数理解析研究所講究録
353巻 1979年 146-151

On the Maximum Number of Prime Implicants

Yoshihide Igarashi,
Department of Computer Science,
Gunma University, Kiryu 376, Japan

Abstract

We formulate an improved lower bound on the maximum number of prime implicants of n-variable Boolean functions. It is given as $n!/(\lfloor n/3\rfloor!\lfloor(n+1)/3\rfloor!\lfloor(n+2)/3\rfloor!) + \hat{g}(n,0,\lfloor(n+1)/3\rfloor-2) + \hat{g}(n,0,\lfloor(n+2)/3\rfloor-2)$, where $\hat{g}(n,0,r)$ is evaluated by the following recursive procedure: $\hat{g}(n,0,r) = 0$ for $r<0$, $\hat{g}(n,0,0) = 1$ and $\hat{g}(n,0,r) = n!/(\lfloor r/2\rfloor!\lfloor(r+1)/2\rfloor!(n-r)!) + \hat{g}(n,0,\lfloor(r+1)/2\rfloor-2)$ for $r\geq 1$.

1. Introduction

Prime implicants play an important role in the minimization problem of Boolean functions. Generating all prime implicants of a given Boolean function is the essential step for most algorithms to find its minimal expression or realization. The problem discussed in this paper is of deriving an improved lower bound on the maximum number of prime implicants of n-variable Boolean functions.

Dunham and Fridshal(2) gave $n!/(\lfloor n/3\rfloor!\lfloor(n+1)/3\rfloor!\lfloor(n+2)/3\rfloor!)$ as a lower bound, and Harrison(3) gave 3^n-2^n as an upper bound on this number. Recently Chandra and Markowsky(1) showed a better upper bound $\binom{n}{\lfloor(2n+1)/3\rfloor} 2^{\lfloor(2n+1)/3\rfloor}$ on the number using a result on maximal sized antichains of partial orders given by Kleitman, Edelberg and Lubell(5). We derive a recursive procedure to compute an improved lower bound on the number. The recursive procedure can be easily evaluated and is conjectured to be optimal.

2. Definitions

In the main we employ definitions and notations used in standard texts of switching theory(3)(6). $\lfloor d \rfloor$ denotes the largest integer k such that $k \leq d$. For convenience we shall often identify a Boolean formula with the Boolean function expressed as the formula. Let e_{i_j} $(1 \leq j \leq n-r)$ be 0 or 1. Then $x_{i_1}^{e_{i_1}} \ldots x_{i_{n-r}}^{e_{i_{n-r}}}$ is an r-cube over n variables, where

$$x_{i_j}^{e_{i_j}} = \begin{cases} \overline{x}_{i_j} & \text{if } e_{i_j} = 0 \\ x_{i_j} & \text{if } e_{i_j} = 1 \end{cases} \quad \text{for } j = 1, \ldots, n-r$$

and $i_s \neq i_t$ if $s \neq t$ for $1 \leq s, t \leq n-r$. The universal upper bound and universal lower bound of the Boolean algebra are denoted by I and $\emptyset$ respectively. Relations $\lessdot$ and $\leqslant$ on n-variable formulas are defined as follows: $\emptyset \lessdot I$. For a pair of a and b in $\{\emptyset, I\}$, $a \leqslant b$ means $a \lessdot b$ or $a = b$. For a pair of n-variable Boolean formulas p and q, $p \leqslant q$ means that for all $(a_1, \ldots, a_n) \in \{\emptyset, I\}^n$ $p(a_1, \ldots, a_n) \leq q(a_1, \ldots, a_n)$. $p \lessdot q$ means that $p \leqslant q$ and for at least one $(a_1, \ldots, a_n) \in \{\emptyset, I\}^n$ $p(a_1, \ldots, a_n) \lessdot q(a_1, \ldots, a_n)$, where $s(a_1, \ldots, a_n)$ is the evaluation of Boolean formula s when x_i is set to be a_i for each i.

A cube p is a prime implicant of an n-variable Boolean formula E if and only if $p \leqslant E$ and there does not exist a cube q such that $p \lessdot q \leqslant E$. SPI(E) and NPI(E) denote the set of prime implicants of E and the number of prime implicants of E respectively. g(n) is defined as $\max\{NPI(E) \mid E$ is an n-variable Boolean formula$\}$. θ_n is a function from n-variable Boolean formulas to sets of n-tuples of 0's and 1's such that $(i_1, \ldots, i_n) \in \theta_n(E)$ if and only if $x_1^{i_1} \ldots x_n^{i_n} \leqslant E$. For $(a_1, \ldots, a_n) \in \{0, 1\}^n$ $w(a_1, \ldots, a_n)$ denotes the Hamming weight of $(a_1, \ldots, a_n)$, and for $S \in \{0, 1\}^n$ $w(S) = \{w(a_1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in S\}$.

The (n,m,r)-regular formula, denoted by R(n,m,r), is the disjunction of (n-m)-cubes consisting of r nonnegated variables and m-r negated variables. Boolean formula E is regular if and only if E is (n,m,r)-regular for some n, m and r. Boolean formula E is semi-regular if and only if E is a disjunction of n-variable regular formulas for some n.

3. An Improved Lower Bound on g(n)

Dunham and Fridshal's formula over n variables, denoted by DF(n), is $R(n, \lfloor(2n+2)/3\rfloor, \lfloor(n+2)/3\rfloor)$ or its variation[2]. The best known lower bound on g(n) is $\max\{NPI(R(n,m,r)) \mid 0 \le m \le n,\ 0 \le r \le m\} = \max\{\binom{n}{m}\binom{m}{r} \mid 0 \le m \le n,\ 0 \le r \le m\} = NPI(DF(n)) = n!/(\lfloor n/3\rfloor!\,\lfloor(n+1)/3\rfloor!\,\lfloor(n+2)/3\rfloor!)$. Analysing DF(n) we notice the following fact: If there exists an n-variable Boolean formula E such that $SPI(DF(n)) \subset SPI(E)$, then any prime implicant of $SPI(E) - SPI(DF(n))$ must be a smaller cube than an $\lfloor n/3\rfloor$-cube[4]. From this observation we formulate an improved lower bound on g(n).

Definition 1. $g'(n,r,s) = \max\{NPI(E) \mid E$ is an n-variable Boolean formula such that $w(\theta_n(E)) \subseteq \{r, r+1, \ldots, s\}\}$.

From the above definition it is obvious that $g(n) = g'(n,0,n)$ and $g'(n,0,r) = g'(n,n-r,n)$.

Theorem 1. $NPI(DF(n)) + g'(n,0,\lfloor(n+1)/3\rfloor-2) + g'(n,0,\lfloor(n+2)/3\rfloor-2) \le g(n)$.

Proof. Since $w(\theta_n(DF(n))) = \{\lfloor(n+2)/3\rfloor, \ldots, \lfloor(n+2)/3\rfloor+\lfloor n/3\rfloor\}$, if $w(\theta_n(F)) \subseteq \{0, \ldots, \lfloor(n+2)/3\rfloor-2\} \cup \{\lfloor(n+2)/3\rfloor+\lfloor n/3\rfloor+2, \ldots, n\}$ then $SPI(DF(n) \vee F) = SPI(DF(n)) \cup SPI(F)$ and $NPI(DF(n) \vee F) = NPI(DF(n)) + NPI(F)$. Therefore the theorem holds. □

Since for $0 \le r \le n$ and $0 \le m \le r$ $w(\theta_n(R(n,n-m,r-m))) \subseteq \{r-m, \ldots, r\}$, $NPI(R(n,n-m,r-m)) + g'(n,0,r-m-2) \le g'(n,0,r)$. If we use this relation and Theorem 1 to evaluate a lower bound on g(n), we only need values of $g'(n,0,r)$'s for $r \le \lfloor(n+2)/3\rfloor-2$. For a given r in this range NPI(R(n,n-m,r-m)) takes its maximum value when $m = \lfloor r/2 \rfloor$. Thus we obtain the next theorem.

Theorem 2. $g'(n,0,r) \geq n!/(\lfloor r/2 \rfloor ! \lfloor (r+1)/2 \rfloor ! (n-r)!) + g'(n,0,\lfloor (r+1)/2 \rfloor -2)$.

Definition 2. $\hat{g}(n,r)$ is recursively defined as follows: $\hat{g}(n,r) = 0$ for $r < 0$, $\hat{g}(n,0) = 1$ and $\hat{g}(n,r) = n!/(\lfloor r/2 \rfloor ! \lfloor (r+1)/2 \rfloor ! (n-r)!) + g'(n, 0, \lfloor (r+1)/2 \rfloor -2)$ for $0 < r \leq n$.

$\hat{g}(n,r)$ is obviously a lower bound on $g'(n,0,r)$. We can evaluate $\hat{g}(n,r)$ repeating not more than $\lfloor \log_2 r \rfloor$ times its recursion.

Theorem 3. The total logarithm computing time cost and the total uniform computing time cost of $\hat{g}(n,r)$ by a random access machine are $O(r \log_2 r \log_2 n)$ and $O(r)$, respectively.

Proof. We use the recursion $\hat{g}(n,r) = n!/(\lfloor r/2 \rfloor ! \lfloor (r+1)/2 \rfloor ! (n-r)!) + \hat{g}(n, \lfloor (r+1)/2 \rfloor -2)$. The computing cost of the first term of the above recursion dominates the total computing cost. Therefore, the order of the total computing cost equals the order of the computing cost of $f(n,r) = n(n-1) \ldots (n-r+1) = n(n-1) \ldots (n-\lfloor r/2 \rfloor +1)(n-\lfloor r/2 \rfloor) \ldots (n-r+1) = f(n,\lfloor r/2 \rfloor) f(n-\lfloor r/2 \rfloor, \lfloor (r+1)/2 \rfloor)$. Let $T(r)$ be the logarithm computing time cost of $f(n,r)$. Then from the relation $f(n,r) = f(n,\lfloor r/2 \rfloor) f(n-\lfloor r/2 \rfloor, \lfloor (r+1)/2 \rfloor)$, we have the following recurrence:

$$T(r) = \begin{cases} \log_2 n & \text{for } r = 2 \\ 2T(r/2) + r \log_2 n & \text{for } r > 2 \end{cases} .$$

The solution of the reccurence is $T(r) = O(r \log_2 r \log_2 n)$.

The total uniform computing time cost of $\hat{g}(n,r)$ is

$\sum_{i=0}^{\lfloor \log_2 r \rfloor} (r/2^i) = O(r)$. Thus the theorem holds. □

We summarize results in this section in the next theorem.

Theorem 4. A lower bound on $g(n)$ is $n!/(\lfloor n/3 \rfloor ! \lfloor (n+1)/3 \rfloor ! \lfloor (n+2)/3 \rfloor !) + \hat{g}(n, \lfloor (n+1)/3 \rfloor -2) + \hat{g}(n, \lfloor (n+2)/3 \rfloor -2)$, where $\hat{g}(n,r)$ is defined in Definition 2. The total logarithm computing time cost and the total uniform computing time cost of this lower bound by a random access machine are $O(n (\log_2 n)^2)$ and $O(n)$, respectively. The ratio of this lower bound to the old lower bound $NPI(DF(n))$ is bounded by $1 + O((1/2)^{n/3})$.

4. Conclusions and Open Problems

As stated in the previous section, our lower bound is a marginal improvement of the old one. However, we cannot find at present any Boolean formula which has more prime implicants than our new lower bound on $g(n)$. We exhaustively examined the number of prime implicants of every symmetric Boolean formula up to 17 variables on the FACOM 230/38 system at Gunma University. We conjecture that our lower bound might be optimal. Since Chandra and Markowsky's upper bound is derived using only a property of antichains, we are more confident in ourselves to conjecture that $g(n)$ might be much more closer to our lower bound than to Chandra and Markowsky's upper bound.

We invite the reader to consider the following open problems:

(1) Does there exist an n-variable semi-regular formula which has $g(n)$ prime implicants for each n ?

(2) Is our lower bound optimal to the maximum number of prime implicants n-variable semi-regula formulas for each n ?

References

(1) A. K. Chandra and G. Markowsky, On the number of prime implicants, IBM Research Report RC-6108, Yorktown Heights, New York, 1976.

(2) B. Dunham and R. Fridshal, The problem of simplifying logical expressions, J. Symbolic Logic, 2, p.47, 1959.

(3) M. A. Harrison, Introduction to Switching and Automata Theory, McGraw-Hill, New York, 1965.

(4) Y. Igarashi, Analysis of Dunham and Fridshal's formulas consisting of large numbers of prime implicants, Technical Report No. 98, Centre for

Computer Studies, University of Leeds, England, 1977.

(5) D. J. Kleitman, M. Edelberg and D. Lubell, Maximal sized antichains in partial orders, Discrete Mathematics, 1, p. 17, 1971.

(6) R. E. Miller, Swiching Theory Vol. 1, John Wiley, New York, 1965.