Discrete Mathematics 24 (1978) 7–11.


# ON THE NUMBER OF PRIME IMPLICANTS

Ashok K. CHANDRA and George MARKOWSKY

*Computer Sciences Department, IBM Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, U.S.A.*

Received 4 July 1977
Revised 17 March 1978

It is shown that any Boolean expression in disjunctive normal form having $k$ conjuncts, can have at most $2^k$ prime implicants. However, there exist such expressions that have $2^{k/2}$ prime implicants. It is also shown that any Boolean expression on $n$ distinct propositional variables can have at most $O(3^n/\sqrt{n})$ prime implicants, and that there exist expressions with $\Omega(3^n/n)$ prime implicants.

## 1. Prime implicants related to the number of conjuncts

**Definition 1.1.** A *literal* is a propositional symbol (variable) or a negated propositional symbol. A *conjunct* is a conjunction $\bigwedge_{i=1}^{k} L_i$, $k \geq 0$, of literals $L_i$ where the empty conjunction stands for *true*. A boolean expression is in *disjunctive normal form* (d.n.f.) if it is a disjunction $\bigvee_{i=1}^{k} A_i$, $r \geq 0$, of conjuncts $A_i$, where the empty boolean expression stands for *false*. A conjunct $A$ is an *implicant* of a boolean expression $E$ if $A \Rightarrow E$ (where $\Rightarrow$ stands for logical implication). Thus all conjuncts of a d.n.f. expression are its implicants. A conjunct $A$ is a *prime implicant* of a boolean expression $E$ (see, for example [2.5]) if $A \Rightarrow E$, but for every conjunct $A'$ each of whose literals is also a literal of $A$, $A' \not\Rightarrow E$. In other words, prime implicants are the minimal implicants of a boolean expression. Let PI $(E)$ be the number of distinct prime implicants of a boolean expression $E$ (two prime implicants are "distinct" if they do not have the same set of literals).

The boolean minimization problem is that of finding short d.n.f. expressions equivalent to some given d.n.f. expression. Minimization can achieve arbitrarily large savings since arbitrarily large expressions can simplify to *true*. We define below the function $f$ which is a measure of how much an expression can be simplified if the conjuncts of the given expression are all prime implicants. $f$ is also a measure of how many prime implicants may be generated when using a minimization method such as the Quine–McCluskey algorithm [4, 6].

**Definition 1.2.** For $k \geq 1$ let $f(k)$ be defined by:

$$f(k) = \text{Max}\{\text{PI}(E): E \text{ is in d.n.f. with } k \text{ conjuncts}\}. \tag{1}$$

We show below that $f(k)$ is finite.

**Theorem 1.3.**

$$3^{\lfloor k/3 \rfloor} \leq f(k) \leq 2^k. \tag{2}$$

*Comment*: $3^{\lfloor k/3 \rfloor} = O(2^{0.53k})$. Also the lower bound can be achieved with $k + \lceil \log_2 k \rceil$ propositional symbols.

**Proof.** *Lower bound.* The cases $k = 1, 2$ are trivial. For $k \geq 3$, let $r = \lfloor \frac{1}{3} k \rfloor$, and $s = \lceil \log_2 r \rceil$. The propositional symbols are $a_1, a_2, \ldots, a_s, b_1, \ldots, b_r, c_1, \ldots, c_r, d_1, \ldots, d_r$.

Let $A_1, \ldots, A_r$ be conjuncts using only $a_1, \ldots, a_s$ such that

$$A_1 \wedge A_j \equiv \text{false} \quad \text{for } i \neq j$$

and

$$\bigvee_{i=1}^{r} A_i \equiv \text{true}. \tag{3}$$

This may be done as follows. For $r = 1$, let $A_1$ be simply the expression which is always true (the empty conjunction). Otherwise, for $r \geq 2$, let $t = 2^s - r (0 \leq t \leq r-2)$. For $i \leq r-t$, let $A_i = \bigvee_{j=1}^{s} x_{ij}$ where $x_{ij}$ is $a_j$ if the $j$th bit in the $s$-bit binary representation of the integer $i-1$ is 1 (high-order bit first), and $x_{ij}$ is $\bar{a}_j$ otherwise. For $r-t < i \leq r$, let $A_i = \bigwedge_{j=1}^{s-1} x_{ij}$ where $x_{ij}$ is $a_j$ if the $j$th bit in the $s$-bit binary representation of $r-t-1+2(i-(r-t)) = 2i-r+t-1$ is 1, and $x_{ij}$ is $\bar{a}_j$ otherwise (comment: $r-t$ is an even integer). Thus for $1 \leq t \leq r-t$, $A_i$ is true for exactly one assignment of truth-values to $a_1, \ldots, a_s$. For $r-t+1 \leq i \leq r$, $A_i$ is true for exactly two assignments of truth-values to $a_1, \ldots, a_s$. Since the assignments are all distinct (they match up with distinct integers) we see that $A_i \wedge A_j \equiv$ false for $i \neq j$. The total number of truth-value assignments thus covered is $r-t+2(r-(r-t+1)+1) = r+t = 2^s$, so the disjunction of the $A_i$ is $\equiv$ true.

Let the expression $E$ be

$$(A_1 \wedge b_1) \vee (A_1 \wedge c_1) \vee (A_1 \wedge d_1) \vee (A_2 \wedge b_2) \vee \cdots \vee (A_r \wedge b_r) \vee (A_r \wedge c_r) \vee (A_r \wedge d_r).$$

Then each of the $3^r$ conjuncts of the form

$$\bigwedge_{i=1}^{r} y_i \quad \text{where } y_i \text{ is } b_i, c_i, \text{ or } d_i \tag{4}$$

is a prime implicant of $E$. To verify this, let $D = \bigwedge_{i=1}^{r} y_i$ be a conjunct of the form (4) above. Then $D \Rightarrow E$, because in any truth assignment for which $D$ is true, at least one of the $A_i$'s must be true by (3); say $A_p$ is true, in which case $A_p \wedge y_p$ is true, i.e., $E$ is true. On the other hand, if $B (B \not\equiv A)$ is a conjunct such that $D \Rightarrow B$ (i.e., $B$ contains a proper subset of the literals in $A$), then $B \not\Rightarrow E$, because we can choose a truth assignment in which $B$ is true and $E$ is false as follows. Say the literal $x_p$ in $D$ is not in $B$, then assign true/false values to the $a_i$'s such that $A_p$ is true, but $A_q$ is false for all $q \neq p$ (this can be done by (3)). Also let $b_p, c_p, d_p$ be false, and $b_q, c_q, d_q$ be true for all $q \neq p$. Then $B$ is true, but $E$ is false.



**Example.** $k = 9$. Then $r = 3$, $s = 2$. The expression $E$ is

$$\bar{a}_1\bar{a}_2b_1 \vee \bar{a}_1\bar{a}_2c_1 \vee \bar{a}_1\bar{a}_2d_1 \vee \bar{a}_1a_2b_2 \vee \bar{a}_1a_2c_2 \vee \bar{a}_1a_2d_2 \vee a_1b_3 \vee a_1c_3 \vee a_1d_3.$$

The prime implicants include $b_1b_2b_3$, $b_1b_2c_3$, $b_1b_2d_3$, $b_1c_2b_3, \ldots, d_1d_2d_3$.

*Upper bound.* Let $E = \bigvee_{i=1}^{k} A_i$ where each $A_i$ is a conjunct. Let $\mathcal{P}$ be the set of prime implicants of $E$. We define the function $\mathcal{F}$

$$\mathcal{F}: \mathcal{P} \to 2^{\{A_i : 1 \leq i \leq k\}}$$

as follows. For $P \in \mathcal{P}$, $\mathcal{F}(P)$ is any subset $\{A_{i_1}, \ldots, A_{i_t}\}$ such that

$$P \Rightarrow \bigvee_{j=1}^{t} A_{i_j} \tag{5a}$$

but

$$P \not\Rightarrow \text{the disjunct of any proper subset of } \mathcal{F}(P). \tag{5b}$$

Clearly $\mathcal{F}(P)$ can be defined since $P \Rightarrow E$, but $P \not\Rightarrow$ the disjunct of the empty set (i.e. false). We will show that if $P_1, P_2$ are distinct elements of $\mathcal{P}$ then $\mathcal{F}(P_1) \neq \mathcal{F}(P_2)$. We will actually show that $\mathcal{F}(P)$ determines $P$ uniquely.

We will first show that for any $P \in \mathcal{P}$, $P = \bigwedge_{m=1}^{s} x_m$, where the $x_m$'s are exactly those literals that occur in some element of $\mathcal{F}(P)$, but whose dual (the dual of $a$ is $\bar{a}$, of $\bar{a}$ is $a$) does not occur in any element of $\mathcal{F}(P)$. For example, if $\mathcal{F}(P) = \{\bar{a}b, \bar{b}c, \bar{c}d\}$, we are asserting that $P$ must be $\bar{a}d$.

First, note that $P$ cannot contain a literal whose dual is in some element of $A_{i_t}$ of $\mathcal{F}(P)$ since then $P$ would imply the disjunct of $\mathcal{F}(P) - \{A_{i_t}\}$, contradicting (5b). Second, $P$ cannot contain a literal which fails to occur in any one of the elements of $\mathcal{F}(P)$, for if, say $x_1$ did not appear in any of the $A_{i_j}$, then it is easy to see that $\bigwedge_{m=2}^{s} x_m \Rightarrow \bigvee_{j=1}^{t} A_{i_j} \Rightarrow E$, contradicting the fact that $P$ is a prime implicant.

Thus we have shown that the only literals which can possibly appear in $P$ are those which appear in some element of $\mathcal{F}(P)$, but whose dual does not appear in any element of $\mathcal{F}(P)$. It remains to show if $x$ is any literal of the type just described, then $x$ appears in $P$.

Assume $x$ does not appear in $P$. Let $G = \bigvee \{A_{i_j} \in \mathcal{F}(P) : x \text{ does not appear in } A_{i_j}\}$, and $H = \bigvee \{A_{i_j} \in \mathcal{F}(P) : x \text{ appears in } A_{i_j}\}$. Then as $P \Rightarrow G \vee H$ by (5a), and neither $x$ not its dual appears in $P$ or in $G$, and $x$ appears in every conjunct of $H$, on substituting false for $x$ we have $P \Rightarrow G$, contradicting (5b).

Clearly, since $\mathcal{F}(P)$ determines $P$, there can be no more than $2^k$ elements in $\mathcal{P}$.

## 2. Prime implicants related to the number of variables

**Definition 2.1.** For $n \geq 1$ let $g(n)$ be defined by

$$g(n) = \text{Max}\{\text{PI}(E) : E \text{ is a boolean function on } n \text{ variables}\}. \tag{6}$$

The function $g$ is a measure of the complexity of boolean functions on $n$ variables, when written in minimal d.n.f. Dunham and Fridshal [1] presented examples showing that

$$g(n) \geq \binom{n}{\lfloor n/3 \rfloor \ \lfloor (n+1)/3 \rfloor \ \lfloor (n+2)/3 \rfloor}$$

and that $g(8) \geq 576$. Harrison [2 p. 117, Example 4], observed that $g(n) \leq 3^n - 2^n$. Vikulin [7] derives the same upper bound we do, but his argument is significantly longer and more complicated. (The authors are indebted to N.J. Pippenger for directing our attention to [7]).

**Theorem 2.2**

$$\binom{n}{\lfloor n/3 \rfloor \ \lfloor (n+1)/3 \rfloor \ \lfloor (n+2)/3 \rfloor} \leq g(n) \leq \binom{n}{\lfloor (n+1)/3 \rfloor} 2^{\lfloor (2n+1)/3 \rfloor} \quad (7)$$

*Comment.* The lower bound is $\Omega(3^n/n)$, the upper bound is $O(3^n/\sqrt{n})$.

**Proof.** The lower bound [1] is obtained by taking the disjunction of all conjuncts containing $\lfloor \frac{1}{3}(n+1) \rfloor + \lfloor \frac{1}{3}(n+2) \rfloor$ variables, exactly $\lfloor \frac{1}{3}(n+1) \rfloor$ of which are negated. If $E$ is the resulting expression, we claim that the prime implicants of $E$ are precisely the conjuncts described. To see this, observe that $E$ is true for a truth assignment if and only if at least $\lfloor \frac{1}{3}(n+1) \rfloor$ variables are assigned false, and at least $\lfloor \frac{1}{3}(n+2) \rfloor$ variables assigned true. Thus no prime implicant of $E$ can have fewer than $\lfloor \frac{1}{3}(n+1) \rfloor$ negated variables, or fewer than $\lfloor \frac{1}{3}(n+2) \rfloor$ unnegated ones. Certainly it can't have more than that of either.

For the upper bound, let $E$ be a boolean function, $E \not\equiv$ true, on $n$ variables $a_1, \ldots, a_n$, and let $\mathscr{C}$ be the set of all conjuncts on $a_1, \ldots, a_n, \bar{a}_1, \ldots, \bar{a}_n$ such that not both $a_i$ and $\bar{a}_i$ appear in the same conjunct (for all $i$). Also equivalent conjuncts are not repeated, e.g., only one of $a_1\bar{a}_2, \bar{a}_2 a_1$ will appear in $\mathscr{C}$. The conjuncts are partially ordered in the standard way by implication i.e., $A_1 \leq A_2$ iff $A_1 \Rightarrow A_2$, i.e., the literals of $A_2$ are a subset of the literals of $A_1$.

Let $\mathscr{P}$ be the set of prime implicants of $E$. Then $\mathscr{P}$ is an antichain in $\mathscr{C}$, i.e., $\mathscr{P} \subset \mathscr{C}$, and for no two distinct conjuncts $A_1, A_2 \in \mathscr{P}$ do we have $A_1 \leq A_2$. Thus $|\mathscr{P}|$ is bounded above by the size of the largest anti-chain in $\mathscr{C}$.

Kleitman et al. [3] have shown that in any partially ordered set there exists an anti-chain of largest size which is invariant under any automorphism of the partially ordered set. Let $\mathscr{Q}$ be such an anti-chain for $\mathscr{C}$.

Let $A = \bigwedge_{i=1}^{t} x_i$ and $B = \bigwedge_{i=1}^{t} y_i$, $A, B \in \mathscr{C}$, both with $t$ literals. Consider any map $\mathscr{F}: \{a_1, \ldots, a_n, \bar{a}_1, \ldots, \bar{a}_n\} \to \{a_1, \ldots, a_n, \bar{a}_1, \ldots, \bar{a}_n\}$ such that: (a) $\mathscr{F}(a_i)$ is the dual of $\mathscr{F}(\bar{a}_i)$, and (b) $\mathscr{F}(A) = B$ under the obvious extension. $\mathscr{F}$ induces an automorphism on $\mathscr{C}$ carrying $A$ to $B$. Since $\mathscr{Q}$ is invariant under all automorphisms, $B \in \mathscr{Q}$. Thus we see that if $\mathscr{Q}$ contains one conjunction of $t$ literals, it must also contain all other conjunctions of $t$ literals. Since $\mathscr{Q}$ is an anti-chain and since



for any conjunct $A$ of $s$ literals, $s \neq t$, there is a conjunct $B$ of $t$ literals such that $A \leq B$ or $B \leq A$, $\mathscr{Q}$ must consist exactly of the set of all conjuncts of $t$ literals, for some $t$.

There are $\binom{n}{t}2^t$ conjuncts of $t$ literals on $n$ variables, and this is maximized when $t = \lfloor \frac{1}{3}(2n+1) \rfloor$—this is seen from the fact $\binom{n}{t}2^t \leq \binom{n}{t+1}2^{t+1}$ iff $3t+1 \leq 2n$. This completes the proof.

## References

[1] B. Dunham and R. Fridshal, The problem of simplifying logical expressions, J. Symbolic Logic 24 (1959) 17–19.
[2] M.A. Harrison, Introduction to Switching and Automata Theory (McGraw-Hill, New York, 1965).
[3] D.J. Kleitman, M. Edelberg and D. Lubell, Maximal sized antichains in partial orders, Discrete Math. (1971) 47–53.
[4] E.J. McCluskey Jr., Minimization of Boolean functions, Bell System Tech. J. 35(6) (1956) 1445–1446.
[5] R.E. Miller, Switching Theory, Vol. I (John Wiley, New York, 1965).
[6] W.V. Quine, A way to simplify truth functions, Am. Math. Monthly 59(8) (1952) 521–531.
[7] A.P. Vikulin, Estimate of the number of conjunctions in reduced d.n.f., Problemy Kibernet. 28 (1974) 151–166 (in Russian).