УДК 519.21

С.В. Поперешняк, к.ф.-м.н., доц.

ГРАНИЧНИЙ РОЗПОДІЛ РАНГУ СИЛЬНОЗАПОВНЕНОЇ ВИПАДКОВОЇ МАТРИЦІ В ПОЛІ GF(2)

Національний авіаційний університет
E-mail: Svitlana.Popereshniak@livenau.net

Отримано теорему про асимптотику $(n \to \infty)$ *розподілу рангу випадкової матриці в полі GF(2) з* T *незалежних випадкових* n*-вимірних рядків за умови відсутності в ній одиничних ліній та в припущенні, що різниця між числом рядків* T *та числом стовпців* n *матриці є фіксоване число довільного знаку,* $T - n = const$.

Ключові слова: випадкова матриця, граничний розподіл рангу, поле GF(2), сильнозаповнена матриця.

Вступ

Інтерес до знаходження розподілів характеристик слабко- та сильнозаповнених випадкових матриць над скінченним полем викликаний прикладними аспектами теорії кодування інформації і захисту її від несанкціонованого доступу, теорії розпізнавання і класифікації. До зазначених характеристик відносять, в першу чергу, ранг матриці і перманентний ранг.

Аналіз досліджень і публікацій

Дослідження характеристик випадкової $(T \times n)$-матриці A, $A = \|a_{tj}\|$, $t = \overline{1,T}$, $j = \overline{1,n}$ у припущенні $p \to 1$, $n \to \infty$, де $p = \mathrm{P}\{a_{tj} = 1\}$, описано в працях [1; 2].

Зокрема, в праці [1] розглянуто питання про розподіл перманента насиченої випадкової матриці A.

Матрицю A будемо називати сильнозаповненою випадковою матрицею, якщо

$$\mathrm{P}\{a_{tj} = 1\} = 1 - \mathrm{P}\{a_{tj} = 0\} = 1 - \frac{1}{n}(\ln n - x_{tj}),$$

де

$$-\infty < a \le x_{tj} < \ln n,$$

$a = \mathrm{const}$,

$t = \overline{1,T}$,

$j = \overline{1,n}$.

З умов теореми, наведеної в праці [2], випливає, що, якщо

$$p = 1 - \frac{\ln n - \omega}{n},$$

$\omega = o(\log\log n)$,

сильнозаповнена випадкова матриця A має розподіл рангу при $n \to \infty$, який збігається з $\pi(k;0;0)$, k – ціле фіксоване число, $k \ge 0$.

Таким чином, відкритим залишається питання про розподіл рангу сильнозаповненої матриці A у припущеннях $T - n = \mathrm{const}$, $n \to \infty$ та існування залежності розподілів елементів матриці A від місця їх розташування.

Мета роботи – отримати граничний $(n \to \infty)$ розподіл рангу за умови, що матриця коефіцієнтів не містить одиничних ліній, рядки матриці є незалежними випадковими n-вимірними (0, 1)-векторами.

Постановка задачі

Розглянемо систему рівнянь у полі GF (2) :

$$\sum_{j=1}^{n} x_j a_{tj} = 0,\ t = \overline{1,T}, \qquad (1)$$

де a_{tj}, $t = \overline{1,T}$, $j = \overline{1,n}$, – випадкові величини, які набувають значення в полі GF (2), $(x_1,...,x_n)$ – n-вимірний вектор невідомих величин, $x_j \in \mathrm{GF}(2)$ для $j = \overline{1,n}$.

Позначимо $L^{(1)}(r_0, s_0)$ подію, яка полягає у тому, що матриця коефіцієнтів $\|a_{tj}\|$ системи (1) має r_0 одиничних рядків та s_0 одиничних стовпців.

Покладемо ν_{nm_0} – кількість нетривіальних розв'язків системи (1), $m_0 = n - T$, m_0 – фіксоване число довільного знака.

Припустимо, що $a_t = (a_{t1},...,a_{tn})$, $t = \overline{1,T}$ – незалежні вектори в полі GF(2).

Сформулюємо теорему.

Теорема. Нехай для деяких послідовностей $m_q \to \infty$, $q \to \infty$, $\psi_n \to \infty$, $n \to \infty$,

$$\lim_{q\to\infty} \overline{\lim_{n\to\infty}} \left[M\left(\nu_{nm_q} / L^{(1)}(0,0) \right) - 2^{m_q} \right] \le 0;$$

$$\lim_{q\to\infty} \overline{\lim_{n\to\infty}} \sum_{0<|x|<\psi_n} M\left(\xi_{m_q}(x) / L^{(1)}(0,0)\right) = 0; \quad (2)$$

$$\lim_{q\to\infty} \lim_{n\to\infty} \max \left| P\left\{ \sum_{j=1}^{n} z_j^{(k)} a_{n-mj} = \varepsilon^{(k)} / \sum_{j=1}^{n} z_j^{(t)} \times \right.\right.$$

$$\left.\left. \times a_{n-mj} = \varepsilon^{(t)}, 1 \le t < k \right\} - \frac{1}{2} \right| = 0, \quad (3)$$

$$\varepsilon^{(1)},...,\varepsilon^{(k)} \in \{0,1\},\ k \ge 1,$$

де максимум береться по $m_0 \le m \le m_q$ і множині наборів $z^{(1)},...,z^{(k)}$ n-вимірних (0, 1)-векторів, для яких

$$\left| z^{(1)} + ... + z^{(k)} \right| = \left| z^{(1)} \right| + ... + \left| z^{(k)} \right|,$$

$$\left| z^{(k)} \right| \ge \alpha \psi_n,\ \alpha > 0.$$

Тоді

$$P\{\nu_{nm_0} = 2^k - 1 / L^{(1)}(0,0)\} = 0,$$

$$k < r, r = \max\{m_0, 0\},$$

$$\lim_{n\to\infty} P\{\nu_{nm_0} = 2^k - 1 / L^{(1)}(0,0)\} = 2^{-k(k-r)} \times$$

$$\times \left\{ \prod_{t=1}^{k-r} (1 - 2^{-t}) \right\}^{-1} \prod_{t=k+1}^{\infty} (1 - 2^{-t}),\ \ k \ge r.$$

Доведенню теореми будуть передувати допоміжні леми.

Допоміжні леми

Лема 1 [3]. Нехай $x^{(1)},...,x^{(r)}$ – лінійно незалежні розв'язки системи $(x, a_t) = 0$, $1 \le t \le n-m$, причому відомо, що нетривіальних розв'язків x, для яких $|x| < k_0$, не існує. Тоді матрицю

$$\left\| x_j^{(t)} \right\| = \left\| \begin{matrix} x_1^{(1)} \dots x_n^{(1)} \\ \dots\dots\dots \\ x_1^{(r)} \dots x_n^{(r)} \end{matrix} \right\|$$

комбінуванням рядків і перестановок стовпців можна привести до вигляду

$$A = \left\| \begin{matrix} \underbrace{111...1}_{k_1} & ... & ... & ... & ... \\ & \underbrace{111...1}_{k_2} & ... & ... & ... \\ & & \underbrace{111...1}_{k_3} & ... & ... \\ 0 & & & 1 & ... \\ & & & & \underbrace{111...1}_{k_r} ... \end{matrix} \right\|,$$

де

$$k_t \ge \frac{k_0}{2^{r-t}},\ 1 \le t \le r.$$

Лема 2. Нехай для деякої послідовності $m_q \to \infty$, $q \to \infty$,

$$\lim_{q\to\infty} \overline{\lim_{n\to\infty}} \left[M\left(\nu_{nm_q} / L^{(1)}(0,0) \right) - 2^{m_q} \right] \le 0. \quad (4)$$

Тоді

$$\lim_{q\to\infty} \lim_{n\to\infty} P\left\{ \nu_{nm_q} = 2^{m_q} - 1 / L^{(1)}(0,0) \right\} = 1. \quad (5)$$

Доведення. Якщо $m \ge 0$, випадкова величина ν_{nm} може дорівнювати або $2^m - 1$, або не менше, ніж $2^{m+1} - 1$. Звідси

$$(2^m - 1)\left[1 - P\{\nu_{nm} \ne 2^m - 1 / L^{(1)}(0,0)\}\right] +$$

$$+ (2^{m+1} - 1)\, P\{\nu_{nm} \ne 2^m - 1 / L^{(1)}(0,0)\} \le$$

$$\le M\left(\nu_{nm} / L^{(1)}(0,0)\right).$$

Отже,

$$P\{\nu_{nm} \ne 2^m - 1 / L^{(1)}(0,0)\} \le$$

$$\le \left(M\left(\nu_{nm} / L^{(1)}(0,0)\right) - 2^m + 1\right) 2^{-m}.$$

Тепер, приймаючи до уваги умову (4), маємо

$$P\left\{ \nu_{nm_q} \ne 2^{m_q} - 1 / L^{(1)}(0,0) \right\} \le 2^{-m_q},$$

звідки випливає, очевидно, співвідношення (5).

Доведення теореми

Використовуючи формулу повної ймовірності, отримуємо

$$P\{\nu_{nm} = 2^m - 1/L^{(1)}(0,0)\} =$$

$$= P\left\{\sum_{1\le|x|\le n} \xi_m(x) = 2^m - 1/L^{(1)}(0,0)\right\} =$$

$$= \sum_{\substack{a+b=2^m-1,\\ a\ge 0, b\ge 0}} P\left\{\sum_{1\le|x|<\psi_n} \xi_m(x) = a, \sum_{\psi_n\le|x|\le n} \xi_m(x) = \right.$$

$$\left. = b/L^{(1)}(0,0) \right\} = P\left\{\sum_{1\le|x|<\psi_n} \xi_m(x) = 0,\right.$$

$$\left.\sum_{\psi_n\le|x|\le n} \xi_m(x) = 2^m - 1/L^{(1)}(0,0)\right\} + \sigma_2,$$

де

$$\sigma_2 = \sum_{\substack{a+b=2^m-1\\ a>0, b\ge 0}} P\left\{\sum_{1\le|x|<\psi_n} \xi_m(x) = a,\right.$$

$$\left.\sum_{\psi_n\le|x|\le n} \xi_m(x) = b/L^{(1)}(0,0)\right\}.$$

Для σ_2 знаходимо за допомогою нерівності Чебишева

$$\sigma_2 \le \sum_{\substack{a+b=2^m-1\\ a>0, b\ge 0}} P\left\{\sum_{1\le|x|<\psi_n} \xi_m(x) \ge 1/L^{(1)}(0,0)\right\} \le$$

$$\le M\left(\sum_{1\le|x|<\psi_n} \xi_m(x)/L^{(1)}(0,0)\right).$$

Фіксуємо $\varepsilon > 0$ і візьмемо таке m, що

$$P\{\nu_{nm} = 2^m - 1/L^{(1)}(0,0)\} \ge 1-\varepsilon; \qquad (6)$$

$$M\left(\sum_{1\le|x|<\psi_n} \xi_m(x)/L^{(1)}(0,0)\right) \le \varepsilon. \qquad (7)$$

Якщо $n > n_\varepsilon$, нерівність (6) можна задовольнити за лемою 2, нерівність (7) – внаслідок виразу (2).

Тоді з імовірністю, не менше $1-2\varepsilon$, відбудеться подія L, яка полягає в тому, що система рівнянь

$$\sum_{j=1}^{n} a_{tj} x_j = 0,$$

$$t = \overline{1, n-m},$$

за умови $L^{(1)}(0,0)$ має рівно m лінійно незалежних розв'язків $z^{(1)}, z^{(2)}, \ldots, z^{(m)}$, причому розв'язків x, для яких $0 < |x| < \psi_n$, не існує.

За умови, що відбулася подія L за лемою 1 існують m лінійно незалежних розв'язків $x^{(1)}, x^{(2)}, \ldots, x^{(m)}$, для яких матрицю $(x_j^{(t)})$, $t = \overline{1,m}$, $j = \overline{1,n}$ можна привести до вигляду $\begin{pmatrix} b^{(1)} \\ \vdots \\ b^{(m)} \end{pmatrix}$, де вектор-рядок

$$b^{(i)} = \left(\underbrace{0\ldots0}_{t_1+\ldots+t_{i-1}} \underbrace{1\ldots1}_{t_i} \ldots\right),$$

$$t_0 = 0,$$

$$t_i \ge \psi_n/2^{m-1},\ i = \overline{1,m}.$$

Доповнимо тепер систему

$$\sum_{j=1}^{n} a_{tj} x_j = 0,\ t = \overline{1, n-m}$$

рівняннями

$$\sum_{j=1}^{n} a_{tj} x_j = 0,\ n-m < t < n-m',\ m_0 \le m' \le m.$$

Тоді за умови L існує базис $u^1, \ldots, u^s$ множини розв'язків доповненої системи

$$\sum_{j=1}^{n} a_{tj} x_j = 0,\ t = \overline{1, n-m'}, \qquad (8)$$

з матрицею коефіцієнтів, що не містить одиничних ліній, який можна привести до вигляду $\begin{pmatrix} c^{(1)} \\ \vdots \\ c^{(s)} \end{pmatrix}$, де вектор-рядок

$$c^{(t)} = \left(\underbrace{0\ldots0}_{\gamma_1+\ldots+\gamma_{t-1}} \underbrace{1\ldots1}_{\gamma_t} \ldots \right),$$

$\gamma_0 = 0$, $\gamma_t \geq \psi_n / 2^{s-t}$, $t = \overline{1,s}$.

Доповнимо систему (8) ще одним рівнянням

$$\sum_{j=1}^{n} a_{n-m'+1\,j}\, x_j = 0$$

так, щоб матриця коефіцієнтів системи

$$\sum_{j=1}^{n} a_{tj} x_j = 0,\ t = \overline{1, n-m'+1},$$

не містила одиничних ліній.

Якщо

$$\sum_{j=1}^{n} a_{n-m'+1\,j}\, c_j^{(t)} = 0,\ 1 \leq t \leq s,$$

то добавлене рівняння не змінить множини розв'язків системи.

У протилежному випадку вимірність множини розв'язків зменшується на одиницю.

Позначимо

$$J_l = \left\{ j : \sum_{k=1}^{l-1} \gamma_k < j \leq \sum_{k=1}^{l} \gamma_k \right\},\ l = \overline{1,s},$$

$$J_s = \left\{ j : \sum_{k=1}^{s} \gamma_k < j \leq n \right\}.$$

Нарешті, через $J_{l,\vec{\varepsilon}}$ позначимо підмножину J_l, для кожного елемента j якого j-й стовпчик матриці $\begin{pmatrix} c^{(1)} \\ \vdots \\ c^{(s)} \end{pmatrix}$ дорівнює s-вимірному вектору-стовпцю $\vec{\varepsilon}$.

Нехай відбулася подія L. Тоді

$$P\left\{ \sum_{j=1}^{n} a_{n-m'+1\,j}\, c_j^{(t)} = 0, 1 \leq t \leq s \right\} =$$

$$= \prod_{k=1}^{s} P\left\{ \sum_{j=1}^{n} a_{n-m'+1\,j}\, c_j^{(k)} = 0 \,/\, \sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(\gamma)} = 0, \right.$$

$$\left. k < \gamma \leq s \right\}. \qquad (9)$$

Усі події розглядаються за умови L.

Для $k = 1,2,\ldots,s$ маємо

$$\sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(k)} = \sum_{j \in J_k} a_{n-m'+1\,j} +$$

$$+ \sum_{l=k+1}^{s+1} \sum_{\vec{\varepsilon}:\varepsilon_k=1} \sum_{j \in J_{l,\vec{\varepsilon}}} a_{n-m'+1\,j}. \qquad (10)$$

Події

$$\sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(\gamma)} = 0,\ k < \gamma \leq s$$

накладають умови лише на потрійну суму у формулі (10). При будь-якому фіксованому значенні цієї потрійної суми рівність

$$\sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(k)} = 0$$

зводиться до рівності

$$\sum_{j \in J_k} a_{n-m'+1\,j} = \delta,\ \delta \in \mathrm{GF}(2).$$

Згідно з виразом (3) ймовірність такої рівності прямує до $1/2$, якщо $n \to \infty$. Звідси, приймаючи до уваги вираз (9), випливає, що за умови L

$$P\left\{ \sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(t)} = 0, 1 \leq t \leq s \right\} \to 2^{-s}, \qquad (11)$$

якщо $n \to \infty$.

Оскільки ймовірність $P\{L\}$ можна зробити як завгодно близькою до 1, а $P\left\{ \sum_{j=1}^{n} a_{n-m'+1\,j} c_j^{(t)} = 0, 1 \leq t \leq s/L \right\}$ як завгодно близькою до 2^{-s} при великих m і n, то

$$\lim_{n\to\infty} P\{\nu_{nm_0} = 2^k - 1/L^{(1)}(0,0)\} = p_\mu(k) =$$

$$= \lim_{m\to\infty} \lim_{n\to\infty} p_\mu^{(m)}(k),$$

де $p_\mu^{(m)}(k)$ визначається так.

Розглянемо випадкове блукання частинки в площині (t, j), яке починається з точки (m, m).

Якщо частинка розташована в точці (t, j), то на наступному кроці вона перейде або в точку $(t, j-1)$, або в точку $(t-1, j-1)$.

Зазначений крок блукання частинки відповідає дописуванню до системи нового рівняння

$$\sum_{\rho=1}^{n} a_{n-m'+1\rho} x_\rho = 0 .$$

Перехід частинки в точку $(t, j-1)$ відповідає події, при якій дописане рівняння не змінює множини розв'язків. Згідно з умовою (11) імовірність цієї події прямує до 2^{-t}, якщо $n \to \infty$. Тоді, якщо $k \geq 0$, $p_\mu^{(m)}(k)$ дорівнює ймовірності попадання частинки в точку (k, m).

Якщо $k < m$, очевидно

$$p_\mu^{(m)}(k) = 0 ,$$

отже,

$$p_\mu(k) = 0 .$$

Якщо $k = m$, з точки (m, m) в точку (μ, μ) існує єдиний шлях і

$$\lim_{n\to\infty} p_\mu^{(m)}(k) = \prod_{t=\mu+1}^{m} (1-2^{-t}) ,$$

тобто

$$p_\mu(\mu) = \prod_{t=\mu+1}^{\infty} (1-2^{-t}) .$$

Якщо $k > m$, буде $k-m$ переходів $(t, j) \to (t-1, j-1)$, тобто

$$\lim_{n\to\infty} p_\mu^{(m)}(k) = \prod_{t=k+1}^{m} (1-2^{-t}) \times$$

$$\times \sum_{k\leq t_1<\ldots<t_{k-\mu}\leq m} 2^{-t_1} \ldots 2^{-t_{k-\mu}},$$

звідки

$$p_\mu(k) =$$

$$= \prod_{t=k+1}^{\infty} (1-2^{-t}) \sum_{k\leq t_1<\ldots<t_{k-\mu}\leq\infty} 2^{-t_1} \ldots 2^{-t_{k-\mu}} =$$

$$= 2^{-k(k-\mu)} \prod_{t=k+1}^{\infty} (1-2^{-t}) \left\{ \prod_{t=k+1}^{k-\mu} (1-2^{-t}) \right\}^{-1} .$$

Теорема доведена.

Висновки

Отримано загальну теорему про асимптотику $(n \to \infty)$ розподілу рангу випадкової матриці в полі $\mathrm{GF}(2)$ з T незалежних випадкових n-вимірних рядків, за умови відсутності в ній одиничних ліній. За допомогою загальної теореми можна знайти граничний $(n \to \infty)$ розподіл рангу сильнозаповненої матриці, утвореної незалежними випадковими величинами з поля $\mathrm{GF}(2)$, за умови відсутності одиничних ліній та при $T - n = \mathrm{const},\ n \to \infty$.

Література

1. *Севастьянов Б.А.* Распределение вероятностей перманентов случайных матриц с независимыми элементами в поле GF(p) / Б.А. Севастьянов // Труды по дискретной математике. – М.: Физ.-мат. лит., 2000. – 3. – С. 235–248.

2. *Cooper C.* On the Rank of Random Matrices / C. Cooper // Random Structures and Algorithms. – 2000. – P. 209–232.

3. *Коваленко И.Н.* Об одной предельной теореме для определителей в классе булевых функций / И.Н. Коваленко // Доклады АН СССР. – 1965. – 161, № 3. – С. 517–519.

Стаття надійшла до редакції 02.07.2012.