ANNOUNCEMENT OF NEW RESULTS

(of authors having an address in Czechoslovakia)

BOOLEAN FUNCTIONS REPRESENTED BY RANDOM FORMULAS

P. Savický (Katedra kybernetiky a informatiky, MFF UK, Malostranské nám. 25, 118 00 Praha 1, Czechoslovakia), received 30.3. 1987

Let $n \geq 1$ be a fixed natural number. A Boolean function of n variables is any function $f:\{0,1\}^n \to \{0,1\}$, cf. [1].

We study the representation of Boolean functions by Boolean formulas of the following type.

Definition 1. Let $x_1, x_2, \dots, x_n$ be variables. Let B be a set of function symbols all of which have the same number of arguments $k \geq 2$. For all $i \geq 0$ let H_i be the set of Boolean formulas defined in the following way.

$H_o = \{x_1, x_2, \dots, x_n, \neg x_1, \neg x_2, \dots, \neg x_n\}$

$H_{i+1} = \{\alpha(\varphi_1, \varphi_2, \dots, \varphi_k); \alpha \in B,\ \varphi_j \in H_i \text{ for } j=1,2,\dots,k\}.$

Elements of H_i for $i=0,1,2,\dots$ are formal expressions of increasing complexity. Given an interpretation of all symbols $\alpha \in B$ as functions $\alpha:\{0,1\}^k \to \{0,1\}$, any formula of H_i for all $i \geq 0$ represents a Boolean function in a natural way.

Definition 2. Let F_i be a random variable whose values are formulas from H_i and the distribution of which is the uniform distribution on H_i.

Our aim is to present some results on the distribution of Boolean functions represented by the formula F_i. For an arbitrary set $A \subseteq \{0,1\}^n$ and $i \geq 0$ let $F_i \restriction A$ denote the restriction of the Boolean function represented by F_i to the set A.

Theorem 1. Let $B=\{\&, \vee\}$ (i.e. k=2) and F_i be as in Definition 2. Then for every $A \subseteq \{0,1\}^n$ and every $f:A \to \{0,1\}$ we have

$$\lim_{i \to \infty} P(F_i \restriction A=f) = \begin{cases} 0 & \text{if } f \text{ is not a constant function} \\ 1/2 & \text{if } f \equiv 0 \text{ or } f \equiv 1 \end{cases}$$

The following theorem deals with the selection function $s(x,y,z)$ defined as $s(0,y,z)=y$ and $s(1,y,z)=z$ for all $y,z \in \{0,1\}$.

Theorem 2. Let $B=\{s\}$ (k=3) and F_i be as in Definition 2. Then for every $A \subseteq \{0,1\}^n$ and every $f:A \to \{0,1\}$ we have

$$\lim_{i \to \infty} P(F_i \restriction A=f) = (1/2)^{|A|}$$

The convergence in Theorem 1 is of the order of magnitude $O(1/i)$ and in Theorem 2 $O(c^i)$ where $c<1$.

Outline of the proofs. Note that $F_{i+1} = \alpha(F_i^1, F_i^2, \dots, F_i^k)$

where F_i^j are independent realizations of the random formula F_i and α is a random element of B independent of F_i^j. Using this we can establish a recurrent relation for $P(F_i \upharpoonright A=f)$. We prove Theorems 1 and 2 for one and two element sets A by a direct computation using this relation. Theorem 1 in the general case is a simple consequence. Theorem 2 for $|A| \geq 3$ can be proved by induction on $|A|$.

An analogous type of probability distribution on formulas was used by Valiant ([2]) in a probabilistic construction of monotone formulas of the size $O(n^{5.3})$, for the majority function.

References:

[1] Savage J.E.: The Complexity of Computing, Wiley-Interscience, New York, 1976.

[2] Valiant L.G.: Short monotone formulae for the majority function, Journal of Algorithms 5(1984), 363-366.