УДК 519.2

П. А. Ендовицкий

Решение обобщенной обратной задачи о днях рождения

(Представлено академиком НАН Украины И. Н. Коваленко)

Доказаны теоремы об асимптотическом поведении решения обобщенной обратной задачи о днях рождения. В теоремах даны асимптотически неулучшаемые оценки в случае неравновероятного и независимого размещения частиц по ячейкам для появления $l \geqslant 1$ k-кратных совпадений. Полученный результат можно применять в криптографии для оценивания трудоемкости построения коллизий хэш-функций.

Задача о днях рождения является классической в теории вероятностей [1]. Задача состоит в нахождении вероятности того, что по крайней мере двое человек из группы, состоящей из n человек, $n \leqslant 365$, родились в один день. При этом предполагается, что все 365 возможных дней рождения равновероятны. Также "задачей о днях рождения" называют [2] задачу нахождения минимального n такого, что в группе из n человек найдутся с вероятностью не меньше чем заданное число $p \in (0;1)$ по крайней мере двое человек, которые родились в один день.

Сформулируем обобщения обеих задач о днях рождения в терминах размещения частиц по ячейкам.

Задача 1. Пусть n частиц независимо размещается в m ячейках (выше было $m = 365$). Вероятности попадания каждой частицы в ячейки равны $p_1, \ldots, p_m$, $\sum\limits_{i=1}^{m} p_i = 1$ (выше было $p_1 = \cdots = p_{365} = 1/365$). Чему равна вероятность $P_k(n,m)$ того, что найдется по крайней мере одна ячейка, содержащая не менее k частиц, $k \geqslant 2$ (выше было $k = 2$)?

Задачу 1 будем называть прямой задачей о днях рождения, так как в ней по заданным параметрам m, n, k надо вычислить вероятность $P_k(n,m)$. Обратной задачей о днях рождения будем называть следующую задачу.

Задача 2. Рассматривается независимое заполнение m ячеек частицами. Вероятности попадания каждой частицы в ячейки равны $p_1, \ldots, p_m$, $\sum\limits_{i=1}^{m} p_i = 1$. Также задано число $p \in (0;1)$. Чему равно минимально необходимое число частиц $n = n(m,p,k)$ такое, что $P_k(n,m) \geqslant p$?

В задаче 2 по заданным параметрам m, k и значению вероятности p надо найти минимальное число частиц n такое, чтобы при размещении n частиц в m ячейках вероятность существования ячейки, содержащей k и более частиц, была не меньше p.

Заметим, что вероятность $P_k(n,m)$ возрастает по n и при этом $P(1) = \cdots = P(k-1) = 0$, $P(m(k-1)+1) = 1$ (для упрощения записи иногда будем писать $P(n)$ вместо $P_k(n,m)$ и n или $n(m)$ вместо $n(m,p,k)$, если это не вызывает неясности) и число частиц $n = n(m)$ из задачи 2 удовлетворяет неравенству

$$P(n-1) < p \leqslant P(n). \tag{1}$$

Например, если $m = 365$, $p_1 = \cdots = p_m = 1/365$, $k = 2$, $p = 1/2$, то $n(365) = 23$, так как в этом случае $P(22) < 1/2 < P(23)$. Т. е. если считать, что каждый из 365 дней рождения

равновероятен, то в группе из 23 человек с вероятностью больше чем 1/2 найдутся по крайней мере двое, которые родились в один день.

Прямая задача о днях рождения (задача 1) рассматривалась в статьях [2–5], обратная (задача 2) — в [2, 6, 7] (см. также [8, 9]).

При решении прямой и обратной задач о днях рождения помогает следующая теорема [9].

Теорема 1. *Пусть n частиц независимо и равновероятно размещаются в m ячейках. Обозначим $\nu_k(n,m)$ — количество ячеек, содержащих k и более частиц, тут $k \geqslant 2$ — фиксированное число. Тогда если $n^k/(k!m^{k-1}) \to \lambda > 0$ при $n,\ m \to \infty$, то $\nu_k(n,m)$ слабо сходится к пуассоновской случайной величине с параметром $\lambda > 0$.*

Из теоремы 1 получаем, что если $n^k/(k!m^{k-1}) \to \lambda > 0$ при $n, m \to \infty$, то

$$P_k(n,m) = P(\nu_k(n,m) \geqslant 1) \to 1 - e^{-\lambda}, \qquad n,m \to \infty. \tag{2}$$

Соотношение (2) дает "первое приближение" для решения прямой задачи о днях рождения в равномерном случае, т. е. когда в задаче 1 $p_1 = \cdots = p_m = 1/m$. Решение же прямой задачи 1 требует получения числового интервала, в котором будет лежать вероятность $P_k(n,m)$, для чего надо, например, оценить скорость сходимости в предельном соотношении (2).

Но в данной работе будет рассматриваться не прямая задача 1, а обратная задача 2. Из теоремы 1 следует теорема 2 об асимптотическом поведении минимально необходимого числа частиц $n(m)$ из задачи 2.

Теорема 2. *Пусть в обратной задаче 2 $p_1 = \cdots = p_m = 1/m$, т. е. рассматривается равномерная схема. Тогда при фиксированных $p \in (0;1)$, $k \geqslant 2$ имеем*

$$n(m) = \sqrt[k]{k!am^{k-1}} + o(m^{(k-1)/k}), \qquad m \to \infty, \tag{3}$$

где $a = -\ln(1-p)$.

В случае $k = 2$ (т. е. когда ищется $n(m)$ — минимальное число n частиц, необходимое для того, чтобы при равновероятном и независимом размещении n частиц в m ячейках с вероятностью не меньше чем p существовала ячейка, содержащая две или более частицы) формула (3) принимает вид

$$n(m) = \sqrt{2am} + o(\sqrt{m}), \qquad m \to \infty,$$

где $a = -\ln(1-p)$.

Целью настоящей работы является уточнение формулы (3), которая описывает асимптотическое поведение минимально необходимого числа частиц $n(m)$ из задачи 2 при $m \to \infty$ и фиксированных $p \in (0;1)$ и $k \geqslant 2$.

При этом сначала формула (3) будет уточнена для равномерной схемы, а далее полученная уточненная формула будет распространена на некоторые полиномиальные схемы, отличные от равномерной.

Сформулируем без доказательства соответствующую теорему для следующего варианта полиномиальной схемы.

Теорема 3. *Пусть задана некоторая неотрицательная, дважды дифференцируемая на отрезке $[0;1]$ функция $p(x)$ такая, что $\int\limits_0^1 p(x)\,dx = 1$. Рассматривается полиномиальная схема $\{p_i(m), m \geqslant 1, i = \overline{1,m}\}$, которая задается через функцию $p(x)$ по формуле: $\forall\, m \geqslant 1$*

$\forall\, i = \overline{1,m}\colon p_i(m) = \int\limits_{(i-1)/m}^{i/m} p(x)dx$ *(при* $p(x) \equiv 1$ *получается равномерная полиномиальная схема).*

Тогда минимальное число частиц $n(m)$ *из задачи 2 будет равняться*

$$n(m) = \sum_{i=0}^{k-1} A_i m^{i/k} + \theta(m), \tag{4}$$

где последовательность $\{\theta(m), m \geqslant 1\}$ *будет ограниченной и*

$$\underline{\lim}\,\theta(m) = 0, \qquad \overline{\lim}\,\theta(m) = 1. \tag{5}$$

Константы $A_0, A_1, \ldots, A_{k-1}$ *из* (4) *определяются следующим образом. Пусть* $a = -\ln(1-p)$, $b = \sqrt[k]{k!a/M_k}$ *(смысл параметров* p *и* k *см. в формулировке задачи 2), а числа* M_l, $l \geqslant 1$, *определяются по формуле*

$$M_l = \int\limits_0^1 p(x)^l dx, \qquad l \geqslant 1, \tag{6}$$

тогда при $i = \overline{0,k-1}$

$$A_i = \frac{b^{k-i}}{k-i}\left(\sum_{l_1+2l_2+\cdots+(k-1)l_{k-1}=k-1-i} \frac{\left(-1+\frac{i}{k}\right)_{l_1+\cdots+l_{k-1}}}{l_1!\cdots l_{k-1}!} B_1^{l_1}\cdot\cdots\cdot B_{k-1}^{l_{k-1}}\right), \tag{7}$$

где суммирование производится по всем решениям уравнения $l_1 + 2l_2 + \cdots + (k-1)l_{k-1} = k-1-i$, $l_s \geqslant 0$, $s = \overline{1,k-1}$.

Также обозначено $(c)_t = c(c-1)\cdots(c-t+1)$, $t \in \mathbb{N}$, $c \in \mathbb{R}$, $(c)_0 = 1$, *а константы* $B_1, \ldots, B_{k-1}$, *в свою очередь, равны*

$$\begin{cases} B_s = \dfrac{(-1)^s}{s!}\dfrac{M_{k+s}}{M_k}\dfrac{k}{k+s}, \qquad s = \overline{1,k-2}, \\ B_{k-1} = \dfrac{(-1)^{k-1}}{(k-1)!}\dfrac{M_{2k-1}}{M_k}\dfrac{k}{2k-1} + \dfrac{k}{2}\dfrac{M_k}{(k-1)!} - \dfrac{M_k}{2(k-2)!}\dfrac{1}{a}. \end{cases} \tag{8}$$

Формула (4) и является уточнением формулы (3).

Замечание 1. Условие (5) позволяет строить хорошие приближения для искомого числа частиц $n(m)$, так как в левой части формулы (4) стоит целое число $n(m)$, а отрезок

$$\left[\sum_{i=0}^{k-1} A_i m^{\frac{i}{k}} + \underline{\lim}\,\theta(m); \sum_{i=0}^{k-1} A_i m^{\frac{i}{k}} + \overline{\lim}\,\theta(m)\right) = \left[\sum_{i=0}^{k-1} A_i m^{\frac{i}{k}}; \sum_{i=0}^{k-1} A_i m^{\frac{i}{k}} + 1\right)$$

содержит ровно одну целую точку, которую можно рассматривать как приближение для $n(m)$.

Пример 1. Приведем асимптотическую формулу для $n(m)$ из теоремы 3 в случае $k = 2$, т. е. для минимального числа частиц $n(m)$, которые надо разместить в m ячейках, чтобы с вероятностью не меньше чем $p \in (0;1)$ существовала ячейка, содержащая по крайней мере две частицы.

В этом случае, при $k = 2$ из (4) имеем

$$n(m) = A_1\sqrt{m} + A_0 + \theta(m),$$

где $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$, а константы A_0 и A_1 определяются следующим образом.

Пусть $a = -\ln(1-p)$, $b = \sqrt{2a/M_2}$, определение чисел M_l, $l \geqslant 1$, см. в формуле (6). Тогда по формуле (8) рассчитываем константу B_1:

$$B_1 = -\frac{2}{3}\frac{M_3}{M_2} + M_2 - \frac{M_2}{2a},$$

и теперь из формулы (7) получаем значения A_0 и A_1:

$$A_1 = \frac{b^1}{1}\sum_{l_1=0}\frac{(-1/2)_{l_1}}{l_1!}B_1^{l_1} = b = \sqrt{\frac{2a}{M_2}},$$

$$A_0 = \frac{b^2}{2}\sum_{l_1=1}\frac{(-1)_{l_1}}{l_1!}B_1^{l_1} = -\frac{b^2}{2}B_1 = a\left(\frac{2}{3}\frac{M_3}{M_2^2} - 1\right) + \frac{1}{2}.$$

Отсюда получаем выражение для $n(m)$ в случае $k = 2$:

$$n(m) = \sqrt{\frac{2a}{M_2}m} + a\left(\frac{2}{3}\frac{M_3}{M_2^2} - 1\right) + \frac{1}{2} + \theta(m). \tag{9}$$

В равномерном случае, когда $M_l = 1$, $l \geqslant 1$, формула (9) принимает вид

$$n(m) = \sqrt{2am} - \frac{a}{3} + \frac{1}{2} + \theta(m), \tag{10}$$

где $a = -\ln(1-p)$, $\underline{\lim}\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$.

Формула (10) получена в [10].

Пример 2. Получим аналогичную формулу для $n(m)$ в случае $k = 3$. Она будет иметь вид

$$n(m) = A_2 m^{2/3} + A_1 m^{1/3} + A_0 + \theta(m),$$

где $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$, а константы A_0, A_1, A_2 определяются следующим образом. Пусть $a = -\ln(1-p)$, $b = \sqrt[3]{6a/M_3}$. Рассчитываем по формулам (8) константы B_1, B_2:

$$B_1 = -\frac{3}{4}\frac{M_4}{M_3}, \qquad B_2 = \frac{3}{10}\frac{M_5}{M_3} + \frac{3}{4}M_3 - \frac{M_3}{2a},$$

и теперь по формулам (7) получаем значения A_0, A_1, A_2:

$$A_2 = \frac{b^1}{1}\sum_{l_1+2l_2=0}\frac{(-1/3)_{l_1+l_2}}{l_1!l_{2!}}B_1^{l_1}B_2^{l_2} = b,$$

$$A_1 = \frac{b^2}{2}\sum_{l_1+2l_2=1}\frac{(-2/3)_{l_1+l_2}}{l_1!l_{2!}}B_1^{l_1}B_2^{l_2} = \frac{b^2}{2}(-(2/3)B_1) = \frac{M_4}{4M_3}b^2,$$

$$A_0 = \frac{b^3}{3}\sum_{l_1+2l_2=2}\frac{(-1)_{l_1+l_2}}{l_1!l_{2!}}B_1^{l_1}B_2^{l_2} = \frac{2a}{M_3}(B_1^2 - B_2) = a\left(\frac{9}{8}\frac{M_4^2}{M_3^3} - \frac{3}{5}\frac{M_5}{M_3} - \frac{3}{2}\right) + 1.$$

Отсюда получаем выражение для $n(m)$ в случае $k = 3$:

$$n(m) = bm^{2/3} + \frac{M_4}{4M_3}b^2m^{1/3} + a\left(\frac{9}{8}\frac{M_4^2}{M_3^3} - \frac{3}{5}\frac{M_5}{M_3} - \frac{3}{2}\right) + 1 + \theta(m), \tag{11}$$

где $a = -\ln(1-p)$, $b = \sqrt[3]{6a/M_3}$, $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$. В равномерном случае, когда $M_l = 1$, $l \geqslant 1$, формула (11) принимает вид

$$n(m) = bm^{2/3} + \frac{b^2}{4}m^{1/3} - \frac{39}{40}a + 1 + \theta(m), \tag{12}$$

где $a = -\ln(1-p)$, $b = \sqrt[3]{6a}$, $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$.

Пример 3. Приведем также формулу для $n(m)$ в случае $k = 4$ (способ ее получения такой же, как и для случаев $k = 2$ и $k = 3$):

$$n(m) = bm^{3/4} + \frac{M_5}{5M_4}b^2m^{2/4} + \left(\frac{7}{50}\frac{M_5^2}{M_4^2} - \frac{1}{12}\frac{M_6}{M_4}\right)b^3m^{1/4} + \\ + a\left(\frac{384}{125}\frac{M_5^3}{M_4^4} - \frac{16}{5}\frac{M_5M_6}{M_4^3} + \frac{12}{21}\frac{M_7}{M_4^2} - 2\right) + \frac{3}{2} + \theta(m), \tag{13}$$

где $a = -\ln(1-p)$, $b = \sqrt[4]{24a/M_4}$, $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$. В равномерном случае, когда $M_l = 1$, $l \geqslant 1$, формула (13) принимает вид

$$n(m) = bm^{3/4} + \frac{b^2}{5}m^{2/4} + \frac{17}{300}b^3m^{1/4} - \frac{4086}{2625}a + \frac{3}{2} + \theta(m), \tag{14}$$

где $a = -\ln(1-p)$, $b = \sqrt[3]{24a}$, $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$.

Если $m = 365$, $p = 1/2$, то (при равновероятном размещении частиц) из формул (10), (12), (14) получаем следующие значения для минимально необходимого числа частиц $n(m)$ в случаях $k = 2$, $k = 3$, $k = 4$ соответственно:

$$n(365) = 23, \qquad n(365) = 88, \qquad n(365) = 187, \tag{15}$$

т. е. в группе из 187 человек с вероятностью больше, чем $1/2$ найдутся 4 человека, родившиеся в один день [2]. Т. е. значения (15), полученные из асимптотических формул (10), (12), (14), совпадают с точными значениями, найденными в [2] (только для этих трех случаев) компьютерным перебором.

Обобщением задач 1 и 2 являются задачи 3 и 4.

Задача 3. Пусть n частиц независимо размещается в m ячейках. Вероятности попадания каждой частицы в ячейки равны $p_1, \ldots, p_m$, $\sum\limits_{i=1}^{m} p_i = 1$. Чему равна вероятность $P_k(n, m, l)$ того, что найдется по крайней мере l ячеек, $l \geqslant 1$, содержащих не менее k частиц, $k \geqslant 2$?

Задача 4. Рассматривается независимое заполнение m ячеек частицами. Вероятности попадания каждой частицы в ячейки равны $p_1, \ldots, p_m, \sum\limits_{i=1}^{m} p_i = 1$. Также задано число $p \in (0; 1)$. Чему равно минимально необходимое число частиц $n = n_l(m)$ такое, что $P_k(n, m, l) \geqslant p$?

Очевидно, что при $l = 1$ в задачах 3 и 4 получаем задачи 1 и 2.

В данном случае из теоремы 1 будет следовать, что если в равномерной схеме $\dfrac{n^k}{k!m^{k-1}} \to \lambda > 0$, то

$$P_k(n, m, l) = P(\nu_k(n, m) \geqslant l) \to 1 - e^{-\lambda}\sum_{t=0}^{l-1}\frac{\lambda^t}{t!}, \qquad n, m \to \infty,$$

и отсюда для минимального числа частиц $n_l(m)$ из задачи 4 будет справедливо представление

$$n_l(m) = \sqrt[k]{k!a_lm^{k-1}} + o(m^{(k-1)/k}), \qquad m \to \infty, \tag{16}$$

где

$$a_l = h_l(1-p), \qquad l \geqslant 1, \tag{17}$$

а функция $h_l(x)\colon (0;1) \to (0;+\infty)$ убывает и определяется своей обратной функцией $h_l^{-1}(x)$: $h_l^{-1}(x) = e^{-x}\sum\limits_{t=0}^{l-1} x^t/t!$, $x > 0$.

Формула (16), как и формула (3), также может быть уточнена. А именно, справедлива следующая теорема.

Теорема 4. *Пусть для произвольных фиксированных $k \geqslant 2$ и $l \geqslant 1$ выполнены условия теоремы 3, тогда*

$$n_l(m) = \sum_{i=0}^{k-1} A_i m^{i/k} + \frac{k(l-1)}{2} + \theta(m), \tag{18}$$

где последовательность $\{\theta(m), m \geqslant 1\}$ ограничена и $\underline{\lim}\,\theta(m) = 0$, $\overline{\lim}\,\theta(m) = 1$. Константы A_i, $i = \overline{0,k-1}$, из (18) определяются так же, как и константы A_i, $i = \overline{0,k-1}$, из (4) в теореме 3. Только везде вместо значения $a = -\ln(1-p)$ в формуле (4) тут надо брать значение $a_l = h_l(1-p)$ из формулы (17).

Замечание 2. Отметим, что в свободном члене в формуле (18) появляется слагаемое $k(l-1)/2$, которого нет в формуле (4), т. е. когда $l = 1$.

Пример 4. Пусть $k = 2$. Приведем асимптотические формулы для $n_1(m)$, $n_2(m)$ и $n_3(m)$ — минимального количества частиц, которое необходимо разместить в m ячейках, чтобы с вероятностью не меньше чем $p \in (0;1)$ существовали по крайней мере соответственно 1, 2, 3 ячейки, содержащие две частицы и более. Имеем

$$n_1(m) = \sqrt{\frac{2a_1}{M_2}m} + a_1\left(\frac{2}{3}\frac{M_3}{M_2^2} - 1\right) + \frac{1}{2} + \theta_1(m),$$

$$n_2(m) = \sqrt{\frac{2a_2}{M_2}m} + a_2\left(\frac{2}{3}\frac{M_3}{M_2^2} - 1\right) + \frac{3}{2} + \theta_2(m),$$

$$n_3(m) = \sqrt{\frac{2a_3}{M_2}m} + a_3\left(\frac{2}{3}\frac{M_3}{M_2^2} - 1\right) + \frac{5}{2} + \theta_3(m),$$

тут $\underline{\lim}\theta_i(m) = 0$, $\overline{\lim}\theta_i(m) = 1$, $i = \overline{1,3}$, числа $a_i = a_i(p)$, $i = \overline{1,3}$, определяются по формуле (17), а числа M_l, $l \geqslant 1$, определены в формуле (6).

Пример 5. Используя уточненные формулы (4) и (18) из теорем 3 и 4, построим таблицу значений $n_l(m)$ в равномерной схеме размещения частиц при $m = 365$, $p = 1/2$, для значений $k = \overline{2,4}$ и $l = \overline{1,5}$ (смысл параметров см. в формулировке задач 3 и 4):

k	l				
	1	2	3	4	5
2	23	36	46	55	62
3	88	120	142	160	175
4	187	240	274	301	323

т. е. чтобы в группе из n человек нашлась с вероятностью не меньше чем $1/2$ по крайней мере одна тройка, где все трое родились в один день, достаточно взять $n = 88$; для того чтобы с вероятностью не меньше чем $1/2$ нашлись по крайней мере две тройки, в каждой из которых все трое родились в один день, достаточно взять $n = 120$ и т. д.

Являются ли значения в таблице решениями задачи 4? Т. е. удовлетворяют ли они неравенству (1)? Ведь эти значения получены при подстановке числовых значений в асимптотические формулы (4) и (18) и про значение величины $\theta(365)$ теоремы 3 и 4 ничего не говорят. Известно лишь, что

$$\underline{\lim}\,\theta(m) = 0, \qquad \overline{\lim}\,\theta(m) = 1,$$

а значения в таблице были получены в предположении, что $0 < \theta(365) < 1$.

Ответить на последний вопрос можно, решав прямую задачу о днях рождения (задачи 1 и 3) для значений, указанных в таблице и соседних к ним. Из условия (5) следует, что для достаточно больших m значения $n(m)$, полученные по асимптотическим формулам (4) и (18), будут либо совпадать с точными решениями задачи 4, либо отличаться от них на 1. Но, как показывают числовые расчеты [2], уже при $m = 365$ первый столбец в таблице, полученный по асимптотическим формулам, совпадает с точным решением.

С помощью полученных формул (4) и (18) можно рассчитывать трудоемкость построения многократных коллизий хэш-функций в криптографии, критические области при проверке статистических гипотез и др.

1. *Feller W.* An introduction to probability theory and its applications. – New York: Wiley, 1958. – 411 p.
2. *McKinney E. H.* Generalized birthday problem // Amer. Math. Monthly. – 1966. – **73**. – P. 385–387.
3. *Levin B.* A representation for multinomial cumulative distribution functions // Ann. Stat. – 1981. – **9**. – P. 1123–1126.
4. *Nunnikhoven T.* A birthday problem solution for nonuniform birth frequencies // Amer. Statist. – 1992. – **46**. – P. 601–606.
5. *Sayrafiezadeh M.* The birthday problem revisited // Math. Mag. – 1994. – **64**. – P. 220–223.
6. *Heuer G. A.* Estimation of a certain probability problem // Amer. Math. Monthly. – 1959. – **66**. – P. 704–706.
7. *Mathis F.* A generalized birthday problem // SIAM Rev. – 1991. – **33**. – P. 265–270.
8. *DasGupta A.* The matching, birthday and strong birthday problem: a contemporary review // J. Statist. Planning and Inference. – 2005. – **130**. – P. 377–389.
9. *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П.* Случайные размещения. – Москва: Наука, 1976. – 224 с.
10. *Ендовицкий П. А.* Уточнение асимптотической аппроксимации размера группы в парадоксе дней рождений // Кибернетика и систем. анализ. – 2010. – **3**. – С. 185–188.

НТУ Украины "Киевский политехнический институт" *Поступило в редакцию 24.10.2011*

П. О. Єндовицький

Розв'язок узагальненої оберненої задачі про дні народження

Доведено теореми про асимптотичну поведінку розв'язку в узагальненій задачі про дні народження. У теоремах наведені асимптотично непокращувальні оцінки у випадку нерівноймовірного та незалежного розміщення частинок по комірках для появи $l \geqslant 1$ k-кратних збігів. Отриманий результат можна застосовувати в криптографії для оцінювання трудомісткості побудови колізій хеш-функцій.

P. A. Yendovitskij

The solution of a generalized inverse birthday problem

Theorems of the asymptotic behavior of the solution of a generalized inverse birthday problem are proved. They give the asymptotically best possible estimates in the case of a nonuniform independent arrangement of particles in cells for the appearance of $l \geqslant 1$ k-fold coincidences. The result can be applied to the evaluation of the laboriousness of a construction of collisions of the hash-functions in cryptography.