Theory of Stochastic Processes
Vol.13 (29), no.1-2, 2007, pp.132-143

VOLODYMYR MASOL AND MYKOLA SLOBODIAN

ESTIMATION OF THE RATE OF CONVERGENCE TO THE LIMIT DISTRIBUTION OF THE NUMBER OF FALSE SOLUTIONS OF A SYSTEM OF NONLINEAR RANDOM BOOLEAN EQUATIONS THAT HAS A LINEAR PART

The theorem on a estimation of the rate of convergence ($n \to \infty$) to the Poisson distribution of the number of false solutions of a beforehand consistent system of nonlinear random equations, that has a linear part, over the field GF(2) is proved.

1. Introduction

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

$$\sum_{k=1}^{g_i(n)} \sum_{1\le j_1<\cdots<j_k\le n} a^{(i)}_{j_1\cdots j_k} x_{j_1}\cdots x_{j_k} = b_i, \quad i = 1, 2, \ldots, N, \tag{1}$$

that satisfies 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 $P\{a^{(i)}_{j_1\ldots j_k} = 1\} = p_{ik}$ and value 0 with probability $P\{a^{(i)}_{j_1\ldots j_k} = 0\} = 1 - p_{ik}$;

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

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

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 $\overline{x}^0$. We are interested in estimation of the rate of convergence to the limit distribution

2000 *Mathematics Subject Classifications.* Primary 60C05, 15A52, 15A03.
Key words and phrases. System of nonlinear random Boolean equations, field GF(2), rate of convergence.

of random variable $\nu_n, n \to \infty$. Such an estimation was considered in [2] under condition that there are no linear terms in each equation of the system (1) with probability 1. Besides, the essential in [2] was the condition $\rho(n) = \rho n, 0 < \rho < 1$.

Theorem. *Assume that the following conditions hold: (A);*

$$n - N = m,\ m = const,\ -\infty < m < \infty; \tag{2}$$

$$0 \le \delta_{i1}(n)\ \le\ p_{i1} \le\ 1 - \delta_{i1}(n),\ \ i = \overline{1,\ N}; \tag{3}$$

there exists a function $\varphi(n)$ such that for any ε_0, $\varepsilon_0 \in (0;1)$, there exists $n_0 = n_0(\varepsilon_0)$, $n_0 \in N$, such that for any $n \ge n_0$ there exists ε, $\varepsilon \in (0,1)$

$$\sum_{i=1}^{N} \exp\{-\varepsilon\varphi(n)\delta_{i1}(n)\} \le \varepsilon_0; \tag{4}$$

for any $i = 1, 2, ..., N$ there exists a set $T_i \ne \emptyset$ such that for all sufficiently large values n

$$T_i\ \subseteq\ \{2,\ \ldots,\ g_i(n)\},\ 0 \le \delta_{it}(n)\ \le\ p_{it} \le\ 1 - \delta_{it}(n), \qquad t \in T_i; \tag{5}$$

for any ε_1, $\varepsilon_1 \in (0;1)$ and any integer $k \ge 0$ there exists $n_1 = n_1(\varepsilon_1, k)$, $n_1 \in N$ such that for any $n \ge n_1$

$$2^{\beta}\, B(n) < \varepsilon_1, \tag{6}$$

where $B(n) = \sum\limits_{i=1}^{N} \exp\{-2 \sum\limits_{t\in T_i} \delta_{it}(n) C^t_{f(n)}\}$, $\beta = \left[\frac{\log_2 \mu(n)}{3}\right]$, $\mu(n) = \frac{n}{\varphi(n)\ln n}$, $\mu(n) \ge 2^{3k}$, $f(n)$ takes integer positive values, $f(n) = o(\varphi(n))$, $n \to \infty$, $[\cdot]$ is a sign of integer part.

Then for fixed $k = 0,\ 1,\ 2,\ \ldots$

$$\left| P\{\nu_n = k\} - \frac{\lambda^k}{k!} e^{-\lambda} \right| \le \left(\frac{2e\lambda}{\beta}\right)^{\beta} \Big[2 + 2^{\beta+1}\, B(n) +$$

$$+\Theta_2 \left(1 + 2^{\beta+1}\, B(n)\right) + 6\,\Theta_1\Big] + \left(\tfrac{2e\lambda}{k}\right)^k \beta e^{2\lambda} B(n) +$$

$$+ \left(\frac{e\lambda}{k}\right)^k \beta e^{\lambda} \left[\Theta_2 \left(1 + 2^{\beta+1}\, B(n)\right) + 6\,\Theta_1\right], \tag{7}$$

where $\lambda = 2^m$, $\delta_i = \min\left\{\delta_{i1}(n),\ \frac{2\ln n}{\sqrt{\varepsilon\varphi(n)}}\right\}$,

$$\Theta_1 = \exp\left\{-2^{-2\beta}\sum_{i=1}^{N} \delta_i + 2^{\beta} + \beta + \ln n - m\ln 2\right\},$$

$$\Theta_2 = 2^{-n} \exp\left\{\varepsilon 2^{\beta}\varphi(n) \left(\beta + \ln\left(\tfrac{ne}{\varepsilon 2^{\beta}\varphi(n)}\right)\right) + 2^{\beta} + 2\ln(\varepsilon 2^{\beta}\varphi(n))\right\}.$$

3. Auxiliary statements

Let $x^1, ..., x^k$ be n-dimensional Boolean vectors which are all distinct and do not coincide with x^0, $x^\nu = (x_1^\nu, ..., x_n^\nu)$, $\nu = \overline{0, k}$, $1 \le k < \infty$. Let $i_{\{u_1,...,u_s\}}$ ($j_{\{u_1,...,u_s\}}$) denote the number of units (zeros) standing at those and only those positions of all vectors $x^{u_1}, ..., x^{u_s}$, where all vectors $x^{u_{s+1}}, ..., x^{u_k}, x^0$ have zeros (units), $u_\nu \in \{1, ..., k\}$, $u_{s+1}, ..., u_k \in \{1, ..., k\} \backslash \{u_1, ..., u_s\}$. See details [1].

Denote by $M\nu_n^{[k]}$ k-th factorial moments of a random variable ν_n; let $M\nu_n^{[0]} \equiv 1$.

Statement. ([1]) *Under condition (A) for* $k \ge 1$

$$M\nu_n^{[k]} = 2^{-kN} S(n,\ k;\ Q), \tag{8}$$

where

$$S(n,\ k;\ Q) = \sum_{s=0}^{n-\rho(n)} \sum (n-\rho(n))! \left((n-\rho(n)-s)! \prod_{i \in I} i! \right)^{-1} \times$$

$$\sum_{s'=0}^{\rho(n)} {\sum}' \rho(n)! \left((\rho(n)-s')! \prod_{j \in J} j! \right)^{-1} Q,\ \ s+s' \ge 1 \tag{9}$$

$$Q = \prod_{i=1}^{N} \left(1 + \sum_{\nu=1}^{k} \sum_{1 \le u_1 < \cdots < u_\nu \le k} \prod_{t=1}^{g_i(n)} (1-2p_{it})^{\Gamma_{t,k}^{\{u_1,\ ...,\ u_\nu\}}} \right); \tag{10}$$

summation $\sum$ $\left({\sum}'\right)$ *is taken over all* $i \in I$ $(j \in J)$, *where* $I = \{i_{\{u_1,...,u_\nu\}} : 1 \le u_1 < \cdots < u_\nu \le k,\ \nu = 1, ..., k\}$ $(J = \{j_{\{u_1,...,u_\nu\}} : 1 \le u_1 < \cdots < u_\nu \le k,\ \nu = 1, ..., k\})$ *such that*

$$\sum_{i \in I} i = s \quad \left(\sum_{j \in J} j = s' \right);$$

numbers i $(i \in I)$, j $(j \in J)$ *in (9) satisfy the following relations*

$$\sum_{i \in I_{\{u\}}, j \in J_{\{u\}}} (i+j) \ge 1, \quad u = 1,\ ...\ ,\ k,$$

$$\sum_{l=0}^{k-2} \sum_{1 \le \mu_1 < ... < \mu_l \le k} \left(i_{\{u_1,\mu_1,...,\mu_l\}} + j_{\{u_1,\mu_1,...,\mu_l\}} + i_{\{u_2,\mu_1,...,\mu_l\}} + j_{\{u_2,\mu_1,...,\mu_l\}} \right) \ge 1,$$

$$1 \le u_1 < u_2 \le k\,;$$

for $1 \le u_1 < ... < u_\nu \le k$, $\nu \in \{1, ..., k\}$, *and* $t \in \{1, ..., n\}$ *the inequality*

$$\Gamma_{t,k}^{\{u_1,...,u_\nu\}} \ge \sum_{(i,j) \in T} \left(C_i^t + C_j^t \right) \tag{11}$$

holds, where $T = I_{\{u_1,...,u_\nu\}} \times J_{\{u_1,...,u_\nu\}}$.
Here

$$I_{\{u_r,...,u_\nu\}} = \left\{ i_{\left\{\sigma_1,...,\sigma_\psi,\, \mu_1,...,\mu_l\right\}} : A\,(\psi,\, l,\, k) \right\},$$

$$J_{\{u_r,...,u_\nu\}} = \left\{ j_{\left\{\sigma_1,...,\sigma_\psi,\, \mu_1,...,\mu_l\right\}} : A\,(\psi,\, l,\, k) \right\},$$

where $A\,(\psi,\, l,\, k)$ *denotes the following constraint set:* $1 \le \sigma_1 < ... < \sigma_\psi \le k,\ \sigma_z \in \{u_1, ..., u_\nu\},\ z = 1, ..., \psi,\ \psi = 1, ..., \nu,\ \psi \equiv 1\,(\mathrm{mod} 2),\ 1 \le \mu_1 < ... < \mu_l \le k,\ \mu_1, ..., \mu_l \notin \{u_1, ..., u_\nu\},\ l = 0, ..., k - \nu.$

The explicit form of $\Gamma_{t,\,k}^{\{u_1,...,u_\nu\}}$ for $1 \le u_1 < ... < u_\nu \le k,\ \ \nu \in \{1, ..., k\}$, $t = 1,\, 2,\, ..., g_i\,(n),\ i = 1, ..., N$ is given in [1].

We use statement 1 and divide the expression (8) into finite number of addends:

$$M\nu_n^{[k]} = 2^{-kN} \sum_{\Delta \ge 0} S^{(\Delta)}(n, k; Q), \tag{12}$$

where $S^{(\Delta)}(n,\, k;\, Q)$ differs from $S(n,\, k;\, Q)$ by all i and j $\quad (i \in I,\ j \in J)$ involved in the expression $S(n,\, k;\, Q)$ according to (9), but accept values such that there exist exactly Δ distinct collections $\omega_\alpha = \{u_1^{(\alpha)},\, \dots,\, u_{\xi_\alpha}^{(\alpha)}\}$ $1 \le u_1^{(\alpha)} < \cdots < u_{\xi_\alpha}^{(\alpha)} \le k,\ \ \xi_\alpha \in \{1,\ ...,\ k\},\ \ \alpha = 1,\ ...,\ \Delta$, such that for each of them there is a $t^{(\alpha)} \in \{2,\ ...,\ r\}$, satisfying the inequality

$$\Gamma_{t^{(\alpha)},\,k}^{\omega_\alpha} < C_r^{t^{(\alpha)}}, \tag{13}$$

and for all collections $\{\upsilon_1, ..., \upsilon_\gamma\},\ 1 \le \upsilon_1 < \cdots < \upsilon_\gamma \le k,\ \gamma = 1, ..., k$, that satisfy $\{\upsilon_1,\ ..., \upsilon_\gamma\} \ne \omega_\alpha,\ \alpha = 1, \dots,\ \Delta$ the estimate

$$\Gamma_{t,\,k}^{\{\upsilon_1,\,\dots\,,\,\upsilon_\gamma\}} \ge C_r^t \tag{14}$$

holds for all $t \in \{2,\, \dots,\, r\}$, where

$$r = [\varepsilon\varphi(n)].$$

To prove the theorem, we use the following lemma.
Lemma 1. *If conditions (2), (5) and (6) hold, then*

$$S_1 = \lambda^k + \theta(k,\, n), \tag{15}$$

where

$$S_1 = 2^{-kN} S^{(0)}(n,\, k;\, Q),$$

$$|\theta(k,\, n)| \le 2^{k+1}u(k) + 2^{mk}\Theta_2 \left(1 + 2^{-mk+k+1}u(k)\right),$$

$$u(k) = 2^{mk} \sum_{i=1}^{N} \exp\left\{-2 \sum_{t \in T_i} \delta_{it}(n) C_r^t\right\},$$

$$0 \leq k \leq \beta. \tag{16}$$

The proof is similar to the proof of Lemma 1 in [2], provided $\Delta = 0$.

Further we will prove that for $\Delta \geq 1$ the following statement takes place:
Lemma 2. *Under conditions of the theorem, for such $k, k \in Z_+ \cup \{0\}$, that satisfy formula (16), and for all sufficiently large values of n*

$$p_1 \leq 6\left(2^{2^k}\right) 2^{(m+1)k-m} \exp\left\{-2^{-2k}\sum_{i=1}^{N}\delta_i + \ln n\right\}, \tag{17}$$

where $p_1 = 2^{-kN}\sum\limits_{\Delta=1}^{2^k-1} S^{(\Delta)}(n,\, k;\, Q)$.

Proof. Denote by M_1 $\left(\tilde{M}_1\right)$ the set of all i, $i \in I$ (j, $j \in J$) that does not belong to I_{ω_α} (J_{ω_α}), $\alpha = 1, ..., \Delta$; and by $M_2 = I \backslash M_1$, $\tilde{M}_2 = J \backslash \tilde{M}_1$. Let R_1 $\left(\tilde{R}_1\right)$ be the cardinal number of M_1 $\left(\tilde{M}_1\right)$. Let z be the smallest integer such that

$$\Delta \leq 2^z - 1, \;\; 1 \leq z \leq k. \tag{18}$$

According to Statement 2.1 in [1] we obtain:

$$R_1 \leq 2^{k-z} - 1; \qquad \tilde{R}_1 \leq 2^{k-z} - 1. \tag{19}$$

If

$$\Gamma_{t,\,k}^{\{u_1,\,...\,,\,u_\nu\}} < C_r^t, \tag{20}$$

for some collection $\{u_1,\, ...,\, u_\nu\}$, $1 \leq u_1 < \cdots < u_\nu \leq k$, $\nu = 1, ..., k$, and some $t \in \{2,\, \dots,\, r\}$, then from (11) we get

$$0 \leq i < r, \quad i \in I_{\{u_1,\,\dots\,,\,u_\nu\}}; \quad 0 \leq j < r, \quad j \in J_{\{u_1,\,\dots\,,\,u_\nu\}}. \tag{21}$$

Further, it follows from (13), (20) and (21) that the inequalities

$$0 \leq i < r \qquad (0 \leq j < r) \tag{22}$$

hold for all $i \in M_2$ $\left(j \in \tilde{M}_2\right)$. Using (3) at $i = \overline{1,\,N}$ and $\alpha = \overline{1,\,\Delta}$ we obtain

$$\left|\prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma_{t,k}^{\omega_\alpha}}\right| \leq (1 - 2\delta_{i1}(n))^{\Gamma_{1,k}^{\omega_\alpha}}. \tag{23}$$

Let restriction G_1 hold: there exist $i \in M_2$ and (or) $j \in \tilde{M}_2$ such that $i \in \left(\frac{r}{E_n},\; r\right]$ and (or) $j \in \left(\frac{r}{E_n},\; r\right]$ where

$$E_n > 3, \quad E_n = o(\ln n), \;\; n \to \infty.$$

Put

$$p_2 = p_1 - S_2, \tag{24}$$

where

$$S_2 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_1)}(n, k;\, Q),$$

$S^{(\Delta)}_{(G_1)}(n, k;\, Q)$ differs from $S^{(\Delta)}(n,\, k;\, Q)$ in such a way that summation over parameter s' in (9) is restricted by G_1.

Let G_1 hold. Using (11) for the some $\alpha,\ \alpha = 1, \ldots, \Delta$, we get

$$\Gamma^{\omega_\alpha}_{1,\,k} \geq \frac{r}{E_n}. \tag{25}$$

Taking into account (23) and (25), we find the estimate

$$\left| \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma^{\omega_\alpha}_{t,\,k}} \right| \leq \exp\left\{ -2\delta_{i1}(n) \frac{r}{E_n} \right\},$$

for $i,\, i = 1, \ldots, N$ and some $\alpha \in \{1, \ldots, \Delta\}$. Now using (18) we obtain

$$Q \leq 2^{zN} \exp\left\{ -2^{-z} \left(N - \sum_{i=1}^{N} \exp\left\{ -2\delta_{i1}(n) \frac{r}{E_n} \right\} \right) \right\}. \tag{26}$$

Thus, using Gelder inequality and relation (4), we estimate Q as

$$Q \leq \hat{Q}, \tag{27}$$

where $\hat{Q} = 2^{zN} \exp\left\{ -2^{-z} \left(N - N^{1-A_n} \right) \right\}$, $A_n = \frac{2\varepsilon}{E_n}$.

Taking into account restriction G_1, relations (19) and (22) we find

$$S_2 \leq 2^{-kN} \sum_{z=1}^{k} \sum_{\Delta=2^{z-1}}^{2^z-1} \sum_{1 \leq \zeta_1 < \ldots < \zeta_d \leq 2^k - 1} \times$$

$$\times \sum_{s=0}^{n-\rho n} C^{s}_{n-\rho(n)} \sum_{s_1+s_2=s} C^{s_1}_{s} \left(\sum_{\sum\limits_{i \in M_2} i = s_1} \frac{s_1!}{\prod\limits_{i \in M_2} i\,!} \right) \left(\sum_{\sum\limits_{i \in M_1} i = s_2} \frac{s_2!}{\prod\limits_{i \in M_1} i\,!} \right) \times$$

$$\times \sum_{s'=0}^{\rho(n)} C^{s'}_{\rho(n)} \sum_{s'_1+s'_2=s'} C^{s'_1}_{s'} \left(\sum_{\sum\limits_{j \in \tilde{M}_2} j = s'_1} \frac{s'_1!}{\prod\limits_{j \in \tilde{M}_2} j\,!} \right) \left(\sum_{\sum\limits_{j \in \tilde{M}_1} j = s'_2} \frac{s'_2!}{\prod\limits_{j \in \tilde{M}_1} j\,!} \right) \hat{Q}. \tag{28}$$

It follows from (27) and (28) that

$$S_2 \leq \frac{2^{2^k} 2^{mk}}{2^m} \exp\left\{ -2^{-k} N \left(1 - N^{-A_n} \right) + 2^k \varepsilon \varphi(n) \ln\left(\frac{ne}{2^k \varepsilon \varphi(n)} \right) \right\}. \tag{29}$$

Let restriction G_2 hold: there exist $i \in M_2$ and (or) $j \in \tilde{M}_2$ such that $i \in \left(\frac{r}{\ln n},\ \frac{r}{E_n}\right]$ and (or) $j \in \left(\frac{r}{\ln n},\ \frac{r}{E_n}\right]$.

Let us consider sum p_3. Put

$$p_3 = p_2 - S_3, \tag{30}$$

where

$$S_3 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_2)}(n, k;\, Q).$$

Here $S^{(\Delta)}_{(G_2)}(n, k;\, Q)$ differs from $S^{(\Delta)}(n, k;\, Q)$ in such a way that summation in (9) is restricted by G_2.

If G_2 hold, then similarly to (27) (we just replace A_n by $\tilde{A}_n = \frac{2\varepsilon}{\ln n}$) we obtain

$$Q \le 2^{zN} \exp\left\{-2^{-k}\left(1 - e^{-2\varepsilon}\right) N\right\}. \tag{31}$$

Using G_2 and relation (19), we find an estimate S_3 (similarly to S_2):

$$S_3 \le \frac{2^{2^k} 2^{mk}}{2^m} \exp\left\{-2^{-k}\left(1 - e^{-2\varepsilon}\right) N + \frac{2^k \varepsilon \varphi(n)}{E_n} \ln\left(\frac{neE_n}{2^k \varepsilon \varphi(n)}\right)\right\}. \tag{32}$$

Let restriction G_3 hold: for all $i \in M_2$ and $j \in \tilde{M}_2$

$$0 \le i \le \frac{r}{\ln n}, \qquad 0 \le j \le \frac{r}{\ln n}. \tag{33}$$

Let us consider sum p_4. Put

$$p_4 = p_3 - S_4, \tag{34}$$

where

$$S_4 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_3, 2^z-2)}(n, k;\, Q).$$

In (34), $S^{(\Delta)}_{(G_3, 2^z-2)}(n, k;\, Q)$ differs from $S^{(\Delta)}(n, k;\, Q)$ in such a way that summation in (9) is restricted by G_3 and $\Delta < 2^z - 1$.

Using (11) we obtain

$$\Gamma^{\omega_\alpha}_{1,\,k} \ge \left(s^{(\alpha)} + \tilde{s}^{(\alpha)}\right) \tag{35}$$

for all $\alpha = 1, \ldots, \Delta$, where $s^{(\alpha)} = \sum\limits_{i \in I_{\omega_\alpha}} i$, $\tilde{s}^{(\alpha)} = \sum\limits_{j \in J_{\omega_\alpha}} j$.

Taking into account (23) and (35) for $i = 1, \ldots, N$ and $\alpha = 1, \ldots, \Delta$,

$$\left|\prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma^{\omega_\alpha}_{t,\,k}}\right| \le \exp\left\{-\frac{2\delta_i}{2^k}\left(s^{(\alpha)} + \tilde{s}^{(\alpha)}\right)\right\}.$$

Using equality $e^{-y} \le 1 - \frac{y}{2}$, $0 \le y < 1$, for $i = 1, \dots, N$, $\alpha = 1, \dots, \Delta$, we get

$$\left| \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma^{\omega\alpha}_{t,k}} \right| \le 1 - \frac{\delta_i}{2^k}(s^{(\alpha)} + \tilde{s}^{(\alpha)}). \qquad (36)$$

Taking into account (5), (6), (14) and (36) we obtain

$$2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_3)}(n, k; Q) \le 2^{-kN} 2^{2^k} \sum_{s=0}^{n-\rho(n)} C^s_{n-\rho(n)} \sum_{s_*=0}^{s} R_1^{s-s_*} \times$$
$$\left(\sum_{\sum_{i\in M_2} i = s_*} \frac{s!}{(s-s_*)!} \left(\prod_{i \in M_2} i! \right)^{-1} \right) \times$$
$$\sum_{s'=0}^{\rho(n)} C^{s'}_{\rho(n)} \sum_{\tilde{s}_*=0}^{s'} \tilde{R}_1^{s'-\tilde{s}_*} \left(\sum_{\sum_{i\in \tilde{M}_2} i = \tilde{s}_*} \frac{s!}{(s'-\tilde{s}_*)!} \left(\prod_{j \in \tilde{M}_2} j! \right)^{-1} \right) \times$$
$$\times \exp\left\{ -2^{-z} \sum_{i=1}^{N} \frac{\delta_i}{2^k} \sum_{\alpha=1}^{\Delta} (s^{(\alpha)} + \tilde{s}^{(\alpha)}) + 2^{k-mk} u(k) \right\}, \quad s + s' \ge 1. \qquad (37)$$

Now, taking into consideration (2), we obtain

$$2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_3)}(n, k; Q) \le$$
$$\le 2^{2^k} 2^{mk} 2^{-zn} (\Delta+1)^N \exp\left\{ \frac{k 2^k \varepsilon\varphi(n) \ln 2}{\ln n} + \frac{2^k \varepsilon\varphi(n)}{\ln n} \ln\left(\frac{en \ln n}{2^k \varepsilon\varphi(n)} \right) \right\} \times$$
$$\times \exp\left\{ -2^{-z+1} \sum_{i=1}^{N} \frac{\delta_i}{2^k} \sum_{\alpha=1}^{\Delta} (s^{(\alpha)} + \tilde{s}^{(\alpha)}) + 2^{k-mk} u(k)) \right\}, \quad s + s' \ge 1, \qquad (38)$$

where $S^{(\Delta)}_{(G_3)}(n,k;Q)$ differs from $S^{(\Delta)}(n,k;Q)$ in such a way that summation in (9) is restricted by G_3.

If $\Delta < 2^z - 1$, then it follows from (38) and the inequality $\max\{s_*, \ \tilde{s}_*\} \le \frac{2^k \varepsilon\varphi(n)}{\ln n}$, that

$$S_4 \le \frac{2^{2^k} 2^{mk}}{2^m} \exp\left\{ -2^{-k} N + 2^{k+1} \varepsilon\varphi(n) \right\}. \qquad (39)$$

Let $\Delta = 2^z - 1$. Then we can put

$$p_5 = p_4 - S_5, \qquad (40)$$

where

$$S_5 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_3, 2^z-1)}(n, k; Q).$$

Here, $S^{(\Delta)}_{(G_3,2^z-1)}(n,k;\,Q)$ differs from $S^{(\Delta)}(n,k;\,Q)$ in such a way that summation in (9) is restricted by G_3 and condition $\Delta = 2^z - 1$. Using (2), (6), (19), the inequality

$$\sum_{\alpha=1}^{\Delta} \left(s^{(\alpha)} + \tilde{s}^{(\alpha)}\right) \geq s_* + \tilde{s}_*, \tag{41}$$

where

$$s_* = \sum_{i\in M_2} i, \quad \tilde{s}_* = \sum_{j\in \tilde{M}_2} j,$$

and relation (37) it is easy to verify that

$$S_5 \leq \frac{2^{2^k} 2^{(m+1)k}}{2^m} \exp\left\{-2^{-2k}\sum_{i=1}^{N}\delta_i + \ln n\right\}, \tag{42}$$

provided

$$s_* + \tilde{s}_* \geq 1. \tag{43}$$

Now, let us check that if $\Delta = 2^z - 1$, $1 \leq z \leq k$, and $z \in \{k, k-1\}$ or $k \in \{1, 2\}$, then there exists some α, $\alpha \in \{1, 2, ..., \Delta\}$, such that $\xi_\alpha \leq 2$. Indeed, when $z = k$ or $k \in \{1, 2\}$, the existence of the mentioned parameter α is obvious. For $z = k - 1$ the existence of the parameter α such that $\xi_\alpha \leq 2$, follows from Remark 2 in [1, p.1217].

Let restrictions G_4 hold:

$$s_* + \tilde{s}_* = 0, \tag{44}$$

$$\xi_\alpha \geq 3,\ \alpha = 1,\ ...,\ \Delta,\ \ \Delta = 2^z - 1,\ \ 1 \leq z \leq k-2,\ \ 3 \leq k < \infty. \tag{45}$$

We can put

$$p_6 = p_5 - S_6, \tag{46}$$

$$S_6 = 2^{-kN}\sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_4)}(n,k;\,Q),$$

where $S^{(\Delta)}_{(G_4)}(n,k;\,Q)$ differs from $S^{(\Delta)}(n,k;\,Q)$ in such a way that summation in (9) is restricted by G_4.

Let restriction (44), $\Delta = 2^z - 1$, $R_1 < 2^{k-z} - 1$, and $\tilde{R}_1 < 2^{k-z} - 1$ hold. Then using (38), by virtue of (19), we obtain the estimate

$$S_6 \leq (1 + o(1))\, 2^{2^k + zN - kN} \sum_{s=0}^{n-\rho(n)} C^s_{n-\rho(n)} \left|M_1\right|^s \sum_{s'=0,\, s'+s\geq 1}^{\rho(n)} C^{s'}_{\rho(n)} \left|\tilde{M}_1\right|^{s'} \leq$$

$$\leq \frac{2^{2^k+1} 2^{mk}}{2^m}\left(1 - 2^{1-k}\right)^n. \tag{47}$$

It remains to check the relation

$$S_7 \le \frac{2^{2^k} 2^{mk}}{2^m} \exp\left\{-n2^{-k+1} + \varepsilon\varphi(n) \ln\left(\frac{n\, e}{\varepsilon\varphi(n)}\right) + \ln\sqrt{\varphi(n)}\right\}, \qquad (48)$$

where

$$S_7 = p_6 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}_{(G_4, \tilde{R}_1)}(n,\, k;\, Q), \qquad (49)$$

under restrictions G_4 and

$$R_1 = \tilde{R}_1 = 2^{k-z} - 1. \qquad (50)$$

In (49), $S^{(\Delta)}_{(G_4,\tilde{R}_1)}(n,\, k;\, Q)$ differs from $S^{(\Delta)}(n,\, k;\, Q)$ in such a way that summation in (9) is restricted by G_4 and (50).

In analogy to how it was done in [1], we make use of conditions (50) and relations G_4 to verify that there exists an element $j_*,\ j_* \in \tilde{M}_1$, satisfying the inequality $j_* \le r$. Therefore, under the restrictions G_4 and (50) we get

$$S_7 \le 2^{2^k} 2^{(k-z)m} \left(1 - \frac{1}{2^{k-z}}\right)^n \sum_{l=0}^{r} C_n^l.$$

Next, taking into account Stirling formula, we obtain (48).

Analyzing restrictions $(G_i), i = 1, 2, 3, 4$, it is easy to verify that (9) holds for all possible values of parameter s, s', i and j ($i \in I$, $j \in J$), that satisfy (13) for which $\Delta \ge 1$.

Equalities (24), (30), (34), (40), (46) and (49) combined with (29), (32), (39), (42), (47) and (48) prove (17) under the conditions of the theorem.

Lemma 3. *Under conditions of the theorem, for such $k, k \in Z_+ \cup \{0\}$, that satisfy formula (16),*

$$M\nu_n^{[k]} = \lambda^k + \Phi(k,\, n), \qquad (51)$$

where $\Phi(k,\, n) = \theta(k,\, n) + p_1$.

Proof. By virtue of (12), Lemma 1 and Lemma 2 imply, obviously, (51), where

$$|\Phi(k,\, n)| \le 2^{mk} \Big(2^{k(1-m)+1} u(k) + \Theta_2 \left(1 + 2^{-mk+k+1} u(k)\right) +$$

$$+6 \exp\left\{-2^{-2k} \sum_{i=1}^{N} \delta_i + 2^k + k + \ln n - m \ln 2\right\}\Big).$$

3. Proof of the theorem

To prove the theorem, we will consider the following inequality for all integer $q, q \ge 0$,

$$\left| P\{\nu_n = q\} - \frac{\lambda^q}{q!} e^{-\lambda} \right| \le R_1 + R_2 + R_3, \qquad (52)$$

where

$$R_1 = \left| P\{\nu_n = q\} - \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q B_{kn} \right|,$$

$$R_2 = \left| \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q \left[B_{kn} - \frac{\lambda^k}{k!} \right] \right|,$$

$$R_3 = \left| \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q \frac{\lambda^k}{k!} - \frac{\lambda^q}{q!} e^{-\lambda} \right|,$$

B_{kn} is the k-th binomial moment of the random variable ν_n.

Choose n such that for any integer $q \geq 0$

$$\frac{\lambda^{q+2\nu}}{q!(2\nu)!} < \left(\frac{2e\lambda}{\beta} \right)^{\beta}, \tag{53}$$

where $2\nu = \beta - q$.

It follows from the inequality

$$R_3 < \frac{\lambda^{q+2\nu}}{q!(2\nu)!} \tag{54}$$

and (53) that

$$R_3 < \left(\frac{2e\lambda}{\beta} \right)^{\beta}. \tag{55}$$

Taking into account (51) we obtain

$$\left| B_{q+2\nu,\,n} - \frac{\lambda^{q+2\nu}}{(q+2\nu)!} \right| = \frac{|\Phi(q+2\nu,\,n)|}{(q+2\nu)!} \leq$$

$$\leq \frac{2^{(q+2\nu)m}}{(q+2\nu)!} \left(6 \exp\left\{ -2^{-2(q+2\nu)} \sum_{i=1}^{N} \delta_i + 2^{q+2\nu} + q + 2\nu + \ln n - m \ln 2 \right\} \right) +$$

$$+ \frac{2^{(q+2\nu)m}}{(q+2\nu)!} \left(2^{q+2\nu+1} B(n) + \Theta_2 \left(1 + 2^{q+2\nu+1} B(n) \right) \right). \tag{56}$$

Thus

$$\left| B_{q+2\nu,\,n} - \frac{\lambda^{q+2\nu}}{(q+2\nu)!} \right| \leq \frac{2^{m\beta}}{\beta!} \left(6\,\Theta_1 + 2^{\beta+1} B(n) + \Theta_2 \left(1 + 2^{\beta+1} B(n) \right) \right). \tag{57}$$

It follows from Bonferronis inequality [3, p. 68] that

$$0 \leq P\{\nu_n = q\} - \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q B_{kn} \leq C_{q+2\nu}^q B_{q+2\nu,\,n}. \tag{58}$$

Applying (53) and (58) to (57), we obtain

$$B_{q+2\nu,\,n}C^q_{q+2\nu} < \left(\frac{2e\lambda}{\beta}\right)^\beta \left(1+2^{\beta+1}B(n)+6\Theta_1+\Theta_2\left(1+2^{\beta+1}B(n)\right)\right). \tag{59}$$

Hence

$$R_1 < \left(\frac{2e\lambda}{\beta}\right)^\beta \left(1+2^{\beta+1}B(n)+6\Theta_1+\Theta_2\left(1+2^{\beta+1}B(n)\right)\right). \tag{60}$$

Further, taking into account (51), it is easy to check that

$$\sup_{q\le k\le q+2\nu-1} C^q_k \left|B_{kn}-\frac{\lambda^k}{k!}\right| \le$$

$$\left(\frac{2e\lambda}{q}\right)^q e^{2\lambda}B(n)+\left(\frac{e\lambda}{q}\right)^q e^\lambda\left(\Theta_2\left(1+2^{\beta+1}B(n)\right)+6\Theta_1\right). \tag{61}$$

Now, using inequality (61), it is easy to verify that

$$R_2 < \sum_{k=q}^{q+2\nu-1} C^q_k\left|B_{kn}-\frac{\lambda^k}{k!}\right| \le \left(\frac{2e\lambda}{q}\right)^q e^{2\lambda}\beta B(n)+$$

$$+\left(\frac{e\lambda}{q}\right)^q e^\lambda\beta\left(\Theta_2\left(1+2^{\beta+1}B(n)\right)+6\Theta_1\right). \tag{62}$$

Thus, with the help (52), (55), (60), and (62) we obtain (7). The theorem is proved.

Bibliography

1. Masol, V. I., *Limit distribution of the number of solutions of a system of random Boolean equations that has a linear part,* Ukr. math. jour., (1998), v. 50, no. 9, 1214–1226 (in Ukrainian).
2. Masol, V. I., Slobodian, M. V., *Estimation of the rate of convergence to the limit distribution of the number of false solutions of a system of nonlinear random Boolean equations,* PT&MS, (2007), (Submitted) (in Ukrainian).
3. Sachkov, V. N., *Introduction to combinatorial methods in discrete mathematics,* M.: Nauka, (1982) (in Russian).

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

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