

AN ESTIMATE FOR THE RATE OF CONVERGENCE
OF THE DISTRIBUTION OF THE NUMBER OF FALSE SOLUTIONS
OF A SYSTEM OF NONLINEAR RANDOM EQUATIONS
IN THE FIELD $GF(2)$

UDC 519.21

V. I. MASOL AND M. V. SLOBODYAN

ABSTRACT. We prove a result on the rate of convergence as $n \rightarrow \infty$ of the distribution of the number of false solutions of a system of nonlinear random equations in the field $GF(2)$ to the Poisson distribution with parameter 2^m . We assume, in particular, that the difference between the number n of unknowns and the number N of equations of the system is a constant m .

1. SETTING OF THE PROBLEM. STATEMENT OF THE RESULT

Consider the following system of equations:

$$(1) \quad \sum_{k=1}^{g_i(n)} \sum_{1 \leq j_1 < \dots < j_k \leq n} a_{j_1 \dots j_k}^{(i)} x_{j_1} \cdots x_{j_k} = b_i, \quad i = 1, 2, \dots, N,$$

in the field $GF(2)$. Throughout the paper we assume that the following conditions are satisfied:

- the coefficients $a_{j_1 \dots j_k}^{(i)}$, $1 \leq j_1 < \dots < j_k \leq n$, $k = 1, 2, \dots, g_i(n)$, $i = 1, 2, \dots, N$, are independent random variables such that

$$\mathbf{P} \left\{ a_{j_1 \dots j_k}^{(i)} = 1 \right\} = 1 - \mathbf{P} \left\{ a_{j_1 \dots j_k}^{(i)} = 0 \right\} = p_{ik};$$

- the elements b_i , $i = 1, 2, \dots, N$, are obtained after the substitution of a fixed n -dimensional $(0, 1)$ -vector \bar{x}^0 with exactly $\rho(n)$ nonzero coordinates to the left hand side of system (1) where

$$(2) \quad \rho(n) = \rho n, \quad \rho = \text{const}, \quad 0 < \rho < 1;$$

- the functions $g_i(n)$ are nonrandom, $g_i(n) \in \{2, 3, \dots, n\}$, $i = 1, 2, \dots, N$.

We denote this set of conditions by (A).

Let ν_n be the total number of false solutions of system (1), that is, the total number of solutions of system (1) that do not coincide with \bar{x}^0 . In this paper, we study the rate of convergence of the distribution of the random variable ν_n to the limit Poisson distribution with parameter 2^m if condition (2) holds.

Theorem. *Suppose the conditions (A) are satisfied. Assume that*

$$(3) \quad n - N = m, \quad m = \text{const}, \quad -\infty < m < \infty,$$

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

Key words and phrases. System of nonlinear random equations, the field $GF(2)$, rate of convergence.

and that for any $i = 1, 2, \dots, N$, there exists a set $T_i \neq \emptyset$ such that

$$(4) \quad T_i \subseteq \{2, \dots, g_i(n)\}, \quad 0 \leq \delta_{it}(n) \leq p_{it} \leq 1 - \delta_{it}(n), \quad t \in T_i,$$

for sufficiently large n , where $\delta_{it}(n)$ are some numbers such that $0 \leq \delta_{it}(n) \leq \frac{1}{2}$. Furthermore, let a function $\varphi(n)$ be such that $\varphi(n) \leq \ln^2 n$. Assume that, given a constant $\varepsilon_0 \in (0; 1)$ and a fixed integer $l \geq 0$, one can find a natural number $n_0 = n_0(\varepsilon_0, l)$ for which

$$(5) \quad 2^{\gamma+1}B(n) < \varepsilon_0$$

for all $n \geq n_0$, where $\gamma = \lceil \log_2 n/6 \rceil$ for $n \geq 2^{6l}$,

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

and $f(n)$ assumes positive integer values and is such that $f(n) = o(\varphi(n))$ as $n \rightarrow \infty$. (Here and in what follows, the symbol $C_{f(n)}^t$ stands for the binomial coefficient $\binom{f(n)}{t}$.)

If $k = 0, 1, 2, \dots$ is fixed, then

$$(6) \quad \left| \mathbb{P}\{\nu_n = k\} - \frac{\lambda^k}{k!} e^{-\lambda} \right| \leq \left(\frac{2e\lambda}{\gamma} \right)^\gamma \{ 2 + 2^{\gamma+1}B(n) + \Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1 \} + e^{4\lambda} \gamma B(n) + e^{2\lambda} \gamma (\Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1),$$

where $\lambda = 2^m$,

$$\begin{aligned} \Theta_1 &= \exp \left\{ -2^{-2\gamma} \sum_{i=1}^N \delta_i + \log_2 \sqrt[6]{n} + \sqrt[6]{n} + \ln(\tilde{\rho}n) - m \ln 2 \right\}, \\ \Theta_2 &= 2^{-n} \exp \left\{ \varepsilon \sqrt[6]{n} \ln^2 n \left(\log_2 \sqrt[6]{n} + \ln \left(\frac{n^{5/6} e}{\varepsilon \ln^2 n} \right) \right) + \sqrt[6]{n} + 2 \ln (\varepsilon \sqrt[6]{n} \ln^2 n) \right\}, \\ \tilde{\rho} &= \max \{ \rho, 1 - \rho \}, \quad \delta_i = \min \left\{ \sum_{t \in T_i} \delta_{it}(n) C_r^{t-1}, \frac{2 \ln n}{\sqrt{\varepsilon \varphi(n)}} \right\}, \end{aligned}$$

$r = \lceil \varepsilon \varphi(n) \rceil$, $0 < \varepsilon < 1$, and $\varepsilon = \text{const}$.

Here and in what follows we assume that $0^0 \equiv 1$.

Remark. Fix arbitrary numbers $\varepsilon_0 \in (0; 1)$ and $\varepsilon \in (0; 1)$. It is easy to check that, given a number $\gamma > 0$, there exists a natural number $n_1 = n_1(\varepsilon_0, \varepsilon, \gamma)$ such that the right hand side of inequality (6) becomes smaller than γ for all $n \geq n_1$.

Example. If $T_i = \{2\}$, $\varphi(n) = \ln^2 n$, $f(n) = \lceil (\ln n)^{3/2} \rceil$, $\delta_{it} = \frac{1}{2}$, $n = 65$, $m = -8$, $\rho = 0.9$, $\varepsilon = 0.25$, and $\varepsilon_0 \leq \varepsilon$, then relations (3)–(5) hold. Applying inequality (6) we obtain

$$\left| \mathbb{P}\{\nu_{65} = k\} - \frac{\lambda^k}{k!} e^{-\lambda} \right| \leq 0.086$$

for all $k \geq 0$.

2. AUXILIARY RESULTS

Denote by $\mathbb{E} \nu_n^{[k]}$ the factorial moment of order k for the random variable ν_n , $k = 1, 2, \dots$. We set $\mathbb{E} \nu_n^{[0]} \equiv 1$.

Proposition ([1]). *If the conditions (A) hold, then, for all $k \geq 1$,*

$$(7) \quad \mathbb{E} \nu_n^{[k]} = 2^{-kN} S(n, k; Q),$$

where

$$(8) \quad S(n, k; Q) = \sum_{s=0}^{n-\rho n} \sum (n - \rho n)! \left((n - \rho n - s)! \prod_{i \in I} i! \right)^{-1} \\ \times \sum_{\substack{s'=0 \\ s'+s \geq 1}}^{\rho n} \sum' (\rho n)! \left((\rho n - s')! \prod_{j \in J} j! \right)^{-1} Q,$$

$$(9) \quad Q = \prod_{i=1}^N \left(1 + \sum_{\nu=1}^k \sum_{1 \leq u_1 < \dots < u_\nu \leq k} \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma_{t,k}^{\{u_1, \dots, u_\nu\}}} \right),$$

and the index of summation in \sum (\sum') runs over all elements $i \in I$ ($j \in J$) such that

$$\sum_{i \in I} i = s, \quad \sum_{j \in J} j = s',$$

where

$$I = \{i_{\{u_1, \dots, u_\nu\}} : 1 \leq u_1 < \dots < u_\nu \leq k, \nu = 1, \dots, k\}, \\ J = \{j_{\{u_1, \dots, u_\nu\}} : 1 \leq u_1 < \dots < u_\nu \leq k, \nu = 1, \dots, k\}.$$

(The definition of the numbers $i_{\{u_1, \dots, u_\nu\}}$ and $j_{\{u_1, \dots, u_\nu\}}$ is given in [1].) The elements $i \in I$ and $j \in J$ in inequality (8) are such that

$$\sum_{\substack{i \in I_{\{u\}}, \\ j \in J_{\{u\}}} (i + j) \geq 1, \quad u = 1, \dots, k,$$

(the sets $I_{\{u\}}$ and $J_{\{u\}}$ are defined below) and

$$\sum_{l=0}^{k-2} \sum_{1 \leq \mu_1 < \dots < \mu_l \leq k} (i_{\{u_1, \mu_1, \dots, \mu_l\}} + j_{\{u_1, \mu_1, \dots, \mu_l\}} + i_{\{u_2, \mu_1, \dots, \mu_l\}} + j_{\{u_2, \mu_1, \dots, \mu_l\}}) \geq 1, \\ 1 \leq u_1 < u_2 \leq k,$$

for $1 \leq u_1 < \dots < u_\nu \leq k$, $\nu \in \{1, \dots, k\}$, and $t \in \{1, \dots, n\}$. Moreover

$$(10) \quad \Gamma_{t,k}^{\{u_1, \dots, u_\nu\}} \geq \sum_{(i,j) \in T} (C_i^t + C_j^t),$$

where

$$T = I_{\{u_1, \dots, u_\nu\}} \times J_{\{u_1, \dots, u_\nu\}}.$$

Here

$$I_{\{u_1, \dots, u_\nu\}} = \{i_{\{\sigma_1, \dots, \sigma_\psi, \mu_1, \dots, \mu_l\}} : A(\psi, l, k)\}, \\ J_{\{u_1, \dots, u_\nu\}} = \{j_{\{\sigma_1, \dots, \sigma_\psi, \mu_1, \dots, \mu_l\}} : A(\psi, l, k)\}$$

are the sets of numbers $i_{\{\sigma_1, \dots, \sigma_\psi, \mu_1, \dots, \mu_l\}}$ and $j_{\{\sigma_1, \dots, \sigma_\psi, \mu_1, \dots, \mu_l\}}$, respectively, satisfying the collection of restrictions $A(\psi, l, k)$, where $A(\psi, l, k)$ means

$$1 \leq \sigma_1 < \dots < \sigma_\psi \leq k, \quad \sigma_z \in \{u_1, \dots, u_\nu\}, \quad z = 1, \dots, \psi, \quad \psi = 1, \dots, \nu, \\ \psi \equiv 1 \pmod{2}, \quad 1 \leq \mu_1 < \dots < \mu_l \leq k, \quad \mu_1, \dots, \mu_l \notin \{u_1, \dots, u_\nu\}, \\ l = 0, \dots, k - \nu.$$

If

$$\rho n - s' \geq t,$$

then

$$(11) \quad \Gamma_{t,k}^{\{u_1, \dots, u_\nu\}} \geq C_{\rho n - s'}^{t-1} \sum_{(i,j) \in T} (i+j).$$

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

To prove the theorem of Section 1, we need the following auxiliary result.

Lemma. *Suppose all the assumptions of the theorem hold for all nonnegative integers k such that*

$$(12) \quad 0 < k \leq \gamma.$$

Then

$$(13) \quad \mathbb{E} \nu_n^{[k]} = \lambda^k + \Delta(k, n)$$

for all sufficiently large n , where

$$(14) \quad \begin{aligned} |\Delta(k, n)| \leq & 2^{(m+1)k+1} u + 2^{mk} \Theta_2 (1 + 2^{k+1} u) + 7 (2^{2^k}) 2^{(m+1)k} \\ & \times \exp \left\{ -2^{-2k} \sum_{i=1}^N \delta_i + \ln(\tilde{\rho} n) - m \ln 2 \right\}, \\ u = & \sum_{i=1}^N \exp \left\{ -2 \sum_{t \in T_i} \delta_{it}(n) C_r^t \right\}. \end{aligned}$$

Proof. Using equality (7), we represent the factorial moment $\mathbb{E} \nu_n^{[k]}$ as follows:

$$(15) \quad \mathbb{E} \nu_n^{[k]} = 2^{-kN} \sum_{\Delta \geq 0} S^{(\Delta)}(n, k; Q),$$

where $S^{(\Delta)}(n, k; Q)$ is defined similarly to the term $S(n, k; Q)$ with additional restrictions imposed on elements $i \in I$ and $j \in J$ appearing in definition (8) of $S(n, k; Q)$, namely, that there are exactly Δ pairwise distinct sets ω_α ,

$$\begin{aligned} \omega_\alpha &= \{u_1^{(\alpha)}, \dots, u_{\xi_\alpha}^{(\alpha)}\}, \\ 1 \leq u_1^{(\alpha)} &< \dots < u_{\xi_\alpha}^{(\alpha)} \leq k, \quad \xi_\alpha \in \{1, \dots, k\}, \quad \alpha = 1, \dots, \Delta, \end{aligned}$$

such that for each of them there exists $t^{(\alpha)} \in \{2, \dots, r\}$ that satisfies

$$(16) \quad \Gamma_{t^{(\alpha)}, k}^{\omega_\alpha} < C_r^{t^{(\alpha)}}$$

and

$$(17) \quad \Gamma_{t,k}^{\{v_1, \dots, v_\gamma\}} \geq C_r^t$$

for all $t \in \{2, \dots, r\}$ and for all sets $\{v_1, \dots, v_\gamma\}$, $1 \leq v_1 < \dots < v_\gamma \leq k$, $\gamma = 1, \dots, k$, such that $\{v_1, \dots, v_\gamma\} \neq \omega_\alpha$, $\alpha = 1, \dots, \Delta$.

It is worth mentioning that the term corresponding to $\Delta = 0$ may indeed appear on the right hand side of (15) (see [1]).

Furthermore, we rewrite equality (15) as follows:

$$(18) \quad \mathbb{E} \nu_n^{[k]} = S_1 + p_1,$$

where

$$S_1 = 2^{-kN} S^{(0)}(n, k; Q), \quad p_1 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S^{(\Delta)}(n, k; Q).$$

Now we turn to the estimation of S_1 . If $\Delta = 0$, we use estimate (17) and condition (4). Then

$$(19) \quad \prod_{i=1}^N \left(1 - 2^k \exp \left\{ -2 \sum_{t \in T_i} \delta_{it}(n) C_r^t \right\} \right) \leq Q \leq \prod_{i=1}^N \left(1 + 2^k \exp \left\{ -2 \sum_{t \in T_i} \delta_{it}(n) C_r^t \right\} \right).$$

Condition (5) and the inequality $r > f(n)$ imply by (12) that

$$(20) \quad 2^k u < \varepsilon_0.$$

Now we use bounds (19) and (20) and the elementary inequalities $1 + u_0 \leq e^{u_0}$ and $e^{u_0} \leq 1 + 2u_0$. Then

$$\prod_{i=1}^N (1 - u_i) \geq 1 - \sum_{i=1}^N u_i, \quad 0 < u_i < 1, \quad i = 0, 1, \dots, N,$$

and

$$(21) \quad Q_* \leq Q \leq Q^*,$$

where

$$Q^* = 1 + 2^{k+1}u, \quad Q_* = 1 - 2^k u.$$

If

$$(22) \quad \Gamma_{t,k}^{\{u_1, \dots, u_\nu\}} < C_r^t$$

for some set $\{u_1, \dots, u_\nu\}$, $1 \leq u_1 < \dots < u_\nu \leq k$, $\nu = 1, \dots, k$, and some $t \in \{2, \dots, r\}$, then inequality (10) holds, whence we get

$$(23) \quad 0 \leq i < r, \quad i \in I_{\{u_1, \dots, u_\nu\}}, \quad 0 \leq j < r, \quad j \in J_{\{u_1, \dots, u_\nu\}}.$$

Applying the polynomial theorem and relation (21) we get

$$(24) \quad 2^{-kN} (2^{nk} - \sigma_0) Q_* \leq S_1 \leq 2^{-kN} (2^{nk} - \sigma_0) Q^*,$$

where

$$(25) \quad \sigma_0 = 1 + \sum_{d=1}^{2^k-1} S_d^{(0)}(n, k; 1).$$

The definition of $S_d^{(0)}(n, k; 1)$ differs from that of the term $S(n, k; 1)$ in that the elements $i \in I$ and $j \in J$ on the right hand side of equality (8) satisfy an extra restriction, namely that there are exactly d elements of the set

$$\left\{ \Gamma_{t,k}^{\{u_1, \dots, u_\nu\}}, 1 \leq u_1 < \dots < u_\nu \leq k, \nu = 1, \dots, k \right\}$$

for which relation (22) holds, $d = 1, 2, \dots, 2^k - 1$.

Let all the expressions

$$\Gamma_{t,k}^{\{u_1, \dots, u_\nu\}}, \quad 1 \leq u_1 < \dots < u_\nu \leq k, \nu = 1, \dots, k,$$

be labeled with the numbers $1, 2, \dots, 2^k - 1$. Assume that this numbering is a one-to-one correspondence between the expressions and the numbers. Then the sum $S_d^{(0)}(n, k; 1)$ can be represented as follows:

$$S_d^{(0)}(n, k; 1) = \sum_{1 \leq \zeta_1 < \dots < \zeta_d \leq 2^k-1} S_{(\zeta_1, \dots, \zeta_d)}^{(0)}(n, k; 1),$$

where the definition of $S_{(\zeta_1, \dots, \zeta_d)}^{(0)}(n, k; 1)$ differs from that of $S_d^{(0)}(n, k; 1)$ by the restriction that relation (22) holds for those expressions $\Gamma_{t,k}^{\{u_1, \dots, u_\nu\}}$ that correspond to the numbers ζ_1, \dots, ζ_d . Denote by $A(\zeta_1, \dots, \zeta_d)$ ($B(\zeta_1, \dots, \zeta_d)$) the set of all $i \in I$ ($j \in J$) that are used in the bound (10) for all ζ_1, \dots, ζ_d . By inequality (22), the number of elements of the set $A(\zeta_1, \dots, \zeta_d)$ ($B(\zeta_1, \dots, \zeta_d)$) is at least 2^{k-1} :

$$(26) \quad |A(\zeta_1, \dots, \zeta_d)| \geq 2^{k-1}, \quad |B(\zeta_1, \dots, \zeta_d)| \geq 2^{k-1}.$$

The sum $S_d^{(0)}(n, k; 1)$ can be represented as follows:

$$(27) \quad \begin{aligned} & S_d^{(0)}(n, k; 1) \\ &= \sum_{1 \leq \zeta_1 < \dots < \zeta_d \leq 2^{k-1}} \sum_{s=0}^{n-\rho n} C_{n-\rho n}^s \\ & \quad \times \sum_{s_1+s_2=s} C_{s_1}^{s_1} \left(\sum^{(1)} \frac{s_1!}{\prod_{i \in A} i!} \right) \left(\sum^{(2)} \frac{s_2!}{\prod_{i \in I \setminus A} i!} \right) \\ & \quad \times \sum_{s'=0}^{\rho n} C_{\rho n}^{s'} \sum_{s'_1+s'_2=s'} C_{s'_1}^{s'_1} \left(\sum^{(3)} \frac{s'_1!}{\prod_{j \in B} j!} \right) \left(\sum^{(4)} \frac{s'_2!}{\prod_{j \in J \setminus B} j!} \right), \end{aligned}$$

where $\sum^{(1)}$ means the sum over all $i \in A(\zeta_1, \dots, \zeta_d)$ such that $\sum i = s_1$, $\sum^{(2)}$ means the sum over all $i \in I \setminus A(\zeta_1, \dots, \zeta_d)$ such that $\sum i = s_2$, $\sum^{(3)}$ means the sum over all $j \in B(\zeta_1, \dots, \zeta_d)$ such that $\sum j = s'_1$, and $\sum^{(4)}$ means the sum over all $j \in J \setminus B(\zeta_1, \dots, \zeta_d)$ such that $\sum j = s'_2$.

Using the polynomial theorem and relations (25)–(27) we obtain the following bound:

$$(28) \quad \begin{aligned} \sigma_0 \leq & 1 + 2^{2^k-1} \sum_{s=0}^{n-\rho n} C_{n-\rho n}^s (2^{k-1} - 1)^s \left(\sum_{s_1 \geq 0} C_{s_1}^{s_1} (2^{k-1})^{s_1} \right) \\ & \times \sum_{s'=0}^{\rho n} C_{\rho n}^{s'} (2^{k-1} - 1)^{s'} \left(\sum_{s'_1 \geq 0} C_{s'_1}^{s'_1} (2^{k-1})^{s'_1} \right). \end{aligned}$$

Taking into account the inequalities $s_1 \leq [r2^k]$ and $s'_1 \leq [r2^k]$, we conclude from (28) that

$$\sigma_0 \leq 2^{2^k} (2^{k-1})^n (2^k)^{r2^k} \left(\sum_{s_1=0}^{[r2^k]} C_{n-\rho n}^{s_1} \right) \left(\sum_{s'_1=0}^{[r2^k]} C_{\rho n}^{s'_1} \right).$$

This implies

$$(29) \quad \sigma_0 \leq 2^{2^k} (2^{k-1})^n (2^k)^{r2^k} (r2^k)^2 \left(C_n^{[r2^k]} \right)^2.$$

Then

$$(30) \quad 0 \leq \sigma_0 \leq 2^{nk} \Theta_2$$

by inequality (29), condition (12), and by the lower bound

$$(31) \quad n! > n^n e^{-n} \sqrt{2\pi n} e^{1/(12n+1)}$$

proved in [2].

Considering condition (3) and relations (21), (24), and (30), we get the following bounds:

$$(32) \quad \begin{aligned} & \lambda^k - \left\{ 2^{(m+1)k} u + 2^{mk} \Theta_2 (1 + 2^k u) \right\} \\ & \leq S_1 \leq \lambda^k + \left\{ 2^{(m+1)k+1} u + 2^{mk} \Theta_2 (1 + 2^{k+1} u) \right\}. \end{aligned}$$

Using restrictions (12) we show that

$$(33) \quad p_1 \leq 7 \left(2^{2^k} \right) 2^{(m+1)k} \exp \left\{ -2^{-2k} \sum_{i=1}^N \delta_i + \ln(\tilde{\rho}n) - m \ln 2 \right\}$$

for $\Delta \geq 1$. Indeed, put

$$p_2 = p_1 - S_2,$$

where

$$(34) \quad S_2 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_0)}^{(\Delta)}(n, k; Q).$$

The definition of $S_{(G_0)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies the additional condition, called G_0 :

$$\rho n - r + 1 \leq s' \leq \rho n.$$

Now we find a bound for S_2 . Denote by M_1 (\tilde{M}_1) the family of all $i \in I$ ($j \in J$) that do not belong to I_{ω_α} (J_{ω_α}), $\alpha = 1, \dots, \Delta$. Also we put

$$M_2 = I \setminus M_1, \quad \tilde{M}_2 = J \setminus \tilde{M}_1.$$

Let R_1 (\tilde{R}_1) denote the number of elements of the set M_1 (\tilde{M}_1). Let z be the minimum number such that

$$(35) \quad \Delta \leq 2^z - 1, \quad 1 \leq z \leq k.$$

According to Proposition 2.1 of [1] we obtain

$$(36) \quad R_1 \leq 2^{k-z} - 1, \quad \tilde{R}_1 \leq 2^{k-z} - 1.$$

If lower bound (17) holds, we take into account (4) and get the following inequality for Q defined in (34):

$$(37) \quad Q \leq 2^{zN} (1 + 2^{-z} (2^k - \Delta - 1) u).$$

Relation (16) implies that

$$(38) \quad 0 \leq i < r \quad (0 \leq j < r)$$

for all $i \in M_2$ ($j \in \tilde{M}_2$) by condition (22) and (23). Using (36)–(38) and condition G_0 , we prove that

$$(39) \quad S_2 \leq 2^{2^k} 2^{(k-1)m} \exp \left\{ -\rho n 2^{-k} + 2^k \varepsilon \ln^2 n \ln \left(\frac{\tilde{\rho} n e}{2^k \varepsilon \ln^2 n} \right) + 2^k u \right\}.$$

Now we introduce condition G_1 : let

$$(40) \quad s' \leq \rho n - r$$

and let there exist $i \in M_2$ and (or) $j \in \tilde{M}_2$ such that $i \in (r/E_n, r]$ and (or) $j \in (r/E_n, r]$, where

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

Let

$$p_3 = p_2 - S_3,$$

where

$$S_3 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_1)}^{(\Delta)}(n, k; Q).$$

The definition of $S_{(G_1)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies the additional condition G_1 .

We show that

$$(41) \quad S_3 \leq \frac{2^{2^k} 2^{mk}}{2^m} \exp \left\{ -2^{-k} N (1 - N^{-A_n}) + 2^k \varepsilon \ln^2 n \ln \left(\frac{\tilde{\rho} n e}{2^k \varepsilon \ln^2 n} \right) \right\}$$

where $A_n = 2\varepsilon/E_n$. If condition G_1 holds, we get

$$(42) \quad \Gamma_{t,k}^{\omega_\alpha} \geq C_r^{t-1} \frac{r}{E_n}$$

for all $t \in \{2, \dots, r\}$ and some $\alpha = 1, \dots, \Delta$ by inequality (11). Using bound (42) and condition (4) we obtain

$$\left| \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma_{t,k}^{\omega_\alpha}} \right| \leq \exp \left\{ -2 \sum_{t \in T_i} \delta_{it}(n) C_r^{t-1} \frac{r}{E_n} \right\}, \quad i = 1, \dots, N.$$

The latter bound implies

$$(43) \quad Q \leq 2^{zN} \exp \left\{ -2^{-z} \left(N - \sum_{i=1}^N \exp \left\{ -2 \sum_{t \in T_i} \delta_{it}(n) C_r^{t-1} \frac{r}{E_n} \right\} \right) \right\}.$$

Relation (43) yields

$$(44) \quad Q \leq \hat{Q}$$

by Hölder's inequality and relation (20), where

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

Now we derive from condition G_1 that

$$(45) \quad S_3 \leq 2^{2^k} \sum_{s=0}^{n-\rho n} C_{n-\rho n}^s \sum_{s_1+s_2=s} C_s^{s_1} \left(\sum_{i \in M_2} \frac{s_1!}{i!} \right) \left(\sum_{i \in M_1} \frac{s_2!}{i!} \right) \\ \times \sum_{s'=0}^{\rho n-r} C_{\rho n}^{s'} \sum_{s'_1+s'_2=s'} C_{s'}^{s'_1} \left(\sum_{j \in \tilde{M}_2} \frac{s'_1!}{j!} \right) \left(\sum_{j \in \tilde{M}_1} \frac{s'_2!}{j!} \right) Q.$$

Relations (36), (38), (44), and (45) prove (41).

Now we introduce condition G_2 : let inequality (40) hold and let there exist $i \in M_2$ and (or) $j \in \tilde{M}_2$ such that $i \in (r/\ln n, r/E_n]$ and (or) $j \in (r/\ln n, r/E_n]$.

Put

$$p_4 = p_3 - S_4,$$

where

$$S_4 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_2)}^{(\Delta)}(n, k; Q).$$

The definition of $S_{(G_2)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in the sum (8) satisfies condition G_2 .

We show that

$$(46) \quad S_4 \leq \frac{2^{2^k} 2^{mk}}{2^m} \exp \left\{ -2^{-k} (1 - e^{-2\varepsilon}) N + \frac{2^k \varepsilon \ln^2 n}{E_n} \ln \left(\frac{\tilde{\rho} n \varepsilon E_n}{2^k \varepsilon \ln^2 n} \right) \right\}.$$

Similarly to the proof of (44) we obtain

$$(47) \quad Q \leq 2^{zN} \exp \{ -2^{-k} (1 - e^{-2\varepsilon}) N \}$$

if condition G_2 holds. Note that the constant $\tilde{A}_n = 2\varepsilon/\ln n$ substitutes the constant $A_n = 2\varepsilon/E_n$ in the proof.

If the indices i and j satisfy condition G_2 , then bound (46) follows from (36) and (47) similarly to the proof of the corresponding bound for S_3 .

The following condition is called G_3 : let inequality (40) hold and let

$$(48) \quad 0 \leq i \leq \frac{r}{\ln n} \quad \text{and} \quad 0 \leq j \leq \frac{r}{\ln n}$$

for all $i \in M_2$ and $j \in \tilde{M}_2$. Put

$$(49) \quad p_5 = p_4 - S_5,$$

where

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

The definition of $S_{(G_3, 2^z-2)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies condition G_3 and that $\Delta < 2^z - 1$.

We show that

$$(50) \quad S_5 \leq \frac{2^{2^k} 2^{mk}}{2^m} \exp \{ -2^{-k} N + 2^k \varepsilon \ln^2 n + 2^k u \}.$$

Using (40) and inequality (10), we get

$$(51) \quad \Gamma_{t,k}^{\omega_\alpha} \geq C_r^{t-1} (s^{(\alpha)} + \tilde{s}^{(\alpha)})$$

for all $t \in \{2, \dots, r\}$ and $\alpha = 1, \dots, \Delta$, where

$$s^{(\alpha)} = \sum_{i \in I_{\omega_\alpha}} i, \quad \tilde{s}^{(\alpha)} = \sum_{j \in J_{\omega_\alpha}} j.$$

According to (4),

$$(52) \quad \left| \prod_{t=1}^{g_i(n)} (1 - 2p_{it})^{\Gamma_{t,k}^{\omega_\alpha}} \right| \leq \prod_{t \in T_i} (1 - 2\delta_{it}(n))^{\Gamma_{t,k}^{\omega_\alpha}}$$

for $i = 1, \dots, N$ and $\alpha = 1, \dots, \Delta$.

Now we apply (51) to the right hand side of (52). Then

$$(53) \quad \prod_{t \in T_i} (1 - 2\delta_{it}(n))^{\Gamma_{t,k}^{\omega_\alpha}} \leq \exp \left\{ -\frac{2\delta_i}{\sqrt[n]{n}} (s^{(\alpha)} + \tilde{s}^{(\alpha)}) \right\}.$$

The inequality $e^{-y} \leq 1 - y/2, 0 \leq y < 1$, implies that

$$(54) \quad \exp \left\{ -\frac{2\delta_i}{\sqrt[n]{n}} (s^{(\alpha)} + \tilde{s}^{(\alpha)}) \right\} \leq 1 - \frac{\delta_i}{\sqrt[n]{n}} (s^{(\alpha)} + \tilde{s}^{(\alpha)})$$

for $i = 1, \dots, N$ and $\alpha = 1, \dots, \Delta$. In turn, inequality (54) yields

$$\begin{aligned}
 & 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_3)}^{(\Delta)}(n, k; Q) \\
 & \leq 2^{-kN} 2^{2^k} (\Delta + 1)^N \\
 & \times \sum_{s=0}^{n-\rho n} C_{n-\rho n}^s \sum_{s_*=0}^s R_1^{s-s_*} \left(\sum_{\sum_{i \in M_2} i = s_*} \frac{s!}{(s-s_*)!} \left(\prod_{i \in M_2} i! \right)^{-1} \right) \\
 & \times \sum_{s'=0}^{\rho n} C_{\rho n}^{s'} \sum_{\tilde{s}_*=0}^{s'} \tilde{R}_1^{s'-\tilde{s}_*} \left(\sum_{\sum_{j \in \tilde{M}_2} j = \tilde{s}_*} \frac{s'!}{(s'-\tilde{s}_*)!} \left(\prod_{j \in \tilde{M}_2} j! \right)^{-1} \right) \\
 & \times \exp \left\{ -2^{-z} \sum_{i=1}^N \frac{\delta_i}{\sqrt[6]{n}} \sum_{\alpha=1}^{\Delta} (s^{(\alpha)} + \tilde{s}^{(\alpha)}) + 2^k u \right\}, \quad s + s' \geq 1,
 \end{aligned}
 \tag{55}$$

where the definition of $S_{(G_3)}^{(\Delta)}(n, k; Q)$ differs from that of $S^{(\Delta)}(n, k; Q)$ in the restriction that the indices in the sum (8) satisfy condition G_3 .

If $\Delta < 2^z - 1$, then (55) implies bound (50) by condition (3), inequalities (36),

$$\max\{s_*, \tilde{s}_*\} \leq 2^k \varepsilon \ln n,$$

and

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

where

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

Now let $\Delta = 2^z - 1$. Put

$$p_6 = p_5 - S_6,$$

where

$$S_6 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_3, 2^z-1)}^{(\Delta)}(n, k; Q).$$

The definition of $S_{(G_3, 2^z-1)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies condition G_3 and $\Delta = 2^z - 1$. If condition G_3 holds and $\Delta = 2^z - 1$, then we use condition (3) and relations (36) and (55) together with inequality (56) to find a bound for S_6 :

$$S_6 \leq 2^{2^k} 2^{mk} \exp \left\{ -2^{-2k} \sum_{i=1}^N \delta_i + k + \ln(\tilde{\rho}n) - m \ln 2 \right\}$$

for the case of

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

Now we show that there exists $\alpha \in \{1, 2, \dots, \Delta\}$ such that $\xi_\alpha \leq 2$ if $\Delta = 2^z - 1$, $1 \leq z \leq k$, and either $z \in \{k, k-1\}$ or $k \in \{1, 2\}$. Indeed, if either $z = k$ or $k \in \{1, 2\}$, then this property is obvious. If $z = k-1$, then we derive this property from Remark 2.2 in [1].

Consider condition G_4 : let inequality (40) hold and let

$$(59) \quad s_* + \tilde{s}_* = 0,$$

$$(60) \quad \xi_\alpha \geq 3, \quad \alpha = 1, \dots, \Delta, \quad \Delta = 2^z - 1, \quad 1 \leq z \leq k - 2, \quad 3 \leq k < \infty.$$

Put

$$p_7 = p_6 - S_7$$

and

$$S_7 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_4)}^{(\Delta)}(n, k; Q),$$

where the definition of $S_{(G_4)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies conditions G_4 .

Now we obtain a bound for S_7 . If (59) holds, $\Delta = 2^z - 1$, and $\tilde{R}_1 < 2^{k-z} - 1$, then we rewrite bound (55) as follows:

$$(61) \quad \begin{aligned} S_7 &\leq 2^{2^k+1+zN-kN} \sum_{s=0}^{n-\rho n} C_{n-\rho n}^s |M_1|^s \sum_{\substack{s'=0 \\ s'+s \geq 1}}^{\rho n} C_{\rho n}^{s'} |\tilde{M}_1|^{s'} \\ &\leq \frac{2^{2^k+1+mk}}{2^m} (1 - 2^{1-k})^{\rho n} \end{aligned}$$

(here we used restrictions (36)).

It remains to check that

$$(62) \quad S_8 \leq \frac{2^{2^k} 2^{mk}}{2^m} \exp \left\{ -\rho n 2^{-k+1} + \varepsilon \ln^2 n \ln \left(\frac{\rho n e}{\varepsilon \ln^2 n} \right) \right\}$$

if the conditions G_4 hold and

$$(63) \quad \tilde{R}_1 = 2^{k-z} - 1,$$

where

$$p_7 = S_8 = 2^{-kN} \sum_{\Delta=1}^{2^k-1} S_{(G_4, \tilde{R}_1)}^{(\Delta)}(n, k; Q).$$

Here the definition of $S_{(G_4, \tilde{R}_1)}^{(\Delta)}(n, k; Q)$ differs from that of the term $S^{(\Delta)}(n, k; Q)$ in that the index of summation s' in (8) satisfies conditions G_4 and (63).

Similarly to the proof in [1] and according to Proposition 2.2 in [1] we conclude from (63) and G_4 that there exists at least one element $j_* \in \tilde{M}_1$ such that $j_* \leq r$. Therefore, under the assumptions of the theorem and conditions G_4 and (63), we get

$$\begin{aligned} S_8 &\leq 2^{2^k} 2^{-kN} 2^{zN} 2^{(k-z)(n-\rho n)} \sum_{\substack{s'=0 \\ s+s' \geq 1}}^{\rho n-r} C_{\rho n}^{s'} \sum_{\sum_{j \in \tilde{M}_1} j = s'} \frac{s'!}{\prod_{j \in \tilde{M}_1} j!} \\ &= 2^{2^k} 2^{-kN} 2^{zN+(k-z)(n-\rho n)} \sum_{\substack{s'=0 \\ s+s' \geq 1}}^{\rho n-r} C_{\rho n}^{s'} \sum_{\substack{s'_1+j_* = s' \\ j_* \leq r}} C_{s'_1}^{s'_1} \left(\sum_{\sum_{j \in \tilde{M}_1 \setminus j_*} j = s'_1} \frac{s'_1!}{\prod_{j \in \tilde{M}_1 \setminus j_*} j!} \right) \\ &\leq 2^{2^k} 2^{(k-z)m} \left(1 - \frac{1}{2^{k-z}} \right)^{\rho n} \sum_{j_*=0}^r C_{\rho n}^{j_*}. \end{aligned}$$

Applying inequality (31) we prove bound (62).

Considering conditions G_0 – G_4 , we make sure that they exhaust all possible cases of summation in (8) with respect to the parameters $s, s', i, j, i \in I$ and $j \in J$ for which inequality (16) holds if $\Delta \geq 1$.

Therefore relations (39), (41), (46), (50), (57), (61), and (62) prove (33) under the assumptions of the lemma. Then, by (18), (32), and (33), we find that $\mathbf{E} \nu_n^{[k]} = \lambda^k + \Delta(k, n)$, where

$$(64) \quad \Delta(k, n) = \psi(k, n) + p_1,$$

$$(65) \quad \begin{aligned} & - \left\{ 2^{(m+1)k} u + 2^{mk} \Theta_2 (1 + 2^k u) \right\} \\ & \leq \psi(k, n) \leq 2^{(m+1)k+1} u + 2^{mk} \Theta_2 (1 + 2^{k+1} u). \end{aligned}$$

Using relations (33) and (65), we complete the proof of (13) and (14). \square

3. PROOF OF THE THEOREM

Fix an integer $q \geq 0$. Consider the following inequality:

$$(66) \quad \left| \mathbf{P}\{\nu_n = q\} - \frac{\lambda^q}{q!} e^{-\lambda} \right| \leq R_1 + R_2 + R_3,$$

where

$$\begin{aligned} R_1 &= \left| \mathbf{P}\{\nu_n = q\} - \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q B_{kn} \right|, \\ R_2 &= \left| \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q \left\{ B_{kn} - \frac{\lambda^k}{k!} \right\} \right|, \\ R_3 &= \left| \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q \frac{\lambda^k}{k!} - \frac{\lambda^q}{q!} e^{-\lambda} \right|, \end{aligned}$$

and B_{kn} denotes the binomial moment of order k for the random variable ν_n . Choose n such that

$$(67) \quad \frac{\lambda^{q+2\nu}}{q! (2\nu)!} < \left(\frac{2e\lambda}{\gamma} \right)^\gamma,$$

where $2\nu = \gamma - q \geq 0$. Such a number n exists in view of $n \geq 2^{6q}$. The inequality

$$(68) \quad R_3 < \frac{\lambda^{q+2\nu}}{q! (2\nu)!}$$

together with (67) implies that

$$(69) \quad R_3 < \left(\frac{2e\lambda}{\gamma} \right)^\gamma.$$

Applying (13) we prove that

$$\begin{aligned}
 & \left| B_{q+2\nu,n} - \frac{\lambda^{q+2\nu}}{(q+2\nu)!} \right| \\
 &= \frac{1}{(q+2\nu)!} |\Delta(q+2\nu, n)| \\
 (70) \quad & \leq \frac{2^{(q+2\nu)m}}{(q+2\nu)!} (2^{q+2\nu+1}B(n) + \Theta_2 (1 + 2^{q+2\nu+1}B(n))) \\
 & \quad + \frac{2^{(q+2\nu)m}}{(q+2\nu)!} \left(7 \exp \left\{ -2^{-2\gamma} \sum_{i=1}^N \delta_i + (q+2\nu) + \sqrt[q]{n} + \ln(\tilde{\rho}n) - m \ln 2 \right\} \right).
 \end{aligned}$$

Taking into account (12), we get

$$(71) \quad \left| B_{q+2\nu,n} - \frac{\lambda^{q+2\nu}}{(q+2\nu)!} \right| \leq \frac{2^{m\gamma}}{\gamma!} (2^{\gamma+1}B(n) + \Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1).$$

By Bonferroni's inequality [3],

$$(72) \quad 0 \leq P\{\nu_n = q\} - \sum_{k=q}^{q+2\nu-1} (-1)^{k-q} C_k^q B_{kn} \leq C_{q+2\nu}^q B_{q+2\nu,n}.$$

Using (67) and (72), we derive from (71) that

$$(73) \quad R_1 < \left(\frac{2e\lambda}{\gamma} \right)^\gamma (1 + 2^{\gamma+1}B(n) + \Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1).$$

Consider

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

It is easy to show that

$$(74) \quad \sup_{q \leq k \leq q+2\nu-1} C_k^q \left| B_{kn} - \frac{\lambda^k}{k!} \right| \leq e^{4\lambda} B(n) + e^{2\lambda} (\Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1)$$

by (12)–(14). Inequality (74) implies

$$(75) \quad R_2 < \sum_{k=q}^{q+2\nu-1} C_k^q \left| B_{kn} - \frac{\lambda^k}{k!} \right| \leq e^{4\lambda} \gamma B(n) + e^{2\lambda} \gamma (\Theta_2 (1 + 2^{\gamma+1}B(n)) + 7\Theta_1).$$

Thus (66), (69), (73), and (75) imply (6). The theorem is proved.

BIBLIOGRAPHY

1. V. I. Masol, *A theorem on the limit distribution of the number of false solutions of a system of nonlinear random Boolean equations*, Teor. Veroyatnost. i Primenen. **43** (1998), no. 1, 41–56; English transl. in Theory Probab. Appl. **43** (1999), no. 1, 75–88. MR1669972 (2000f:60040)
2. W. Feller, *An Introduction to Probability Theory and its Applications*, 3rd ed., vol. I, John Wiley & Sons, New York–London–Sydney, 1968. MR0228020 (37:3604)
3. V. N. Sachkov, *Introduction to Combinatorial Methods of Discrete Mathematics*, “Nauka”, Moscow, 1982. (Russian) MR700691 (85g:05001)

DEPARTMENT OF PROBABILITY THEORY AND MATHEMATICAL STATISTICS, FACULTY FOR MECHANICS AND MATHEMATICS, NATIONAL TARAS SHEVCHENKO UNIVERSITY, ACADEMICIAN GLUSHKOV AVENUE 6, KYIV 03127, UKRAINE

E-mail address: `vimasol@ukr.net`

DEPARTMENT OF PROBABILITY THEORY AND MATHEMATICAL STATISTICS, FACULTY FOR MECHANICS AND MATHEMATICS, NATIONAL TARAS SHEVCHENKO UNIVERSITY, ACADEMICIAN GLUSHKOV AVENUE 6, KYIV 03127, UKRAINE

E-mail address: `mslob@ukr.net`

Received 10/FEB/2006

Translated by S. KVASKO