from some known natural probability distribution. We prove that TH is Polynomial learning time learnable when examples are drawn according to the uniform distribution. This contrasts with the fact that TH is not polynomial learning time learnable unless RP=NP. We also proved that for fixed t t−MDNF is polynomial learning time learnable by the class of monotone disjunctive normal form formulae when the examples are drawn according to uniform distribution. It is noted that t−MDNF is not polynomial learning time learnable unless RP=NP.

Chapter 7 gives a summery of this dissertation.

# 審 査 結 果 の 要 旨

問題を解くのに必要な計算時間（計算量）を求めることは，効率の良いアルゴリズムの設計に係る重要な問題である。これまで，具体的な問題を解くアルゴリズムの設計や，そのアルゴリズムの計算量の評価に関して個別に研究されているが，計算量を増す要因となる一般的な性質や，アルゴリズムを機械的に求める手順についてはさほど研究されていない。著者は，計算量を増す要因として論理関数の増幅の概念を取り上げ，与えられた増幅度を達成するための計算量について論じるとともに，アルゴリズムを求める手順を学習モデルとして定式化し，その計算量を評価した。本論文はその成果をまとめたもので，全編７章よりなる。

第１章は序論であり，第２章では論理関数の増幅の概念について説明している。

第３章では，深さｄに制限のある単調論理回路モデルのもとで，与えられた増幅度要求（ｍ，ｃ）を実現するための回路のサイズの上界と下界を求めている。この上界と下界は，いずれもＥＸＰ（Ｒ（ｄ－１）（ｍ／ｃ））の形の式で与えられ，指数部の定数Ｒの違いを除き一致している。また，この結果を利用して，多項式サイズのしきい値回路を実現し，回路の深さは従来のものの１／２というほぼ最適の値を達成している。

第４章では，アルゴリズムが論理式として表現できる場合を対象にし，外界より得られる論理式に関する部分的な情報をもとに，その論理式を機械的に求める手順を学習モデルで定式化し，次いで，外界との通信により情報を得る際の制約をプロトコルとして規定している。

第５章では論理式のクラスとして，ｔ個以下の項からなる積和論理式からなるクラスｔ－ＤＮＦとｔ－ＤＮＦに属する単調な論理式からクラスｔ－ＭＤＮＦ，さらにしきい値論理式のクラスＴＨの３つの基本的なクラスを取り上げ，これらのクラスの論理式を学習するアルゴリズムを与えるとともに，それの学習時間と通信時間を評価している。

第６章では，プロトコルを限定して例題による学習を取り上げ，例題が一様分布に従って生起するとした場合について，多項式学習時間でＴＨとｔ－ＭＤＮＦを学習するアルゴリズムをそれぞれ与えている。この結果は，一様分布の仮定を取り除くと，ＴＨとｔ－ＭＤＮＦはともに多項式学習時間では学習できないという既に知られている結果と対比すると興味深い。第７章は結論である。

以上要するに本論文は，計算量を増す要因となる増幅の概念に注目し，与えられた増幅度を実現する回路のサイズを評価するとともに，各種の学習アルゴリズムとその計算量を求め，アルゴリズムの設計と解析に係る有用な知見を与えたもので，情報工学の発展に寄与するところが少なくない。

よって，本論文は工学博士の学位論文として合格と認める。