数理解析研究所講究録
1054巻 1998年 87-95

Prelude to Local Complexity Theory

Hajime Machida

Department of Mathematics
Hitotsubashi University
Tokyo 186 JAPAN

E-mail: machida@math.hit-u.ac.jp

1 Introduction

In Boolean complexity theory, the circuit-size complexity and other types of complexity are normally defined with respect to some complete basis such as the set of all 2-variable functions or the set {AND, OR, NOT}. In other cases, C. P. Schnorr, A. A. Razborov and many others have investigated Boolean complexity with respect to some incomplete basis. Typically, they have considered the complexity over the set {AND, OR}.

On the other hand, the concept of a *clone* has been known for decades in the field of universal algebra and in multiple-valued logic. And, when the term clone is introduced into the theory of Boolean complexity, those "incomplete" bases as mentioned above naturally turn out to be "complete" bases for some suitable clones. In other words, one may take up arbitrary clone and construct a complexity theory exclusively within that clone. Thus, to each clone corresponds its own complexity theory.

In this context, one should be justified to call the standard, normal complexity theory as the *global complexity theory* and the complexity theory over a clone as the *local complexity theory.*

In this paper, we start with reviewing the definition of a clone and some basic facts about clones and, then, develop a framework for the local complexity theory. We also give "global" bounds for the local complexity. Finally, as a typical example, a couple of well-known results from monotone complexity are summarized from the viewpoint of our local complexity theory.

The reader should not expect to find any essentially new results in this paper. Instead, the purpose of this paper is to provide the reader with a framework for new perspective in Boolean complexity theory.

2 Clone

In general, the term *clone* is defined over arbitrary non-empty set in the following way.

Let A be a non-empty set and $O_A^{(n)}$ be the set of all functions from A^n into A and

$$O_A = \bigcup_{n=1}^{\infty} O_A^{(n)} .$$

Let J_A be the set of all projections pr_i^n over A where pr_i^n is defined as

$$pr_i^n(x_1, \cdots, x_i, \cdots, x_n) = x_i$$

for every $(x_1, \cdots, x_n) \in A^n$.

Definition 2. 1 *A subset C of O_A is a* **clone** *over A if and only if*

(1) C contains J_A

and

(2) C is closed under (functional) composition.

Definition 2. 2 *The set of all clones over A is called the* **lattice of clones** *over A, or the* **space of clones** *over A, and is denoted by $\mathcal{L}_A$.*

Notation For a clone C and $n > 0$, we shall denote by $C^{(n)}$ the subset of all n-variable functions in C, *i.e.*, $C^{(n)} = C \cap O_A^{(n)}$.

So far, we have introduced the concept of a clone and the space of clones in the general setting.

In this paper, we are interested only in the Boolean case, that is, the case where the set A contains only two elements, namely, $A = \{0, 1\}$. In this case, we shall denote $O_A, O_A^{(n)}$ and $\mathcal{L}_A$ by $O_2, O_2^{(n)}$ and $\mathcal{L}_2$, respectively. Thus, the set O_2 is the set of all Boolean functions and the space $\mathcal{L}_2$ is the space of all clones defined over Boolean functions. Up to now, this space has been thoroughly studied. In particular, its lattice structure was completely determined by E. L. Post[4]. $\mathcal{L}_2$ is often called the *Post lattice.* The diagram of the Post lattice is given in the Appendix A.

There are several remarkable distinctions between $\mathcal{L}_2$ and $\mathcal{L}_A$ for $|A| \geq 3$. Most significant is the cardinality: As one can see from the Appendix A, the cardinality of $\mathcal{L}_2$ is countable, whereas $\mathcal{L}_A$ for each A with $|A| \geq 3$ is known to have the cardinality of continuum (This is due to Y. I. Yanov and A. A. Muchnik [11]). Another distinction, which is related to the above distinction, is that every clone in $\mathcal{L}_2$ is finitely generated, whereas there exist clones which have no basis, neither finite nor infinite, in each $\mathcal{L}_A$ with $|A| \geq 3$. The list of generators for every clone in $\mathcal{L}_2$ is shown in the Appendix B.

3 Local Complexity — Computational Complexity over a Clone

In the following, we are only concerned with the Boolean case: $A = \{0, 1\}$. Also, the term basis always means finite basis.

Normally, the circuit-size complexity of a Boolean function f is defined as follows:

Definition 3. 1 *Let Ω_0 be a basis for the set O_2 of all Boolean functions, that is, Ω_0 is a complete basis in a usual sense. For an n-variable function f in $O_2^{(n)}$, the* **circuit-size complexity of f with respect to Ω_0** *is defined to be the minimum of the number of gates in a (combinatorial) circuit C where C ranges over all circuits that use functions in Ω_0 as gates and compute f. This complexity is denoted by $\mathrm{C}_{\Omega_0}(f)$.*

The circuit-size complexity over arbitrary clone C can be defined analogously:

Definition 3. 2 *Let C be a clone and Ω be a basis for C. For an n-variable function f in C, the* **circuit-size complexity of f with respect to Ω** *is defined to be the minimum of the number of gates in a (combinatorial) circuit C where C ranges over all circuits that use functions in Ω as gates and compute f. This complexity is denoted by $\mathrm{C}_{\Omega}(f)$.*

In order to make clear distinction between the above two complexities, one may be tempted to call the former (the circuit-size complexity with respect to some complete basis) the *global* circuit-size complexity and the latter (the circuit-size complexity over a clone) a *local* circuit-size complexity.

Deapth complexity and formula-size complexity for the local case can also be defined similarly to the normal (global) case, but we shall not consider them here.

The following relation between the local and the global complexities is obvious.

Proposition 3. 1 *Let C be a clone. Let Ω_0 be a basis for the set O_2 of all Boolean functions and Ω be a basis for C. Then, there exists a constant $m \geq 1$ which satisfies*

$$\mathrm{C}_{\Omega_0}(f) \leq m\, \mathrm{C}_{\Omega}(f)$$

for any $f \in O_2^{(n)}$.

Proof This follows from the fact that each function in Ω can be constructed by a fixed number of gates in Ω_0. □

Similar argument implies the following:

Proposition 3. 2 *Let C be a clone and Ω_1 and Ω_2 be two bases for C. Then, there exist constants $m_1, m_2 \geq 1$ which satisfy*

$$\mathrm{C}_{\Omega_1}(f) \leq m_1\, \mathrm{C}_{\Omega_2}(f) \quad \textit{and} \quad \mathrm{C}_{\Omega_2}(f) \leq m_2\, \mathrm{C}_{\Omega_1}(f)$$

for any $f \in O_2^{(n)}$.

Thus, the local complexity is, in a sense, characteristic to a clone and independent of the choice of a basis in a clone.

4 "Global" Bound for Local Complexity

First, we shall consider the "global" upper bound for the local complexity.

Proposition 4. 1 *Let C be a clone and Ω be a basis for C. For each $n > 0$ and any function f in $C^{(n)}$,*

$$\mathrm{C}_\Omega(f) < |C^{(n)}|.$$

Proof Consider a minimal computation sequence $\mathcal{S}_0$ for f with respect to Ω :

$$\mathcal{S}_0 : x_1, x_2, \cdots, x_n, f_1, f_2, \cdots, f_{r-1}, f_r(= f).$$

Here, $f_1, f_2, \cdots, f_{r-1}$, and f_r can be considered as n-variable functions in C, and these functions are mutually distinct to each other since $\mathcal{S}_0$ is minimal. Therefore,

$$r \leq |C^{(n)}| - n < |C^{(n)}|.$$

□

In other words, we have, for example, the following upper bound.

Corollary 4. 1 *Let C be a clone and Ω be a basis for C. Suppose $|C^{(n)}| \leq p(n)$ for some polynomial $p(n)$. Then, for any function f in $C^{(n)}$,*

$$\mathrm{C}_\Omega(f) < p(n).$$

Corollary 4. 2 *Under the same situation as in the above corollary and for arbitrary complete basis Ω_0 (e.g., $\Omega_0 = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$), we have*

$$\mathrm{C}_{\Omega_0}(f) < m\,p(n)$$

for some constant m.

Proof Clear from Proposition 3.1 and Corollary 4.1. □

Now, we turn to the "global" lower bound for the local complexity.

Proposition 4. 2 *Let C be a clone and Ω be a basis for C. For sufficiently large $n > 0$, there exists a function f in $C^{(n)}$ that satisfies*

$$\mathrm{C}_\Omega(f) \geq \frac{\log_2 |C^{(n)}|}{n}.$$

The proof proceeds analogously to the proof for the global case, which is originally due to C. E. Shannon[7]. (See, *e.g.*, I. Wegener[10].)

Proof Let s be the number of functions in Ω and t be the maximum arity of the functions in Ω.

It is the key observation that the number of n-variable functions computable by circuits with at most b functions (gates) in Ω does not exceed

$$V(b, n) = (b + n - 1)^{tb}\, s^b\, b \,/\, b!.$$

Let b be the maximum complexity of functions in $C^{(n)}$ with respect to Ω . Then, we have

$$V(b,n) \geq |C^{(n)}|.$$

By the Stirling's formula, which asserts

$$b\,! \geq c\, b^{b+\frac{1}{2}}\, e^{-b}$$

for some constant $c > 0$, the inequality

$$\log_2 V(b,n) \geq \log_2 |C^{(n)}|$$

yields

$$\begin{aligned} &tb \log_2(b+n-1) + b\log_2 s + \log_2 b \\ &\quad - \log_2 c - (b+\frac{1}{2})\log_2 b + b\log_2 e \;\; \geq \;\; \log_2 |C^{(n)}|\,. \end{aligned}$$

We may assume that $b \geq n-1$ and $(t-1)b \geq \frac{1}{2}$, and then from the above inequality the following inequality is obtained for some constants $k_1, k_2 > 0$:

$$k_1 b \log_2 b + k_2 b \geq \log_2 |C^{(n)}|.$$

Now, suppose that

$$b \leq \frac{\log_2 |C^{(n)}|}{n}.$$

This implies

$$k_1 \frac{\log_2 |C^{(n)}|}{n}(\log_2 \log_2 |C^{(n)}| - \log_2 n) + k_2 \frac{\log_2 |C^{(n)}|}{n} \geq \log_2 |C^{(n)}|,$$

which is false for sufficiently large n. Therefore, we have

$$b > \frac{\log_2 |C^{(n)}|}{n}$$

for sufficiently large n. □

The previous proposition implies the well-known "global" lower bound for the global complexity.

Corollary 4. 3 *Let Ω_0 be a complete basis for O_2. For sufficiently large $n > 0$, there exists a function f in $O_2^{(n)}$ that satisfies*

$$\mathrm{C}_{\Omega_0}(f) \geq \frac{2^n}{n}.$$

Proof It suffices to note that $|O_2^{(n)}| = 2^{2^n}$. □

5 Monotone Clone

The full list of clones in $\mathcal{L}_2$, with sets of generators, is given in Appendix B. In the list, M_1 is the clone generated by the set $\{\text{AND}, \text{OR}, 0, 1\}$ and M_4 is the clone generated by the set $\{\text{AND}, \text{OR}\}$. The clone M_1 is the set of all monotone functions and may be called the *monotone clone*. The so-called monotone complexity is the local complexity over M_1 or over M_4 in our terminology.

Thanks to many researchers including N. J. Pippenger, C. P. Schnorr and A. A. Razborov, we already have a relatively good amount of research on the local complexity over the monotone clone. Mainly as an illustrative purpose, we shall state some of these results.

The global lower bound for the local complexity over the monotone clone is due to N. J. Pippenger[2].

Lemma 5. 1 $|M_4| \geq 2^{\,{}_n\mathrm{C}_{\lfloor n/2 \rfloor}}$.

Proposition 5. 1 *Let C be the clone M_1 (or M_4) and Ω be a basis* $\{\text{AND}, \text{OR}, 0, 1\}$ *(or* $\{\text{AND}, \text{OR}\}$*). For sufficiently large $n > 0$, there exists a function f in $C^{(n)}$ that satisfies*

$$\mathrm{C}_\Omega(f) \geq c\frac{2^n}{n\sqrt{n}}$$

for some constant $c > 0$.

Proof This follows from Proposition 4.2, Lemma 5.1 and the following inequality :

$${}_n\mathrm{C}_{\lfloor n/2 \rfloor} \geq c\, 2^n\, n^{-1/2}$$

for some constant $c > 0$. □

One of the fundamental problems in the local complexity theory is to determine the difference in complexity between two clones, one of which is a subclone of the other. Let C_1 and C_2 be two clones with Ω_1 and Ω_2 as basis, respectively, and suppose that $C_1 \subseteq C_2$. For a function f in C_1, we have $\mathrm{C}_{\Omega_2}(f) \leq m\, \mathrm{C}_{\Omega_1}(f)$ for some constant m (not depending on f). Now, the question is how far this difference could be. The monotone clone provides an example which shows that an extremal difference is achievable. This result is a well-known result of E. Tardos[9], which is an improvement over A. A. Razborov[6].

Proposition 5. 2 *Let Ω_0 be a basis for the set O_2 and Ω be a basis for M_1. There exists a sequence of functions $\{f^{(n)}\}$ where $f^{(n)} \in M_1^{(n)}$ which satisfies that* (1) $\mathrm{C}_{\Omega_0}(f)$ *is polynomially bounded and* (2) $\mathrm{C}_\Omega(f)$ *is exponential.*

6 For the Future

There are numerous problems concerning this subject. We conclude this article by posing the followng two problems:

For a clone C with a basis Ω and $n > 0$, let $\mu(C;n)$ be a function that satisfy the inequalities:

$$\forall f \in C^{(n)} \quad \mu(C;n) \geq m_1 \, \mathrm{C}_\Omega(f)\,,$$
$$\exists f \in C^{(n)} \quad \mu(C;n) \leq m_2 \, \mathrm{C}_\Omega(f)$$

where $m_1, m_2 > 0$ are constants.

Problem 1: For every clone C, determine $\mu(C;n)$. (Note: It is well-known that $\mu(C_1;n) = 2^n/n$ (O. B. Lupanov and C. E. Shannon). For most of the small clones C which sit near the bottom of the Post Lattice, $\mu(C;n)$ is easily obtained.)

The next question is to locate a sequence of functions corresponding to some combinatorial problem in the Post Lattice. In particular, we ask:

Problem 2: For any NP-complete problem A, determine the minimal clone that contains a sequence $\{f^{(n)}\}$ corresponding to A. (Note: From the lattice structure of L_2, it is easy to see that for any subset S of O_2 there exists the minimal clone among all clones containing S.)

References

[1] Dunne, P. E., *The Complexity of Boolean Networks*, A.P.I.C. Series No. 29, Academic Press, 1988.

[2] Pippenger, N. J., The complexity of monotone Boolean functions, *Math. Sys. Theory*, 11, 1978, 289-316.

[3] Pöschel, R. and Kalužnin, L. A., *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften, 1979.

[4] Post, E. L., *The two-valued iterative systems of mathematical logic*, Ann. Math. Studies 5, Princeton Univ. Press, 1941.

[5] Razborov, A. A., Lower bounds on the monotone complexity of some Boolean Functions (Russian), *Dokl. Akad. Nauk*, 281, 1985, 798-801 (Transl: Sov. Math. Doklady, 31, 354-357).

[6] Razborov, A. A., A lower bound on the monotone complexity of the logical permanent (Russian), *Matemat. Zametki*, 37, 1985, 887-901 (Transl: Mathem. Notes of the Acad. of Sci. of the USSR, 37, 485-493).

[7] Shannon, C. E., The synthesis of two-terminal switching circuits, *Bell System Tech. Journal*, 28, 1949, 59-98.

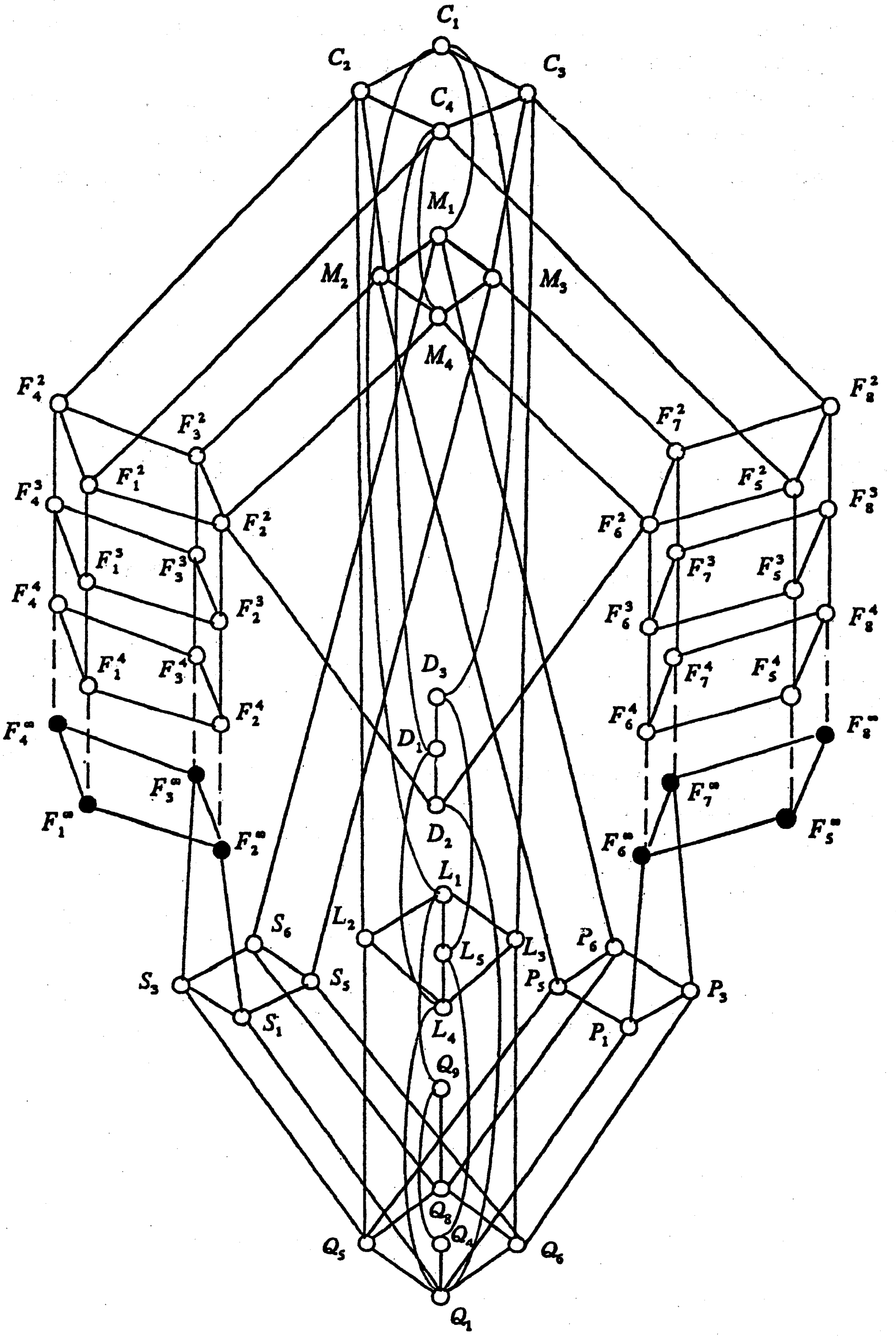
[8] Szendrei, Á., *Clones in Universal Algebra*, Université de Montréal, 1986.

[9] Tardos, E., The gap between monotone and non-monotone circuit complexity is exponential, *Combinatorica*, 7(4), 1987, 141-142.

[10] Wegener, I., *The Complexity of Boolean Functions* (Wiley–Teubner series in computer science), John Wiley & Sons and B.G. Teubner, 1987.

[11] Yanov, Y. I. and Muchnik, A. A., Existence of k-valued closed classes without a finite basis (Russian), *Dokl. Akad. Nauk.*, 127, 1959, 44-46.

Appendix A : Post Lattice $\mathcal{L}_2$



Appendix B : Generators for each clone in the Post Lattice

Clone	Set(s) of Generators	Remark	Dual
C_1	$< x \wedge y,\ x \vee y,\ \neg x >,\ < x \oplus y,\ x \wedge y,\ 1 >$	$= O_2$, All Functions	
C_3	$< x \vee y,\ x \wedge (\neg y) >$	$f(0, \cdots, 0) = 0$	C_2
C_4	$< x \wedge y,\ x \vee (y \wedge (\neg z)) >$	$f(x, \cdots, x) = x$	
M_1	$< x \wedge y,\ x \vee y,\ 0,\ 1 >$	Monotone Functions	
M_3	$< x \wedge y,\ x \vee y,\ 0 >$		M_2
M_4	$< x \wedge y,\ x \vee y >$		
D_3	$<$ Maj$(x, y, z),\ x \oplus y \oplus z,\ \neg x >$	Self Dual Functions	
D_1	$<$ Maj$(x, y, z),\ x \oplus y \oplus z >$		
D_2	$<$ Maj$(x, y, z) >$		
L_1	$< x \oplus y,\ \neg x >,\ < x \oplus y,\ 1 >$	Linear Functions	
L_3	$< x \oplus y(, 0) >$		L_2
L_5	$< x \oplus y \oplus z,\ \neg x >$		
L_4	$< x \oplus y \oplus z >$		
P_6	$< x \wedge y,\ 0,\ 1 >$		S_6
P_3	$< x \wedge y,\ 0 >$		S_3
P_5	$< x \wedge y,\ 1 >$		S_5
P_1	$< x \wedge y >$		S_1
Q_9	$< \neg x,\ 0 >,\ < \neg x,\ 1 >$		
Q_8	$< 0,\ 1 >$		
Q_6	$< 0 >$		Q_5
Q_4	$< \neg x >$		
Q_1	$< \ >$	$= J_2$, Projections	
F_8^{n-1}	$< (\neg x) \wedge y,\ d_n >$	$n \geq 3$	F_4^n
F_8^∞	$< (\neg x) \wedge y >$		F_4^∞
F_5^{n-1}	$< x \wedge (y \equiv z),\ d_n >$	$n \geq 3$	F_1^n
F_5^∞	$< x \wedge (y \equiv z) >$		F_1^∞
F_7^{n-1}	$< x \wedge (y \vee z),\ d_n,\ 0 >$	$n \geq 3$	F_3^n
F_7^∞	$< x \wedge (y \vee z),\ 0 >$		F_3^∞
F_6^{n-1}	$< x \wedge (y \vee z),\ d_n >$	$n \geq 3$	F_2^n
F_6^∞	$< x \wedge (y \vee z) >$		F_2^∞

N.B. $d_n(x_1, x_2, \ldots, x_n) = x_2 x_3 \cdots x_n \vee x_1 x_3 \cdots x_n \vee \ldots \vee x_1 x_2 \cdots x_{n-1}$