数理解析研究所講究録
976 巻 1997 年 34-37

On Buss and Turán's extensions of Haken's results

神戸大・自然 菊池 誠 (MAKOTO KIKUCHI)

In this note, we shall consider about Buss and Turán's extensions of Haken's result about the length of resolution derivations of the pigeonhole principle.

To determine whether if there exists a propositional proof system with short proofs of tautologies is one of the most fundamental problem in logic and computational complexity theory. A system S is called *super* iff there is a polynomial $p(x)$ such that for every tautology ϕ, S has a proof with length less than $p(|\phi|)$, where $|\phi|$ is the length of ϕ, and Cook and Reckhow showed in 1970's that the existence of a super system is equivalent to NP=co-NP. However, it seems that we have not have enough information about propositional proof systems nor a strategy which might lead us to the solution of the problem directly. Nowadays, showing a given system is not super and separating two systems with respect to the length of proofs are rather important as a research problem.

There are four typical propositional proof systems, called *resolution, bounded depth Frege, Frege*, and *extended Frege*, which are ordered from weaker one to stronger one (cf. [3, 6, 8]). It is known that resolution and bounded depth Frege are not super, and the pigeonhole principle plays a central role in their proof. Let PHP_n^m be a propositional formula which means that every function from $\{0, 1, \ldots, m-1\}$ to $\{0, 1, \ldots, n-1\}$ is not one-to-one. Then, PHP_n^m is a tautology whenever $n < m$.

Consider PHP_n^{n+1}. Haken [5] proved that every resolution derivation of PHP_n^{n+1} contains exponentially many clauses, and this shows that resolution is not super. Ajtai [1] showed that bounded depth Frege does not have polynomial size proofs of PHP_n^{n+1} by using some connection between bounded depth Frege and a system of bounded arithmetic and forcing arguments on models of arithmetic. Buss [2] proved that Frege has a polynomial size proof of PHP_n^{n+1}, and this fact shows the existence of a gap between bounded depth Frege and Frege with respect to the length of proofs. It is unknown that whether if Frege is a super system.

Consider PHP_n^{2n}. By using a result about the provability of the pigeonhole principle in bounded arithmetic which has been shown in Paris, Wilkie and Woods [7], we can show that bounded depth Frege has proofs of PHP_n^{2n} with the length $O(n^{\log n})$. Buss and Turán [4] extended the proof of Haken [5] and showed that every resolution derivation of PHP_n^{2n} needs the length $O(e^n)$, hence it turns out that there is a gap between resolution and bounded depth Frege with respect to the length of proofs. However, it is still unknown that whether if every resolution derivation of $\mathrm{PHP}_n^{n^2}$ contains exponentially many clauses.

Let $p(n,m)$ be a binary function. By extending Haken's argument, Buss and Turán's proved that we can show that every resolution derivation of PHP_n^m contains

$$\frac{1}{2}\left(\frac{2}{3}\right)^{\frac{1}{2}p(n,m)} \tag{1}$$

clauses if

$$\frac{i(m-2k-i-1)}{\frac{2}{3}(k-i+1)(k-i+2)} < 1 \tag{2}$$

for $0 \leq i \leq p(n,m)$. This shows that every resolution derivation of PHP_n^m contains exponentially many clauses if $m = O(n)$ since $\frac{1}{25}\frac{n^2}{m}$ satisfies this condition. However, this term is useless for the case $m = O(n^2)$ since $\frac{1}{25}\frac{n^2}{m} = O(1)$ when $m = O(n^2)$. In the following, we shall consider how one can find the term $\frac{1}{25}\frac{n^2}{m}$, and show that their result is optimal, in the sense that we cannot prove that every resolution derivation of $\mathrm{PHP}_n^{n^2}$ contains exponentially many clauses by modifying the term $\frac{1}{25}\frac{n^2}{m}$.

Let

$$\begin{aligned} q(i) &:= 2\left(\frac{n}{4}-i\right)^2 - 3i\left(m-\frac{n}{2}+i\right) \\ &= -i^2 + \left(\frac{n}{2}-3m\right)i + \frac{n^2}{8}. \end{aligned}$$

Since $k = (n/4)$,

$$\frac{i\,(m-2k-i-1)}{\frac{2}{3}(k-i+1)(k-i+2)} < \frac{3i\left(m-\frac{n}{2}+i\right)}{2\left(\frac{n}{4}-i\right)^2},$$

hence it is enough to show $q(i) > 0$ in order to prove (2). Furthermore, $q(i) > 0$ holds for $0 \leq i \leq p(n,m)$ if

$$q(p(n,m)) > 0 \tag{3}$$

since $q(0) > 0$ and the coefficient of i^2 in $q(i)$ is negative. Let $\xi(n,m)$ be the positive solution of $q(i) = 0$:

$$\xi(n,m) = \frac{1}{2}\left(-\left(3m - \frac{n}{2}\right) + \sqrt{\left(3m - \frac{n}{2}\right)^2 + \frac{n^2}{2}}\right).$$

Then (3) holds if and only if

$$p(n,m) < \xi(n,m). \tag{4}$$

Consider the case $m = an$. Then,

$$\xi = \frac{1}{2}\left(-\left(3a - \frac{1}{2}\right) + \sqrt{\left(3a - \frac{1}{2}\right)^2 + \frac{1}{2}}\right) n.$$

Hence, (4) holds if $p(n, an) = bn$ for sufficiently small b. Haken's $\frac{n}{25}$ can be obtained in this way while we must use a slightly different estimation of (2) for the case $m = n + 1$.

Consider the case $m = an^2$. In this case,

$$\begin{aligned} q(i) &= -i^2 + \left(\frac{n}{2} - 3an^2\right) i + \frac{n^2}{8} \\ &= \left(\frac{1}{8} - 3ai\right) n^2 + \frac{i}{2} n - i^2, \end{aligned}$$

so $q(b) < 0$ for any $b > \frac{1}{24a}$ for sufficiently large n, hence $\lim_{n\to\infty} \xi(n, an^2) \leq \frac{1}{24a}$. Therefore, any $p(n,m)$ with $p(n,m) = \omega(\log(n))$ does not satisfy (4), and this means that we cannot show that every resolution proof of PHP_n^m contains exponentially many clauses for the case $m = O(n^2)$ in this way.

Now we shall consider the case $p(n,m)$ is a monomial

$$p(n,m) = sn^t m^u,$$

where $s > 0$ and t and u are integers. Assume that $p(n,m)$ satisfy (4). By the above consideration, $p(n, an)$ must be $O(n)$ and $p(n, an^2)$ must be $O(1)$. So we have $t + u = 1$ and $t + 2u = 0$. Therefore, $t = 2$ and $u = -1$, and one can also determine s by the condition (3).

References

1. Ajtai, M., *The complexity of the pigeonhole principle*, Proc. IEEE 29th. FOCS, 1988, pp. 346–355.
2. Buss, S.R., *Polynomial size proof of the propositional pigeonhole principle*, J. Symbolic Logic **52** (1987), 916–927.
3. ———, *Weak Formal Systems and Connections to Computational Complexity Theory*, Lecture Notes, UCB, 1988.
4. Buss, S.R. and Turán, G., *Resolution proofs of generalized pigeonhole principle*, Theoretical Comp. Sci. **62** (1988), 311–317.
5. Haken, A., *The intractability of resolution*, Theoretical Comp. Sci. **39** (1985), 297–308.
6. Krajíček, J., *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge, 1995.
7. Paris, J.B., Wilkie, A.J. and Woods, A.R., *Provability of the pigeonhole principle and the existence of infinitely many primes*, J. Symbolic Logic **53** (1988), 1235–1244.
8. Urquhart, A., *The complexity of propositional proofs*, Bull. Symbolic Logic **1** (1995), 425–467.

THE GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, KOBE UNIVERSITY, ROKKODAI, NADA, KOBE 657, JAPAN

E-mail address: kikuchi@pascal.seg.kobe-u.ac.jp