УДК 519.21 **Поперешняк С.В.**

ПРО ШВИДКІСТЬ ЗБЛИЖЕННЯ РОЗПОДІЛІВ РАНГУ ВИПАДКОВОЇ РОЗРІДЖЕНОЇ МАТРИЦІ У ПОЛІ $GF(2)$ ТА ПУАССОНА

Вступ

Розвиток технічних засобів збереження, обробки та передачі інформації вимагає на сучасному етапі поглиблених досліджень характеристик випадкової матриці над полем, що складається з двох елементів, та удосконалені шляхів їх практичного застосування.

Знання розподілів характеристик випадкових матриць над полем, що складається з двох елементів використовується в задачах захисту інформації від несанкціонованого доступу, кодуванні інформації для передачі її каналами зв'язку, розпізнавання, класифікації тощо.

Однією з пріоритетних характеристик випадкових матриць над скінченним полем є її ранг. Вивчення розподілу рангу зазначених матриць розпочалося наприкінці 19 століття (Landsberg G. (1895)) і особливо велику увагу привернуло до себе з середини 20 століття, про що свідчать роботи Slepian D. (1955), Erdös P., Renyi A.(1963), Коваленка І.М. (1965, 1975), Козлова М.В.(1966), Левитської А.О.(1986) та інших авторів.

Інтерес фахівців спрямований, головним чином, на отримання розподілу рангу матриці при різноманітних припущеннях щодо розподілу елементів матриці, кількості рядків та стовпців в ній тощо.

Загальна характеристика робіт по дослідженню розподілу рангу випадкової матриці у полі $GF(2)$

Розглянемо матрицю A, $A=\|a_{tj}\|$ $t=\overline{1,T}$, $j=\overline{1,n}$, у полі $GF(2)$, що складається з двох елементів; $a_{tj}\in GF(2)$, $t=\overline{1,T}$, $j=\overline{1,n}$. Тут $T(n)-$ кількість рядків(стовпців) матриці A.

Наприкінці 19 століття з'явилися перші публікації про розподіл рангу матриці A, $r(A)$, утвореної випадковими величинами (див., наприклад, [1]). З часом потреби кодування інформації та передачі її каналами зв'язку привели до значного зростання робіт в напрямку дослідження розподілу $r(A)$.

Фундаментальні теореми Коваленка І.М. (1975) про область інваріантності розподілу рангу випадкової матриці у полі $GF(2)$, що складається з двох елементів, вплинули на формування подальших напрямків наукових досліджень ([2]). У статті [2] знайдено за певних умов граничний $(n\to\infty)$ розподіл рангу матриці A (яка має також назву "булева матриця") і визначена область інваріантності граничного $(n\to\infty)$ значення ймовірності $\mathrm{P}\{r(A)=k\}$, $k\ge 0$, від вигляду розподілів випадкових елементів матриці A. Один з напрямів стосується вивчення розподілу рангу матриці поза областю інваріантності Коваленка І.М. Аналіз публікацій Балакіна Г.В. (1968), Масола В.І. (1980), Blömer J., Karp R., Welrl E. (1997), Cooper C. (2000), Колчіна В.Ф. (2004) та інших авторів засвідчив, що у переважній більшості з них розглядається розподіл рангу слабкозаповненої матриці, утвореної незалежними однаково розподіленими випадковими елементами.

Результати роботи Cooper C. (2000) дають граничний ($n\to\infty$) розподіл рангу сильнозаповненої ($n\times n$)-матриці (також утвореної незалежними однаково розподіленими елементами) при певних обмеженнях на кількість одиничних рядків та стовпців в ній.

Проте існуючи прикладні задачі потребують розробок які врахували б залежність розподілів елементів матриці як слабкозаповненої, так і сильнозаповненої, від місць їх (елементів) розташування. Тому актуальними є задачі дослідження розподілів рангів слабкозаповнених випадкових матриць, утворених не обов'язково однаково розподіленими елементами.

Актуальними є також проблеми оцінювання швидкості збіжності до граничних значень вказаних розподілів. Про підвищення інтересу до отримання оцінок та асимптотичних формул, які можуть бути застосовані в задачах перетворення інформації, побудови

випадкових функцій тощо, свідчать публікації Савчука М.М.(2003, 2004), Ковальчук Л.В. (2006), Міхайлова В.Г.(1998, 2000, 2001), Наконечного О.М (2005) та інших фахівців.

Постановка задачі.

Матриця A над полем $GF(2)$, що складається з двох елементів, називається розрідженою булевою матрицею, якщо ймовірність появи в ній одиниці на позиції з номером (i, j) дорівнює $1/n\left(\ln n + x_{ij}\right)$, де $\left|x_{ij}\right| \le c$, $c = const$, $i = \overline{1,T}$, $j = \overline{1,n}$, $T / n /$ - число рядків /стовпців/ матриці A.

В роботах [3], [4] різними методами встановлено граничний пуассонівський розподіл рангу $r(A)$ випадкової розрідженої булевої матриці A, коли $T = T(n)$ і $n \to \infty$. Для скінчених значень параметрів T і n розподіл рангу $r(A)$ може бути представлений через відповідні вирази для факторіальних моментів випадкової величини $r(A)$, що встановлені в [5]. Асимптотика цих моментів при певних умовах, зокрема, $x_{ij} = x_i$, $i = \overline{1,T}$, $j = \overline{1,n}$ $n - T = const$ при $n \to \infty$ наведені в ([6], теорема 4).

Питання про швидкість зближення розподілу рангу зазначеної матриці A до розподілу Пуассона з належним чином підібраним параметром до цього часу не розглядалось. Дослідженню цього питання присвячена дана робота.

Підгрунтям для доведення основного результату статті (теореми 1) слугує теорема про швидкість зближення в схемі Пуассона [7, с.67]. Зазначимо також, що на відміну від [3], [4] в даній роботі розглядається випадкова матриця A, розподіли елементів якої можуть залежати від місць їх (елементів) розташування.

Основний результат

Нехай елементи $T \times n$ матриці $A = \left\| a_{ij} \right\|$, $i = \overline{1,T}$, $j = \overline{1,n}$, - незалежні випадкові величини, які набувають значення у полі $GF(2)$ і мають наступний розподіл

$$P\{a_{ij} = 1\} = 1 - P\{a_{ij} = 0\} = \frac{\ln n + x_{ij}}{n}, \tag{1}$$

де

$$\left|x_{ij}\right| \le c, \; c = const, \; i = \overline{1,T}, \; j = \overline{1,n}. \tag{2}$$

Будемо вважати, що матриця A має принаймні n_0 стовпців так, що для $n \ge n_0$ задання розподілів (1) є коректним.

Позначимо $r(A)$ ранг матриці A і покладемо

$$\lambda = \frac{1}{n}\sum_{i=1}^{T} \exp\left\{-\frac{1}{n}\sum_{j=1}^{n} x_{ij}\right\}. \tag{3}$$

Теорема 1. *Нехай виконуються умови (1), (2),*

$$\frac{T}{n} \le 1 - \frac{\log_2 \ln n}{(\ln n)^q}, \;\; q = const, \;\; 0 < q < 1, \tag{4}$$

$$\lim_{n\to\infty} \frac{T}{n} > 0. \tag{5}$$

Тоді для к, к=0,1,2,...,

$$\left| P\{r(A) = T - k\} - \frac{e^{-\lambda} \cdot \lambda^k}{k!} \right| \le 2(1+\delta) c(n,k) \frac{\ln^4 n}{n(\ln \ln n)^2},$$

де $1 < \underline{\lim}_{n\to\infty} c(n,k) \le \overline{\lim}_{n\to\infty} c(n,k) \le e^{e^c}$, $\delta > 0$, $\delta = const$.

Зауваження. Явний вигляд коефіцієнта $c(n,k)$ дає рівність (23).

Допоміжні твердження

Позначимо $\xi_{n,T}$ число нульових рядків матриці А.

Лема 1. *При виконані умов (1) та (2) для розподілу випадкової величини* $\xi_{n,T}$ *справджується нерівність* $\left|P\{\xi_{n,T}=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le Q(n,k)$, *де* $Q(n,k)=\frac{\ln^2 n}{n}c_1(n,k)$ *і*

$0<\underline{\lim}_{n\to\infty}c_1(n,k)\le\overline{\lim}_{n\to\infty}c_1(n,k)\le e^{-1}$ *при* $к=0$, $0<\underline{\lim}_{n\to\infty}c_1(n,k)\le\overline{\lim}_{n\to\infty}c_1(n,k)\le\frac{k^k}{k!}e^{-k}\max\left(k,e^c\right)$ *при* $k\ge 1$.

Доведення. Ймовірність $p_n^{(i)}$ того, що *i*-тий рядок матриці А складається повністю з нулів, дорівнює, очевидно, $p_n^{(i)}=\prod_{j=1}^{n}\left(1-\frac{\ln n+x_{ij}}{n}\right)$, $i=\overline{1,T}$.

Покладемо $a=p_n^{(1)}+p_n^{(2)}+...+p_n^{(n)}$.

Згідно з теоремою Пуассона [5, с. 67] маємо

$$\left|P\{\xi_{n,T}=k\}-\frac{e^{-a}\cdot a^k}{k!}\right|\le\sum_{i=1}^{T}\left(p_n^{(i)}\right)^2. \tag{6}$$

Застосовуючи нерівність $p_n^{(i)}\le\frac{1}{n}\exp\left\{-\frac{1}{n}\sum_{j=1}^{n}x_{ij}\right\}$ у правій частині (6), знаходимо

$$\left|P\{\xi_{n,T}=k\}-\frac{e^{-a}\cdot a^k}{k!}\right|\le\frac{1}{n^2}\sum_{i=1}^{T}\exp\left\{-\frac{2}{n}\sum_{j=1}^{n}p_{ij}\right\}. \tag{7}$$

Оскільки

$$\lambda(1-\gamma_n)\le a\le\lambda, \tag{8}$$

де $\gamma_n=\left(\frac{\ln^2 n}{2n}\right)\frac{\left(1-c(\ln n)^{-1}\right)^2}{1-(\ln n-c)n^{-1}}$ (при обґрунтуванні (8) були використанні нерівності $-u-\frac{u^2}{2(1-u)}\le\ln(1-u)\le -u$ при $|u|<1$, $\prod_{i=1}^{n}(1-x_i)\ge 1-\sum_{i=1}^{n}x_i$, $0\le x_i\le 1$, $i=\overline{1,n}$), то з урахуванням оцінки $e^y\le 1+y\left(1+\frac{y}{2}e^y\right)$ для $y\ge 0$, маємо

$$-\lambda^{k+1}e^{-\lambda}\gamma_n\left(1+\frac{\lambda\gamma_n}{2}e^{\lambda\gamma_n}\right)\le\lambda^k e^{-\lambda}-a^k e^{-a}\le\lambda^k e^{-\lambda}k\gamma_n.$$

Звідси

$$\left|\lambda^k e^{-\lambda}-a^k e^{-a}\right|\le\lambda^k e^{-\lambda}\gamma_n\max\left\{k,\lambda\left(1+\frac{\lambda\gamma_n}{2}e^{\lambda\gamma_n}\right)\right\}. \tag{9}$$

Поєднання співвідношень (7) та (9) приводить до

$$\left|P\{\xi_{n,T}=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le\frac{1}{n^2}\sum_{i=1}^{T}\exp\left\{-\frac{2}{n}\sum_{j=1}^{n}p_{ij}\right\}+\frac{\lambda^k e^{-\lambda}}{k!}\gamma_n\max\left\{k,\lambda\left(1+\frac{\lambda\gamma_n}{2}e^{\lambda\gamma_n}\right)\right\},$$

або

$$\left|P\{\xi_{n,T}=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le Q(n,k),$$

де

$$Q(n,k)=\frac{\ln^2 n}{n}c_1(n,k), \tag{10}$$

$$c_1(n,k)=\frac{1}{n\ln^2 n}\sum_{i=1}^{T}\exp\left\{-\frac{2}{n}\sum_{j=1}^{n}p_{ij}\right\}+\frac{\lambda^k e^{-\lambda}}{2\,k!}\frac{\left(1-c(\ln n)^{-1}\right)^2}{1-(\ln n-c)n^{-1}}\max\left\{k,\lambda\left(1+\frac{\lambda\gamma_n}{2}e^{\lambda\gamma_n}\right)\right\},$$

$0<\underline{\lim}_{n\to\infty}c_1(n,k)\le\overline{\lim}_{n\to\infty}c_1(n,k)\le e^{-1}$ *при* $к=0$, $0<\underline{\lim}_{n\to\infty}c_1(n,k)\le\overline{\lim}_{n\to\infty}c_1(n,k)\le\frac{k^k}{k!}e^{-k}\max\left(k,e^c\right)$ *при* $k\ge 1$.

Лему 1 доведено.

Позначимо $S_1(A)$ максимальне число незалежних критичних наборів матриці А (див. [4, с. 147]), кожен з яких містить хоча б один ненульовий рядок.

Лема 2. *При виконанні умови (1) математичне сподівання випадкової величини* $S_1(A)$ *дорівнює*

$$MS_1(A)=\sum_{k=0}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\frac{1}{2^n}\prod_{j=1}^{n}\left(1+\prod_{s=1}^{k}\left(1-\frac{2\left(\ln n+x_{i_s j}\right)}{n}\right)\right)-\sum_{k=0}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}\prod_{j=1}^{n}\left(1-\frac{\ln n+x_{i_s j}}{n}\right).$$

Доведення. Скористаємось тим, що ймовірність того, що кількість успіхів в k незалежних випробуваннях з ймовірністю успіху p_i, $i=\overline{1,k}$, є парним числом, дорівнює $\frac{1}{2}+\frac{1}{2}\prod_{i=1}^{k}(1-2p_i)$.

(Переконатися у цьому неважко, використовуючи метод повної математичної індукції за параметром $k\ge 1$.)

Отже, для ймовірності того, що k рядків утворюють критичний набір маємо вираз $\frac{1}{2^n}\prod_{j=1}^{n}\left(1+\prod_{i=1}^{k}\left(1-\frac{2\left(\ln n+x_{ij}\right)}{n}\right)\right)$.

Зазначимо, що ймовірність того, що в k рядках немає жодної одиниці, дорівнює $\prod_{i=1}^{k}\prod_{j=1}^{n}\left(1-\frac{\ln n+x_{ij}}{n}\right)$.

Звідси неважко завершити доведення леми 2.

Покладемо $f(n)=(\ln\ln n)^{-1}(1+\delta_1)\ln n$, $\mu(n)=\sum_{k=0}^{f(n)}\sum_{1\le i_1<\ldots<i_k\le T}\exp\left\{-\sum_{s=1}^{k}\sum_{j=1}^{n}\frac{\ln n+x_{i_s j}}{n}\right\}$, $\delta_1=const$, $\delta_1>0$.

Лема 3. *Якщо виконуються умови (1), (2), (5) та*

$$T\le n, \tag{11}$$

то має місце

$$1<\underline{\lim_{n\to\infty}}\,\mu(n)\le\overline{\lim_{n\to\infty}}\,\mu(n)\le e^{e^c}. \tag{12}$$

Доведення. Дамо оцінку для $\mu(n)$ зверху. Суму $\mu(n)$ можна подати в наступному вигляді:

$$\mu(n)=\theta_1(n)-\theta_2(n), \tag{13}$$

де $\theta_1(n)=\sum_{k=0}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\exp\left\{-\sum_{s=1}^{k}\sum_{j=1}^{n}\frac{\ln n+x_{i_s j}}{n}\right\}$, $\theta_2(n)=\sum_{k=f(n)+1}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\exp\left\{-\sum_{s=1}^{k}\sum_{j=1}^{n}\frac{\ln n+x_{i_s j}}{n}\right\}$.

Введемо позначення $a_i=\frac{1}{n}\exp\left\{-\frac{1}{n}\sum_{j=1}^{n}x_{ij}\right\}$, $i=\overline{1,T}$. Тоді для $\theta_1(n)$ знаходимо

$$\theta_1(n)=\sum_{k=0}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}\frac{1}{n}\exp\left\{-\frac{1}{n}\sum_{j=1}^{n}x_{i_s j}\right\}=\sum_{k=0}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}a_{i_s}=\prod_{i=1}^{T}(1+a_i). \tag{14}$$

Із (14) випливає з урахуванням (3)

$$\theta_1(n)\le e^{\lambda}. \tag{15}$$

Оскільки $\theta_2(n)\ge 0$, то (13) та (15) дають співвідношення

$$\mu(n)\le e^{\lambda}. \tag{16}$$

Оцінимо $\mu(n)$ знизу.

$$\theta_1(n)=\prod_{i=1}^{T}(1+a_i)\ge\exp\left\{\sum_{i=1}^{T}a_i-\frac{1}{2}\sum_{i=1}^{T}a_i^2\right\}=e^{\lambda}\exp\left\{-\frac{1}{2n^2}\sum_{i=1}^{T}\exp\left(-\frac{2}{n}\sum_{j=1}^{n}x_{ij}\right)\right\}.$$

Отже $\mu(n)\ge e^{\lambda}\exp\left\{-\frac{1}{2n^2}\sum_{i=1}^{T}\exp\left(-\frac{2}{n}\sum_{j=1}^{n}x_{ij}\right)\right\}-\theta_2(n)$.

З останньої нерівності та (16) випливає

$$e^{\lambda}\exp\left\{-\frac{1}{2n^2}\sum_{i=1}^{T}\exp\left(-\frac{2}{n}\sum_{j=1}^{n}x_{ij}\right)\right\}-\theta_2(n)\le\mu(n)\le e^{\lambda}. \tag{17}$$

Для $\theta_2(n)$ знаходимо, враховуючи умову (2), що

$$\theta_2(n)=\sum_{k=f(n)+1}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}a_{i_s}\le\sum_{k=f(n)+1}^{T}\left(\frac{T\cdot const}{n}\right)^k\frac{1}{k!},$$

звідси, приймаючи до уваги (11),

$$\theta_2(n)\to 0\ \text{ при }\ n\to\infty. \tag{18}$$

В нерівності (17) переходимо до границі при $n\to\infty$ і в силу (18) та умов (2), (5) та (11) отримуємо (12).

Лему 3 доведено.

Покладемо $\Gamma(n)=u\left(1+\frac{u(1+\delta_1)}{2}e^{u(1+\delta_1)}\right),\ u=\frac{\ln^4 n}{n(\ln\ln n)^2}$.

Враховуючи громіздкість викладу матеріалу наступні декілька лем будуть наведені без доведення.

Лема 4. *Якщо виконуються умови (1), (2), то має місце нерівність*

$$\sum_{k=0}^{f(n)}\sum_{1\le i_1<\ldots<i_k\le T}\frac{1}{2^n}\prod_{j=1}^{n}\left(1+\prod_{s=1}^{k}\left(1-\frac{2(\ln n+x_{i_sj})}{n}\right)\right)\le\mu(n)+\mu(n)(1+\delta)\Gamma(n).$$

Лема 5. *Якщо виконуються умови (1), (2), (5) та (11), то має місце нерівність*

$$\sum_{k=0}^{f(n)}\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}\prod_{j=1}^{n}\left(1-\frac{\ln n+x_{i_sj}}{n}\right)\ge\mu(n)-c_2(n)\frac{\ln^3 n}{n\cdot\ln\ln n},$$

де $\frac{(1+\delta_1)}{2}<\underline{\lim}_{n\to\infty}c_2(n)\le\overline{\lim}_{n\to\infty}c_2(n)\le\frac{e^{e^c}}{2}(1+\delta_1)$.

Лема 6. *Якщо виконуються умови (1), (2), (5) та (11), то має місце нерівність*

$$\sum_{k:\frac{n}{2}\left(1-\frac{1}{\ln n}\right)\le k\le\frac{n}{2}\left(1+\frac{1}{\ln n}\right)}\binom{n}{k}\frac{1}{2^n}\sum_{l=f(n)}^{T}\binom{T}{l}\left(\left(1-\frac{2(\ln n-c)}{n}\right)^k\right)^l\le\left(\frac{c_3(n)}{f(n)}\right)^{f(n)}\cdot\frac{1}{\sqrt{f(n)}}\cdot c_4(n),$$

де $0<\underline{\lim}_{n\to\infty}c_3(n)\le\overline{\lim}_{n\to\infty}c_3(n)\le e^{2+c}$, $\lim_{n\to\infty}c_4(n)=(2\pi)^{-1/2}$.

Лема 7. *Якщо виконуються умови (1), (2), (4) та (5), то має місце нерівність*

$$\sum_{k=f(n)+1}^{T}\sum_{1\le i_1<\ldots<i_k\le T}\frac{1}{2^n}\prod_{j=1}^{n}\left(1+\prod_{s=1}^{k}\left(1-\frac{2(\ln n+x_{i_sj})}{n}\right)\right)\le c_5(n)\cdot(\ln n)^{-\frac{n\cdot c_6(n)}{(\ln n)^q}}+$$

$$+\left(\frac{c_3(n)}{f(n)}\right)^{f(n)}\cdot\frac{1}{\sqrt{f(n)}}\cdot c_4(n)+c_7(n)\cdot\exp\left\{-\frac{n}{2\ln^2 n}c_8(n)\right\},$$

де $\lim_{n\to\infty}c_5(n)=(2\pi)^{-1/2}$, $\lim_{n\to\infty}c_6(n)=1-q$, $\lim_{n\to\infty}c_8(n)=1$, $\sqrt{\frac{2}{\pi}}<\underline{\lim}_{n\to\infty}c_7(n)\le\overline{\lim}_{n\to\infty}c_7(n)\le\frac{e^{c+1}+e^{c-1}}{\sqrt{2\pi}}$.

Позначимо $S(A)$ максимальне число незалежних критичних наборів матриці A.

Лема 8. *При виконанні умов (1) та (2) для довільного к, к=0, 1, 2, . . . , має місце нерівність*

$$\left|P\{S(A)=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le 2MS_1(A)+Q(n,k),$$

де $MS_1(A)$ *знайдено в лемі 2, а* $Q(n,k)$ *- в лемі 1.*

Доведення. Враховуючи лему 1, маємо

$$\left|P\{S(A)=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le\left|P\{S(A)=k\}-P\{\xi_{n,T}(A)=k\}\right|+Q(n,k)=$$

$$=\left|P\{S_1(A)+\xi_{n,T}(A)=k\}-P\{\xi_{n,T}(A)=k\}\right|+Q(n,k).$$

Застосовуючи співвідношення $P\{S_1(A)+\xi_{n,T}=k\}=\sum_{l=0}^{k}P\{S_1(A)=l,\xi_{n,T}=k-l\}$,

$\left|P\{S_1(A)=0,\xi_{n,T}=k\}-P\{\xi_{n,T}=k\}\right|\le P\{S_1(A)\ge 1\}$ та нерівність Чебишева, знаходимо

$$\left|P\{S(A)=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le 2P\{S_1(A)\ge 1\}+Q(n,k)\le 2MS_1(A)+Q(n,k).$$

Лему 8 доведено.

Доведення теореми 1

Дамо оцінку для $MS_1(A)$. З цією метою позначимо для $k\ge 0$

$$\Delta_1(k)=\sum_{1\le i_1<\ldots<i_k\le T}\frac{1}{2^n}\prod_{j=1}^{n}\left(1+\prod_{s=1}^{k}\left(1-\frac{2(\ln n+x_{i_s j})}{n}\right)\right),\qquad \Delta_2(k)=\sum_{1\le i_1<\ldots<i_k\le T}\prod_{s=1}^{k}\prod_{j=1}^{n}\left(1-\frac{\ln n+x_{i_s j}}{n}\right)$$

і за допомогою леми 2 представимо $MS_1(A)$ у вигляді

$$MS_1(A)=\sum_{k=0}^{f(n)}\Delta_1(k)+\sum_{k=f(n)+1}^{T}\Delta_1(k)-\left(\sum_{k=0}^{f(n)}\Delta_2(k)+\sum_{k=f(n)+1}^{T}\Delta_2(k)\right).$$

Звідси $MS_1(A)\le \sum_{k=0}^{f(n)}\Delta_1(k)+\sum_{k=f(n)+1}^{T}\Delta_1(k)-\sum_{k=0}^{f(n)}\Delta_2(k)$.

В силу лем 4 та 5 знаходимо

$$\sum_{k=0}^{f(n)}\Delta_1(k)-\sum_{k=0}^{f(n)}\Delta_2(k)\le \mu(n)+\mu(n)(1+\delta)\Gamma(n)-\left(\mu(n)-c_2(n)\frac{\ln^3 n}{n\cdot\ln\ln n}\right)=$$

$$=\mu(n)(1+\delta)\Gamma(n)+c_2(n)\frac{\ln^3 n}{n\cdot\ln\ln n}. \tag{19}$$

Поєднуючи (19) з оцінкою суми $\sum_{k=f(n)+1}^{T}\Delta_1(k)$, отриманою в лемі 7, маємо

$$MS_1(A)\le \mu(n)(1+\delta)\Gamma(n)+F(n), \tag{20}$$

де

$$F(n)=c_2(n)\frac{\ln^3 n}{n\cdot\ln\ln n}+c_5(n)\cdot(\ln n)^{-\frac{n\cdot c_6(n)}{(\ln n)^q}}+$$

$$+\left(\frac{c_3(n)}{f(n)}\right)^{f(n)}\cdot\frac{1}{\sqrt{f(n)}}\cdot c_4(n)+c_7(n)\cdot\exp\left\{-\frac{n}{2\ln^2 n}c_8(n)\right\}. \tag{21}$$

Згідно (20) та леми 8 $\left|P\{S(A)=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le 2\left[\ \mu(n)(1+\delta)\Gamma(n)+F(n)\ \right]+Q(n,k)$.

Скориставшись явним виглядом $\Gamma(n)$, запишемо

$$\left|P\{S(A)=k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le 2(1+\delta)c_{11}(n)u+2F(n)+Q(n,k),$$

де

$$c_{11}(n)=\mu(n)+\mu(n)\frac{u}{2}(1+\delta)\exp\{u(1+\delta)\}, \tag{22}$$

З останньої нерівності та співвідношення $r(A)+s(A)=T$ (див. [2, с.148]) випливає

$$\left|P\{r(A)=T-k\}-\frac{e^{-\lambda}\cdot\lambda^k}{k!}\right|\le 2(1+\delta)c(n,k)\frac{\ln^4 n}{n(\ln\ln n)^2},$$

де

$$c(n,k)=c_{11}(n)+\frac{F(n)}{(1+\delta)u}+\frac{Q(n,k)}{2u(1+\delta)}, \tag{23}$$

$c_{11}(n)$, $F(n)$ та $Q(n,k)$ визначені відповідно рівностями (22), (21) і (10).

Граничний розподіл рангу випадкової розрідженої матриці у полі $GF(2)$

Теорема 2. ***I.*** *Нехай виконуються умови теореми 1 та*

$$\lambda\to\lambda_0 \quad при \quad n\to\infty \tag{24}$$

тоді $0<\lambda_0<\infty$ *і для к, к=0,1,2,... має місце співвідношення*

$$P\{r(A) = T - k\} \to e^{-\lambda_0} \frac{\lambda_0}{k!}, \quad n \to \infty \tag{25}$$

II. *Якщо виконуються умови (1), (2), (4), (24) та* $\lambda_0 > 0$, *то* $\lambda_0 < \infty$ *і має місце (25).*

З урахуванням теореми 1 доведення теореми 2 не викликає труднощів.

Наслідок. Якщо виконується умова (1), в якій $x_{ij} = x$, $i = \overline{1,T}$, $j = \overline{1,n}$, x - фіксоване число, і при $n \to \infty$ $\frac{T}{n} \to \alpha$, де $0 < \alpha < 1$, то має місце співвідношення (25), в якому $\lambda_0 = \alpha e^{-x}$.

Для доведення наслідку достатньо помітити, що умови першої (або другої) частини теореми 2 виконуються тривіальним чином при виконанні умов наслідку.

Зауваження 2. Результат наведеного вище наслідку отримано, зокрема, в ([3], теорема 1) та в ([4], теореми 3.1.1 та 3.3.1).

Висновки.У статті знайдені оцінки швидкості зближення розподілу рангу випадкової розрідженої булевої матриці до розподілу Пуассона (теорема 1). За допомогою теореми 1 отримана теорема 2, яка узагальнює відомий результат про граничний розподіл рангу зазначеної матриці на випадок, коли розподіли її елементів залежать від місць їх (елементів) розташування, а відношення числа рядків до числа стовпців матриці не перевищує $1 - \gamma(n)$, де $\gamma(n)$ повільно прямує до нуля, набуваючи лише додатних значень.

Список літератури

1. *Landsberg G.* Uber eine Anzhlbestimmung und eine damit Zusammenhangende Reihe // J. Reine Angew. Math. – 1895. – III . – P. 87–88.
2. *Коваленко И.Н.* О теоремах инвариантности для случайных булевых матриц // Кибернетика. – 1975. – . 5. – С. 138–152.
3. *Балакин Г.В.* Распределение ранга случайных матриц над конечным полем. // Теория вероятностей и её применения. – 1968. – в. XIII, №4. – С. 631-641.
4. *Колчин В.Ф.* Случайные графы. – М.: Физматлит, 2004. – 256 с.
5. *Masol V.I.* Moments of the number solutions of system of random Boolean equations// Random Oper. and Stoch. Equations. – 1993. – 1, N 2. – pp. 171-179.
6. *Masol V.I.* Theorems of invariance for systems of random Boolean equations// Sixth Intern. Vilnus Conf. of Probability Theory and Math. Statist.: Abstr. of Communic. – 1993. – pp. 19-20.
7. *Севастьянов Б.А.* Курс теории вероятностей и математической статистики. – М.: Наука, 1982. – 256 с.

Рецензент: д.т.н., проф. Петров О.С.

Надійшла 06.04.2010 р.