Theory of Stochastic Processes
Vol. 12 (28), no. 1–2, 2006, pp. 116–126

UDC 519.21

VOLODYMYR I. MASOL AND SVITLANA Y. SLOBODYAN

THE NORMAL LIMIT DISTRIBUTION OF THE NUMBER OF FALSE SOLUTIONS OF A SYSTEM OF NONLINEAR RANDOM EQUATIONS IN THE FIELD GF(2)

The theorem on a normal limit ($n \to \infty$) distribution of the number of false solutions of a beforehand consistent system of nonlinear random equations in the field GF(2) with independent coefficients is proved. In particular, we assume that each equation has coefficients that take values 0 and 1 with equal probability; the system has a solution where the number of ones equals $[\rho n]$, $\rho = const$, $0 < \rho < 1$.

Statement of the problem. Formulation of the theorem

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

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

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 $P\{a^{(i)}_{j_1 \ldots j_k} = 1\} = p_{ik}$ 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 $\overline{x}^0$, that has $[\rho n]$ $/n - [\rho n]/$ components equal to one /zero/, $\rho = const$, $0 < \rho < 1$ on the left-hand side of 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 system (1) different from the vector $\overline{x}^0$.

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

Theorem. *Let, for an arbitrary i, $i = 1, \ldots, N$, there exist a nonempty set*

$$(2) \qquad T_i \subseteq \{2, 3, \ldots, \varphi(n)\}, \ \ T_i \ne \emptyset,$$

such that

$$(3) \qquad p_{it} = \frac{1}{2} \ \ for \ \ t \in T_i,$$

2000 *AMS Mathematics Subject Classification.* Primary 60C05.

Key words and phrases. The nonlinear random equations in the GF(2), normal limit distribution, number of false solutions.

where the function $\varphi(n)$ takes integer values,

$$2 \le \varphi(n) \le \varepsilon \frac{n^{1-p}}{\ln n}, \tag{4}$$

$$p = const, \ \ 0 < p < 1, \tag{5}$$

$$\varepsilon \ \textit{is a positive number}, \ \ 0 < \varepsilon < \frac{\rho}{2}, \tag{6}$$

and

$$m = [\log_2 (\frac{p}{14} \log_2 n)]. \tag{7}$$

Then

$$\lambda \to \infty, \ \ n \to \infty, \tag{8}$$

where $\lambda = M\nu_n$, and the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$ has asymptotically $(n \to \infty)$ standard normal distribution.

Auxiliary statements

Proposition 1. ([1]) *Let X and Y be random variables that take non-negative integer values, and $\lambda = MX$. If the distributions of the random variables are changed so that*

$$\sup_{1 \le r \le 7\lambda} \left| M(X)_r (M(Y)_r)^{-1} - 1 \right| \frac{e^{2\lambda}}{\sqrt{\lambda}} \to 0 \tag{9}$$

and, for all $r \le 7\lambda$,

$$M(Y)_r \le C\lambda^r \tag{10}$$

with some constant C, then

$$\max_{1 \le r \le 2\lambda} |P\{X \ge t\} - P\{Y \ge t\}| \to 0. \tag{11}$$

Proposition 2. ([2]) *If condition (A) holds, then the expectation of the random variable ν_n equals*

$$M\nu_n = \sum_{i=0}^{n-[\rho n]} C_{n-[\rho n]}^{i} \sum_{j=0}^{[\rho n]} C_{[\rho n]}^{j} \prod_{i=1}^{N} \left(\frac{1}{2} + \frac{1}{2} \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma_t} \right), \tag{12}$$

where $\Gamma_t = C_{i+[\rho n]-j}^{t} + C_{[\rho n]}^{t} - 2C_{[\rho n]-j}^{t}$, $t = 1, ..., g_i(n)$, $i + j \ge 1$.

Proposition 3. ([3]) *If condition (A) holds, then, for integer $r \ge 1$,*

$$M\left(\nu_n\right)_r = 2^{-rN} S(n, r; Q), \tag{13}$$

where

$$\begin{aligned} S(n,r;Q) = & \sum_{s=0}^{n-[\rho n]} \sum (n - [\rho n])! \left((n - [\rho n] - s)! \prod_{i \in I} i! \right)^{-1} \times \\ & \sum_{\substack{s'=0 \\ s'+s \ge 1}}^{[\rho n]} \sum{}' ([\rho n])! \left(([\rho n] - s')! \prod_{j \in J} j! \right)^{-1} Q, \end{aligned} \tag{14}$$

$$Q=\prod_{i=1}^{N}\left(1+\sum_{\nu=1}^{r}\sum_{1\le u_1<\ldots<u_\nu\le r}\prod_{t=1}^{g_i(n)}\left(1-2p_{it}\right)^{\Gamma_{t,r}^{\{u_1,\ldots,u_\nu\}}}\right), \tag{15}$$

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

$$\sum_{i\in I} i=s\qquad\left(\sum_{j\in J} j=s'\right); \tag{16}$$

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

$$\sum_{i\in I_{\{u\}},j\in J_{\{u\}}}(i+j)\ge 1,\ \ u=1,\ldots,r, \tag{17}$$

in equality (14),

$$\sum_{l=0}^{r-2}\sum_{1\le\mu_1<\ldots<\mu_l\le r}\left(i_{\{u_1,\mu_1,\ldots,\mu_l\}}+j_{\{u_1,\mu_1,\ldots,\mu_l\}}+i_{\{u_2,\mu_1,\ldots,\mu_l\}}+j_{\{u_2,\mu_1,\ldots,\mu_l\}}\right)\ge 1, \tag{18}$$
$$1\le u_1<u_2\le r\,;$$

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

$$\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}\ge\sum_{(i,j)\in T}\left(C_i^t+C_j^t\right) \tag{19}$$

holds true, where $T=I_{\{u_1,\ldots,u_\nu\}}\times J_{\{u_1,\ldots,u_\nu\}}$; *and if*

$$[\rho\,n]-s'\ge t, \tag{20}$$

then

$$\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}\ge C_{[\rho\,n]\,-s'}^{t-1}\sum_{(i,j)\in T}(i+j)\,. \tag{21}$$

Here,

$$I_{\{u_r,\ldots,u_\nu\}}=\left\{\,i_{\{\sigma_1,\ldots,\sigma_\psi,\,\mu_1,\ldots,\mu_l\}}:A\,(\psi,\,l,\,r)\right\},$$
$$J_{\{u_r,\ldots,u_\nu\}}=\left\{\,j_{\{\sigma_1,\ldots,\sigma_\psi,\,\mu_1,\ldots,\mu_l\}}:A\,(\psi,\,l,\,r)\right\},$$

where $A\,(\psi,\,l,\,r)$ *is a notation for the following set of restrictions:* $1\le\sigma_1<\ldots<\sigma_\psi\le r$, $\sigma_z\in\{u_1,\ldots,u_\nu\}$, $z=1,\ldots,\psi$, $\psi=1,\ldots,\nu$, $\psi\equiv 1\,(\mathrm{mod}2)$, $1\le\mu_1<\ldots<\mu_l\le r$, $\mu_1,\ldots,\mu_l\notin\{u_1,\ldots,u_\nu\}\,,l=0,\ldots,r-\nu$.

Remark 1. The explicit expression $\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}$ for $1\le u_1<\ldots<u_\nu\le r$, $\nu\in\{1,\ldots,r\}$, $t=1,\,2,\,\ldots,g_i\,(n)$, $i=1,\ldots,N$ is given in [3].

Let W be a set of all nonempty subsets of the set Ω, the potency of which equals $|\Omega|=k$, $1\le k<\infty$. Let us define two subsets W_Δ and I_s of the set W:

$$W_\Delta\subseteq W,\ \ W_\Delta=\{\omega_1,\ldots,\omega_\Delta\}\,,\ \ |W_\Delta|=\Delta\,,\ \ \Delta\ge 1,\ \ \omega_i\ne\omega_j$$

for $i\ne j$, $i,\,j\in\{1,\ldots,\Delta\}$;

$$I_s\subseteq W,\ \ I_s=\{m_1,\ldots,m_s\}\,,\ \ |I_s|=s,\ \ s\ge 0,\ \ m_i\ne m_j$$

for $i\ne j$, $i,\,j\in\{1,\ldots,s\}$.

Proposition 4. ([3]) *Let*

$$|m_i \cap \omega_j| \equiv (\mathrm{mod}2),\ \ i = 1, ..., s,\ \ j = 1, ..., \Delta; \tag{22}$$

$$\Delta \in [2^{r-1}, 2^r - 1]\,,\ \ 1 \le r \le k. \tag{23}$$

Then

$$s \le 2^{k-r} - 1. \tag{24}$$

Proposition 5. ([3]) *Let* $\Omega = \{1, ..., k\}\,,\ \ 3 < k < \infty$. *If conditions* (22),

$$\Delta = 2^r - 1,\ \ s = 2^{k-r} - 1,\ \ 1 \le r \le k - 2; \tag{25}$$

$$|\omega_j| \ge 3,\ \ j = 1, ..., \Delta, \tag{26}$$

hold for the sets W_Δ *and* I_s, *then there exists such a number* α, $\alpha \in \{1, ..., \Delta\}$, *that, for some* m_{i_ν}, $m_{i_\nu} \in I_s$, $\nu = 1, 2, 3$,

$$|\omega_\alpha \cap m_{i_\nu}| = 2,\ \ \nu = 1, 2, 3,\ \ |\omega_\alpha \cap (a \cup b)\,| = 3, \tag{27}$$

where $a \ne b$, $a, b \in \{m_{i_\nu} : \nu = 1, 2, 3\}$.

Remark 2. Condition (26) does not hold for $r = k - 1$ and $s = 1$. This fact follows from the proof of Proposition 5 (see also [3, p.45]).

Proof of the theorem

Let us show that, under the conditions of the theorem, we can use Proposition 1.

Let the random variable Y in the mentioned proposition have the Poisson distribution with parameter 2^m, while the distribution of the random variable X coincides with the distribution of the random variable ν_n.

Provided that condition (3) holds, Proposition 2 implies

$$M\nu_n = 2^m - \frac{1}{2^N}. \tag{28}$$

Next, using relation (28), conditions (5) and (7), it is easy to show that (8) is valid and inequality (10) is fulfilled with $C \ge 2$ for all n, beginning from some n_0, $n \ge n_0$.

Let us proceed to the verification of condition (9).To achieve this, we will use equality (13) written as

$$M\,(\nu_n)_r = \frac{1}{2^{rN}} \sum_{\Delta=0}^{2^r-1} S^{(\Delta)}\,(n, r; Q), \tag{29}$$

where $S^{(\Delta)}\,(n, r; Q)$ differs from $S\,(n, r; Q)$ so that all i and j, $i \in I$, $j \in J$, participating in the notation $S\,(n, r; Q)$ given by (14) take only such values that there exist precisely Δ various sets

$$\begin{gathered}\omega_\alpha = \left\{u_1^{(\alpha)}, ..., u_{\xi_\alpha}^{(\alpha)}\right\},\ \ 1 \le u_1^{(\alpha)} < ... < u_{\xi_\alpha}^{(\alpha)} \le r, \\ \xi_\alpha \in \{1, 2, ..., r\}\,,\ \ \alpha = 1, 2, ..., \Delta,\end{gathered} \tag{30}$$

for each of which a number $t^{(\alpha)} \in \{2, ..., \varphi\,(n)\}$ can be found such that

$$\Gamma^{\omega_\alpha}_{t^{(\alpha)},\, r} = 0, \tag{31}$$

and, for the sets $\{\vartheta_1, ..., \vartheta_\gamma\}\,,\ \ 1 \le \vartheta_1 < ... < \vartheta_\gamma \le r,\ \ \gamma = 1, ..., r$, satisfying the relation

$$\{\vartheta_1, ..., \vartheta_\gamma\} \ne \omega_\alpha,\ \ \alpha = 1, 2, ..., \Delta, \tag{32}$$

the estimate

$$\Gamma_{t,\,r}^{\{\vartheta_1,\ldots,\vartheta_\gamma\}} \geq 1 \tag{33}$$

is valid for all $t \in \{2, ..., \varphi(n)\}$.

Let us show that

$$\sup_{1\leq r\leq 7\lambda} \left| \frac{S^{(0)}(n,\, r;\, Q)}{2^{r\,N} M(Y)_r} - 1 \right| \frac{e^{2\lambda}}{\sqrt{\lambda}} \to 0, \quad n \to \infty. \tag{34}$$

Firstly, we state that the equality $\Delta = 0$ can really be achieved.

Indeed, if the inequality $i \geq \varphi(n)$, $j \geq \varphi(n)$, holds for all i, $i \in I$ and (or) j, $j \in J$, then, by virtue of (19), estimation (33) holds true for all sets $\{\vartheta_1, ..., \vartheta_\gamma\}$, $1 \leq \vartheta_1 < ... < \vartheta_\gamma \leq r$, $\gamma = 1, ..., r$, and $t \in \{2, ..., \varphi(n)\}$; and the inequality $\max(|I|\,\varphi(n), |J|\,\varphi(n)) \leq \min(n - [\rho n], [\rho n])$ holds for $r \leq 7\lambda$.

Thus, the equality $\Delta = 0$ can be really reached.

With $\Delta = 0$, estimate (33) and condition (3) imply

$$Q = 1. \tag{35}$$

Hence, by the polynomial theorem,

$$S^{(0)}(n,\, r;\, Q) = S^{(0)}(n, r;\, 1) = 2^{r\,n} - \sigma_0, \tag{36}$$

where

$$\sigma_0 = 1 + \sum_{q=1}^{2^r-1} S_q^{(0)}(n,\, r;\, 1), \tag{37}$$

$S_q^{(0)}(n,\, r;\, 1)$ differs from $S(n,\, r;\, 1)$ so that the numbers $i \in I$ and $j \in J$ on the right-hand side of (14) are changed so that there exist precisely q expressions of the type $\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}$, for each of which

$$\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}} = 0, \tag{38}$$

where $q = 1, 2, 3, ..., 2^r - 1$.

Let all expressions $\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}$, $1 \leq u_1 < ... < u_\nu \leq r$, $\nu \in \{1, ..., r\}$, be numbered by $1, 2, 3, ..., 2^r - 1$. Then the sum $S_q^{(0)}(n,\, r;\, 1)$ can be written as

$$S_q^{(0)}(n,\, r;\, 1) = \sum_{1\leq\gamma_1<\ldots<\gamma_q\leq 2^r-1} S_{\langle\gamma_1,\ldots,\gamma_q\rangle}^{(0)}(n,\, r;\, 1), \tag{39}$$

$q = 1, 2, 3, ..., 2^r - 1$, where $S_{\langle\gamma_1,\ldots,\gamma_q\rangle}^{(0)}(n,\, r;\, 1)$ differs from $S_q^{(0)}(n,\, r;\, 1)$ so that relation (38) holds only for those expressions $\Gamma_{t,\,r}^{\{u_1,\ldots,u_\nu\}}$ to which the numbers $\gamma_1, \gamma_2, ..., \gamma_q$ correspond. Denote, by $A(\gamma_1, ..., \gamma_q)$ $/B(\gamma_1, ..., \gamma_q)/$, the set of all those $i \in I$ $/j \in J/$ that are used in estimate (19) for all $\gamma_1, \gamma_2, ..., \gamma_q$. By virtue of (38), the number of elements in the set $A(\gamma_1, ..., \gamma_q)$ $/B(\gamma_1, ..., \gamma_q)/$ is not less than 2^{r-1}:

$$|A(\gamma_1, ..., \gamma_q)| \geq 2^{r-1}, \tag{40}$$

$$|B(\gamma_1, ..., \gamma_q)| \geq 2^{r-1}. \tag{41}$$

Now, the sum $S_q^{(0)}\,(n,\, r;\, 1)$ can be given as

$$\begin{aligned} S_q^{(0)}\,(n,\, r;\, 1) = \sum_{1\le\gamma_1<\ldots<\gamma_q\le 2^r-1} \; \sum_{s=0}^{n-[\rho\, n]} C^{s}_{n-[\rho\, n]} \times \\ \times \sum_{s_1+s_2=s} C_s^{s_1} \left\{ \sum\nolimits_1 \frac{s_1\,!}{\prod\limits_{i\in A(\gamma_1,\ldots,\,\gamma_q)} i\,!} \right\} \left(\sum\nolimits_2 \frac{s_2\,!}{\prod\limits_{i\in I\setminus A(\gamma_1,\ldots,\,\gamma_q)} i\,!} \right) \times \\ \times \sum_{s'=0}^{[\rho\, n]} \sum_{s_1'+s_2'=s'} C_{s'}^{s_1'} \left\{ \sum\nolimits_3 \frac{s_1'!}{\prod\limits_{j\in B(\gamma_1,\ldots,\,\gamma_q)} j\,!} \right\} \left(\sum\nolimits_4 \frac{s_2'!}{\prod\limits_{j\in J\setminus B(\gamma_1,\ldots,\,\gamma_q)} j\,!} \right), \end{aligned} \tag{42}$$

where $\sum_1$ is the sum over all $i \in A\,(\gamma_1, ..., \gamma_q)$ such that $\sum i = s_1$, $\sum_2$ is the sum over all $i \in I\backslash A\,(\gamma_1, ..., \gamma_q)$ such that $\sum i = s_2$, $\sum_3$ is the sum over all $j \in B\,(\gamma_1, ..., \gamma_q)$ such that $\sum j = s_1'$, and $\sum_4$ is the sum over all $j \in j\backslash B\,(\gamma_1, ..., \gamma_q)$ such that $\sum j = s_2'$.

Relations (37), (39) – (42), and the polynomial formula allow us to obtain the following estimate for σ_0:

$$\sigma_0 \le 2^{2^r-1} 2^{(r-1)n} \left(\sum_{s_1\ge 0} C^{s_1}_{n-[\rho\, n]} \left(2^{r-1}\right)^{s_1} \right) \left(\sum_{s_1'\ge 0} C^{s_1'}_{[\rho\, n]} \left(2^{r-1}\right)^{s_1'} \right). \tag{43}$$

Since $s_1 \le 2^r \varphi\,(n)$ and $s_1' \le 2^r \varphi\,(n)$, relation (43) can be rewritten in the following way:

$$\sigma_0 \le 2^{2^r-1} 2^{(r-1)n} 2^{r\, 2^{r+1}\varphi\,(n)} \left(\sum_{s_1=0}^{2^r\varphi\,(n)} C^{s_1}_{n-[\rho\, n]} \right) \left(\sum_{s_1'=0}^{2^r\varphi\,(n)} C^{s_1'}_{[\rho\, n]} \right). \tag{44}$$

Next, we can use the fact that, under the conditions of the theorem for $1 \le r \le 7\lambda$,

$$2^{r+1} \varphi\,(n) \le \min\,(n - [\rho n], [\rho n])\,. \tag{45}$$

This allows us to proceed from (44) to the estimate

$$\sigma_0 \le 2^{2^r-1} 2^{(r-1)\,n} 2^{r\;2^{r+1}\varphi\,(n)} \left(2^r \varphi\,(n)\right)^2 C^{2^r\varphi\,(n)}_{n-[\rho\, n]} C^{2^r\varphi\,(n)}_{[\rho\, n]},$$

from whence, with the help of the Stirling's formula, we can obtain

$$\sigma_0 \le 2^{2^r-1} 2^{(r-1)\,n} \frac{2^r \varphi\,(n)}{2\pi} \left(\frac{(n - [\rho\, n])\,[\rho\, n]\, e^2}{\varphi^2\,(n)} \right)^{2^r\varphi\,(n)}. \tag{46}$$

Now it is easy to verify that

$$\sup_{1\le r\le 7\lambda} \frac{\sigma_0}{2^{r\, n}} \frac{e^{2\lambda}}{\sqrt{\lambda}} \to 0 \tag{47}$$

as $n \to \infty$.

Indeed, by virtue of (46), we can find

$$\begin{aligned} \sup_{1\le r\le 7\lambda} \frac{\sigma_0}{2^{r\, n}} \frac{e^{2\lambda}}{\sqrt{\lambda}} \le \frac{1}{4\pi} \exp\big\{ 2^{7\lambda} \ln 2 + 7\lambda \ln 2 + \\ + 2^{7\lambda} \varphi\,(n) \ln \left(\frac{(n - [\rho\, n])\,[\rho\, n]\, e^2}{\varphi^2\,(n)} \right) + \ln \varphi\,(n) + 2\lambda - \frac{1}{2} \ln \lambda - n \ln 2 \Big\}. \end{aligned} \tag{48}$$

Conditions (4), (7) and relation (28) allow us to conclude that

$$0 \le 2^{7\lambda}\varphi\left(n\right) \le \varepsilon \frac{n^{1-\frac{p}{2}}}{\ln n}. \tag{49}$$

In response to (48) and (49), we can apparently obtain (47).
From the relations (36), (47) and equality $M\left(Y\right)_r = 2^{r\,m}$, (34) follows.

By virtue of (29) and (34), in order to complete the checking of condition (9), it is necessary to establish that, for $1 \le r \le 7\lambda$,

$$\frac{1}{2^{r\,N+r\,m}}\left(\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}\left(n,\, r;\, Q\right)\right)\frac{e^{2\lambda}}{\sqrt{\lambda}} \to 0 \tag{50}$$

as $n \to \infty$.

Let us show that the restriction (R_0)

$$[\rho\, n] - \varphi\left(n\right) + 1 \le s' \le [\rho\, n], \tag{51}$$

where s' is the summation parameter introduced in (14), implies (50).

Let $S^{(\Delta)}_{\langle (R_0);\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, 1\right)$ be defined in analogy to $S^{(0)}_{\langle\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, 1\right)$ with the additional condition (R_0). Then, under condition (51), we have

$$\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}\left(n,\, r;\, Q\right) = \sum_{z=1}^{r}\ \sum_{\Delta=2^{z-1}}^{2^z-1}\ \sum_{1\le\gamma_1<\ldots<\gamma_\Delta\le 2^r-1} S^{(\Delta)}_{\langle (R_0);\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, Q\right). \tag{52}$$

Each term on the right-hand side of (52) can be estimated as

$$S^{(\Delta)}_{\langle (R_0);\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, Q\right) \le \left(\Delta+1\right)^N S^{(\Delta)}_{\langle (R_0);\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, 1\right). \tag{53}$$

Denote, by M_1 /$\tilde{M}_1$/, the set of all i, $i \in I$ /j, $j \in J$/, that do not belong to I_{ω_α} /J_{ω_α}/, $\alpha = 1, \dots, \Delta$ and put $M_2 = I\backslash M_1$, $\tilde{M}_2 = J\backslash \tilde{M}_1$.

Let z be the minimal integer number such that

$$\Delta \le 2^z - 1,\ \ 1 \le z \le r. \tag{54}$$

Then by Proposition 4, the number of elements of the set M_1 /$\tilde{M}_1$/ does not exceed

$$|M_1| \le 2^{r-z} - 1,\ \ \left|\tilde{M}_1\right| \le 2^{r-z} - 1. \tag{55}$$

With the help of (55), we find the estimate

$$\begin{aligned} &S^{(\Delta)}_{\langle (R_0);\,\gamma_1,\dots,\gamma_\Delta\rangle}\left(n,\, r;\, 1\right) \le \\ &\le \sum_{s=0}^{n-[\rho\, n]} C^{s}_{n-[\rho\, n]}\left(2^{r-z}-1\right)^{s} \sum_{\substack{s_2=0\\ s_2\le(2^r-1)\varphi\,(n)}}^{s} C^{s_2}_{s}\left(2^r-1\right)^{s_2}\times \\ &\times\left(2^{r-z}-1\right)^{[\rho\, n]} \sum_{s'=[\rho\, n]-\varphi(n)+1}^{[\rho\, n]} C^{s'}_{[\rho\, n]} \sum_{\substack{s_2'=0\\ s_2'\le(2^r-1)\varphi(n)}}^{s'} C^{s_2'}_{s'}\left(2^r-1\right)^{s_2'}, \end{aligned} \tag{56}$$

where $s_2 = \sum\limits_{i\in M_1} i$, $s_2' = \sum\limits_{j\in\tilde{M}_2} j$.

Relations (52) – (54) and (56) provide the inequality

$$\begin{aligned}\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n,\, r;\, Q) \le 2^{2^r+r\,n-m}\left(1-\frac{1}{2^{r-1}}\right)^{[\rho\, n]}(2^r-1)^{2(2^r-1)\varphi\,(n)}\times\\ \times\left(\sum_{s_2=0}^{(2^r-1)\varphi\,(n)} C^{s_2}_{n-[\rho\, n]}\right)\left(\sum_{s_2'=0}^{(2^r-1)\varphi\,(n)} C^{s_2'}_{[\rho\, n]}\right)\sum_{s'=0}^{\varphi\,(n)} C^{s'}_{[\rho\, n]}.\end{aligned} \tag{57}$$

Let us observe that

$$\sum_{s_2=0}^{(2^r-1)\varphi\,(n)} C^{s_2}_{n-[\rho\, n]} \le \left(\frac{(n-[\rho\, n])\, e}{(2^r-1)\,\varphi\,(n)}\right)^{(2^r-1)\varphi\,(n)}\sqrt{(2^r-1)\,\varphi\,(n)}\,, \tag{58}$$

$$\sum_{s_2'=0}^{(2^r-1)\varphi\,(n)} C^{s_2'}_{[\rho\, n]} \le \left(\frac{[\rho\, n]\, e}{(2^r-1)\,\varphi\,(n)}\right)^{(2^r-1)\varphi\,(n)}\sqrt{(2^r-1)\,\varphi\,(n)}\,, \tag{59}$$

$$\sum_{s'=0}^{\varphi\,(n)} C^{s'}_{[\rho\, n]} \le \left(\frac{[\rho\, n]\, e}{\varphi\,(n)}\right)^{\varphi\,(n)}\sqrt{\varphi\,(n)}\,. \tag{60}$$

Using (58) – (60), (7), and (29), we find that when the restriction (R_0) holds for $1 \le r \le 7\lambda$ and all n, beginning from some n_1, $n \ge n_1$,

$$\begin{aligned}\frac{1}{2^{r\,N+r\,m}}\left(\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n,\, r;\, Q)\right)\frac{e^{2\lambda}}{\sqrt{\lambda}} \le 2^{2^{7\,\lambda}-m}\left(1-\frac{1}{2^{7\,\lambda-1}}\right)^{[\rho\, n]}\times\\ \times\left(\frac{(n-[\rho\, n])\,[\rho\, n]\, e^2}{\varphi^2\,(n)}\right)^{(2^{7\,\lambda}-1)\varphi\,(n)}\left(\frac{[\rho\, n]\, e}{\varphi\,(n)}\right)^{\varphi\,(n)}\frac{e^{2\lambda}}{\sqrt{\lambda}}\left(2^{7\lambda}-1\right)(\varphi\,(n))^{3/2}\,.\end{aligned} \tag{61}$$

With the help of relation (61) and conditions (4) and (7), it is easy to verify that (50) follows from (51).

Let now

$$0 \le s' \le [\rho\, n] - \varphi\,(n)\,. \tag{62}$$

Next, we will use the following lemma.

Lemma. *If condition* (62) *and restriction* (R^*),

(R^*): *there exists* $i \in M_2$ *and (or)* $j \in \tilde{M}_2$ *such that*

$$0 \le i \le \varphi\,(n) \;\; \textit{and (or)} \;\; 0 \le j \le \varphi\,(n)\,,$$

hold, then, for an arbitrary Δ, $1 \le \Delta \le 2^r-1$,

$$0 \le S^{(\Delta)}(n,\, r;\, Q) \le C^{\Delta}_{2^r-1} 2^{r\,n-m+r}\left(1-\frac{1}{2^r}\right)^{[\rho\, n]}\left(\frac{n\, e}{\varphi\,(n)}\right)^{2(2^r-1)\varphi(n)}\varphi\,(n)\,. \tag{63}$$

With the help of the lemma, we find that (62) and (R^*) imply the inequality

$$\begin{aligned}\frac{1}{2^{r\,N+r\,m}}\left(\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n,\, r;\, Q)\right)\frac{e^{2\lambda}}{\sqrt{\lambda}} \le \frac{1}{2^{r\,N+r\,m}} 2^{2^r+r\,n-m}\left(1-\frac{1}{2^r}\right)^{[\rho\, n]}\times\\ \times\left(\frac{n\, e}{\varphi\,(n)}\right)^{2(2^r-1)\varphi\,(n)}\sqrt{\varphi\,(n)}\,\frac{e^{2\lambda}}{\sqrt{\lambda}}\,.\end{aligned}$$

Hence, for $1 \le r \le 7\lambda$, we obtain

$$\frac{1}{2^{r\,N+r\,m}}\left(\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}\,(n,\,r;\,Q)\right)\frac{e^{2\lambda}}{\sqrt{\lambda}} \le \exp\left\{2^{7\lambda}\ln 2 - m\ln 2 - \right. \tag{64}$$

$$\left. -\frac{[\rho\,n]}{2^{7\lambda}} + 2\left(2^{7\lambda}-1\right)\varphi\,(n)\ln\frac{n\,e}{\varphi\,(n)} + \frac{1}{2}\ln\varphi\,(n) + 2\lambda - \frac{1}{2}\ln\lambda\right\}.$$

Using (4), (7), and estimate $\lambda \le 2^m$, we find that

$$\frac{2^{14\lambda+1}\varphi\,(n)}{[\rho\,n]}\ln\frac{n\,e}{\varphi\,(n)} \le 2\frac{\varepsilon}{\rho}\left(1+\frac{1}{\ln n}\ln\frac{e}{2}\right) < 1 \tag{65}$$

holds for $0 < \varepsilon < \frac{\rho}{2}$ and $n \to \infty$.

Relations (64) and (65) allow us, apparently, to conclude that (50) holds true under the conditions of the lemma.

The validity of condition (9) follows from relations (29), (34), and (50). Hence, the conditions of Proposition 1 hold. Using Proposition 1, we obtain

$$\max_{1\le r\le 2\lambda}\left|P\left\{\nu_n \ge t\right\} - P\left\{Y \ge t\right\}\right| \underset{n\to\infty}{\to} 0.$$

The statement of the theorem follows now from the last relation and the fact that the random variable $(Y-2^m)\,(2^{m/2})^{-1}$ has the standard normal distribution as $m\to\infty$.

Proof of the lemma. Indeed, for $S^{(\Delta)}\,(n,\,r;\,Q)$, we have the obvious estimate

$$S^{(\Delta)}\,(n,\,r;\,Q) \le \sum_{1\le\gamma_1<\ldots<\gamma_\Delta\le 2^r-1} S^{(\Delta)}_{\langle\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,Q), \tag{66}$$

where $S^{(\Delta)}_{\langle\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,Q)$ is determined in accordance to $S^{(\Delta)}\,(n,\,r;\,Q)$ but with an additional condition, namely that relation (38) holds true only for those expressions $\Gamma^{\{u_1,\ldots,u_\nu\}}_{t,\,r}$, $1 \le u_1 < \ldots < u_\nu \le r$, $\nu \in \{1,\ldots,r\}$, to which the numbers $\gamma_1,\,\gamma_2,\ldots,\,\gamma_\Delta \in \{1,\,2,\,3,\ldots,\,2^r-1\}$ correspond.

Let z be the minimal integer number for which the inequality $\Delta \le 2^z - 1$ is valid. Then, providing that conditions (62), (3) and restrictions (R_1),

(R_1): there exists $i \in M_2$ and (or) $j \in \tilde{M}_2$ such that

$$1 \le i \le \varphi\,(n) \;\; and \;\; (or) \;\; 1 \le j \le \varphi\,(n)\,,$$

hold and taking into account relation (21), it is easy to check that

$$Q \le \left(2^z-1\right)^N. \tag{67}$$

With the help of (66) and (67), we find that (63) and (R_1) prove the correctness of the inequality

$$S^{(\Delta)}\,(n,\,r;\,Q) \le \left(2^z-1\right)^N \sum_{1\le\gamma_1<\ldots<\gamma_\Delta\le 2^r-1} S^{(\Delta)}_{\langle(R\,_1);\,\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,1), \tag{68}$$

where $S^{(\Delta)}_{\langle(R\,_1);\,\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,1)$ differs from $S^{(\Delta)}_{\langle\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,1)$ by the additional condition (R_1). In turn, accordingly to (56), we obtain

$$\left(2^z-1\right)^N S^{(\Delta)}_{\langle(R\,_1);\,\gamma_1,\ldots,\gamma_\Delta\rangle}\,(n,\,r;\,1) \le 2^{r\,n-m}\left(1-\frac{1}{2^r}\right)^N \left(2^r-1\right)^{2(2^r-1)\varphi(n)} \times$$

$$\times \sum_{s_2=0}^{(2^r-1)\varphi(n)} C^{s_2}_{n-[\rho\,n]} \sum_{s_2'=0}^{(2^r-1)\varphi(n)} C^{s_2'}_{[\rho\,n]},$$

or, taking into account (58) and (59),

$$(2^z-1)^N\, S^{(\Delta)}_{\langle (R_1);\,\gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,1) \le 2^{r\,n-m}\left(1-\frac{1}{2^r}\right)^N\left(\frac{n\,e}{\varphi(n)}\right)^{2(2^r-1)\varphi(n)}\times \tag{69}$$
$$\times\,(2^r-1)\,\varphi(n)\,.$$

Since $[\rho\, n] < N = n - m$ for quite large values of n and $\varphi(n) \ge 2$ by virtue of (4), relations (68) and (69) imply inequality (63).

Denote, by (R_2), the restrictions

(R_2): (62); $i = j = 0$ for all $i \in M_2$ and $j \in \tilde{M}_2$.

Let us show that (63) holds under restrictions (R_2).

Indeed, if, for the parameter Δ, the restrictions

$$\Delta < 2^z - 1 \;\; or \;\; \Delta = 2^z - 1 \;\; and \;\; \left|\tilde{M}_1\right| < 2^{r-z} - 1, \tag{70}$$

hold, then (66) implies

$$S^{(\Delta)}(n,\,r;\,Q) \le \sum_{1\le\gamma_1<\ldots<\gamma_\Delta\le 2^r-1} S^{(\Delta)}_{\langle (R_2);\,(70);\,\gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,Q), \tag{71}$$

where $S^{(\Delta)}_{\langle (R_2);\,(70);\,\gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,Q)$ differs from $S^{(\Delta)}_{\langle \gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,Q)$ by the additional conditions (R_2) and (70).

Each term on the right-hand side of (71) can be estimated in the following way:

1) for $\Delta < 2^z - 1$, we have

$$S^{(\Delta)}_{\langle (R_2);\,(70);\,\gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,Q) \le 2^{r\,n-z(n-N)}\left(1-\frac{1}{2^r}\right)^N, \tag{72}$$

2) for $\Delta = 2^z - 1$ and $\left|\tilde{M}_1\right| < 2^{r-z} - 1$, we have

$$S^{(\Delta)}_{\langle (R_2);\,(70);\,\gamma_1,\ldots,\gamma_\Delta\rangle}(n,\,r;\,Q) \le 2^{r\,n-m}\left(1-\frac{1}{2^r}\right)^{[\rho\,n]}, \tag{73}$$

Combining (71) – (73), we come to the conclusion that (63) holds under the restrictions (R_2) and (70).

Denote, by s_* and $\tilde{s}_*$, the sums $s_* = \sum\limits_{i\in M_2} i$ and $\tilde{s}_* = \sum\limits_{j\in\tilde{M}_2} j$. From the conditions (R_2), we obviously have

$$s_* + \tilde{s}_* = 0. \tag{74}$$

Next, let us verify that equality (74) implies that $\xi_\alpha \ge 3$ for all $\alpha \in \{1, 2, ..., \Delta\}$, where ξ_α is the parameter from definition (30). Indeed, inequalities (17) and (18) allow us to conclude that if $\xi_\alpha \le 2$ for some $\alpha \in \{1, 2, ..., \Delta\}$, then $s_* + \tilde{s}_* \ge 1$, which contradicts equality (74).

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

Therefore, it remains to check relation (63) under restrictions (R_3):

$$\xi_\alpha \ge 3, \;\; \alpha \in \{1, 2, 3, ..., \Delta\}\,, \tag{75}$$

$$\Delta = 2^z - 1, \tag{76}$$

$$\left|\tilde{M}_1\right| = 2^{r-z} - 1 \;\; for \;\; 1 \le z \le r-2, \;\; 3 \le r < \infty. \tag{77}$$

In analogy to how it was done in work [3], we make use of Proposition 5 and conditions (75) – (77) to verify that there exists an element $j_*,\;\; j_* \in \tilde{M}_1$, satisfying the inequality $j_* \le \varphi(n)$. This allows us to obtain the estimation

$$S^{(\Delta)}_{\langle (R_3);\, \gamma_1,\ldots,\gamma_\Delta\rangle}(n,\, r;\, Q) \le 2^{r\,n - z\,m} \left(1 - \frac{1}{2^r}\right)^{[\rho\, n]} \left(\frac{[\rho\, n]\, e}{\varphi(n)}\right)^{\varphi(n)} \sqrt{\varphi(n)}. \tag{78}$$

Relation (78) and inequality

$$S^{(\Delta)}(n,\, r;\, Q) \le \sum_{1 \le \gamma_1 < \ldots < \gamma_\Delta \le 2^r - 1} S^{(\Delta)}_{\langle (R_3);\, \gamma_1,\ldots,\gamma_\Delta\rangle}(n,\, r;\, Q)$$

prove (63) under the restrictions (R_3).

Analyzing restrictions $(R_i), i = 1, 2, 3$, it is easy to verify that (63) holds for all possible values of the parameter s and those values of the parameters s', i, and j that satisfy (62) and (R^*), for which $\Delta \ge 1$. The lemma is proved.

Bibliography

1. V.G. Mikhailov, *The limit theorems for the number of nontrivial solutions of a system of random equations in the field GF(2)*, Theory of probability and it's application. **XLIII** (1998), no. 3, 598–606. (in Russian)
2. V.I. Masol, *Moments of the number of solutions of a system of random Boolean equations*, Random Oper. and Stoch. Equations. **1** (1993), no. 2, 171–179.
3. V.I. Masol, *The theorem on the limit distribution of the number of false solutions of a system of nonlinear random Boolean equations*, Theory of probability and it's application. **XLIII** (1998), no. 1, 41–56. (in Russian)

Department of Probability Theory and Mathematical Statistics, Taras Shevchenko Kyiv National University, 6 Academician Glushkov Str., Kyiv 03127, Ukraine.

E-mail: vimasol@ukr.net

Department of Probability Theory and Mathematical Statistics, Taras Shevchenko Kyiv National University, 6 Academician Glushkov Str., Kyiv 03127, Ukraine.

E-mail: sv_yaros@rambler.ru