

УДК 519.2

П.О. Єндовицький

ТОЧНА АСИМПТОТИЧНА ОЦІНКА РОЗМІРУ ГРУПИ В УЗАГАЛЬНЕННІ ПАРАДОКСУ ДНІВ НАРОДЖЕНЬ**Вступ**

Як правило, під парадоксом днів народжень розуміється наступна ймовірнісна схема [1, 2]. Нехай є група з n чоловік ($n \leq 365$). Будемо вважати, що день народження кожної людини з групи припадає з рівною ймовірністю на один із 365 днів. Нехай ймовірність того, що в групі знайдуться принаймні дві людини, в яких збігаються дні народження, дорівнює $P(n)$. Тоді розмір групи, де з ймовірністю $p = 1$ знайдуться принаймні дві людини з однаковими днями народження, дорівнює 366, а для $p < 1$ розмір групи буде значно меншим, наприклад $P(23) = 0,507\dots$. Парадокс полягає в уявному протиріччі малого розміру групи при заданому $p \in (0; 1)$ з очікуваним розміром.

Оцінки ймовірностей і розміру групи в задачі про дні народження мають важливі застосування при побудові хеш-функцій, у кодуванні, у криптоаналізі та при розв'язанні систем рівнянь над скінченними алгебричними структурами.

Постановка задачі

Метою даної статті є встановлення асимптотичної поведінки розміру групи в поліноміальній схемі розміщення частинок по комірках, тобто при незалежному, але не обов'язково рівноймовірному розміщенні частинок по комірках.

Основні результати

Сформулюємо задачу про розмір групи в парадоксі днів народжень у загальному випадку (у термінах розміщення частинок по комірках). Нехай задано числа $m, n \in \mathbb{N}$; тут m – число комірок (в парадоксі $m = 365$); n – число частинок (в парадоксі n – розмір групи). Вважаємо, що кожна частинка розміщується незалежно від інших, а ймовірності потрапляння в ко-

мірки дорівнюють p_1, \dots, p_m , $\sum_{i=1}^m p_i = 1$. Нехай також $P_m(n)$ – ймовірність, що при розміщенні n частинок по m комірках принаймні дві частинки потраплять в одну комірку. Позначимо $Q_m(n) = Q_m(n, p_1, \dots, p_m) = 1 - P_m(n)$ – ймовірність, що всі частинки потраплять у різні комірки. Тоді матимемо

$$1 + \sum_{n=1}^{\infty} Q_m(n) \frac{x^n}{n!} = (1 + p_1 x) \dots (1 + p_m x) = f(x). \quad (1)$$

Звідси отримаємо

$$Q(n) = f^{(n)}(0) \quad (2)$$

(для спрощення запису іноді будемо писати $Q(n)$ і $P(n)$ замість $Q_m(n)$ і $P_m(n)$). Тоді $P_m(n) \uparrow$ – зростає за n при фіксованому m , $P(0) = P(1) = 0$, $P(m+1) = 1$.

Визначимо тепер за заданим числом $p \in (0; 1)$ натуральне число $n = n(m) \in [1; m+1]$, яке залежить від m і p , з такої умови:

$$P(n-1) < p \leq P(n), \quad (3)$$

тобто $n(m)$ – це мінімальне число n частинок, таке, що при розміщенні n частинок у m комірках ймовірність потрапляння принаймні двох частинок в одну комірку не менше p . Наприклад, якщо $p = \frac{1}{2}$, $m = 365$, $p_1 = \dots = p_{365} = \frac{1}{365}$, то

$$n(365) = 23, \text{ оскільки } P(22) < \frac{1}{2} < P(23).$$

Розглянемо питання про асимптотичну поведінку $n(m)$. Відомий [3] такий результат про мінімально необхідну кількість частинок (розмір групи) $n(m)$:

$$n(m) = \sqrt{\frac{2am}{T_2(m)}} + o(\sqrt{m}), \quad m \rightarrow \infty, \quad (4)$$

де $a = -\ln(1-p) > 0$; $T_2(m) = m(p_1^2 + \dots + p_m^2)$ за умови $T_2(m) = O(1)$, $m \rightarrow \infty$.

Метою даної статті є доведення теореми, яка істотно посилює цей результат.

Теорема 1. Нехай задано деяку неперервну функцію $p(x)$, таку, що $p(x) \in C([0; 1])$, $p(x) \geq 0$, $\int_0^1 p(x) dx = 1$, і нехай $\forall m \geq 1$ $p_i = p_i(m) =$

$\int_{\frac{i-1}{m}}^{\frac{i}{m}} p(x) dx, i = \overline{1, m}$. Позначимо цю групу умов

для ймовірностей у поліноміальній схемі (*). Тоді розмір групи $n(m)$ з (3) становитиме

$$n(m) = \sqrt{\frac{2am}{T_2(m)}} + \frac{1}{2} + a \left(\frac{2}{3} \frac{T_3(m)}{T_2(m)^2} - 1 \right) + \gamma(m), \quad (5)$$

де $a = -\ln(1-p)$; $T_k(m) = m^{k-1}(p_1^k + \dots + p_m^k), k \geq 1$. Послідовність $\{\gamma(m), m \geq 1\}$ при цьому буде обмежена і $\lim_{m \rightarrow \infty} \gamma(m) = 0, \lim_{m \rightarrow \infty} \overline{\gamma(m)} = 1$.

Зауваження 1. В умовах теореми 1 виконуються таке співвідношення:

$$\forall k \geq 1 \quad \lim_{m \rightarrow \infty} T_k(m) = M_k = \int_0^1 p(x)^k dx. \quad (6)$$

При цьому замінити в (5) значення $T_2(m)$ на M_2 не можна, оскільки треба враховувати швидкість збіжності $T_2(m)$ до M_2 . Якщо додатково припустити, що $p(x) \in C^{(2)}([0;1])$, то можна показати, що

$$\lim_{m \rightarrow \infty} m^2(M_2 - T_2(m)) = \frac{1}{12} \int_0^1 p'(x)^2 dx, \quad (7)$$

і тоді з (5) отримуємо теорему 2.

Теорема 2. Нехай у теоремі 1 виконується додаткова умова $p(x) \in C^{(2)}([0;1])$. Тоді маємо

$$n(m) = \sqrt{\frac{2am}{M_2}} + \frac{1}{2} + a \left(\frac{2}{3} \frac{M_3}{M_2^2} - 1 \right) + \gamma(m); \quad (8)$$

позначення залишаються такі ж, як і в (5), (6).

Зауваження 2. Умова (*) в теоремі 1 є аналогом класичної умови регулярності [3]:

$$\exists C_1, C_2 > 0 \quad \forall m \geq 1: \frac{C_1}{m} \leq \min_{1 \leq i \leq m} p_i \leq \max_{1 \leq i \leq m} p_i \leq \frac{C_2}{m}. \quad (9)$$

З умови (*) випливає друга нерівність в (9), але перша при цьому може не виконуватися.

Регулярні схеми (9) є "близькими" до рівномірної схеми (коли в (*) $p(x) \equiv 1$), а результати, отримані в рівномірному випадку, можуть бути узагальнені і на регулярний випадок. Наприклад, формула (5) є узагальненням аналогічної формули для рівномірного випадку [4], коли $\forall k \geq 1, \forall m \geq 1 T_k(m) = M_k = 1$.

Зауваження 3. Оскільки $\forall m \geq 1 1 \leq T_2(m) \leq M_2$ (за нерівністю Коші–Буняковського), то за умови (*) з (5) отримуємо, що $n(m) = O(\sqrt{m}), m \rightarrow \infty$, тобто в даному варіанті регулярної схеми зберігається той самий порядок росту $n(m)$, як і в рівномірному випадку.

Доведення теореми 1. З (1) маємо

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^m \frac{p_i}{1 + p_i x} = h(x),$$

тобто

$$f'(x) \equiv f(x) h(x),$$

$$f^{(n+1)}(x) = (f(x) h(x))^{(n)} = \sum_{k=0}^n C_n^k f^{(n-k)}(x) h^{(k)}(x).$$

Але

$$h^{(k)}(x) = (-1)^k k! \left(\frac{p_1^{k+1}}{(1 + p_1 x)^{k+1}} + \dots + \frac{p_m^{k+1}}{(1 + p_m x)^{k+1}} \right),$$

$$h^{(k)}(0) = (-1)^k k! (p_1^{k+1} + \dots + p_m^{k+1}).$$

З (2) отримуємо

$$\begin{aligned} Q(n+1) &= f^{(n+1)}(0) = \sum_{k=0}^n C_n^k h^{(k)}(0) f^{(n-k)}(0) = \\ &= \sum_{k=0}^n (-1)^k C_n^k k! (p_1^{k+1} + \dots + p_m^{k+1}) Q(n-k) = \\ &= \sum_{k=0}^n (-1)^k \frac{(n)_k}{m^k} Q(n-k) T_{k+1} \end{aligned}$$

(для спрощення запису іноді будемо писати T_k замість $T_k(m)$). Таким чином, дістанемо

$$Q(n+1) = \sum_{k=0}^n (-1)^k \frac{(n)_k}{m^k} Q(n-k) T_{k+1}(m). \quad (10)$$

Співвідношення (10) допоможе в подальшому визначити асимптотичну поведінку $Q(n)$.

Доведемо таку лему.

Лема 1. Ряд (10) є обгортаючим, тобто

$$\begin{aligned} \forall t \geq 0 \quad \sum_{k=0}^{2t+1} (-1)^k \frac{(n)_k}{m^k} Q(n-k) T_{k+1} &\leq Q(n+1) \leq \\ &\leq \sum_{k=0}^{2t} (-1)^k \frac{(n)_k}{m^k} Q(n-k) T_{k+1} \end{aligned}$$

або

$$Q(n+1) = \sum_{k=0}^{t-1} (-1)^k \frac{(n)_k}{m^k} Q(n-k) T_{k+1} +$$

$$+ \theta(-1)^t \frac{\binom{n}{t}}{m^t} Q(n-t) T_{t+1}, \theta \in [0; 1]. \quad (11)$$

Доведення. Для доведення (11) достатньо довести формулу

$$\begin{aligned} \forall t \geq 1 \quad Q(n+1) - \sum_{k=0}^{t-1} (-1)^k \binom{n}{k} Q(n-k) S_{k+1} = \\ = (-1)^t \binom{n}{t} \sum_{i_1, \dots, i_{n+1-t}} p_{i_1} \dots p_{i_{n-t}} p_{i_{n+1-t}}^{t+1}; \end{aligned} \quad (11a)$$

тут і далі сумування ведеться по всіх невпорядкованих наборах (i_1, \dots, i_n) з попарно нерівними компонентами. Доведемо рівність (11a) індукцією по t . Для $t = 1$ маємо

$$\begin{aligned} Q(n+1) - Q(n) &= \sum_{i_1, \dots, i_{n+1}} p_{i_1} \dots p_{i_{n+1}} - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} = \\ &= \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} \sum_{i_{n+1} \notin \{i_1, \dots, i_n\}} p_{i_{n+1}} - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} = \\ &= - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} \left(1 - \sum_{i_{n+1} \notin \{i_1, \dots, i_n\}} p_{i_{n+1}} \right) = \\ &= - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} (p_{i_1} + \dots + p_{i_n}) = - \sum_{i_1, \dots, i_n} (p_{i_1}^2 \dots p_{i_n}^2 + \\ &+ \dots + p_{i_1} \dots p_{i_n}^2) = - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} \left(1 - \sum_{i_{n+1} \notin \{i_1, \dots, i_n\}} p_{i_{n+1}} \right) = \\ &= - \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n} (p_{i_1} + \dots + p_{i_n}) = \\ &= - \sum_{i_1, \dots, i_n} (p_{i_1}^2 \dots p_{i_n}^2 + \dots + p_{i_1} \dots p_{i_n}^2) = - n \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_{n-1}} p_{i_n}^2. \end{aligned}$$

Формула (11a) доведена для $t = 1$. Індукційний перехід відбувається аналогічно. Якщо (11a) вірна для $j = t$, то для $j = t + 1$ маємо

$$\begin{aligned} Q(n+1) - \sum_{k=0}^t (-1)^k \binom{n}{k} Q(n-k) S_{k+1} = \\ = Q(n+1) - \sum_{k=0}^{t-1} (-1)^k \binom{n}{k} Q(n-k) S_{k+1} - (-1)^t \binom{n}{t} \times \\ \times Q(n-t) S_{t+1} = (-1)^t \binom{n}{t} \sum_{i_1, \dots, i_{n+1-t}} p_{i_1} \dots p_{i_{n-t}} p_{i_{n+1-t}}^{t+1} - \\ - (-1)^t \binom{n}{t} \sum_{i_1, \dots, i_{n-t}} p_{i_1} \dots p_{i_{n-t}} \sum_{i=1}^m p_i^{t+1} = \\ = (-1)^{t+1} \binom{n}{t} \sum_{i_1, \dots, i_{n-t}} p_{i_1} \dots p_{i_{n-t}} (p_{i_1}^{t+1} + \dots + p_{i_{n-t}}^{t+1}) = \end{aligned}$$

$$\begin{aligned} = (-1)^{t+1} \binom{n}{t} \binom{n-t}{t} \sum_{i_1, \dots, i_{n-t}} p_{i_1} \dots p_{i_{n-t}} p_{i_{n-t}}^{t+2} = \\ = (-1)^{t+1} \binom{n}{t+1} \sum_{i_1, \dots, i_{n-t}} p_{i_1} \dots p_{i_{n-t}} p_{i_{n-t}}^{t+2}. \end{aligned}$$

Формулу (11a) і лему 1 доведено.

Нам знадобиться також така лема. Позначимо $Q_0(n) = Q\left(n, \frac{1}{m}, \dots, \frac{1}{m}\right)$ і $n_0(m)$ відповідно ймовірність і розмір групи (див. (1) і (3)) у рівномірному випадку.

Лема 2. Виконується нерівність $Q(n) = Q(n, p_1, \dots, p_m) \leq Q\left(n, \frac{1}{m}, \dots, \frac{1}{m}\right) = \frac{\binom{m}{n}}{m^n}$ (тобто ймовірність відсутності комірки, що містить принаймні дві частинки, досягає максимального значення при рівноймовірному виборі комірок).

Доведення. Лему можна довести через пошук умовного екстремуму функції $Q(n, p_1, \dots, p_m) = \sum_{i_1, \dots, i_n} p_{i_1} \dots p_{i_n}$ на множині $D = \{(p_1, \dots, p_m) : p_1 + \dots + p_m = 1\}$.

Тепер з леми 2 та умови (3) випливає, що $n(m) \leq n_0(m)$, тобто при заданому m розмір групи буде найбільшим у рівномірному випадку. Але відомо [4], що $\lim_{m \rightarrow \infty} \frac{n_0(m)}{m} = 0$. Отже, й

$$\lim_{n \rightarrow \infty} \frac{n(m)}{m} = 0. \quad (12)$$

Покажемо, що

$$\lim_{m \rightarrow \infty} n(m) = +\infty. \quad (13)$$

З (11) маємо

$$Q(k+1) = Q(k) - \theta_{k-1} Q(k-1) \frac{k}{m} T_2(m), \theta_{k-1} \in (0; 1).$$

Звідси при фіксованому k отримаємо, що $Q_m(k+1) = Q_m(k) + o(1)$, $m \rightarrow \infty$, тобто для фіксованого k маємо

$$Q_m(k) = Q_m(1) + o(1) = 1 + o(1), m \rightarrow \infty. \quad (14)$$

Якщо тепер $\exists \{m_k : k \geq 1\}$, $M \geq 1 \forall k \geq 1 : n(m_k) < M$, то з умови (3) і співвідношення (14) дістанемо

$$1 - p \geq Q_{m_k}(n(m_k)) > Q_{m_k}(M) \rightarrow 1, k \rightarrow \infty.$$

Отримали протиріччя. Отже, $\lim_{m \rightarrow \infty} n(m) = +\infty$.

Співвідношення (12) і (13) дають деяку інформацію про поведінку $Q(n)$, $m \rightarrow \infty$, яка допоможе одержати співвідношення (5) і (8).

З (11) маємо

$$Q(n+1) = Q(n) - \frac{n}{m} Q(n-1) T_2 + \theta_{n-2} \frac{n(n-1)}{m^2} Q(n-2) T_3, \theta_{n-2} \in (0;1), \quad (15)$$

$$Q(n) = Q(n-1) - \mu_{n-2} \frac{n-1}{m} Q(n-2) T_2, \mu_{n-2} \in (0;1). \quad (16)$$

Помножимо (16) на $\frac{n}{m} T_2$ і додамо до (15).

Отримаємо

$$Q(n+1) = Q(n) \left(1 - \frac{n}{m} T_2\right) + \frac{n(n-1)}{m^2} Q(n-2) (\theta_{n-2} T_3 - \mu_{n-2} T_2^2)$$

або

$$Q(n+1) = Q(n) \left(1 - \frac{n}{m} T_2\right) + \kappa_n C_p \frac{n^2}{m^2}, |\kappa_n| < 1, \quad (17)$$

де константа C_p визначається тільки функцією $p(x)$, наприклад $C_p = M_3 + M_2^2$. Звідси

$$\begin{aligned} \ln Q(n+1) &= \ln \left(Q(n) \left(1 - \frac{n}{m} T_2\right) + \kappa_n C_p \frac{n^2}{m^2} \right) = \\ &= \ln Q(n) \left(1 - \frac{n}{m} T_2\right) + \ln \left(1 + \frac{\kappa_n C_p}{Q(n) \left(1 - \frac{n}{m} T_2\right)} \frac{n^2}{m^2} \right), \\ \ln Q(n+1) - \ln Q(n) &= \\ &= \ln \left(1 - \frac{n}{m} T_2\right) + \ln \left(1 + \frac{\kappa_n C_p}{Q(n) \left(1 - \frac{n}{m} T_2\right)} \frac{n^2}{m^2} \right), \quad (18) \end{aligned}$$

$$\ln Q(n+1) = \sum_{k=0}^n (\ln Q(k+1) - \ln Q(k)) =$$

$$= \sum_{k=0}^n \ln \left(1 - \frac{k}{m} T_2\right) + \sum_{k=0}^n \ln \left(1 + \frac{\kappa_n C_p}{Q(k) \left(1 - \frac{k}{m} T_2\right)} \frac{k^2}{m^2} \right).$$

Але з допомогою (12) і (13) можна показати, що

$$\begin{aligned} \sum_{k=0}^n \ln \left(1 + \frac{\kappa_n C_p}{Q(k) \left(1 - \frac{k}{m} T_2\right)} \frac{k^2}{m^2} \right) &= O \left(\frac{n^3}{m^2} \right) = \\ &= o \left(\frac{n^2}{m} \right), \quad m \rightarrow \infty, \end{aligned}$$

$$\begin{aligned} \sum_{k=0}^n \ln \left(1 - \frac{k}{m} T_2\right) &= -\frac{n(n+1)}{2m} T_2 + O \left(\frac{n^3}{m^2} \right) = \\ &= -\frac{n^2}{2m} T_2 + o \left(\frac{n^2}{m} \right), \quad m \rightarrow \infty. \end{aligned}$$

Звідси отримаємо

$$\ln Q(n) = -\frac{n^2}{2m} T_2 + o \left(\frac{n^2}{m} \right), \quad m \rightarrow \infty. \quad (19)$$

Оцінимо різницю між $\ln Q(n)$ і $-a$. З (3) і (18) маємо

$$\begin{aligned} 0 \leq \ln Q(n) + a \leq \ln Q(n) - \ln Q(n+1) = \\ = \frac{n}{m} T_2 + O \left(\frac{n^2}{m^2} \right), \quad m \rightarrow \infty. \quad (20) \end{aligned}$$

Тепер з (19) і (20) отримуємо, що

$$a = \frac{n^2}{2m} T_2 + o \left(\frac{n^2}{m} \right), \quad m \rightarrow \infty,$$

звідки матимемо

$$n(m) = \sqrt{\frac{2am}{T_2(m)}} + o(\sqrt{m}), \quad m \rightarrow \infty. \quad (21)$$

Отже, отримали перший доданок у формулі (5). Для того щоб дістати другий доданок, запишемо аналог рівності (15)

$$\begin{aligned} Q(n+1) &= Q(n) - \frac{n}{m} Q(n-1) T_2 + \\ &+ \frac{n(n-1)}{m^2} Q(n-2) T_3 + \theta_{n-3} \frac{n(n-1)(n-2)}{m^3} \times \\ &\times Q(n-3) T_4, \theta_{n-3} \in (0;1), \quad (22) \end{aligned}$$

і з нього отримаємо аналог рівності (19):

$$\ln Q(n) = -\frac{n^2}{2m} T_2 + \frac{n}{2m} T_2 +$$

$$+ \frac{n^3}{3m^2} \left(T_3 - \frac{3}{2} T_2^2 \right) + O \left(\frac{n^2}{m^2} \right), m \rightarrow \infty. \quad (23)$$

Тепер з (23), (21) і (20) отримаємо формулу (5). Теорему 1 доведено.

Зауваження 4. Формули (5) і (8) дають добре асимптотичне наближення для $n(m)$, оскільки $\overline{\lim} \gamma(m) - \underline{\lim} \gamma(m) = 1$, тобто відрізок

$$\left(\sqrt{\frac{2am}{M_2}} + \frac{1}{2} + a \left(\frac{2}{3} \frac{M_3}{M_2^2} - 1 \right) + \lim_{m \rightarrow \infty} \gamma(m); \right. \\ \left. \sqrt{\frac{2am}{M_2}} + \frac{1}{2} + a \left(\frac{2}{3} \frac{M_3}{M_2^2} - 1 \right) + \overline{\lim}_{m \rightarrow \infty} \gamma(m) \right)$$

містить не більше, ніж одну цілу точку, яку можна розглядати як наближення для $n(m)$.

Приклад. Нехай у теоремі 1 $m = 10^6$, $p = 1/2$, $p_0(x) \equiv 1$, $p_1(x) = 2x$, $x \in [0; 1]$. Позна-

чимо розміри групи в обох випадках $n_0(m)$, $n_1(m)$. Тоді з формули (8) матимемо такі асимптотичні наближення:

$$n_0(m) = 1178, n_1(m) = 1020.$$

Відзначимо, що $n_0(m) \geq n_1(m)$, як і має бути (див. міркування після леми 2).

Висновки

Формули (5) і (8) дають вираз для розміру групи в парадоксі днів народжень у випадку нерівномірного розподілу частинок по комірках. Наведені формули можна застосувати в статистиці: з їх допомогою можна будувати критичні області в різноманітних задачах [5, 6] (наприклад, для вирішення питання, чи є вибірка рівномірно розподіленою). Також ці результати можна застосувати в криптографії для оцінювання ймовірності колізії хеш-функцій і трудомісткості побудови колізій [7].

П.А. Ендовицкий

ТОЧНАЯ АСИМПТОТИЧЕСКАЯ ОЦЕНКА РАЗМЕРА ГРУППЫ В ОБОБЩЕНИИ ПАРАДОКСА ДНЕЙ РОЖДЕНИЙ

Доказана теорема об асимптотическом поведении размера группы в парадоксе дней рождений. В теореме даны асимптотически неулучшаемые оценки для размера группы в случае неравновесного и независимого размещения частиц по ячейкам.

P.O. Yendovitskij

EXACT ASYMPTOTIC APPROXIMATION OF THE GROUP SIZE IN GENERALIZATION OF BIRTHDAY PARADOX

This paper aims to prove the theorem on asymptotic behavior of a group size in the birthday paradox. In fact, the theorem presents asymptotically imperfect estimates for the group size in case of non-uniform and independent particle's cell occupancy.

1. *Ширяев А.Н.* Вероятность. – М.: Наука, 1980. – 576 с.
2. *Секей Г.* Парадоксы в теории вероятностей и математической статистике. – М.: Мир, 1990. – 240 с.
3. *Колчин В.Ф., Севастьянов Б.А., Чистяков В.П.* Случайные размещения. – М.: Наука, 1976. – 224 с.
4. *Ендовицкий П.А.* Уточнение асимптотической аппроксимации размера группы в парадоксе дней рождений // Кибернетика и системный анализ. – 2010. – № 3. – С. 185–188.
5. *Иванов В.А., Ивченко Г.И., Медведев Ю.И.* Дискретные задачи в теории вероятностей // Теория вероятностей. Мат. статистика. Теорет. кибернетика. Т. 22 (Итоги науки и техники ВИНТИ АН СССР). – М., 1984. – С. 3–61.
6. *Good I.* Saddle-point methods for the multinomial distribution // Ann. of math. statistics. – 1957. – 28, N 4. – P. 861–881.
7. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

Рекомендована Радою
Фізико-технічного інституту
НТУУ “КПІ”

Надійшла до редакції
31 травня 2010 року