

Лекция № 12

О повторениях в случайных последовательностях

Лектор: Н.Ю. Золотых

Записал: Д. Скотов

29 ноября 2008

Пусть задана функция $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ и начальная точка $x_0 \in \mathbb{Z}_n$. По заданным f и x_0 строится последовательность:

$$x_n = f(x_{n-1}), n \geq 1. \quad (1)$$

Рассмотрим случай первого появления повторения в генерируемой последовательности: в процессе итерации появился такой элемент x_s , что все элементы $x_0, \dots, x_{s-1}$ различны, и среди этих s элементов существует единственный элемент $x_h = x_s$. Нас интересует, сколько в среднем шагов от начальной точки x_0 нужно сделать, чтобы получить это первое повторение.

Утверждение 1. Для любых случайных $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, $x_0 \in \mathbb{Z}_n$, среднее время до первого появления повторения в последовательности (1) не превосходит величины $O(\sqrt{n})$.

Доказательство. Построим вероятностное пространство $\langle \Omega, \mathcal{F}, \mathbf{Pr} \rangle$.

1. $\Omega = \{(f, x_0), f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n, x_0 \in \mathbb{Z}_n\}$.

Множество $\mathbb{Z}_n$ содержит n различных элементов, каждый из которых можно отобразить в один из n элементов. Поэтому существует n^n различных функций $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$.

Точку x_0 можно выбрать из $\mathbb{Z}_n$ n различными способами.

Таким образом, $|\Omega| = n \cdot n^n = n^{n+1}$.

2. Пусть случайная величина ξ есть номер шага (начиная с нулевого), на котором было получено первое повторение в последовательности, генерируемой (1). Нас интересует вероятность события $\{\xi = s\}$, $s \in \mathbb{N}_0$. Подсчитаем кол-во исходов, благоприятствующих событию.

Элементы $x_0, \dots, x_{s-1}$ должны быть различны, а x_s должен совпадать с одним из них. Подсчитаем количество отображений f , приводящих к этой конфигурации. Точку x_0 можно отобразить в x_1 $n-1$ способами, x_2 в $x_1 - n-2$ способами, $\dots$, x_{s-2} в $x_{s-1} - n-s+1$ способами. Все элементы $x_0, \dots, x_{s-2}$ различны и дают $s-1$ различных элементов множества $\mathbb{Z}_n$, — тем самым мы построили отображение f для этих $s-1$ элементов. Далее, x_{s-1} в x_s можно отобразить только s способами, чтобы он совпал с одним из предшествующих элементов. Тем самым построено отображение f для s различных элементов $\mathbb{Z}_n$, т. к. $x_0, \dots, x_{s-1}$ все различны. Осталось построить f для оставшихся $n-s$ элементов множества $\mathbb{Z}_n$. Любой из этих $n-s$ элементов можно отобразить в любой из n элементов $\mathbb{Z}_n$, а это можно сделать n^{n-s} способами.

Точку x_0 можно выбрать произвольным образом из n элементов.

Пользуясь правилом произведения, получаем:

$$\mathbf{Pr}(\{\xi = s\}) \stackrel{\text{def}}{=} \mathbf{Pr}(s) = \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-s+1) \cdot s \cdot n^{n-s}}{n^{n+1}} = \frac{n! \cdot s}{(n-s)! \cdot n^{s+1}}.$$

Подсчитаем среднее значение величины s . Заметим, что конфигурация первого повторения невозможна при значениях s , отличных от значений из $\{1, \dots, n\}$, поэтому вероятность

таких значений полагается равной 0. Действительно, при $s = 0$ конфигурация не имеет смысла, а при $s > n$ она невозможна, так как имеется не более n различных значений элементов. Поэтому матожидание величины s выражается конечной суммой:

$$\begin{aligned}
Ms &= \sum_{s=1}^n s \cdot \mathbf{Pr}(s) = \sum_{s=1}^n s^2 \cdot \frac{n!}{(n-s)! \cdot n^{s+1}} = \sum_{s=1}^n \binom{n}{s} \frac{s!}{n^{s+1}} s^2 = \\
&= \sum_{s=1}^n \binom{n}{s} \frac{s! \cdot s}{n^s} \left(1 - \frac{n-s}{n}\right) = \sum_{s=1}^n \left[\frac{s}{n^s} \binom{n}{s} s! - \frac{s}{n^s} \binom{n-1}{s} s! \right] = \\
&= \sum_{s=1}^n \frac{s}{n^s} \binom{n}{s} s! - \sum_{s=1}^n \frac{s}{n^{s+1}} \binom{n}{s+1} (s+1)! = \\
&= \sum_{s=1}^n \frac{s}{n^s} \binom{n}{s} s! - \sum_{s=2}^n \frac{s-1}{n^s} \binom{n}{s} s! = \sum_{s=1}^n \frac{s}{n^s} \binom{n}{s} s! - \sum_{s=1}^n \frac{s-1}{n^s} \binom{n}{s} s! = \\
&= \sum_{s=1}^n \frac{s!}{n^s} \binom{n}{s} = \left\{ s! = \Gamma(s+1) = \int_0^\infty e^{-t} t^s dt \right\} = \sum_{s=1}^n \frac{1}{n^s} \binom{n}{s} \int_0^\infty e^{-t} t^s dt = \\
&= \int_0^\infty e^{-t} \left[\sum_{s=1}^n \binom{n}{s} \left(\frac{t}{n}\right)^s \right] dt = \int_0^\infty e^{-t} \left[\left(1 + \frac{t}{n}\right)^n - 1 \right] dt = \\
&= \int_0^\infty e^{-t} \left(1 + \frac{t}{n}\right)^n dt - 1 = \int_0^\infty e^{\{n \ln(1 + \frac{t}{n}) - t\}} dt - 1 = \{n \rightarrow \infty\} = \\
&= \int_0^\infty e^{\{n [\frac{t}{n} - \frac{t^2}{2n^2} + o(\frac{t}{n})^3] - t\}} dt - 1 = \int_0^\infty e^{\{t - \frac{t^2}{2n} + no(\frac{t}{n})^3 - t\}} dt - 1 = \\
&= \mathcal{O} \left(\int_0^\infty e^{-\frac{t^2}{2n}} dt \right) = \mathcal{O} \left(\int_0^\infty e^{-\left\{ \frac{t}{\sqrt{2n}} \right\}^2} dt \right) = \left\{ x = \frac{t}{\sqrt{2n}} \right\} = \\
&= \mathcal{O} \left(\sqrt{2n} \int_0^\infty e^{-x^2} dx \right) = \mathcal{O} \left(\sqrt{2n} \frac{\sqrt{\pi}}{2} \right) = \mathcal{O}(\sqrt{n}).
\end{aligned}$$

Здесь мы воспользовались свойствами Гамма-функции и интеграла Пуассона. □

Список литературы

- [1] Кнут Д.Э. Искусство программирования. Т.1: Основные алгоритмы. 3-е изд. — М.: «Вильямс», 2006. — п.1.2.11.3.