Труды Карельского научного центра РАН
№ 4. 2014. С. 75–79

УДК 519.115:519.2

ПРИМЕНЕНИЕ ОБОБЩЕННОЙ СХЕМЫ РАЗМЕЩЕНИЯ К ИЗУЧЕНИЮ ОДНОГО КЛАССА ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОРОЖДАЕМЫХ РЕГИСТРОМ СДВИГА

А. В. Колчин

Рассматривается пример применения обобщенной схемы размещения к изучению асимптотического поведения комбинаторных объектов. В настоящей работе изучаются размещения наборов из 0 и 1 на окружности, вырабатываемых регистрами сдвига при определенных условиях.

Ключевые слова: обобщенная схема размещения, локальные предельные теоремы.

A. V. Kolchin. AN APPLICATION OF THE GENERALISED ALLOCATION SCHEME TO ANALYSING A CLASS OF SEQUENCES GENERATED BY A SHIFT REGISTER

We consider an example of application of the generalised allocation scheme to studying the asymptotic behaviour of combinatorial objects. In this research, we analyse the allocation of tuples of zero and ones onto a circle which are generated by a shift register under certain conditions.

Key words: generalised allocation scheme, local limit theorems.

Рассматривается задача, связанная с размещением наборов из 0 и 1 длины m в 2^m равноотстоящих точках окружности, занумерованных числами $1, 2, \ldots, 2^m$ таким образом, что каждый последующий набор начинается с $m-1$ последних членов предыдущего набора. Нетрудно видеть, что такое плотное размещение 2^m различных наборов возможно: действительно, такие наборы вырабатываются регистром сдвига с m ячейками, и при некоторых условиях, налагаемых на функцию усложнения f (функцию обратной связи регистра), регистр вырабатывает одноцикловую последовательность, содержащую все $N = 2^m$ различных наборов длины m (см., например, [5]).

Напомним (см. [5, 6]), что под регистром сдвига подразумевают техническое устройство, реализующее процедуру построения рекуррентной последовательности. Регистр сдвига состоит из конечного числа ячеек, которые занумерованы числами от 1 до m и могут содержать элементы конечного алфавита A, и правила преобразования совокупности заполнений этих ячеек. Как правило, на практике используются регистры сдвига с двоичным алфавитом $A = \{0, 1\}$ и правилом преобразования, состоящим в вычислении значения булевой функции обратной связи f от заполнений ячеек, перемещении заполнения ячейки с номером k в ячейку с номером $k-1$, $k = 2, \ldots, m$, и засылке вычисленного значения функции f в ячейку с номером m; значения, выходящие из ячейки с номером 1, образуют выходную последовательность, кото-

рая может использоваться, например, как последовательность псевдослучайных чисел при статистическом моделировании или шифровании сообщений. Достоинством такого способа порождения псевдослучайных последовательностей являются простота конструкции, высокая скорость и возможность теоретического исследования условий, обеспечивающих заданную величину периода выходной последовательности, а также некоторых ее свойств.

Если функция обратной связи неизвестна, то при некоторых условиях для ее восстановления достаточно знать ее значения на некотором достаточном числе наборов аргументов. Предположим, что для нескольких наборов, скажем, для n наборов, случайно равновероятно выбранных из $\binom{N}{n}$ таких возможных наборов, нам известны значения функции обратной связи. Возможность ее восстановления зависит от того, как эти n наборов расположены. В частности, возможность восстановления может зависеть от числа наборов, занимающих на окружности подряд идущие позиции. В таком случае интерес представляет характеристика, равная максимальному числу таких подряд идущих (соседних) наборов в случайной последовательности длины n.

Поскольку выбранная последовательность наборов случайна, рассмотрим следующую вероятностную задачу.

Занумеруем расположенные на окружности $N = 2^m$ наборов длины m числами от 1 до N в порядке их расположения на окружности в направлении по часовой стрелке, начиная с произвольно выбранного набора.

Среди N наборов случайно выбирается n наборов. На окружности с 2^m равноотстоящими точками они представлены n точками, образующими некоторое число s связных дуг (подряд расположенных точек). Занумеруем эти дуги в порядке возрастания номеров первых точек дуг. Пусть $r_1, \ldots, r_s$ — длины этих дуг; ясно, что

$$r_1 + \cdots + r_s = n.$$

Промежутки между дугами имеют положительные длины $j_1, \ldots, j_s$, где j_1 есть число точек на окружности между первой и второй дугами, j_k есть число точек на окружности между k-й и $(k+1)$-й дугами и j_s есть число точек между последней и первой дугами. Такое расположение точек на окружности будем называть конфигурацией с параметрами $(r_1, \ldots, r_s; j_1, \ldots, j_s)$.

Без ограничения общности будем считать, что первая дуга (длины r_1) начинается в точке окружности с номером 1, так что последняя, s-я дуга оканчивается в точке $n - j_s$.

Найдем число конфигураций с фиксированными $r_1, \ldots, r_s$ и различными допустимыми $j_1, \ldots, j_s$. Нетрудно видеть, что число наборов длин $j_1, \ldots, j_s$ этих дуг можно вычислить, расположив составляющие их $N - n = j_1 + \cdots + j_s$ точек, занумерованных числами $1, \ldots, N - n$, на окружности с $N-n$ равноотстоящими точками и выбрав среди $N - n$ промежутков между этими точками всеми различными способами s промежутков. В результате получаем все различные наборы разделяющих дуг всевозможных положительных длин, и выбрать промежутки, разделяющие s дуг на окружности с $N - n$ точками, можно $\binom{N-n}{s}$ способами. Поэтому число конфигураций с ровно s дугами равно $\binom{N-n}{s}$. Для простоты будем считать, что при $s = 0$ существует ровно одна конфигурация. Кроме того, будем считать две конфигурации совпадающими, если они совпадают при некотором сдвиге их дуг на окружности с $N = 2^m$ равноотстоящими точками с сохранением промежутков между ними. Поэтому будем считать, что n выбрано так, что все конфигурации различны. Можно показать, что это требование выполняется, если n нечетно (см. [1]).

При случайном выборе n наборов число s дуг наборов есть случайная величина, которую обозначим $\nu_{n,N}$. Ее естественно интерпретировать как число ячеек, в которые проводится размещение n частиц. При $\nu_{n,N} = s$ числа $r_1, \ldots, r_s$ будем понимать как заполнения ячеек с номерами $1, \ldots, s$ соответственно. При случайном выборе n наборов эти величины являются случайными, при $\nu_{n,N} = s$ обозначим их $\eta_1, \ldots, \eta_s$. Чтобы нумерация не влияла на вероятностное распределение величин $\eta_1, \ldots, \eta_s$, в качестве первой всегда берем дугу, содержащую первую размещенную точку при последовательном случайном размещении единиц на окружности с $N = 2^m$ равноотстоящими точками, и сдвинем ее так, что ее первая единица расположится в точке окружности с номером 1.

Как было отмечено выше, число различных выборов разделяющих промежутков равно $\binom{N-n}{s}$. С учетом соглашения, что при $s = 0$ (тогда и $n = 0$) существует ровно одна конфигурация, суммируя по s от 0 до $N - n$, получаем, что общее число различных равновероятных исходов равно

$$\sum_{s=0}^{N-n} \binom{N-n}{s} = 2^{N-n}.$$

Таким образом, справедливо следующее утверждение.

Теорема 1. *Случайная величина $\nu_{n,N}$ имеет биномиальное распределение с параметрами $(N-n, 1/2)$, иными словами,*

$$\mathsf{P}\{\nu_{n,N} = s\} = \binom{N-n}{s}\frac{1}{2^{N-n}}, \quad s = 0, 1, \ldots, N-n.$$

Напомним, что класс конфигураций, циклические сдвиги которых различны (не совпадают при наложении), называется ожерельем [4]. Известна формула для числа ожерелий при заданных n и N (см. [4]), из которой в нашем случае, где N — четное число, а n нечетно, следует, что число ожерелий равно $\frac{1}{N}\binom{N}{n}$. Число конфигураций равно $\binom{N}{n}$, так что в среднем на одно ожерелье приходится N конфигураций. Число сдвигов одной конфигурации равно N, и ожерелье не может содержать больше, чем N конфигураций, поэтому каждое ожерелье содержит ровно N конфигураций, то есть все сдвиги любой конфигурации различны. Таким образом, справедливо следующее утверждение.

Теорема 2. *Если N — четное число, а n нечетно, то все сдвиги любой конфигурации различны, то есть не совпадают при сдвигах на не кратное N число вершин.*

Далее будем считать, что $\nu_{n,N} = s$, и полученные результаты затем можно усреднить по распределению $\nu_{n,N}$. Обратимся к случайным величинам $\eta_1, \ldots, \eta_s$. Справедливо следующее утверждение.

Теорема 3. *При условии, что $\nu_{n,N} = s$, справедливо равенство*

$$\mathsf{P}\{\eta_1 = r_1, \ldots, \eta_s = r_s\} = \mathsf{P}\{\xi_1 = r_1, \ldots, \xi_s = r_s \mid \xi_1 + \cdots + \xi_s = n\}, \tag{1}$$

где $\xi_1, \ldots, \xi_s$ — независимые одинаково распределенные случайные величины, принимающие значения $1, \ldots, n$ с одинаковыми вероятностями, целые $r_1, \ldots, r_s \geqslant 1$, $r_1 + \cdots + r_s = n$. Иными словами, случайные величины $\eta_1, \ldots, \eta_s$ образуют обобщенную схему размещения с равномерно распределенными случайными величинами $\xi_1, \ldots, \xi_s$.

Доказательство. Поскольку n вершин окружности с N вершинами выбираются из N вершин равновероятно, вне зависимости от значений $r_1, \ldots, r_s$, справедливо равенство

$$\mathsf{P}\{\eta_1 = r_1, \ldots, \eta_s = r_s\} = \binom{n}{s}^{-1}, \tag{2}$$

где $r_1 + \cdots + r_s = n$, $r_1, \ldots, r_s \geqslant 1$. С другой стороны, для таких $r_1, \ldots, r_s$

$$\mathsf{P}\{\xi_1 = r_1, \ldots, \xi_s = r_s \mid \xi_1 + \cdots + \xi_s = n\} = \frac{\mathsf{P}\{\xi_1 = r_1, \ldots, \xi_s = r_s\}}{\mathsf{P}\{\xi_1 + \cdots + \xi_s = n\}}. \tag{3}$$

Здесь

$$\mathsf{P}\{\xi_1 = r_1, \ldots, \xi_s = r_s\} = \frac{1}{n^s}, \tag{4}$$

и

$$\mathsf{P}\{\xi_1 + \cdots + \xi_s = n\} = \sum_{\substack{r_1,\ldots,r_s \\ r_1+\cdots+r_s=n}} \mathsf{P}\{\xi_1 = r_1, \ldots, \xi_s = r_s\} = \frac{1}{n^s}\binom{n}{s}. \tag{5}$$

Равенство (1) следует из (2)–(5). □

Теорема 3 позволяет для изучения поведения $\eta_1, \ldots, \eta_s$ применить хорошо известные методы, используемые в контексте обобщенной схемы размещения (см., например, [2, 3]).

Однако без использования обобщенной схемы размещения можно также получить результат, представляющий самостоятельный интерес. Обозначим через ρ_s максимальное значение величин $\eta_1, \ldots, \eta_s$ и оценим вероятность того, что выполнено неравенство $\rho_s \leqslant r$, где r — целое положительное число. Получим оценку вероятности

$$\mathsf{P}\{\rho_s \leqslant 1\} = \mathsf{P}\{\rho_s = 1\}$$

как раз вне рамок обобщенной схемы размещения.

Ясно, что в этом случае каждая из n размещаемых частиц должна окаймляться дугами положительной длины, состоящими из оставшихся $N-n$ точек окружности, и $s = n$. Поскольку число произвольных (без этого ограничения) размещений n вершин на N позициях на окружности равно $\binom{N}{n}$, а число разбиений $N-n$ вершин на окружности на n дуг ненулевых длин равно $\binom{N-n}{n}$, для искомой вероятности справедливо равенство

$$\mathsf{P}\{\rho_s = 1\} = \mathsf{P}\{\rho_n = 1\} = \binom{N-n}{n}\binom{N}{n}^{-1}. \tag{6}$$

Используя равенство (6), получаем следующее утверждение.

Теорема 4. *Если $N \to \infty$ и n есть либо постоянная, либо $n \to \infty$ таким образом, что*

$$\frac{n^2}{N} \to 0,$$

то

$$\mathsf{P}\{\rho_s = 1\} \to 1.$$

Если $N, n \to \infty$ так, что

$$\frac{n^2}{N} \to a > 0,$$

то

$$\mathsf{P}\{\rho_s = 1\} \to e^{-a}.$$

Если $N, n \to \infty$ так, что

$$\frac{n^2}{N} \to \infty,$$

то

$$\mathsf{P}\{\rho_s = 1\} \to 0.$$

Доказательство. Используя соотношение (6), получаем равенство

$$\mathsf{P}\{\rho_s = 1\} = \binom{N-n}{n}\binom{N}{n}^{-1} = \\ = \frac{(N-n)!}{(N-2n)!\,n!}\frac{n!\,(N-n)!}{N!}.$$

Применяя известную формулу Стирлинга при $N \to \infty$ и $N - 2n \to \infty$, находим, что

$$\binom{N-n}{n}\binom{N}{n}^{-1} = \\ = \frac{(\sqrt{2\pi(N-n)}(N-n)^{N-n}e^{-N+n})^2}{\sqrt{2\pi N}N^N e^{-N}\sqrt{2\pi(N-2n)}(N-2n)^{N-2n}} \times \\ \times \frac{(1+O(1/N))}{e^{-N+2n}} = \\ = \frac{2\pi(N-n)(N-n)^{2N-2n}}{2\pi\sqrt{N}N^N\sqrt{N-2n}(N-2n)^{N-2n}} \times \\ \times (1+O(1/N)) = \\ = \frac{(N-n)N^{2N-2n}}{\sqrt{(N-2n)N}(N-2n)^{N-2n}N^N} \times \\ \times (1+O(1/N)).$$

Главный член первого множителя есть

$$a_1 = \frac{N-n}{\sqrt{(N-2n)N}} = \\ = \frac{N(1+O(n/N))}{N\sqrt{1-2n/N}} = \\ = 1 + o(1),$$

а главный член второго множителя есть

$$a_2 = \frac{(N-n)^{2N-2n}}{(N-2n)^{N-2n}} = \\ = \frac{(1-n/N)^{2N-2n}N^{2N-2n}}{N^{2N-2n}(1-2n/N)^{N-2n}} = \\ = \frac{(1-n/N)^{2N-2n}}{(1-2n/N)^{N-2n}}.$$

Пусть $n^2/N \to 0$, тогда

$$\ln a_2 = \ln(1-n/N)^{2N-2n} - \ln(1-2n/N)^{N-2n} = \\ = (2N-2n)(-n/N + O(n^2/N)) - \\ - (N-2n)(-2n/N)^{N-2n} = \\ = -2n + O(n^2/n) + 2n + O(n^2/N).$$

Таким образом, $\ln a_2 \to 0$, и значит, $a_2 \to 1$. Отсюда следует первое утверждение теоремы 4.

Пусть теперь $n, N \to \infty$ таким образом, что $n^2/N \to a > 0$. Тогда, как и выше, $a_1 \to 1$, а

$$\ln a_2 = (2N-2n)\ln(1-n/N) - \\ - (N-2n)\ln(1-2n/N) = \\ = -(2N-2n)(-n/N - n^2/(2N^2) + \\ + O(n^3/N^3)) - \\ - (N-2n)(-2n/N - n^2/(2N^2) + \\ + O(n^3/N^3)) = \\ = -2n - \frac{n^2}{N} + \frac{2n^2}{N} + \\ + 2n + \frac{2n^2}{N} - \frac{4n^2}{N} + O\left(\frac{n^3}{N^2}\right) = \\ = -\frac{n^2}{N} + O\left(\frac{n^3}{N^2}\right). \qquad (7)$$

Таким образом, в этом случае $\ln a_2 \to -a$, иными словами,

$$\mathsf{P}\{\rho_s = 1\} \to e^{-a},$$

и второе утверждение теоремы 4 доказано.

Пусть теперь $n, N \to \infty$ так, что $n^2/N \to \infty$. Нетрудно видеть, что в этом случае для логарифма $\ln a_2$ справедливо соотношение (7), из которого следует, что a_2 стремится к нулю. □

Литература

1. *Виленкин Н. Я.* Комбинаторика. М.: Наука, 1969.

2. *Колчин А. В.* Предельные теоремы для обобщенной схемы размещения // Дискретная математика. 2003. Т. 15, № 4. С. 148–157.

3. *Колчин А. В.* Предельные теоремы для обобщенной схемы размещения // Обозрение прикладной и промышленной математики. 2009. Т. 16, № 3. С. 432–435.

4. *Риордан Дж.* Введение в комбинаторный анализ. М.: Изд-во иностранной литературы, 1963.

5. *Golomb S. W.* Shift Register Sequences Ægean Park Press, Laguna Hills, California, 1982.

6. *Menezes A. J., van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, 1997.

СВЕДЕНИЯ ОБ АВТОРЕ:

Колчин Андрей Валентинович
к. ф.-м. н.
эл. почта: andrei.kolchin@gmail.com

Kolchin, Andrey
e-mail: andrei.kolchin@gmail.com