I. N. Kovalenko

1965

SovietRxiv

Abstract

Full Text

I. N. Kovalenko

ON A LIMIT THEOREM FOR DETERMINANTS IN THE CLASS OF BOOLEAN FUNCTIONS

(Presented by Academician V. M. Glushkov on 26 X 1964)

1.

In some problems of computer engineering and automata theory there arises the question of the existence and uniqueness of a solution of a system of n linear equations with n unknowns in the class of Boolean functions, when the coefficients of these equations are random variables. As is known, for the existence of a unique solution of the system of equations

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad 1 \le i \le n, \tag{1}$$

it is necessary and sufficient that its determinant Δ_n be equal to 1. Of interest is the computation of the quantities $\pi_n = \mathbf{P}\{\Delta_n = 1\}$ and the estimation of the limiting behavior of π_n as $n \to \infty$. In the case where a_{ij} are random variables, independent in the aggregate and taking the values 0 and 1 with equal probabilities, the formula

$$\pi_n = \prod_{i=1}^{n}(1 - 2^{-i});$$

is valid; this result is well known. In the present note it is established that, as $n \to \infty$, there is a certain invariance of $\pi = \lim_{n\to\infty} \pi_n$ with respect to the distribution of the random variables $\{a_{ij}\}$.

Theorem. Let $\{a_{ij}\}$ be random variables independent in the aggregate; $\mathbf{P}\{a_{ij} = 1\} = p_{ij}$, $\mathbf{P}\{a_{ij} = 0\} = 1 - p_{ij}$, $1 \le i, j \le n$. Then, if

$$0 < \delta \le p_{ij} \le 1 - \delta, \qquad n \ge 1, \qquad 1 \le i,\ j \le n, \tag{2}$$

then the formula

$$\lim_{n\to\infty} \pi_n = \prod_{i=1}^{\infty}(1 - 2^{-i}) \approx 0.29. \quad (3)$$

is valid.

2. Proof.

Consider the process of computing the determinant Δ_n, consisting in the following. If in the first row of the determinant $a_{1k} < a_{1j}$, $1 \leq k < j$, then the j-th column is added to all the remaining columns whose first elements are equal to 1. In the determinant of order $(n-1)$ obtained, the process is repeated, etc.; the addition of columns is each time performed from left to right.

Let us note that the property $\{\delta \leq p \leq 1-\delta\}$ is invariant with respect to the operation of addition modulo 2: if to a random vector for which the conditional probability that any fixed component is equal to one, given the values of the remaining components, satisfies this inequality, one applies a nonsingular linear transformation with a matrix independent of the vector components, then for the random vector obtained as a result of the transformation this will also be satisfied

this estimate. Consequently, under all transformations, for the probability that an element of the resulting determinant is equal to one, the estimate $\delta \leqslant p \leqslant 1-\delta$ will hold.

On the basis of this property we conclude that the probability that any fixed r elements of the initial determinant, or of determinants obtained as a result of reduction, are equal to zero does not exceed $(1-\delta)^r$. Fix integers m and k satisfying the condition $0 < k < m < n$, and denote by Δ'_{n-m} the determinant of order $(n-m)$ obtained after the m-th reduction.

On the basis of the preceding we conclude that this determinant will be computed, i.e. that the process will not terminate in m steps, with probability not less than

$$1 - (1-\delta)^n - (1-\delta)^{n-1} - \cdots$$

$$\cdots - (1-\delta)^{n-m+1} > 1 - \delta^{-1}(1-\delta)^{n-m+1}.$$

Let us now estimate the probability α that in the determinant Δ'_{n-m} none of the first k columns of the initial determinant Δ_n remains (it is assumed that the number of a column is preserved when a column standing to the left is added to it). If, during the first m reductions, the element standing in the first column and the first row assumes the value 1 at least k times, then the event of interest to us will occur; consequently,

$$\alpha \geqslant 1 - \sum_{i=0}^{k-1} C_m^i \max\{\delta^i (1-\delta)^{m-i},\ \delta^{m-i}(1-\delta)^i\}. \tag{4}$$

We obtain that, with probability not less than

$$1 - \delta^{-1}(1-\delta)^{n-m+1} - \sum_{i=0}^{k-1} C_m^i \max\{\delta^i (1-\delta)^{m-i},\ \delta^{m-i}(1-\delta)^i\} = \beta,$$

the determinant Δ'_{n-m} will have the following structure. Let $\sigma_1, \sigma_2, \dots, \sigma_{n-m}$ be the columns of this determinant; then one can write

$$\sigma_i = s_{r_{i1}} + s_{r_{i2}} + \dots + s_{r_{i\nu_i}}, \tag{5}$$

where $s_1, s_2, \dots$ are the columns of the initial determinant Δ_n in which the first m elements have been deleted. We shall assume that if some column s_j was added to the column from which σ_i is obtained an even number of times, then this s_j does not enter into the expression (5). Denote by ξ_{ij} the random variable equal to the value of the characteristic function of the set $\{r_{i1}, r_{i2}, \dots\}$ at the element j. By virtue of the estimate obtained above, with probability not less than β, an event will occur under which the conditional probabilities of the different values of ξ_{ij} will satisfy the estimate

$$\delta^N \leqslant \mathbf{P}\{\xi_{ij} = l_{ij},\ (i,j) \in I\} \leqslant (1-\delta)^N, \tag{6}$$

where $\{l_{ij}\}$ is any collection of zeros and ones, and I is any set of pairs of indices for which $1 \leqslant i \leqslant n-m,\ 1 \leqslant j \leqslant k$. The probability that each of the sets $\{r_{i1}, r_{i2}, \dots\}$, $1 \leqslant i \leqslant n-m$, contains at least t elements not contained in the remaining sets is estimated from below by the expression

$$1 - (n-m) \sum_{i=0}^{t-1} C_k^i \delta^{i(n-m)} (1-\delta)^{(k-i)(n-m)}.$$

But if this event takes place, then, as is easy to show, for fixed values of all elements of the determinant Δ'_{n-m} except one, the latter is equal to 1 or 0 with probabilities differing from 1/2 by no more than $\frac{1}{2}(1-2\delta)^t$.

Finally, let us derive the last auxiliary estimate. Suppose that there is a determinant of order h, whose elements are equal to 1 or 0 with probabilities p_{ij}, where $|p_{ij} - 1/2| \leq \gamma < 1/2$. Then, from the probability measure defined on the set of possible values of the corresponding matrix, one can single out a component with total measure $(1-2\gamma)^{h^2}$ in such a way that, for this component, the distribution of the values of the elements will be equiprobable. Consequently, the probability that the given determinant is equal to one differs from

$$\prod_{i=1}^{h}(1-2^{-i})$$

(which corresponds to the case when $p_{ij}=1/2$) by no more than $1-(1-2\gamma)^{h^2}$.

Combining the estimates obtained, we arrive at the inequality

$$\left|\pi_n-\prod_{i=1}^{\infty}(1-2^{-i})\right|<\delta^{-1}(1-\delta)^{n-m+1}+ \\ +\sum_{i=0}^{k-1}C_m^i\delta^i(1-\delta)^{m-i}+(n-m)\sum_{i=0}^{t-1}C_k^i\delta^{i(n-m)}(1-\delta)^{(k-i)(n-m)}+ \\ +1-\left[1-(1-2\delta)^t\right]^{(n-m)^2}+\left[\prod_{i=1}^{n-m}(1-2^{-i})\right]\left[1-\prod_{i=n-m+1}^{\infty}(1-2^{-i})\right]. \tag{7}$$

On the right-hand side of formula (7) there are the parameters n, m, k, and t. The remaining part of the proof consists in their appropriate choice.

First we fix $n-m$ in such a way that $(1-\delta)^{n-m+1}<\varepsilon\delta$ and

$$1-\prod_{i=n-m+1}^{\infty}(1-2^{-i})<\varepsilon.$$

Then we choose t from the condition

$$1-\left[1-(1-2\delta)^t\right]^{(n-m)^2}<\varepsilon.$$

Obviously, one can next choose k so large that

$$(n-m)\sum_{i=0}^{t-1}C_k^i\delta^{i(n-m)}(1-\delta)^{(k-i)(n-m)}<\varepsilon.$$

The term

$$\sum_{i=0}^{k-1}C_m^i\delta^i(1-\delta)^{m-i}$$

will be less than ε for fixed $n-m$, k, and t, by choosing n sufficiently large. The theorem is proved.

Since, obviously, the convergence to the limit is not uniform with respect to δ in the interval $(0, 1)$, it is of interest to investigate the asymptotics of π_n as $n \to \infty$ and p_{ij} tend to 0 or to 1. However, the author of the present paper has not set himself the goal of solving this problem.

The result obtained may find application in questions connected with the numerical solution, on digital computers, of systems of equations with random errors.

Received
25 IX 1964

Note: Figure translations are in progress. See original paper for figures.