Theory of Stochastic Processes
Vol.13 (29), no.1-2, 2007, pp.144-151

VOLODYMYR MASOL AND SVITLANA SLOBODYAN

ON THE ASYMPTOTIC NORMALITY OF THE NUMBER OF FALSE SOLUTIONS OF A SYSTEM OF NONLINEAR RANDOM BOOLEAN EQUATIONS

The theorem on a normal limit ($n \to \infty$) distribution of the number of false solutions of a system of nonlinear Boolean equations with independent random coefficients is proved. In particular, we assume that each equation has coefficients that take value 1 with probability that varies in some neighborhood of the point $\frac{1}{2}$; the system has a solution with the number of ones equals $\rho(n)$, $\rho(n) \to \infty$ as $n \to \infty$. The proof is constructed on the check of auxiliary statement conditions which in turn generalizes one well-known result.

1. Introduction

Let us consider a system of equations over the field GF(2) consisting of two elements

$$\sum_{k=1}^{g_i(n)} \sum_{1 \le j_1 < \ldots < j_k \le n} a^{(i)}_{j_1 \ldots j_k} x_{j_1} \ldots\ x_{j_k} = b_i, \ \ i = 1, \ldots, N, \tag{1}$$

that satisfies condition (A).

Condition (A):

1) Coefficients $a^{(i)}_{j_1 \ldots j_k}$, $1 \le j_1 < \ldots < j_k \le n$, $k = 1, \ldots, g_i(n)$, $i = 1, \ldots, N$, are independent random variables that take value 1 with probability $P\left\{ a^{(i)}_{j_1 \ldots j_k} = 1 \right\} = p_{ik}$ and value 0 with probability $P\left\{ a^{(i)}_{j_1 \ldots j_k} = 0 \right\} = 1 - p_{ik}$.

2) Elements b_i, $i = 1, \ldots, N$, are the result of the substitution of a fixed n-dimensional vector $\bar{x}^0$, which has $\rho(n)$ $/n - \rho(n)/$, components equal to one /zero/ into the left-hand side of the system (1).

3) Function $g_i(n)$, $i = 1, \ldots, N$, is nonrandom, $g_i(n) \in \{2, \ldots, n\}$, $i = 1, \ldots, N$.

2000 *Mathematics Subject Classifications.* Primary 60C05, 15A52, 15A03.

Key words and phrases. The nonlinear random Boolean equations, normal limit distribution, number of false solutions

Denote by ν_n the number of false solutions of the system (1), i.e. the number of solutions of the system (1) different from the vector $\bar{x}^0$.

We are interested in the conditions under which the random variable ν_n has a normal limit $(n \to \infty)$ distribution.

2. Formulation of the theorem

Theorem. *Let condition (A) hold, and moreover*

$$[\lambda] = 2^m, \tag{2}$$

where $m = n - N$, $[\cdot]$ *is the sign of the integral part,*

$$\lambda = \frac{1}{2(1+\alpha+\omega)} \log_2 \frac{\rho(n)}{\varphi(n)\ln n}, \quad \varphi(n) > 0, \tag{3}$$

$$\lambda \to \infty, \tag{4}$$

$$\lambda\,(\alpha \ln \alpha - \alpha - 1) \to \infty, \tag{5}$$

$$\omega\sqrt{\lambda} \to \infty \tag{6}$$

as $n \to \infty$;
let for any arbitrary i, $i = 1, ..., N$, *there exist a nonempty set* T_i *such that for all sufficiently large values of* n

$$T_i \subseteq \{2, 3, ..., g_i(n)\}, \; T_i \neq \emptyset,$$

$$\delta_{it}(n) \leq p_{it} \leq 1 - \delta_{it}(n), \quad t \in T_i; \tag{7}$$

$$\overline{\lim_{n\to\infty}}\, (\alpha+\omega)\,\lambda\, B\;(\rho(n)-1,\,1) < \infty, \tag{8}$$

$$B\;(X,Y) = \sum_{i=1}^{N} \exp\left\{-2 \sum_{t\in T_i} \delta_{it}(n) C_X^{t-Y}\right\};$$

$$(2 + (1+\alpha+\omega)\ln 2)\lambda - \frac{\ln\lambda}{2} + \ln B\,(\varepsilon\varphi(n), 0) \to -\infty \;\; (n \to \infty), \tag{9}$$

where $\varepsilon = const$, $0 < \varepsilon < 1$;

$$\overline{\lim_{n\to\infty}}\, (-\ln N + \ln B\,(\varepsilon\varphi(n), 1)) < 0 \;\; (n \to \infty). \tag{10}$$

Then distribution function of the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$ *tends to the standard normal distribution function .*

3. Auxiliary statements

Lemma 1. *Let ξ and η be random variables that take non-negative integer values. If*

$$\max_{1\le r\le T}\left|M(\xi)_r(M(\eta)_r)^{-1}-1\right|=\varepsilon_T<1; \tag{11}$$

$$M(\eta)_r\le C\lambda_1^r,\ \ 1\le r\le T, \tag{12}$$

where $M(\zeta)_r$ denotes r–factorial moment of a random variable ζ, $r\ge 1$, then for an arbitrary t, $0\le t\le T-\alpha\lambda_1$ and $\alpha>1$,

$$\begin{gathered}|P\{\xi\ge t\}-P\{\eta\ge t\}|\le\\ \le\frac{C}{\sqrt{2\pi\max(1,\lambda_1-1)}}\left(\varepsilon_T e^{2\lambda_1}+\frac{1+\varepsilon_T}{\sqrt{2\pi\max(1,\alpha\lambda_1)}}\exp\left\{(t+\lambda_1-T)u(\alpha)\right\}\right),\end{gathered} \tag{13}$$

where $u(\alpha)=(\alpha-1)^{-1}(\alpha\ln\alpha-\alpha-1)$ for $2>\ln\alpha>0$, and $u(\alpha)=\ln\alpha-1$ for $\ln\alpha\ge 2$.

Proof. By virtue of Bonferrony inequalities, for any arbitrary random variable ζ that takes non-negative integer values, and for any arbitrary integers $t>0$ and $d\ge 0$

$$\sum_{r=t}^{t+2d+\beta}(-1)^{r+t}C_{r-1}^{t-1}\frac{1}{r!}M(\zeta)_r\le P\{\zeta\ge t\}\le\sum_{r=t}^{t+2d}(-1)^{r+t}C_{r-1}^{t-1}\frac{1}{r!}M(\zeta)_r, \tag{14}$$

where $\min\left(M(\zeta)_{t+2d+\beta},\, M(\zeta)_{t+2d}\right)<\infty,\ \ \beta\in\{-1,1\}$. (Proof of relation (14) for $\beta=-1$, $M(\zeta)_{t+2d-1}<\infty$ look, for example, in ([1], p.136, 223))

Let numbers t and T have identical parity. Then, using (14) for $\beta=-1$, we receive

$$P\{\xi\ge t\}-P\{\eta\ge t\}\le\Gamma(T)+M(\xi)_T C_{T-1}^{t-1}\frac{1}{T!}, \tag{15}$$

$$P\{\xi\ge t\}-P\{\eta\ge t\}\ge\Gamma(T)-M(\eta)_T C_{T-1}^{t-1}\frac{1}{T!}, \tag{16}$$

where $\Gamma(T)=\sum\limits_{r=t}^{T-1}(-1)^{r+t}C_{r-1}^{t-1}\frac{1}{r!}M(\eta)_r\left(\frac{M(\xi)_r}{M(\eta)_r}-1\right)$.

If the difference $P\{\xi\ge t\}-P\{\eta\ge t\}$ is non-negative /non-positive/that we obtain

$$|P\{\xi\ge t\}-P\{\eta\ge t\}|\le|\Gamma(T)|+\frac{1}{T!}C_{T-1}^{t-1}\max\left(M(\xi)_T,M(\eta)_T\right) \tag{17}$$

by virtue of conditions (15), (16).
It is easy to check up that

$$\max\left(M(\xi)_T,M(\eta)_T\right)\le M(\eta)_T\left(1+\left|\frac{M(\xi)_r}{M(\eta)_r}-1\right|\right). \tag{18}$$

Using (17), (18) and conditions (11), (12), we obtain

$$|P\{\xi \geq t\} - P\{\eta \geq t\}| \leq \\ \leq C\left(\varepsilon_T \sum_{r=t}^{T-1} C_{r-1}^{t-1} \tfrac{1}{r!}\lambda_1^r + (1+\varepsilon_T)\,\lambda_1^T \tfrac{1}{T!} C_{T-1}^{t-1}\right). \tag{19}$$

Hence

$$|P\{\xi \geq t\} - P\{\eta \geq t\}| \leq C\left(\frac{\lambda_1^t}{t!} e^{\lambda_1}\varepsilon_T + (1+\varepsilon_T)\frac{\lambda_1^{T-t}}{(T-t)!}\frac{\lambda_1^t}{t!}\right). \tag{20}$$

Below the following relations will be established for the integer u, $u \geq 1$,

$$\frac{\lambda_1^u}{u!} \leq (2\pi \max(1, \lambda_1 - 1))^{-1/2} e^{\lambda_1}; \tag{21}$$

for the integer N, $N \geq \max(1, \alpha\lambda_1)$,

$$\frac{\lambda_1^N}{N!} \leq (2\pi \max(1, \alpha\lambda_1))^{-1/2} \exp\{(\lambda_1 - N)u(\alpha) - \lambda_1\}, \tag{22}$$

where $u(\alpha) = (\alpha - 1)^{-1}(\alpha \ln \alpha - \alpha - 1)$ for $2 > \ln \alpha > 0$, $u(\alpha) = \ln \alpha - 1$ for $\ln \alpha \geq 2$.
Relations (20)–(22) prove (13), when t and T have identical parity .

Let now parameters t and T have different parity. Let us show, that we can obtain (17) in this case. Using (14) for some $d \geq 0$, $\beta = 1$ and $t + 2d = T - 1$, we receive

$$P\{\xi \geq t\} - P\{\eta \geq t\} \leq \Gamma(T) + M(\eta)_T \frac{1}{T!} C_{T-1}^{t-1}, \tag{23}$$

$$P\{\xi \geq t\} - P\{\eta \geq t\} \geq \Gamma(T) - M(\xi)_T \frac{1}{T!} C_{T-1}^{t-1}. \tag{24}$$

By virtue of (23), (24), we obtain (17) similarly when we used inequalities (15) and (16).

To complete the proof of Lemma 1 it is, therefore, enough to establish (21) and (22).

Let us check (21). Indeed, it follows from Stirling formula that $u! \geq (u/e)^u\sqrt{2\pi u}$. Hence

$$\frac{\lambda_1^u}{u!} \leq \left(\frac{\lambda_1 e}{u}\right)^u \frac{1}{\sqrt{2\pi u}}. \tag{25}$$

Let $\varphi(u) = \left(\frac{\lambda_1 e}{u}\right)^u$ and let us show that

$$\max_{u \geq \lambda_1 - 1} \varphi(u) = \varphi(\lambda_1). \tag{26}$$

Indeed, the first derivative $\varphi'(u) = \varphi(u)(\ln \lambda_1 - \ln u)$ and $\varphi'(u) = 0$ at $u = \lambda_1$. Since the second derivative $\varphi''(u) = \varphi(u)((\ln \lambda_1 - \ln u)^2 - u^{-1})$

is negative at $u = \lambda_1$, $\varphi''(\lambda_1) < 0$, relation (26) holds. Using (26), we establish (21) for $u \geq \max(1, \lambda_1 - 1)$.

Let further $1 \leq u \leq \lambda_1 - 1$; and let $\psi(u) = \left(\frac{\lambda_1 e}{u}\right)^u \frac{1}{\sqrt{u}}$, then

$$\max_{1\leq u\leq \lambda_1 - 1} \psi(u) = \psi(\lambda_1 - 1). \tag{27}$$

Indeed,

$$\psi'(u) = \psi(u)(\ln \lambda_1 - f(u)), \tag{28}$$

where $f(u) = \ln u + (2u)^{-1}$.

Let us show that function $f(u)$ takes its maximal value on an interval $1 \leq u \leq \lambda_1 - 1$ at $u = \lambda_1 - 1$,

$$\max_{1\leq u\leq \lambda_1 - 1} f(u) = f(\lambda_1 - 1). \tag{29}$$

Indeed, $f'(u) = u^{-1} - \frac{1}{2}u^{-2}$, and $f'(u) = 0$ at $u = \frac{1}{2}$. At the same time $f''(u)|_{u=\frac{1}{2}} = (-u^{-2} + u^{-3})|_{u=\frac{1}{2}} = 4$. Therefore, function $f(u)$ increases for $u > \frac{1}{2}$ and (29) holds on the interval $1 \leq u \leq \lambda_1 - 1$. As a result we get

$$\psi'(u) > 0 \quad \text{for} \quad 1 \leq u \leq \lambda_1 - 1. \tag{30}$$

Indeed, taking into account (29),

$$\begin{gathered} \ln \lambda_1 - f(u) \geq \\ \geq \ln\left(1 + \tfrac{1}{\lambda_1 - 1}\right) - \tfrac{1}{2(\lambda_1 - 1)} \geq \tfrac{1}{2(\lambda_1 - 1)}\left(1 - \tfrac{1}{\lambda_1 - 1}\right) > 0 \end{gathered} \tag{31}$$

for $\lambda_1 > 2$. (Here the inequality $\ln(1 + x) > x - \frac{1}{2}x^2$ has been used for $x > 0$.)

Relations (28) and (31) prove (30). Estimate (30) allows, apparently, to conclude that equality (27) holds. With the help of (25) and (27) we find

$$\frac{\lambda_1^u}{u!} \leq \left(\frac{\lambda_1 e}{\lambda_1 - 1}\right)^{\lambda_1 - 1} \frac{1}{\sqrt{2\pi(\lambda_1 - 1)}} \leq \frac{e^{\lambda_1}}{\sqrt{2\pi(\lambda_1 - 1)}} \tag{32}$$

for $1 \leq u \leq \lambda_1 - 1$.
Estimate (32) proves (21) for $1 \leq u \leq \lambda_1 - 1$. Relation (21) is proved.

Let us check (22). With the help of Stirling formula and inequality $\frac{\lambda_1}{N} \leq \frac{1}{\alpha}$, we can obtain

$$\begin{gathered} \tfrac{\lambda_1^N}{N!} \leq \tfrac{1}{\sqrt{2\pi N}} e^{\lambda_1(1-\ln\alpha)} \times \\ \times \exp\left\{\left(1 - \ln\alpha + \tfrac{2-\ln\alpha}{\alpha - 1}\right)(N - \lambda_1)\right\} \exp\left\{-\lambda_1(2 - \ln\alpha)\right\}. \end{gathered} \tag{33}$$

By virtue of conditions $N \geq \alpha\lambda_1$, $2 - \ln\alpha > 0$, and $\alpha > 1$, the right-hand side of the inequality (33) can be estimate as follows

$$\begin{gathered} \tfrac{1}{\sqrt{2\pi N}} e^{\lambda_1(1-\ln\alpha)} \exp\left\{\left(1 - \ln\alpha + \tfrac{2-\ln\alpha}{\alpha-1}\right)(N - \lambda_1)\right\} \times \\ \times \exp\left\{-\lambda_1(2 - \ln\alpha)\right\} \leq \tfrac{1}{\sqrt{2\pi N}} e^{-\lambda_1} \exp\left\{(\lambda_1 - N)\tfrac{\alpha\ln\alpha - \alpha - 1}{\alpha - 1}\right\}. \end{gathered} \tag{34}$$

From relations (33) and (34) the estimate (22) follows for $\alpha < e^2$.

Let now $\alpha \geq e^2$. Then

$$\frac{\lambda_1^N}{N!} \leq \frac{1}{\sqrt{2\pi N}} e^{-\lambda_1} \exp\{-(N-\lambda_1)(\ln\alpha - 1)\}.$$

Relation (22) is proved for all $\alpha > 1$. Lemma 1 is proved.

Lemma 2. *Let X and Y be random variables that take non-negative integer values, and $MX = \lambda^*$. If for all $r \leq (\alpha+\gamma)\lambda^*$*

$$M(Y)_r \leq C(\lambda^*)^r \tag{35}$$

with some constant C, and

$$\lambda^* (\alpha \ln\alpha - \alpha - 1) \to \infty, \tag{36}$$

$$\gamma \geq 0, \tag{37}$$

$$\max_{1 \leq r \leq (\alpha+\gamma)\lambda^*} \left| M(X)_r (M(Y)_r)^{-1} - 1 \right| \frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0 \tag{38}$$

as $\lambda^* \to \infty$,
then

$$\max_{0 \leq t \leq \gamma\lambda^*} |P\{X \geq t\} - P\{Y \geq t\}| \to 0 \;\; (\lambda^* \to \infty). \tag{39}$$

Proof. Assumptions (35) and (38) imply the conditions of Lemma 1, by virtue of which (13) holds for $0 \leq t \leq \gamma\lambda^*$, $\alpha > 1$. Using (36) and (37) it is easy to show that $\exp\{(t + \lambda^* - (\alpha+\gamma)\lambda^*)\, u(\alpha)\} \to 0$ as $\lambda^* \to \infty$ uniformly for $0 \leq t \leq \gamma\lambda^*$. Taking into account (38), it follows from the last statement that the right-hand side of the inequality (13) tends to zero as $\lambda^* \to \infty$ uniformly, for $0 \leq t \leq \gamma\lambda^*$. The left-hand side of the inequality (13) tends, therefore, to zero too for λ^* and t mentioned above, which proves, obviously, (39). Lemma 2 is proved.

Remark. The lemma 2 (for $\alpha = 5$ and $\gamma = 2$) follows from the lemma 3 in [2].

4. Proof of the theorem

Let us show that under the conditions of the theorem we can use Lemma 2. Let the random variable Y in the mentioned lemma have a Poisson distribution with parameter 2^m, while the distribution of the random variable X coincides with the distribution of the random variable ν_n. Then

$M(Y)^r = 2^{mr},\ \ r \geq 1$, while expectation $M\nu_n$ can, by virtue of its explicit form obtained in [3], be presented in the following way

$$M\nu_n = 2^m \left(1 - \frac{1}{2^n}\right) \tilde{M}, \tag{40}$$

where $\exp\{-B(\rho(n)-1,1)\} \leq \tilde{M} \leq \exp\{B(\rho(n)-1,1)\}$.
Now condition (35) becomes

$$2^{mr} \leq C(M\nu_n)^r. \tag{41}$$

It follows from (40) that inequality (41) holds true for $r \leq (1+\alpha+\omega)M\nu_n$ and

$$C \geq \left(1 - \frac{1}{2^n}\right)^{-(1+\alpha+\omega)M\nu_n} \exp\{(1+\alpha+\omega)B(\rho(n)-1,1)M\nu_n\}. \tag{42}$$

By virtue of conditions (3), (8), and equality (40), the right-hand side of (42) is limited as $n \to \infty$. Therefore, it is possible to choose a limited constant $C < \infty$ such that condition (35) holds true.

Further we note that under conditions (3)–(10) relation (38) is established in [4] for $\alpha = 5$ and $\omega = 1$. For arbitrary α and ω satisfying conditions of the theorem, verification of the relation (38) can be executed similarly.

By virtue of Lemma 2, we obtain

$$\max_{0 \leq t \leq (1+\omega)\lambda^*} |P\{\nu_n \geq t\} - P\{Y \geq t\}| \to 0 \ \text{ as } \ n \to \infty, \tag{43}$$

where $\lambda^* = M\nu_n$ according to the notations introduced above. By virtue of (40) and conditions (3) and (8), the last equality allows to present λ^* as

$$\lambda^* = [\lambda]\left(1 + r(n)\right), \tag{44}$$

where

$$r(n) = O\left(B(\rho(n)-1,1)\right) + O\left(\frac{1}{2^n}\right) \tag{45}$$

and $r(n) \to 0$ as $n \to \infty$.
We can write relation (43) in the following way

$$\max_{-\sqrt{\lambda^*} \leq l \leq \omega\sqrt{\lambda^*}} \left| P\left\{\frac{\nu_n - \lambda^*}{\sqrt{\lambda^*}} \geq l\right\} - P\left\{\frac{Y - \lambda^*}{\sqrt{\lambda^*}} \geq l\right\}\right| \to 0, \ \ n \to \infty, \tag{46}$$

where $l = \frac{t-\lambda^*}{\sqrt{\lambda^*}}$.

Let us show that distributions of the random variables $\frac{\nu_n-\lambda^*}{\sqrt{\lambda^*}}$ and $\frac{\nu_n-\lambda}{\sqrt{\lambda}}$ coincide as $n \to \infty$. Indeed,

$$\frac{\nu_n - \lambda^*}{\sqrt{\lambda^*}} = \frac{\nu_n - \lambda}{\sqrt{\lambda}} + \eta_n, \tag{47}$$

where $\eta_n = \frac{\nu_n - \lambda}{\sqrt{\lambda}} \left(O\left(\frac{\varepsilon(n)}{\lambda}\right) + O(r(n)) \right) - \frac{\lambda r(n) - \varepsilon(n)(1+r(n))}{\sqrt{\lambda^*}}$, $[\lambda] = \lambda - \varepsilon(n)$, $0 \le \varepsilon(n) < 1$.
The random variable η_n tends in probability to zero as $n \to \infty$. Indeed, for an arbitrary $\varepsilon > 0$

$$P\{|\eta_n| > \varepsilon\} \le \frac{1}{\varepsilon} M |\eta_n| \le \frac{1}{\varepsilon} \left(\left| O\left(\frac{1}{\sqrt{\lambda}}\right) \right| + \left| O\left(\sqrt{\lambda} r(n)\right) \right| \right) \qquad (48)$$

and, by virtue of (3), (8), and (45), the right-hand side of (48) tends to zero as n increases, i.e.

$$P\{|\eta_n| > \varepsilon\} \to 0, \quad n \to \infty. \qquad (49)$$

Relations (47), (49), and theorem ([5], p.157) prove that distributions of the random variables $\frac{\nu_n - \lambda^*}{\sqrt{\lambda^*}}$ and $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$ coincide as $n \to \infty$. Similarly we can verify that distributions of $\frac{Y - \lambda^*}{\sqrt{\lambda^*}}$ and $\frac{Y - [\lambda]}{\sqrt{[\lambda]}}$ are the same as $n \to \infty$.

Thus, relation (46) can be writen as

$$\max_{-\sqrt{\lambda^*} \le l \le \omega\sqrt{\lambda^*}} \left| P\left\{ \frac{\nu_n - \lambda}{\sqrt{\lambda}} \ge l \right\} - P\left\{ \frac{Y - [\lambda]}{\sqrt{[\lambda]}} \ge l \right\} \right| \to 0, \quad n \to \infty. \qquad (50)$$

Finally we notice that the random variable $\frac{Y - [\lambda]}{\sqrt{[\lambda]}}$ has the standard normal distribution as $\lambda \to \infty$. The theorem is proved.

Bibliography

1. Zubkov A.M., Sevastianov B.A., Chistyakov V.P., *The collection of problems in probability theory,* Moscow, Nauka,(1989). (in Russian)
2. Zubkov A.M., *Inequalities for transitions with prohibitions ,* The mathematical collection, (1979), v.109 (151), no.4 (11), 491–532. (in Russian)
3. Masol V.I., *Moments of the number of solutions of system of random Boolean equations,* Random Oper. and Stoch. Equations, (1993), vol. 1, no. 2, 171–179.
4. Masol V.I., Slobodyan S.Y., *On the convergence to the normal limit distribution of the number of false solutions of a system of nonlinear random Boolean equations*, PT&MS, (2007), (Submitted). (in Ukrainian)
5. Chistyakov V.P., *Course of probability theory,* Moscow, Nauka, (2003). (in Russian)

Department of Probability Theory and Mathematical Statistics, Kyiv National Taras Shevchenko University, Kyiv, Ukraine.
E-mail address: vimasol@ukr.net

Department of Probability Theory and Mathematical Statistics, Kyiv National Taras Shevchenko University, Kyiv, Ukraine.
E-mail address: sv_yaros@rambler.ru