数理解析研究所講究録
第 1799 巻 2012 年 81-83

Limiting Negations in Probabilistic Circuits

Hiroki Morizumi
Interdisciplinary Faculty of Science and Engineering, Shimane University
morizumi@cis.shimane-u.ac.jp

Abstract

The minimum number of NOT gates in a Boolean circuit computing a Boolean function f is called the inversion complexity of f. In 1958, Markov determined the inversion complexity of every Boolean function and particularly proved that $\lceil\log_2(n+1)\rceil$ NOT gates are sufficient to compute any Boolean function on n variables. In this note, we consider circuits computing probabilistically, and prove that the decrease of the inversion complexity is at most a constant if probabilistic circuits compute a correct value with probability $1/2+p$ for some constant $p>0$.

1 Introduction

When we consider Boolean circuits with a limited number of NOT gates, there is a basic question: Can a given Boolean function be computed by a circuit with a limited number of NOT gates? This question was answered by Markov [2] in 1958 and the result plays an important role in the study of the negation-limited circuit complexity. The *inversion complexity* of a Boolean function f is the minimum number of NOT gates required to construct a Boolean circuit computing f, and Markov completely determined the inversion complexity of every Boolean function f. In particular, it has been shown that $\lceil\log_2(n+1)\rceil$ NOT gates are sufficient to compute any Boolean function.

The inversion complexity has been studied for many circuit models such as constant depth circuit [5], bounded depth circuits [6], formulas [3], bounded treewidth and upward planar circuits [1], and non-deterministic circuits [4]. In this note, we consider the inversion complexity in probabilistic circuits.

2 Preliminaries

A *circuit* is an acyclic Boolean circuit which consists of AND gates of fan-in two, OR gates of fan-in two and NOT gates. A *probabilistic circuit* is a circuit with actual inputs $(x_1,\ldots,x_n)\in\{0,1\}^n$ and some further inputs

$(r_1, \ldots, r_m) \in \{0,1\}^m$ called *random inputs* which take the values 0 and 1 independently with probability 1/2. For $0 < p \leq 1/2$, a probabilistic circuit $C(x)$ computes a Boolean function $f(x)$ with probability $1/2 + p$ if

$$\mathrm{Prob}[C(x) = f(x)] \geq 1/2 + p \quad \text{for each } x \in \{0,1\}^n.$$

In this note, we call a circuit without random inputs a *deterministic circuit* to distinguish it from a probabilistic circuit.

Let x and x' be Boolean vectors in $\{0,1\}^n$. $x \leq x'$ means $x_i \leq x'_i$ for all $1 \leq i \leq n$. $x < x'$ means $x \leq x'$ and $x_i < x'_i$ for some i.

The theorem of Markov [2] is in the following. We denote the inversion complexity of a Boolean function f in deterministic circuits by $I(f)$. A *chain* is an increasing sequence $x^1 < x^2 < \cdots < x^k$ of Boolean vectors in $\{0,1\}^n$. The *decrease* $d_X(f)$ of a Boolean function f on a chain X is the number of indices i such that $f(x^i) \not\leq f(x^{i+1})$. The *decrease* $d(f)$ of f is the maximum of $d_X(f)$ over all increasing sequences X. Markov gave the tight bound of the inversion complexity for every Boolean function.

Theorem 1 (Markov[2]). *For every Boolean function f,*

$$I(f) = \lceil \log_2(d(f) + 1) \rceil.$$

In Theorem 1, the Boolean function f can also be a multi-output function.

3 Inversion Complexity in Probabilistic Circuits

3.1 Result

We denote by $I_{pc}(f, q)$ the inversion complexity of a Boolean function f in probabilistic circuits with probability q. We consider only single-output Boolean functions since probabilistic circuits are not defined as ones computing multi-output Boolean functions.

Theorem 2. *For every Boolean function f,*

$$I_{pc}(f, 1/2 + p) \geq \lceil \log_2(2p \cdot d(f) + 1) \rceil.$$

By Theorem 1 and Theorem 2, if p is a constant, then the decrease of the inversion complexity from deterministic circuits is at most a constant, which means that probabilistic computation save only the constant number of NOT gates. Especially, if $p = 1/4$, then,

Corollary 1. *For every Boolean function f,*

$$I_{pc}(f, 3/4) \geq I(f) - 1.$$

3.2 Proof

Proof (of Theorem 2). Let C be a probabilistic circuit computes f with probability $1/2+p$, and let X be a chain such that $d_X(f) = d(f)$, i.e., the decrease of f is the maximum on X. Consider some i such that $f(x^i) = 1$ and $f(x^{i+1}) = 0$. Since C computes each of $f(x^i)$ and $f(x^{i+1})$ correctly with at least $2^m(1/2+p)$ random inputs, the number of random inputs such that C computes both of $f(x^i) = 1$ and $f(x^{i+1}) = 0$ correctly is at least,

$$2^m \cdot (1 - 2 \cdot (1 - (1/2 + p))) = 2^m \cdot 2p.$$

Since, for all i such that $f(x^i) = 1$ and $f(x^{i+1}) = 0$, the number of random inputs such that C computes both of $f(x^i) = 1$ and $f(x^{i+1}) = 0$ correctly is at least $2^m \cdot 2p$, there is random inputs r such that C with r computes $f(x^i) = 1$ and $f(x^{i+1}) = 0$ correctly for at least $2p \cdot d(f)$ i's. Let C' be a circuit which obtained by fixing random inputs in C to r. C' is a deterministic circuit and computes a Boolean function f' such that $d(f') \geq 2p \cdot d(f)$. By Theorem 1, C' includes at least $\lceil \log_2(2p \cdot d(f) + 1) \rceil$ NOT gates, which is also included in C. $\square$

References

[1] J. He, H. Liang and J.M.N. Sarma, Limiting negations in bounded treewidth and upward planar circuits, *Proc. of 35th MFCS*, LNCS vol. 6281, pp. 417–428, 2010.

[2] A.A. Markov, On the inversion complexity of a system of functions, *J. ACM* 5(4), pp. 331–334, 1958.

[3] H. Morizumi, Limiting negations in formulas, *Proc. of 36th ICALP*, LNCS vol. 5555, pp. 701–712, 2009.

[4] H. Morizumi, Limiting negations in non-deterministic circuits, *Theoret. Comput. Sci.* 410(38–40), pp. 3988–3994, 2009.

[5] M. Santha and C. Wilson, Limiting negations in constant depth circuits, *SIAM J. Comput.* 22(2), pp. 294–302, 1993.

[6] S. Sung and K. Tanaka, Limiting negations in bounded-depth circuits: an extension of Markov's theorem, *Proc. of 14th ISAAC*, LNCS vol. 2906, pp. 108–116, 2003.