Slobodian S.Ya.

THE NORMAL LIMIT DISTRIBUTION OF THE NORMALIZED NUMBER OF FALSE SOLUTIONS OF ONE SYSTEM OF NONLINEAR RANDOM EQUATIONS OVER THE FIELD GF(2)

The theorem on a normal limit distribution of the normalized number of false solutions of a beforehand consistent system of nonlinear random equations over the field GF(2) is proved. The results with the additional condition on the number of nonzero components both false solutions and true solution of the solutions are obtained.

Key words and phrases: nonlinear random equation, field GF(2), normal limit distribution.

Vasyl Stefanyk Precarpathian National University, 57 Shevchenka str., 76018, Ivano-Frankivsk, Ukraine

E-mail: slobodian_s@ukr.net

INTRODUCTION

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

$$\sum_{k=1}^{g_q(n)} \sum_{1 \le j_1 < \ldots < j_k \le n} a_{j_1 \ldots j_k}^{(q)} x_{j_1} \ldots x_{j_k} = b_q, \quad q = 1, 2, \ldots, N, \tag{1}$$

that satisfies condition (A).

Condition (A):

1) coefficients $a_{j_1 \ldots j_k}^{(q)}$ $(1 \le j_1 < \ldots < j_k \le n, \ k = 1, \ldots, g_q(n), \ q = 1, 2, \ldots, N)$ are independent random variables, $P\{a_{j_1 \ldots j_k}^{(q)} = 1\} = 1 - P\{a_{j_1 \ldots j_k}^{(q)} = 0\} = p_{qk}$;

2) elements b_q $(q = 1, 2, \ldots, N)$ are the result of the substitution of a fixed n-dimensional (0,1)-vector $\bar{x}^0$, that has $\rho(n)$ components equal to one, $\rho(n) = |\bar{x}^0|$, in the left-hand side of the system (1);

3) the function $g_q(n)$ is nonrandom, $g_q(n) \in \{2, 3, \ldots, n\}, q = 1, 2, \ldots, N$.

Denote by $M(\bar{x}^0, f(n))$ the set of all n-dimensional vectors $\bar{x}$, which do not coincide with $\bar{x}^0$. These vectors have the number $|\bar{x}|$ of nonzero components satisfying inequality $|\bar{x}| \ge f(n)$, $f(n) \in \{0, 1, 2, \ldots, n\}$.

Denote by ν_n the number of all solutions $\bar{x}, \bar{x} \in M(\bar{x}^0, f(n))$ of the system (1) and we shall name their false. Most attention was paid to finding conditions for the convergence of the distribution of the random variable ν_n to a Poisson distribution as $n \to \infty$ in the previously published papers (see review article [2]). We are interested in the conditions under which in appropriate way normalized random variable ν_n has a normal limit $(n \to \infty)$ distribution and $n - \rho(n) \to \infty \ (n \to \infty)$, $f(n) \ge 2$. The case $\rho(n) \to \infty \ (n \to \infty)$ and $f(n) = 0$ is considered in [5]. Put λ is a positive real number such that $[\lambda] = 2^m$, $m = n - N$, $[\cdot]$ is the sign of the integer part.

1   FORMULATION OF THE THEOREM

Theorem. *Let the condition (A) holds, parameters n and N are changed so that*

$$\lambda = \frac{1}{v(1+\alpha+\omega)} \log_2 \frac{n-\rho(n)}{f(n)\ln n},$$

(2)

$$v = v(n) \geq 2, \quad \alpha = \alpha(n), \quad \omega = \omega(n), \quad \alpha > exp\{1 + \alpha^{-1}\},$$

$$\lambda \to \infty,$$

(3)

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

(4)

as $n \to \infty$; for an arbitrary $q, q = 1, 2, \ldots, N$, exist a nonempty set T_q such that for all sufficiently large values of n

$$T_q \subseteq \{2, \ldots, g_q(n)\} \cap \{2, \ldots, \varepsilon f(n)\}, \quad T_q \neq \varnothing, \quad 0 < \varepsilon < 1, \quad \varepsilon = const,$$

(5)

$$\frac{1}{2} - \delta_{qt} \leq p_{qt} \leq \frac{1}{2} + \delta_{qt}, \quad \delta_{qt} = \delta_{qt}(n), \quad t \in T_q, \quad q = 1, \ldots, N,$$

(6)

$$(2 + (1+\alpha+\omega)\ln 2)\lambda - \frac{\ln\lambda}{2} + \ln\left(\sum_{q=1}^{N}\prod_{t\in T_q} 2\delta_{qt}\right) \to -\infty \quad (n \to \infty).$$

(7)

Then the distribution function of the random variable $\frac{v_n - \lambda}{\sqrt{\lambda}}$ tends $(n \to \infty)$ to the standard normal distribution function.

2   AUXILIARY STATEMENTS

Let $M(v_n)_r$ denotes r-factorial moment of a random variable v_n.

Proposition. *If the condition (A) holds, then for integer $r \geq 1$*

$$M(v_n)_r = 2^{-rN} S(n, r; Q),$$

(8)

where

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

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

(9)

$$Q = \prod_{q=1}^{N}\left(1 + \sum_{v=1}^{r}\sum_{1\leq u_1<\cdots<u_v\leq r}\prod_{t=1}^{g_q(n)}(1 - 2p_{qt})^{\Gamma_{t,r}^{\{u_1,\ldots,u_v\}}}\right),$$

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

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

in accordance to (9), the numbers $i \ (i \in I), j \ (j \in J)$ satisfy the relations

$$\sum_{i\in I_{\{u\}}, j\in J_{\{u\}}} (i + j) \geq 1, \quad u = 1, \ldots, r,$$

(10)

$$\sum_{i \in I_{\{u\}}} i + \rho(n) - \sum_{j \in J_{\{u\}}} j \geq f(n), \quad u = 1, \ldots, r, \tag{11}$$

$$\sum_{i \in I_{\{u_1, u_2\}}, j \in J_{\{u_1, u_2\}}} (i + j) \geq 1, \quad 1 \leq u_1 < u_2 \leq r; \tag{12}$$

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

$$\Gamma_{t,r}^{\{u_1, \ldots, u_\nu\}} \geq \sum_{(i,j) \in T} \left(C_i^t + C_j^t \right), \tag{13}$$

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

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

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

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

The proof of the proposition is realized similarly to the proof of the theorem 1 from the work [3], which holds true for $f(n) = 0$.

Lemma 1. *Let conditions* (10) *and* (11) *hold. Then the inequality*

$$\Gamma_{t,r}^{\{u\}} \geq C_{f(n)-1}^{t-1}, \quad u = 1, \ldots, r, \tag{14}$$

holds true.

Proof. Using the equalities (2)–(4) from the work [3], we obtain

$$\Gamma_{t,r}^{\{u\}} = C_{F_u + \Phi_u}^t + C_{\rho(n)}^t - 2C_{\Phi_u}^t, \quad u = 1, \ldots, r, \tag{15}$$

where $F_u = \sum_{i \in I_{\{u\}}} i$, $\Phi_u = \rho(n) - \Phi_u^*$, $\Phi_u^* = \sum_{j \in J_{\{u\}}} j$. By virtue of (10) $F_u + \Phi_u^* \geq 1$. In order to prove of Lemma 1 it is, therefore, sufficiently to find the estimation for $\Gamma_{t,r}^{\{u\}}$ in two cases: $\Phi_u^* \geq 0$ $(F_u \geq 1)$ and $\Phi_u^* \geq 1$ $(F_u \geq 0)$.

Let $\Phi_u^* \geq 0$. Then $F_u \geq 1$ and taking into account (15)

$$\Gamma_{t,k}^{\{u\}} \geq C_{F_u + \rho(n)}^t - C_{\rho(n)}^t \geq C_{1+\rho(n)}^t - C_{\rho(n)}^t \geq C_{f(n)-1}^{t-1}, \quad u = 1, \ldots, r. \tag{16}$$

Here, with the help of (11) and accepted designations, the fact $F_u + \rho(n) - \Phi_u^* \geq f(n)$ has been used.

Let now $\Phi_u^* \geq 1$. Then $F_u \geq 0$ and similarly to (16), we find

$$\Gamma_{t,k}^{\{u\}} \geq C_{\rho(n)}^t - C_{\rho(n)-\Phi_u^*}^t \geq C_{\rho(n)}^t - C_{\rho(n)-1}^t \geq C_{\rho(n)-1}^{t-1} \geq C_{f(n)-1}^{t-1}, \quad u = 1, \ldots, r. \tag{17}$$

Considering estimations (16) and (17), we can obtain (14). Lemma 1 is proved. $\square$

Lemma 2. *Let conditions* (11) *and* (12) *hold. Then the inequality*

$$\Gamma_{t,r}^{\{u_1, u_2\}} \geq C_{f(n)-1}^{t-1}, \quad 1 \leq u_1 < u_2 \leq r,$$

holds.

Proof. Using equalities (2)–(4) from the work [3], we find

$$\Gamma_{t,r}^{\{u_1,u_2\}} = C_{F_{u_1}+\Phi_{u_1}}^t + C_{F_{u_2}+\Phi_{u_2}}^t - 2C_{F_{u_1u_2}+\Phi_{u_1u_2}}^t, \quad 1 \le u_1 < u_2 \le r, \tag{18}$$

where $F_{u_1u_2} = \sum\limits_{l=0}^{r-2} \sum\limits_{\substack{\mu_l \notin \{u_1,u_2\} \\ 1\leqslant\mu_1<\cdots<\mu_l\leqslant r}} i_{\{u_1u_2\mu_1\ldots\mu_l\}}$,

$$\Phi_{u_1,u_2} = \rho(n) - \sum\limits_{l=0}^{r-2} \sum\limits_{\substack{\mu_l \notin \{u_1,u_2\} \\ 1\leqslant\mu_1<\cdots<\mu_l\leqslant r}} \left(j_{\{u_1\mu_1\ldots\mu_l\}} + j_{\{u_2\mu_1\ldots\mu_l\}} \right)$$

$$- \sum\limits_{l=0}^{r-2} \sum\limits_{\substack{\mu_l \notin \{u_1,u_2\} \\ 1\leqslant\mu_1<\cdots<\mu_l\leqslant r}} j_{\{u_1u_2\mu_1\ldots\mu_l\}}, \quad 1 \le u_1 < u_2 \le r.$$

We can write relation (18) in the following way:

$$\Gamma_{t,r}^{\{u_1,u_2\}} = C_{F_{u_1}+\Phi_{u_1}}^t - C_{F_{u_1u_2}+\Phi_{u_1u_2}}^t + C_{F_{u_2}+\Phi_{u_2}}^t - C_{F_{u_1u_2}+\Phi_{u_1u_2}}^t, \quad 1 \le u_1 < u_2 \le r. \tag{19}$$

Using definitions of $F_u, \Phi_u,$ $(u = u_1, u_2)$ and $F_{u_1u_2}, \Phi_{u_1u_2}$, we can present (19) in the following way:

$$\Gamma_{t,r}^{\{u_1,u_2\}} = C_{F_{u_1}+\Phi_{u_1}}^t - C_{F_{u_1}+\Phi_{u_1}-\psi_*}^t + C_{F_{u_2}+\Phi_{u_2}}^t - C_{F_{u_2}+\Phi_{u_2}-\psi^*}^t, \quad 1 \le u_1 < u_2 \le r, \tag{20}$$

where

$$\psi_* = \sum\limits_{l=0}^{r-2} \sum\limits_{\substack{\mu_l \notin \{u_1,u_2\} \\ 1\leqslant\mu_1<\cdots<\mu_l\leqslant r}} \left(i_{\{u_1\mu_1\ldots\mu_l\}} + j_{\{u_2\mu_1\ldots\mu_l\}} \right), \quad \psi^* = \sum\limits_{l=0}^{r-2} \sum\limits_{\substack{\mu_l \notin \{u_1,u_2\} \\ 1\leqslant\mu_1<\cdots<\mu_l\leqslant r}} \left(i_{\{u_2\mu_1\ldots\mu_l\}} + j_{\{u_1\mu_1\ldots\mu_l\}} \right).$$

According to condition (12), the inequality $\psi_* + \psi^* \ge 1$ holds true. Let us find the estimation $\Gamma_{t,r}^{\{u_1,u_2\}}$ when $\psi_* \ge 0$ and $\psi_* \ge 1$.

If relation $\psi_* \ge 0$ holds, then from the equality (20), using lemma 7 from [3] and (11), we can obtain $\Gamma_{t,r}^{\{u_1,u_2\}} \ge C_{F_{u_2}+\Phi_{u_2}}^t - C_{F_{u_2}+\Phi_{u_2}-1}^t \ge C_{F_{u_2}+\rho(n)-\Phi_{u_2}^*-1}^{t-1} \ge C_{f(n)-1}^{t-1}, \quad 1 \le u_1 < u_2 \le r.$ If inequality $\psi_* \ge 1$ satisfies, it is similarly easy to receive an estimation $\Gamma_{t,r}^{\{u_1,u_2\}} \ge C_{F_{u_1}+\Phi_{u_1}}^t - C_{F_{u_1}+\Phi_{u_1}-1}^t \ge C_{F_{u_1}+\rho(n)-\Phi_{u_1}^*-1}^{t-1} \ge C_{f(n)-1}^{t-1}, \quad 1 \le u_1 < u_2 \le r.$ $\square$

3 PROOF OF THE THEOREM

Let us show that under the conditions of the theorem we can use Lemma 2 from the work [5]. 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; and put $\gamma = 1 + \omega$.

Let us check up condition (35) of the mentioned Lemma 2 of the work [5], that is let us show existence of the constant C such, that the estimation $M(Y)_r \le C(\lambda^*)^r$ satisfies for $r \le (\alpha + \gamma)\lambda^*$, where $\lambda^* = M\nu_n$.

Using the equality (8) as $r = 1$, let us evaluate of the expectation of the random variable ν_n. Further we note that conditions (3), (5)–(7) and Lemma 1 (as $r = 1$) provide the relation

$$Q = 1 + O\left(\sum_{q=1}^{N} \prod_{t \in T_q} 2\delta_{qt} \right), \quad n \to \infty. \tag{21}$$

By virtue of relation (21), the expectation of the random variable ν_n can be presented in the following way:

$$M\nu_n = 2^{-N} \sum_{i=0}^{n-\rho(n)} C_{n-\rho(n)}^i \sum C_{\rho(n)}^j Q$$

$$= 2^{-N} \left(1 + O\left(\sum_{q=1}^{N}\prod_{t\in T_q} 2\delta_{qt}\right)\right) \left(\sum_{i=0}^{n-\rho(n)} C_{n-\rho(n)}^i \sum_{j=0}^{\rho(n)} C_{\rho(n)}^j - \sigma_0\right), \quad n \to \infty,$$

(22)

where $\sigma_0 = \sum_{i=0}^{n-\rho(n)} C_{n-\rho(n)}^i \sum_{j=0}^{\rho(n)} C_{\rho(n)}^j$ on the assumption of $i + j \geq 1, i + \rho(n) - j < f(n)$;
the sign $\sum$ denotes the summation over parameter $j, j = 0, \ldots, \rho(n)$, and additional conditions $i + j \geq 1, i + \rho(n) - j \geq f(n)$. It is easy to show that inequality for σ_0

$$\sigma_0 \leq \exp\{o(n)\}, \quad n \to \infty,$$

(23)

satisfies. With the help of (22) and (23) we find

$$M\nu_n = 2^{-N}(2^n - 1 - \exp\{o(n)\}) \left(1 + O\left(\sum_{q=1}^{N}\prod_{t\in T_q} 2\delta_{qt}\right)\right), \quad n \to \infty,$$

(24)

or according to the notations introduced above, we can write

$$\lambda^* = [\lambda](1 + o(1)), \quad n \to \infty.$$

(25)

By virtue of (2), (7) and relations $M(Y)_r = 2^{mr}, m = n - N$, (27), we find that condition (35) of Lemma 2 from the work [5] holds true for $C > 1$.

Let us proceed to verification of condition (38) (Lemma 2, [5]), according to which, the relation

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

satisfies for all $r \leq (\alpha + \gamma)\lambda^*$.
To achieve this, we write equality (8) in the following way:

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

(26)

where $S^{(\Delta)}(n, r; Q)$ differs from $S(n, r; Q)$ so that all i та $j, i \in I, j \in J$, participating in the notation $S(n, r; Q)$ given by (9) take only such values that there exist precisely Δ of various sets

$$\omega_\alpha = \left\{u_1^{(\alpha)}, \ldots, u_{\xi_\alpha}^{(\alpha)}\right\}, \quad 1 \leq u_1^{(\alpha)} < \cdots < u_{\xi_\alpha}^{(\alpha)} \leq r, \quad \xi_\alpha \in \{1, 2, \ldots, r\}, \quad \alpha = 1, 2, \ldots, \Delta,$$

for each of which a number $t^{(\alpha)} \in \{2, \ldots, k\}, k = [\varepsilon f(n)]$ can be found such that

$$\Gamma_{t^{(\alpha)}, r}^{\omega_\alpha} = 0,$$

(27)

and for the sets $\{\vartheta_1, \ldots, \vartheta_q\}, 1 \leq \vartheta_1 < \cdots < \vartheta_q \leq r, q = 1, \ldots, r$, satisfying the relation $\{\vartheta_1, \ldots, \vartheta_q\} \neq \omega_\alpha, \alpha = 1, 2, \ldots, \Delta$, the estimate

$$\Gamma_{t, r}^{\{\vartheta_1, \ldots, \vartheta_q\}} \geq 1$$

(28)

is valid for all $t \in \{2, \ldots, k\}$.

Let us show that

$$\sup_{1 \leq r \leq (\alpha+\gamma)\lambda^*} \left| \frac{S^{(0)}(n, r; Q)}{2^r N M(Y)_r} - 1 \right| \frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0, \quad n \to \infty. \tag{29}$$

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

Indeed, if for all i, $i \in I$, and (or) j, $j \in J$, at least one of two inequalities $i \geq k$ or $j \geq k$, holds, then, by virtue of (13), estimation (28) holds true for all sets $\{\vartheta_1, \ldots, \vartheta_q\}$, $1 \leq \vartheta_1 < \cdots < \vartheta_q \leq r$, $q = 1, \ldots, r$ та $t \in \{2, \ldots, k\}$. In turn, equality $i = k$ and (or) $j = k$ can satisfies for all $i \in I$, and (or) $j \in J$, since, taking into account condition (2) and equality (25), the relation

$$2^r k \leq \max(n - \rho(n), \rho(n)) \tag{30}$$

holds for $r \leq (\alpha + \gamma)\lambda^*$. Thus, the equality $\Delta = 0$ can really be reached.

Let $u = (2^r - 1) \sum_{q=1}^{N} \prod_{t \in T_q} 2\delta_{qt}$. Then for $\Delta = 0$, using inequalities (6), (28) and relation

$$u \to 0, \quad n \to \infty, \tag{31}$$

which follows from (7), product Q can be written as $Q = 1 + \varsigma(n)u + O(u^2)$, $|\varsigma(n)| \leq 1$ as $n \to \infty$. Hence by the polynomial theorem and equality (9)

$$S^{(0)}(n, r; Q) = (2^{rn} - \sigma_1 - \sigma_2)\left(1 + \varsigma(n)u + O(u^2)\right), \tag{32}$$

where

$$\sigma_1 = \sum_{\mu=1}^{r} \sum_{1 \leq u_1 < \cdots < u_\mu \leq r} S^{(0)}_{\langle u_1, \ldots, u_\mu \rangle}(n, r; 1), \tag{33}$$

addendums $S^{(0)}_{\langle u_1, \ldots, u_\mu \rangle}(n, r; 1)$, $1 \leq u_1 < \cdots < u_\mu \leq r$, $\mu = 1, \ldots, r$, in the right-hand side of (33) are

$$\begin{aligned} S^{(0)}_{\langle u_1, \ldots, u_\mu \rangle}(n, r; 1) = \sum_{s=0}^{n-\rho(n)} \sum (n - \rho(n))! \left((n - \rho(n) - s)! \prod_{i \in I} i!\right)^{-1} \\ \times \sum_{\substack{s'=0 \\ s'+s \geq 1}}^{\rho(n)} {\sum}' (\rho(n))! \left((\rho(n) - s')! \prod_{j \in J} j!\right)^{-1}, \end{aligned} \tag{34}$$

the signs Σ (Σ') are defined in the relation (9) with additional condition

$$\sum_{i \in I_{\{u\}}} i + \rho(n) - \sum_{j \in J_{\{u\}}} j < f(n), \qquad u \in \{u_1, u_2, \ldots, u_\mu\},$$

$$\sum_{i \in I_{\{u\}}} i + \rho(n) - \sum_{j \in J_{\{u\}}} j \geq f(n), \qquad u \in \{1, 2, \ldots, r\} \setminus \{u_1, u_2, \ldots, u_\mu\},$$

and

$$\Gamma_{t,r}^{\{\vartheta_1, \ldots, \vartheta_\mu\}} \geq 1, \quad 1 \leq \vartheta_1 < \cdots < \vartheta_\mu \leq r, \quad \mu = 1, \ldots, r; \tag{35}$$

$$\sigma_2 = 1 + \sum_{q=1}^{2^r-1} S_q^{(0)}(n, r; 1), \tag{36}$$

$S_q^{(0)}(n, r; 1)$ differs from $S(n, r; 1)$ so that the numbers $i \in I$ and $j \in J$ in the right-hand side of (9) are changing so that there exist precisely q of the expressions of the type $\Gamma_{t,r}^{\{u_1,\dots,u_v\}}$ for each of which

$$\Gamma_{t,r}^{\{u_1,\dots,u_v\}} = 0, \tag{37}$$

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

Let us estimate σ_1. Firstly, for that we evaluate $S_{\langle u_1,\dots,u_\mu \rangle}^{(0)}(n, r; 1)$. We notice that

$$S_{\langle u_1,\dots,u_\mu \rangle}^{(0)}(n, r; 1) \leq S_{\langle u_1 \rangle}^{(0)}(n, r; 1), \tag{38}$$

since there is no restriction $\sum_{i \in I_{\{u\}}} i + \rho(n) - \sum_{j \in J_{\{u\}}} j < f(n)$, $u \in \{u_2, \dots, u_\mu\}$, in the right-hand side of the inequality. In turn the sum $S_{\langle u_1 \rangle}^{(0)}(n, r; 1)$ can be written in the following way:

$$\begin{aligned}
S_{\langle u_1 \rangle}^{(0)}(n, r; 1) = &\sum_{s=0}^{n-\rho(n)} \sum (n - \rho(n))! \left((n - \rho(n) - s)! \prod_{i \in I} i! \right)^{-1} \\
&\times \sum_{\substack{s'=0 \\ s'+s \geq 1}}^{\rho(n)} \sum{}' (\rho(n))! \left((\rho(n) - s')! \prod_{j \in J} j! \right)^{-1}
\end{aligned} \tag{39}$$

with additional conditions $\sum_{i \in I_{\{u_1\}}} i + \rho(n) - \sum_{j \in J_{\{u_1\}}} j < f(n)$ and (35).

Denote by $A(u_1)$ the set of the elements $i_{u_1 \mu_1 \dots \mu_l}$, $1 \leq \mu_1 < \cdots < \mu_l \leq r$, $l = 0, 1, 2, \dots, r-1$, $\mu_l \notin \{u_1\}$. The number of elements in the set $A(u_1)$ equals 2^{r-1}

$$|A(u_1)| = 2^{r-1}. \tag{40}$$

By virtue of (39) and (40), the sum $S_{\langle u_1 \rangle}^{(0)}(n, r; 1)$ can be given as

$$\begin{aligned}
S_{\langle u_1 \rangle}^{(0)}(n, r; 1) = &\sum_{s=0}^{n-\rho(n)} C_{n-\rho(n)}^s \\
&\times \sum_{s_1+s_2=s} C_s^{s_1} \left\{ \sum_1 \frac{s_1!}{\prod_{i \in A(u_1)} i!} \right\} \left(\sum_2 \frac{s_2!}{\prod_{i \in I \setminus A(u_1)} i!} \right) \sum_{s'=0}^{\rho(n)} C_{\rho(n)}^{s'} (2^r - 1)^{s'},
\end{aligned} \tag{41}$$

where $\sum_1 -$ is the sum over all $i \in A(u_1)$ such that $\sum i = s_1$, $\sum_2 -$ is the sum over all $i \in I \setminus A(u_1)$ such that $\sum i = s_2$.

Relations (34)–(41) and the polynomial formula let us obtain the estimate for $S_{\langle u_1,\dots,u_\mu \rangle}^{(0)}(n, r; 1)$:

$$S_{\langle u_1,\dots,u_\mu \rangle}^{(0)}(n, r; 1) \leq (2^{r-1})^{n-\rho(n)} \left(\sum_{s_1} C_{n-\rho(n)}^{s_1} \left(2^{r-1} \right)^{s_1} \right) 2^{r\rho(n)}, \tag{42}$$

where the summation over parameter s_1 occurs on the interval $0 \leq s_1 \leq 2^{r-1}k$. Upper restriction for s_1 in the last inequality follows from (13), (27) and the assumption $i \in A(u_1)$.

Since $0 \leq s_1 \leq 2^{r-1}k$ and (30), the relation (42) can be rewritten in the following way:

$$S_{\langle u_1,\dots,u_\mu \rangle}^{(0)}(n, r; 1) \leq 2^{(r-1)(n+2^{r-1}\varepsilon f(n))+\rho(n)} \left(2^{r-1}\varepsilon f(n) + 1 \right) C_{n-\rho(n)}^{2^{r-1}\varepsilon f(n)},$$

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

$$S^{(0)}_{\langle u_1,\ldots,u_\mu \rangle}(n, r; 1) \leq 2^{(r-1)(n+2^{r-1}\varepsilon f(n))+\rho(n)} \left(2^{r-1}\varepsilon f(n) + 1\right)$$
$$\times \left(\frac{(n-\rho(n))e}{2^{r-1}[\varepsilon f(n)]}\right)^{2^{r-1}\varepsilon f(n)} \frac{1}{\sqrt{2^r \pi [\varepsilon f(n)]}}. \tag{43}$$

Substitution (43) in (33) gives

$$\sigma_1 \leq 2^{r(n+\frac{3}{2})-n+\rho(n)-1} \left(\frac{(n-\rho(n))e}{[\varepsilon f(n)]}\right)^{2^{r-1}\varepsilon f(n)} \sqrt{\frac{\varepsilon f(n)}{\pi}}. \tag{44}$$

In analogy to how it was estimated of σ_0 in ([6], inequality (46)), we receive the estimation for σ_2:

$$\sigma_2 \leq \frac{2^{2^r-2+(r-1)n+r\varepsilon f(n)}}{\pi} \left(\frac{(n-\rho(n))\rho(n)e^2}{\varepsilon^2 f^2(n)}\right)^{2^r \varepsilon f(n)}. \tag{45}$$

Taking into account (32), the fraction $\frac{S^{(0)}(n,r;Q)}{2^{rN}2^{mr}}$ can be given as $1 - \frac{\sigma_1}{2^{rn}} - \frac{\sigma_2}{2^{rn}} + O(u)$, in view of which the relation (29) can be rewritten in the following way:

$$\sup_{1 \leq r \leq (\alpha+\gamma)\lambda^*} \left(\frac{\sigma_1}{2^{rn}} + \frac{\sigma_2}{2^{rn}} + O(u)\right) \frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0, \quad n \to \infty. \tag{46}$$

Using conditions (2), (3), (7) and relations (24), (44), (45), it is easy to show that

$$u\frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0, \quad \frac{\sigma_1}{2^{rn}}\frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0, \quad \frac{\sigma_2}{2^{rn}}\frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0 \tag{47}$$

as $n \to \infty$. Using (47), we obtain (46). From the relation (46) and equality $M(Y)_r = 2^{rm}$, (29) follows.

By virtue of (26) and (29), in order to complete the checking of the condition (38) (Lemma 2, [5]) it is necessary to establish that for $1 \leq r \leq (\alpha + \gamma)\lambda^*$

$$\frac{1}{2^{rN+rm}} \left(\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q)\right) \frac{e^{2\lambda^*}}{\sqrt{\lambda^*}} \to 0, \quad n \to \infty. \tag{48}$$

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}/, $\alpha = 1,\ldots,\Delta$, and put $M_2 = I\backslash M_1$, $\tilde{M}_2 = J\backslash\tilde{M}_1$.

Let z be the least integer number such that $\Delta \leq 2^z - 1$, $1 \leq z \leq r$. Then by Proposition 1 from the work [4], the number of elements of the set M_1 /$\tilde{M}_1$/ does not exceed

$$|M_1| \leq 2^{r-z} - 1 \quad / \left|\tilde{M}_1\right| \leq 2^{r-z} - 1/. \tag{49}$$

Let

$$\Delta < 2^z - 1. \tag{50}$$

With the help of (50), we denote the $S^{(\Delta)}(n, r; Q)$ from the relation (48) by $S^{(\Delta)}_{(2^z-2)}(n, r; Q)$. Then

$$\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q) = \sum_{\Delta=1}^{2^r-1} S^{(\Delta)}_{(2^z-2)}(n, r; Q) \tag{51}$$

exists under the relation (50). Taking into account (5) and (6), the estimation (28) gives the next inequality for Q in the right-hand side of (51)

$$|Q| \leq 2^{zN}Q_1, \tag{52}$$

where $Q_1 = \left(1 - \frac{1}{2^z}\right)^N \exp\left\{\frac{2^r - \Delta - 1}{(2^z - 1)(2^r - 1)} u\right\}$.

By virtue of (52), each addendum in the right-hand side of (51) admits the estimation

$$S_{(2^z-2)}^{(\Delta)}(n, r; Q) \le 2^{zN} S_{(2^z-2)}^{(\Delta)}(n, r; 1) Q_1. \tag{53}$$

Further, for all $i \in M_2$ $(j \in \tilde{M}_2)$

$$0 \le i \le k \ (0 \le j \le k) \tag{54}$$

follows from (13) and (27). Using (49)–(54), we find

$$\frac{e^{2\lambda^*} \lambda^{*-\frac{1}{2}}}{2^{rN+rm}} \sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q)$$

$$\le \exp\left\{-\frac{N}{2^z}\left(1 + O\left(\frac{2^{z+1}(2^r - 1)f(n)}{N} \ln\left(\frac{ne}{[\varepsilon f(n)]}\right)\right) + o(u)\right)\right\},$$

the right-hand side of which tends to zero for $1 \le r \le (\alpha + \gamma)\lambda^*$ as $n \to \infty$ in view of (2), (3), (24) and (31). Therefore, the relation (48) holds under restrictions (49) and (50).

Let

$$\Delta = 2^z - 1, \ 1 \le z \le r, \tag{55}$$

$$|M_1| < 2^{r-z} - 1, \ |\tilde{M}_1| < 2^{r-z} - 1. \tag{56}$$

Accordingly to (51), we put

$$\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q) = \sum_{\Delta=1}^{2^r-1} S_{(2^z-1)}^{(\Delta)}(n, r; Q), \tag{57}$$

where $S_{(2^z-1)}^{(\Delta)}(n, r; Q)$ coincides with $S^{(\Delta)}(n, r; Q)$ under restrictions (55) and (56).

Taking into account conditions (5), (6) and relation (28), we obtain the next inequality for Q in the right-hand side of (57)

$$|Q| \le 2^{zN} Q_2, \tag{58}$$

where $Q_2 = \exp\left\{\frac{2^r - \Delta - 1}{(2^z - 1)(2^r - 1)} u\right\}$. With the help of (55)–(58), we find the inequality

$$\frac{e^{2\lambda^*} \lambda^{*-\frac{1}{2}}}{2^{rN+rm}} \sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q)$$

$$\le \exp\left\{-\frac{n}{2^{r-z}}\left(1 + O\left(\frac{2^{r-z+1}(2^r - 1)f(n)}{n} \ln\left(\frac{ne}{[\varepsilon f(n)]}\right)\right) + o(u)\right)\right\}, \tag{59}$$

the right-hand side of which tends to zero for $1 \le r \le (\alpha + \gamma)\lambda^*$ as $n \to \infty$ by virtue of (2), (3), (24) and (31). Therefore, the relation (48) holds true under restrictions (55) and (56).

Next, let us check that if $\Delta = 2^z - 1, 1 \le z \le r, i z \in \{r, r-1\}$ or $r \in \{1, 2\}$, then there exists some α, $\alpha \in \{1, 2, \ldots, \Delta\}$ such that $\xi_\alpha \le 2$. Indeed, when $z = r$ or $r \in \{1, 2\}$, then, obviously, there exists mentioned parameter α. For $z = r - 1$ the existence of the parameter α such that $\xi_\alpha \le 2$ follows from the Remark 2 from the work [4]. Since, the inequality $\Gamma_{t,r}^{\omega_\alpha} \ge 1$ holds true for values of the parameter α, $\alpha \in \{1, 2, \ldots, \Delta\}$ such that $\xi_\alpha \le 2$ (by virtue of Lemmas 1, 2 and condition (5), then below the notation $\Delta = 2^z - 1$ extends for all z, $1 \le z \le r - 2, 3 \le r < \infty$, and value $\alpha \in \{1, 2, \ldots, \Delta\}$ such that $\xi_\alpha \ge 3$.

Let restrictions

$$\xi_\alpha \geq 3, \ \alpha = 1, \ldots, \ \Delta, \ \Delta = 2^z - 1, \ 1 \leq z \leq r - 2, \ 3 \leq r < \infty, \tag{60}$$

$$|M_1| = |\tilde{M}_1| = 2^{r-z} - 1 \tag{61}$$

hold true. Put

$$\sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q) = \sum_{\Delta=1}^{2^r-1} S^{(\Delta)}_{(2^z-1)}(n, r; Q), \tag{62}$$

where $S^{(\Delta)}_{(2^z-1)}(n, r; Q)$ coincides with $S^{(\Delta)}(n, r; Q)$ under restrictions (60) and (61).

If (60) and (61) holds true, then according to Proposition 2 in [4] the set M_1 $(\tilde{M}_1)$ contains no less than three elements $i_{m_\nu} \in M_1$ $(j_{\tilde{m}_\nu} \in \tilde{M}_1)$, $\nu = \overline{1,3}$, such that for some $\alpha \in \{1, \ldots, \Delta\}$ $(\tilde{\alpha} \in \{1, \ldots, \Delta\})$

$$|\omega_\eta \cap m(\eta, \nu)| = 2, \ \nu = \overline{1,3}, \ |\omega_\eta \cap (a_\eta \cup b_\eta)| = 3, \ \eta \in \{\alpha, \tilde{\alpha}\}, \tag{63}$$

for any $a_\eta, b_\eta \in \{m(\eta, \nu) : \nu = \overline{1,3}\}, a_\eta \neq b_\eta$, where $m(\eta, \nu) = \{m_\nu, \text{ as } \eta = \alpha; \ \tilde{m}_\nu, \text{ as } \eta = \tilde{\alpha}\}$, $\nu = \overline{1,3}$. With the help of (20) of the work [4] and (63), for above mentioned η

$$\Gamma^{\omega_{\tilde{\alpha}}}_{t,r} \geq \gamma_t^{\{a_{\tilde{\alpha}} \cup b_{\tilde{\alpha}}\}}, \ t \in \{2, \ldots, k\}, \tag{64}$$

$$\Gamma^{\omega_\alpha}_{t,r} \geq \gamma_t^{\{a_\alpha \cap b_\alpha\}}.$$

According to (23), established in [4], the right-hand side of (64) can be estimated as

$$\gamma_t^{\{a_{\tilde{\alpha}} \cup b_{\tilde{\alpha}}\}} \geq t^{-1} j_* (j^* - 2^{-1}(j_* - 1)) C^{t-2}_{(j^*/2)+(3j_*/4)+5/4} \tag{65}$$

under condition $j_* \geq t$, where $j_* = \min\{j_{a_{\tilde{\alpha}}}, j_{b_{\tilde{\alpha}}}\}$, $j^* = \max\{j_{a_{\tilde{\alpha}}}, j_{b_{\tilde{\alpha}}}\}$.
Analogy to (23) from the work [4], we can find

$$\gamma_t^{\{a_\alpha \cap b_\alpha\}} \geq t^{-1} i_* (i^* - 2^{-1}(i_* - 1)) C^{t-2}_{(i^*/2)+(3i_*/4)+5/4} \tag{66}$$

under condition $i_* \geq t$, where $i_* = \min\{i_{a_\alpha}, i_{b_\alpha}\}$, $i^* = \max\{i_{a_\alpha}, i_{b_\alpha}\}$.

If $i_* \geq \sqrt{\varepsilon} f(n), j_* \geq \sqrt{\varepsilon} f(n)$ satisfy, then inequalities $i_* \geq t, j_* \geq t, t \in \{2, \ldots, k\}$, obviously, hold true for $0 < \varepsilon < 1$ and

$$\Gamma^{\omega_\eta}_{t,r} \geq \varepsilon (2t)^{-1} (\varphi(n))^2 C^{t-2}_{(5\sqrt{\varepsilon} f(n)/4)-5/4}, \ n \to \infty, \ \eta \in \{\alpha, \tilde{\alpha}\}$$

follows from (65) and (66), which contradicts the equality (27) under the sufficiently small $\varepsilon > 0$ and $t \in \{2, \ldots, k\}$.

Therefore, under restrictions (60) and (61) at least one element $i_* \in M_1$ $(j_* \in \tilde{M}_1)$ satisfy inequalities

$$i_* < \sqrt{\varepsilon} f(n) \ (j_* < \sqrt{\varepsilon} f(n)). \tag{67}$$

Let us observe that the inequality (58) in the right-hand side of (62) holds true for parameter Q, we find the estimation according to (60)–(62) and (67)

$$\frac{e^{2\lambda^*} \lambda^{*-\frac{1}{2}}}{2^{rN+rm}} \sum_{\Delta=1}^{2^r-1} S^{(\Delta)}(n, r; Q) \leq \exp\left\{ -\frac{n}{2^r} \left(1 + O\left(\frac{r \, 2^{2r+1} f(n) \ln n}{n} \right) + o(u) \right) \right\}, \tag{68}$$

the right-hand side of which tends to zero for $1 \leq r \leq (\alpha + \gamma)\lambda^*$ as $n \to \infty$ by virtue of (2), (3), (7), (24) and (31).
If (60) and $|M_1| = 2^{r-z} - 1$, $|\tilde{M}_1| < 2^{r-z} - 1$ or $|M_1| < 2^{r-z} - 1$, $|\tilde{M}_1| = 2^{r-z} - 1$ hold, then in the same way, taking into account which, (59) and (68) was found, we obtain (48).

Relations (26), (29) and (48) prove the condition (38) from the work [5], where the random variable Y have a Poisson distribution with parameter 2^m.

Therefore, conditions of the Lemma 2 in [5] checked up and with the help of this Lemma, (2) and (25)

$$\max_{0 \leq t \leq (1+\omega)\lambda^*} |P\{\nu_n \geq t\} - P\{Y \geq t\}| \to 0 \text{ as } n \to \infty. \tag{69}$$

We can write relation (69) in the following way:

$$\max_{-\sqrt{\lambda^*} \leq l \leq \omega\sqrt{\lambda^*}} \left| P\left\{ \frac{\nu_n - \lambda^*}{\sqrt{\lambda^*}} \geq l \right\} - P\left\{ \frac{Y - \lambda^*}{\sqrt{\lambda^*}} \geq l \right\} \right| \to 0, \ n \to \infty, \tag{70}$$

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

By the virtue of (24), (25) and Theorem ([1], p.157), we find that the distribution of the random variable $\frac{\nu_n - \lambda^*}{\sqrt{\lambda^*}} \Big/ \frac{Y - \lambda^*}{\sqrt{\lambda^*}} \Big/$ coincides with distribution of the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}} \Big/ \frac{Y - [\lambda]}{\sqrt{[\lambda]}} \Big/$ as $n \to \infty$.

Therefore, we can write the relation (70) in the following way:

$$\max_{-\sqrt{\lambda} \leq l \leq \omega\sqrt{\lambda}} \left| P\left\{ \frac{\nu_n - \lambda}{\sqrt{\lambda}} \geq l \right\} - P\left\{ \frac{Y - [\lambda]}{\sqrt{[\lambda]}} \geq l \right\} \right| \to 0, \ n \to \infty. \tag{71}$$

Finally we notice that the random variable $\frac{Y - [\lambda]}{\sqrt{[\lambda]}}$ has the standard normal distribution as $\lambda \to \infty$. Therefore, by virtue of C and (71), the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$ has the normal distribution with parameters (0,1) as $\lambda \to \infty$. The theorem is proved.

Example 1. *Let $\alpha = 5$, $\omega = 1$, $\nu = 2$, $\varepsilon = const$, $o < \varepsilon < 1$, $\rho(n) = \frac{n}{2}$, $T_q = \{2\}$, $q = 1, \ldots, N$, $f(n) = \ln n$, $\delta_{qt} = \frac{1}{2n^2}$, $t \in T_q$, $q = 1, \ldots, N$, satisfy. Parameters n, N, p_{qt} are changed so that $2^{n-N} = \left[\frac{1}{14} \log_2 \frac{n}{2(\ln n)^2} \right]$ and the condition (6) holds.*

Then the conditions of the theorem hold true and the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$, where $\lambda = \frac{1}{14} \log_2 \frac{n}{2(\ln n)^2}$, has a normal limit $(n \to \infty)$ distribution.

Example 2. *Let $\alpha = 5$, $\omega = 1$, $\nu = 2$, $\varepsilon = \frac{1}{2}$, $\rho(n) = \frac{n}{2}$, $T_q = \{2\}$, $q = 1, \ldots, N$, $f(n) = 4$, $\delta_{qt} = 0$, $t \in T_q$, $q = 1, \ldots, N$, satisfy. Parameters n, N, p_{qt} are changed so that $2^{n-N} = \left[\frac{1}{14} \log_2 \frac{n}{8 \ln n} \right]$ and condition (6) holds.*

Then the conditions of the theorem hold true and the random variable $\frac{\nu_n - \lambda}{\sqrt{\lambda}}$, where $\lambda = \frac{1}{14} \log_2 \frac{n}{8 \ln n}$, has a normal limit $(n \to \infty)$ distribution.

REFERENCES

[1] Chistyakov V.P. Course of probability theory. Nauka, Moscow, 2003. (in Russian)

[2] Levitskaia A.A. *Systems of random equations over finite algebraic structures*. Cybernetics and Systems Analysis 2005, **41** (1), 82–116. (in Russian)

[3] Masol V.I. *Moments of the number of solutions of a system of random Boolean equations*. Random Oper. and Stoch. Equ. 1993, **1** (2), 171–179. doi:10.1515/rose.1993.1.2.171

[4] Masol V.I. *Limit distribution of the number of solutions of a system of random Boolean equations with a linear part*. Ukrainian Math. J. 1998, **50** (9), 1389–1404. doi:10.1007/BF02525245 (translation of Ukr. Mat. Zhurn. **50** (9), 1214–1226. (in Ukrainian))

[5] Masol V.I., Slobodyan S.Y. *On the asymptotic normality of the number of false solutions of a system of nonlinear random Boolean equations*. Theory Stoch. Process. 2007, **13(29)** (1–2), 144–151.

[6] Masol V.I., Slobodyan S.Y. *The normal limit distribution of the number of false solutions of a system of nonlinear random equations in the field GF(2)*. Theory Stoch. Process. 2006, **12(28)** (1–2), 116–126.

Слободян С.Я. *Нормальний граничний розподіл нормованого числа сторонніх розв'язків однієї системи нелінійних випадкових рівнянь над полем GF(2)* // Карпатські матем. публ. — 2014. — Т.6, №1. — С. 149–160.

Доведена теорема про нормальний граничний розподіл нормованого числа сторонніх розв'язків наперед сумісної системи нелінійних випадкових рівнянь над полем GF(2). Результати отримано з додатковою умовою на кількість ненульових компонент як цих розв'язків, так і правдивого розв'язку.

Ключові слова і фрази: нелінійні випадкові рівняння над полем GF(2), граничний нормальний розподіл, число розв'язків.

Слободян С.Я. *Нормальное предельное распределение нормированного числа посторонних решений одной системы нелинейных случайных уравнений над полем GF(2)* // Карпатские матем. публ. — 2014. — Т.6, №1. — С. 149–160.

Доказана теорема о нормальном предельном распределении нормированного числа посторонних решений заранее совместной системы нелинейных случайных уравнений над полем GF(2). Результаты получены с дополнительным условием на количество ненулевых компонент как этих решений, так и истинного решения.

Ключевые слова и фразы: нелинейные случайные уравнения над полем GF(2), нормальное предельное распределение, число решений.