Mathematical Problems of Computer Science 45, 14–18, 2016.

Asymptotic Estimates of the Number of Solutions of Systems of Equations with Partial Boolean Functions

Eduard V. Yeghiazaryan

Yerevan State University
e-mail: eduardyeg@mail.ru

Abstract

In this paper a class of systems of equations with partial (not everywhere defined) Boolean functions is investigated. The asymptotic estimate of the number of solutions of systems of equations is determined for the "typical" case.

Keywords: Boolean equations, Solution of equation, Partial boolean functions.

1. Introduction

Many problems of discrete mathematics, including problems which are traditionally considered to be complex, lead to the solutions of the systems of Boolean equations of the form

$$\left\{\begin{array}{l} f_i\left(x_1,\ldots,x_n\right)=1, \\ i=1,...,l, \end{array}\right. \tag{1}$$

or to the reveal of those conditions, under which the system (1) has a solution. In general problem of realizing whether the system (1) has a solution or not is NP-complete [1]. Therefore, it is often necessary to consider special classes of the systems of equations, using their specificity, or explore a number of solutions for the "typical" case.

2. Definitions and Result Formulation

Let $\{M(n)\}_{n=1}^{\infty}$ be the collection of sets, such that $|M(n)| \to \infty$ when $n \to \infty$, ($|M|$ is the power of the set M), and $M^s(n)$ is the subset of all the elements from $M(n)$, which have the property S. We say, that almost all the elements of the set $M(n)$ have the property$S$, if $\left|M^S(n)\right| / \left|M(n)\right| \to 1$, when $n \to \infty$.

We denote by $S_{n,l}$ the set of all the systems of the form (1), where $f_i\left(x_1,\ldots,x_n\right), i = 1,...,l-$ pairwise different Boolean functions of variables $x_1, x_2, ..., x_n$. It is easy to see, that $|S_{n,l}| = C_{2^{2^n}}^l$.

Let $\{M(n)\}_{n=1}^{\infty}$ be the collection of sets, such that $|M(n)| \to \infty$ when $n \to \infty$, ($|M|$ is the power of the set$M$), and $M^s(n)$ is the subset of all the elements from $M(n)$, which have the property S. We say, that almost all the elements of the set $M(n)$ have the property S, if $\left|M^S(n)\right| / \left|M(n)\right| \to 1$, when $n \to \infty$.

We denote by $S_{n,l}$ the set of all the systems of the form (1), where $f_i\left(x_1,\ldots,x_n\right), i = 1,...,l-$ pairwise different Boolean functions of variables $x_1, x_2, ..., x_n$. It is easy to see, that $|S_{n,l}| = C^l_{2^{2^n}}$.

Let $B = \{0,1\}$,$B^n = \{\tilde{\alpha}/\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n), \alpha_i \in B, 1 \leq i \leq n\}$. The vector $\tilde{\alpha}_i = (\alpha_1, \alpha_2, ..., \alpha_n) \in B^n$ is called a solution of (1), if

$$\begin{cases} f_i(\alpha_1, \alpha_2, ..., \alpha_n) = 1, \\ i = 1, ..., l. \end{cases}$$

We denote by $t(S)$ the number of the solutions of the system S. In [2,3] the asymptotics of the number of the solutions $t(S)$ is shown for almost all the systems S of the set $S_{n,l}$ the whole range of parameter l changes, when $n \to \infty$.

In this work a class of systems of equations with partial (not everywhere defined) Boolean functions is considered. The asymptotic behavior of the number of solutions of systems of equations is found for a “typical” case.

Partial Boolean function $f\left(x_1,\ldots,x_n\right)$ on the vector $\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n) \in B^n$ or is not defined, or is 0 or 1. Let $Q(n)$ denote the set of all partial Boolean functions, depending on variables $x_1, x_2, ..., x_n$. Obviously, $|Q(n)| = 3^{2^n}$.

Let $R(n,l)$ denote the set of all systems of l equations of the form (1), where $f_i\left(x_1,\ldots,x_n\right), i = 1, ..., l$ are pairwise differing partial Boolean functions of the variables $x_1, x_2, ..., x_n$ ($f_i \neq f_j$ if $i \neq j$ condition persists). It is easy to see, that $|R_{n,l}| = C^l_{3^{2^n}}$.

For the numbers of the solutions $t(S)$ of almost all the systems S of the set $R(n,l)$ the following statement is true:

Theorem 1:
1. If $n - \ell \log 3 \to \infty$ when $n \to \infty$, then for almost all the systems $S$of the set $R(n,l)$ occurs $t(S) \sim 2^n 3^{-l}$.
2. If $n - \ell \log 3 \to -\infty$ when $n \to \infty$, then almost all the systems $S$of the set $R(n,l)$ have no solutions.
3. If $n - \ell \log 3$is restricted when $n \to \infty$, then for almost all the systems of the set $R(n,l,m)$ the number of the solutions $t(S)$is restricted from above by an arbitrary function $\varphi(n)$, satisfying the condition $\varphi(n) \to \infty$, when $n \to \infty$.

Here and further $f(n) \sim g(n)$, if $f(n)/g(n) \to 1$ when $n \to \infty$, $f(n) = o(g(n))$ if $f(n)/g(n) \to 0$ when $n \to \infty$. Everywhere the log is regarded as a logarithm to the base 2.

3. Proof of Theorem 1

The following known or easily checking inequalities hold:
1) The first Chebyshev inequality ([4]). Let the random variable ξ take the non-negative values and have mathematical expectation $M\xi$. Then for any $t > 0$ rightly

$$P(\xi \geq t) \leq M\xi/t.$$

2) The second Chebyshev inequality ([4]). Let the above random variable ξ have a dispersion $D\xi$. Then for any $t > 0$ rightly

$$P(|\xi - M\xi| \geq t) \leq D\xi/t^2.$$

3) For any $x > 1$

$$\left(1 - \frac{1}{x}\right)^x < e^{-1} .$$

4) For any natural n and $m^2 = o(n)$

$$C_n^m \sim \frac{n^m}{m!}.$$

5) For any natural n and $1 \leq m \leq n$

$$C_n^m < \left(\frac{en}{m}\right)^m .$$

6) Let $b(k; n, p) = C_n^k p^k q^{n-k}$, where $0 < p, q < 1, p + q = 1$. Then for $r > np$

$$\sum_{j=0}^{n-r} b(r + j; n, p) < b(r; n, p)(r + 1)q/(r + 1 - (n + 1)p)$$

(the estimate of the "tail" of the binomial distribution ([4])).

Let S be a system in $R(n, l)$. Arranging (transpositions by all the variations) the equations in S, we obtain ! new systems, differing from each other by transposition of the equations. Thus, from the set $R(n, l)$ we obtain a new set $R'(n, l)$ of ordered and nonrepetitive (not containing the equivalent equations) systems. It's evident that

$$|R'(n, l)| = |R(n, l)|l!. \tag{2}$$

Let almost all the systems of the set $R'(n, l)$ have the property E, which is invariant for any transposition of the equations of the system. It's easy to see, that almost all the systems of the set $R(n, l)$will also have the property E. Thus, for the proof of the Theorem it will be enough to consider the set $R'(n, l)$ instead of $R(n, l)$.

Next, we denote by $R^{''}(n, l)$ expansion of the set $R'(n, l)$ - in the systems from $R'(n, l)$ allowed a same equations. It is easy to see, that

$$|R''(n, l)| = 3^{l2^n}. \tag{3}$$

From (2), (3) and 4) we obtain, that

$$\frac{|R'(n, l)|}{|R''(n, l)|} = \frac{l!C_{3^{2^n}}^l}{3^{l2^n}} \to 1,$$

when $l^2 = o\left(3^{2^n}\right)$ $(n \to \infty)$. Thus, if $l^2 = o\left(3^{2^n}\right)$, any assertion for almost all systems of the set $R''(n, l)$ is true for almost all the systems of the set $R'(n, l)$.

We consider $R''(n, l)$ as a space of events, where every event $S \in R''(n, l)$ takes place with the probability $1/|R''(n, l)| = 3^{-l2^n}$.

Consider the random value $\xi_S(\tilde{\alpha})$, which is connected with $S \in R'(n, l)$ as follows: $\xi_S(\tilde{\alpha}) = 1$, if $\tilde{\alpha}$ is the solution of the system S, and $\xi_S(\tilde{\alpha}) = 0$ in another case.

From the definition it follows, that the number of the system $S \in R'(n, l)$, for which $\tilde{\alpha}$ is a solution, equal to $3^{l(2^n-1)}$. From this and (3) it follows, that $P(\xi_S(\tilde{\alpha}) = 1) = 3^{-l}$.

Consider another random value $v = \sum\limits_{\tilde{\alpha} \in B^n} \xi_S(\tilde{\alpha})$. Random value v has a binomial distribution, because

$$p\,(v = j) = C_{2^n}^{j} 3^{-lj} (1 - 3^{-l})^{2^n - j}.$$

Hence, $Mv = 2^n 3^{-l}$ and $Dv = 2^n 3^{-l} \left(1 - 3^{-l}\right)$, where Mv and Dv are the mathematical expectation and dispersion of the random value v, accordingly.

Let $n - \ell \log 3 \to \infty$ when $n \to \infty$. It means, that $Mv = 2^n 3^{-l} = 2^{n - l \log 3} \to \infty$ when$n \to \infty$. Using the Chebishev's inequation 2) when $t = Mv/\sqrt{n - l \log 3}$, we obtain, $P\left(|v - Mv| \geq Mv/\sqrt{n - l \log 3}\right) \leq (n - l \log 3)(1 - 3^{-l})/2^{n - l \log 3} \to 0$ when $n \to \infty$. Hence and from the definition of random value v it follows, that almost all the systems of the set $R''(n, l)$ have the number of solutions, which asymptotically equals Mv.

Since under $n - \ell \log 3 \to \infty$ is performed $l^2 = o\left(3^{2^n}\right)$, almost all the systems of the set $R(n, l)$ have also number of solutions, asymptotically equal to $Mv = 2^n 3^{-l}$. The first statement of the Theorem is proved.

Let $n - \ell \log 3 \to -\infty$ when $n \to \infty$. Then $Mv = 2^n 3^{-l} = 2^{n - l \log 3} \to 0$ $(n \to \infty)$. Using Chebishev's first inequation when t=l, we obtain $P\,(v \geq 1) \to 0$ when $n \to \infty$ and therefore , $P\,(v = 0) \to 1$ when $n \to \infty$. Hence it follows, that almost all the systems S of the set $R''(n, l)$ have no solution. Therefore, when $l^2 = o\left(3^{2^n}\right)$ the second statement of the Theorem is proved. It is easy to see, that for the greater values of the parameter l the statement of the Theorem also holds (the number of solutions of the system does not increase with the number of equations).

Now let $n - \ell \log 3$ be restricted, when $n \to \infty$. Then $Mv = 2^n 3^{-l} = 2^{n - l \log 3}$ is also restricted when $n \to \infty$. Using the inequations 6), 5) and 3), we obtain

$$P\,(v > r) = \sum_{i=0}^{2^n - r} C_{2^n}^{r+i} 3^{-l(r+i)} (1 - 3^{-l})^{2^n - r - i} \leq C_{2^n}^{r} 3^{-lr} (1 - 3^{-l})^{2^n - r} \times$$

$$\times\,(r + 1)\left(1 - 3^{-l}\right) / \left(r + 1 - (2^n + 1)\, 3^{-l}\right) \leq (e 2^n 3^{-l} r^{-1})^r \leq \left(\frac{eMv}{r}\right) \to 0,$$

when $r \to \infty$, because Mv is restricted . Therefore, for almost all the systems of the set $R''(n, l)$ the third statement of the Theorem holds. Since $n - \ell \log 3$ is restricted, then $l^2 = o\left(3^{2^n}\right)$ is performed, and, therefore, for almost all the systems of the set $R(n, l)$ the third statement of the Theorem holds. Theorem is completely proved.

References

[1] M. Geri and D. Johnson, *Computers and Intractability*, (In Russian), Moscow, Mir, 1982.

[2] E. V. Yeghiazaryan, “Metric properties of systems of Boolean equations”, *DAN Armenian SSR*,(In Russian), vol. 72, no.2, pp. 67–72, 1981.

[3] E. V. Yeghiazaryan, “Estimates related to the number of solutions of Boolean equations”, *Coll. Tasks of Cybernetics. Combinatorial analysis and graph theory*, (In Russian) Moscow, pp. 124–130, 1980.

[4] W. Feller, *An Introduction to Probability Theory and Its Applications*, (In Russian), vol. 1, Moscow, Mir, 1976 .

Submitted 15.11.2015, accepted 22.01.2016

Մասնակի բուլյան ֆունկցիաներով հավասարումների համակարգերի լուծումների քանակի ասիմպտոտիկ գնահատականներ

Է. Եղիազարյան

Ամփոփում

Տրվում են մասնակի (ոչ ամերուրեք որոշված) բուլյան ֆունկցիաներից կազմված հավասարումների համակարգերի լուծումների քանակի ասիմպտոտիկ գնահատականներ «տիպիկ» դեպքի համար:

Асимптотические оценки числа решений систем уравнений с частичными булевыми функциями

Э. Егиазарян

Аннотация

Определяются асимптотические оценки числа решений систем уравнений с частичными (не всюду определенными) булевыми функциями для "типичного" случая.