В. Н. С у р и к о в (Москва, ТВП). **Задача о ключах.**

Введение. При организации выборочного контроля, исследовании популяций, криптографическом анализе широко применяется вероятностная модель, которую В. Феллер назвал *задачей о ключе*. «Человек хочет открыть свою дверь. У него n ключей, из которых только один подходит к двери. По причине, о которой можно только догадываться, он пробует ключи случайно, так что при каждой попытке каждый ключ имеет вероятность быть выбранным n^{-1} и все возможные исходы, отвечающие данному числу попыток, равновероятны» (см. [1, с. 68]).

Мы усложним задачу. Для того чтобы попасть в дом, человеку необходимо открыть k дверей. Так же, как в задаче 11 [1, с. 74], для каждой двери он испытывает ключи последовательно, выбирая из связки без возвращения до момента открытия двери, после чего все ключи, включая подошедший, возвращаются в связку, и начинается процедура испытания ключей для очередной двери. Двери могут иметь одинаковые ключи, но человек не знает, каким дверям соответствуют одинаковые ключи.

Требуется описать вероятностное распределение количества дверей, открытых после N попыток.

Математическая постановка задачи. Основные результаты. Рассмотрим серии независимых в совокупности случайных величин $\xi_1^{(n)}, \xi_2^{(n)}, \ldots$, $n = 1, 2, \ldots$, каждая из которых имеет равномерное распределение на множестве $\{1, 2, \ldots, n\}$, т. е. $\mathbf{P}\{\xi_i^{(n)} = \nu\} = 1/n$, $i = 1, 2, \ldots$, $\nu = 1, 2, \ldots, n$.

Для каждой серии образуем последовательность случайных величин $S_0^{(n)} = 0$, $S_k^{(n)} = \sum_{i=1}^{k} \xi_i^{(n)}$, $k = 1, 2, \ldots$.

Зафиксируем натуральное число N и определим случайные величины $\tau_N^{(n)} = \max\{k\colon\ S_k^{(n)} \leqslant N\}$.

По смыслу $\xi_i^{(n)}$ равна числу попыток до открытия i-й двери, $S_k^{(n)}$ — число попыток до момента открытия k дверей, а $\tau_N^{(n)}$ — число открытых дверей после N попыток.

При помощи формулы Сильвестра (принцип включения и исключения) [2] доказано следующее вспомогательное утверждение.

Лемма. *Для натуральных k, n и N справедливы равенства*

$$\begin{aligned} \mathbf{P}\{\tau_N^{(n)} \geqslant k\} &= \frac{1}{n^k} \sum_{0 \leqslant \nu < (N-k)/n} (-1)^\nu \binom{k}{\nu} \binom{N-\nu n}{k}, \qquad k \geqslant \frac{n}{N}, \\ \mathbf{M}\,\tau_N^{(n)} &= \sum_{0 \leqslant \nu < N/(n+1)} (-1)^\nu \binom{N-\nu n}{\nu} \left(\frac{1}{n}\right)^\nu \left(1 + \frac{1}{n}\right)^{N-\nu n-\nu} - 1. \end{aligned} \tag{1}$$

Как правило, в приложениях величина N/n ограничена, и значения $\mathbf{P}\{\tau_N^{(n)} \geqslant k\}$ и $\mathbf{M}\,\tau_N^{(n)}$ легко вычисляются при помощи приведенных выше формул.

При подборе необходимых для приложений значений N и k весьма полезны соотношения, приведенные в следующем утверждении.

Следствие. *Пусть n, N стремятся к бесконечности так, что $N/n \to t < +\infty$. Тогда*

$$\begin{aligned} \lim_{n, N \to \infty} \mathbf{P}\{\tau_N^{(n)} \geqslant k\} &= \sum_{0 \leqslant \nu < t} \frac{(-1)^\nu (t-\nu)^k}{\nu!\,(k-\nu)!} = P_k(t), \qquad k \geqslant t, \\ \lim_{n, N \to \infty} \mathbf{M}\,\tau_N^{(n)} &= e^t \sum_{0 \leqslant \nu < t} \frac{(\nu - t)^\nu}{\nu!} e^{-\nu} - 1 = M(t). \end{aligned} \tag{2}$$

Аналоги соотношений (1) и (2) можно найти в [1, с. 298].

При каждом фиксированном n случайный процесс $\nu^{(n)}(t) = \max\{k\colon\ S_k^{(n)} \leqslant tn\}$, $t \geqslant 0$, является процессом восстановления. Точные формулы для вычисления одномерных распределений и функции восстановления этого процесса приведены в лемме. При разных n случайные процессы $\nu^{(n)}(t)$ заданы на различных вероятностных пространствах, и напрямую воспользоваться результатами из [3] о слабой сходимости распределений считающих процессов не представляется возможным.

Преодолеть эту трудность позволяет следующая конструкция. Рассмотрим последовательность независимых в совокупности случайных величин $\xi_1, \xi_2, \ldots$, каждая из которых имеет равномерное распределение на интервале [0,1], т. е. $\mathbf{P}\{\xi_1 < x\} = x$, $0 \leqslant x \leqslant 1$.

Образуем случайные последовательности $\overline{S}_0 = 0$, $\overline{S}_k = \sum_{i=1}^k \xi_i$, $\overline{S}_0^{(n)} = 0$, $\overline{S}_k^{(n)} = \sum_{i=1}^k n^{-1}\{\xi_i n\}$, $k = 1, 2, \ldots$, где $\{x\}$ обозначаем минимальное целое число, не меньшее x.

Определим процессы восстановления $\nu(t) = \max\{k\colon\ \overline{S}_k \leqslant t\}$, $\nu_n(t) = \max\{k\colon\ \overline{S}_k^{(n)} \leqslant t\}$, $t \geqslant 0$. Распределения процессов $\nu_n(t)$ и $\nu^{(n)}(t)$ совпадают. Их предельное поведение описано в следующей теореме, доказательство которой основано на теореме 1.2 из [3].

Теорема. *При $n \to \infty$ конечномерные распределения случайного процесса $\nu_n(t)$ слабо сходятся к конечномерным распределениям считающего процесса $\nu(t)$.*

СПИСОК ЛИТЕРАТУРЫ

1. *Феллер В.* Введение в теорию вероятностей и ее приложения, т. 1. М.: Мир, 1984, 528 с.
2. *Холл М.* Комбинаторный анализ. М.: Иностранная литература, 1963, 98 с.
3. *Кабанов Ю. М.*, *Липцер Р. Ш.*, *Ширяев А. Н.* Слабая и сильная сходимость распределений считающих процессов. — Теория вероятн. и ее примен., 1983, т. XXVIII, в. 2, с. 288–319.