Труды по дискретной математике
Том 5, с. 167–172
М.: ФИЗМАТЛИТ, 2002

ИССЛЕДОВАНИЕ ЧИСЛА ЦИКЛИЧЕСКИХ ТОЧЕК АВТОМАТА ИЗ РЕГИСТРОВ С НЕРАВНОМЕРНЫМ ДВИЖЕНИЕМ

В.Г. МИХАЙЛОВ

С целью разработки математических методов исследования датчиков с неравномерным движением регистров строится комбинаторно-вероятностная модель, позволяющая оценивать значения ряда важных характеристик графа внутренних состояний датчика. В работе получены оценки для среднего числа точек, лежащих на циклах графа внутренних состояний, показывающие, что таких точек в графе датчика довольно много. В рассмотренных случаях их число существенно больше числа циклических точек в графе равновероятного случайного отображения.

Рассмотрим автомат A, содержащий r регистров сдвига с линейными или нелинейными обратными связями и блок управления движением, который по набору текущих состояний регистров определяет, на сколько шагов должен продвинуться (в смысле движения текущего состояния по циклу внутренних состояний) каждый из регистров за один такт. При неравномерном движении регистров граф внутренних состояний автомата A, вообще говоря, не будет циклическим, а будет отвечать некоторому отображению множества внутренних состояний в себя. Поэтому число реально используемых внутренних состояний в процессе работы может уменьшаться и оказаться существенно меньше общего числа внутренних состояний $L = l_1 \dots l_r$, где $l_1 \le \dots \le l_r$ — длины циклов регистров. Этот процесс редукции множества внутренних состояний будет проходить до тех пор, пока не останутся только точки, лежащие на циклах графа отображения. Эти точки обычно называются циклическими.

При изучении типичных значений числа циклических точек и других характеристик графа внутренних состояний полезной является математическая модель, введенная и изученная в 70-е годы А. П. Алферовым и Г. В. Проскуриным. Согласно этой модели эволюция внутреннего состояния датчика описывается случайным блужданием на окружности (при $r = 1$) или торе (при $r \ge 2$). Используя эту модель, мы получим неравенства и точные выражения для среднего числа циклических точек в случайном автомате из исследуемого класса. Будет также показано, что в рассмотренном автомате число циклических точек существенно больше, чем число циклических точек в графе равновероятного случайного отображения.

Опишем формально исследуемый класс датчиков. С математической точки зрения любой программный датчик представляет собой автономный конечный автомат, определяемый конечными множествами Q и Y и функциями $g\colon Q \to Q$, $f\colon Q \to Y$, описывающими правило смены внутреннего состояния

$$q_{t+1} = g(q_t)$$

и правило выработки знака выходной последовательности

$$y_t = f(q_t).$$

© В.Г. Михайлов, 2002

Схематически автономный конечный автомат может быть изображен в виде помеченного ориентированного графа G, вершинами которого являются элементы множества Q (внутренние состояния), а дугами (направленными ребрами) — пары $(q, g(q))$. Каждая вершина помечена знаком $y = f(q)$, который вырабатывается при выходе из вершины. При изучении интересующих нас свойств графа G метки никакого значения не имеют, поэтому мы далее их рассматривать не будем.

В нашем случае внутреннее состояние естественно описывать вектором $q = (q^1, \dots, q^r)$, где $q^i \in Q^i = \{0, 1, \dots, l_i - 1\}$, $i = 1, \dots, r$. Функция переходов в нашем случае описывается равенствами

$$g(q) = \big(q^1 + k^1(q), \dots, q^r + k^r(q)\big), \tag{1}$$

с заранее заданными функциями

$$k^i \colon Q \to \{1, \dots, K_i\}, \quad i = 1, \dots, r, \tag{2}$$

при некоторых заданных числах $1 \le K_i \le l_i$, причем сложения в (1) производятся по модулям $l_1, \dots, l_r$, соответственно. Параметры $l_1, \dots, l_r$, $K_1, \dots, K_r$ и условие (2) определяют интересующий нас класс конечных автоматов $\mathcal{A}$. Всего в классе $\mathcal{A}$ содержится $(\prod_{i=1}^{r} K_i)^{l_1 \dots l_r}$ конечных автоматов.

Основные результаты работы формулируются следующим образом. Выберем случайно и равновероятно автомат A_{rand} из $\mathcal{A}$. (Все характеристики этого автомата также будем помечать индексом rand.) Отвечающие этому случайному автомату функции $k^1_{\text{rand}}, \dots, k^r_{\text{rand}}$ будут независимыми, а набор $k^1_{\text{rand}}(q), \dots, k^r_{\text{rand}}(q)$ $(q \in Q)$, будет системой независимых в совокупности равновероятно распределенных на соответствующих конечных множествах случайных величин. Выберем произвольное начальное внутреннее состояние $q_0 \in Q$. Пусть $C(A, n)$ — множество циклических точек автомата A, лежащих на циклах длины n, $C(A)$ — множество всех циклических точек.

Пусть

$$B_K(n, m) = \frac{1}{K^n} \sum \frac{n!}{n_1! \dots n_K!},$$

где K — целое положительное число и суммирование проводится по всем наборам неотрицательных целых чисел $n_1, \dots, n_k$, удовлетворяющих условиям

$$n_1 + n_2 + \dots + n_K = n, \qquad n_1 + 2n_2 + \dots + Kn_K = m.$$

Заметим, что

$$B_K(n, m) = 0, \quad \text{если } n > m \quad \text{или} \quad \text{если } Kn < m. \tag{3}$$

Теорема 1. *При* $n \ge 1$

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}}, n)\} \le \prod_{i=1}^{r} \Bigg(\sum_{n/l_i \le d_i \le K_i n/l_i} B_{K_i}(n, d_i l_i) \Bigg), \tag{4}$$

причем при $n < 2M$, *где* $M = \max_i\{l_i/K_i\}$, *в* (4) *имеет место равенство.*

Замечание 1. Равенство в (4) имеет особенно простой вид при $K_1 = \dots = K_r = 2$. Тогда, если $l_r/2 \le n < l_1$, то

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}}, n)\} = \frac{1}{2^{rn}} \prod_{i=1}^{r} \frac{n!}{(l_i - n)!(2n - l_i)!}. \tag{5}$$

Равенство (4) (при $n < 2M$) и очевидное неравенство

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}})\} \ge \prod_{n=1}^{m} \mathbf{P}\{q_0 \in C(A_{\text{rand}}, n)\}, \quad 1 \le L, \tag{6}$$

влекут следующие оценки для характеристик распределения общего числа циклических точек.

СЛЕДСТВИЕ 1. *Выполняются неравенства*

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}})\} \geq \sum_{n=1}^{2M-1} \prod_{i=1}^{r} \Bigg(\sum_{n/l_i \leq d_i \leq K_i n/l_i} B_{K_i}(n, d_i l_i) \Bigg),$$

$$\mathbf{E}|C(A_{\text{rand}})| \geq L \sum_{n=1}^{2M-1} \prod_{i=1}^{r} \Bigg(\sum_{n/l_i \leq d_i \leq K_i n/l_i} B_{K_i}(n, d_i l_i) \Bigg).$$

Пусть $N(q_0)$ — число автоматов в классе $\mathcal{A}$, для которых точка q_0 является циклической. С помощью равенства

$$|\mathcal{A}| = \Bigg(\prod_{i=1}^{r} K_i \Bigg)^{l_1 \ldots l_r}$$

утверждению следствия 1 можно придать следующий вид.

СЛЕДСТВИЕ 2. *Выполняется неравенство*

$$N(q_0) \geq \sum_{n=1}^{2M-1} \prod_{i=1}^{r} \Bigg(K_i^{l_1 \ldots l_r} \sum_{n/l_i \leq d_i \leq K_i n/l_i} B_{K_i}(n, d_i l_i) \Bigg).$$

Из равенства (5) можно вывести асимптотические выражения для среднего числа вершин графа внутренних состояний автомата A_{rand}, лежащих на циклах длин $n < 2M$, и асимптотическое выражение для нижней оценки общего числа циклических точек этого автомата. Получаемый при этом результат является новым лишь отчасти (аналогичные результаты были получены в свое время Г.В. Проскуриным). Но он важен для изложения, поскольку наглядно демонстрирует степень редукции множества активных внутренних состояний.

Пусть ζ — число вершин графа внутренних состояний автомата A_{rand}, лежащих на циклах длины не более $2M - 1$.

ТЕОРЕМА 2. *Пусть* $K_1 = \ldots = K_r = 2$, $l_1 = l \to \infty$, $l_i = l + s_i l^{1/2} + o(l^{1/2})$, $i = 2, \ldots, r$. *Тогда равномерно по* z *из любого фиксированного конечного интервала*

$$\mathbf{E}\left| C\left(A_{\text{rand}}, \frac{2l}{3} + z l^{1/2} \right) \right| = \left(\frac{3l}{\pi} \right)^{r/2} \exp\left\{ -\frac{27r}{4}\left(z - \frac{2\sigma}{3r} \right)^2 - \frac{3\Sigma}{2r} \right\}(1 + o(1)), \quad (7)$$

где $\sigma = s_1 + \ldots + s_r$, $\Sigma = \sum_{i,j=1}^{r} (s_i - s_j)^2$. *Кроме того,*

$$\mathbf{E}|C(A_{\text{rand}})| \geq \mathbf{E}\zeta = \frac{2\pi}{9\sqrt{r}} \left(\frac{3l}{\pi} \right)^{(r+1)/2} \exp\left\{ -\frac{3\Sigma}{2r} \right\}(1 + o(1)). \quad (8)$$

З а м е ч а н и е 2. Теорема 2 показывает, что в рассмотренном случае редукция множества активных внутренних состояний случайного датчика из множества $\mathcal{A}$ относительно умеренна. Чтобы убедиться в этом, достаточно сравнить оценку (8) с известной асимптотикой среднего числа циклических точек равновероятного случайного отображения на множестве из $L = l^r$ элементов (см. [1, с. 238]). Эта асимптотика имеет вид

$$\sqrt{\pi/2}\, l^{r/2}(1 + o(1)), \quad l \to \infty,$$

что по порядку в $\sqrt{l}$ раз меньше, чем в оценке (8) теоремы 2.

З а м е ч а н и е 3. Непосредственными вычислениями можно показать, что при $r = 1$, $l \to \infty$

$$\mathbf{E}|C(A_{\text{rand}})| = \mathbf{E}\zeta(1 + o(1)).$$

Поэтому при $r = 1$ выражение в правой части (8) совпадает с асимптотическим выражением для среднего числа циклических точек автомата A_{rand} с одним регистром.

Доказательство теоремы 1. Рассмотрим случайное блуждание $S(t) = (S_1(t), \dots, S_r(t))$ на множестве Q, выходящее из точки $S(0) = q_0$ и определяемое при $t = 1, 2, \dots$ равенствами

$$S_i(t) = S_i(t-1) + X_i(t) \bmod l_i, \quad i = 1, \dots, r, \tag{9}$$

где $\{X_i(t) \in \{1, \dots, K_i\},\ i = 1, \dots, r,\ t = 1, 2, \dots\}$ — система независимых в совокупности равновероятно распределенных на соответствующих конечных множествах случайных величин. Далее будем использовать векторную запись равенств (9)

$$S(t) \equiv S(t-1) + X(t),$$

подразумевая под ней систему равенств (9). Аналогично запишем уравнение эволюции внутренних состояний случайного автомата:

$$q_{\text{rand}}(t+1) \equiv q_{\text{rand}}(t) + k_{\text{rand}}(q(t)).$$

Наши рассуждения опираются на следующее свойство, вытекающее из равновероятности и независимости величин $k^1_{\text{rand}}(q), \dots, k^r_{\text{rand}}(q)$, $q \in Q$.

Лемма 1. *При всех неотрицательных целых $n \le |Q|$ и всех наборах попарно различных $q_0, q_1, \dots, q_{n-1} \in Q$ условные функции распределения*

$$\mathcal{L}\left(X(1), \dots, X(n) | S(1) = q_1, \dots, S(n-1) = q_{n-1}\right),$$

$$\mathcal{L}\left(k_{\text{rand}}(q_{\text{rand},0}), \dots, k_{\text{rand}}(q_{\text{rand},n-1}) | q_{\text{rand},1} = q_1, \dots, q_{\text{rand},n-1} = q_{n-1}\right)$$

совпадают (заметим, что $q_{\text{rand},0} = q_0$).

Вернемся к доказательству теоремы 1. Нам достаточно рассмотреть случай $m \le L$. Воспользуемся леммой 1 при анализе вероятности события $\{q_0 \in C(A_{\text{rand}}, m)\}$. Обозначим через Q_{n-1} множество всех $(|Q| - 1)_{n-1}$ наборов $(q_1, \dots, q_{n-1})$ из попарно различных $q_1, \dots, q_{n-1} \in Q \backslash \{q_0\}$.

Очевидно, что

$$\{q_0 \in C(A_{\text{rand}}, n)\} = \bigcup_{Q_{n-1}} \{k_{\text{rand},s} \equiv q_t - q_{t-1}, t = 1, \dots, n-1, k_{\text{rand},n-1} \equiv q_0 - q_{0-1}\}.$$

Используя лемму 1, находим, что

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}}, m)\} = \mathbf{P}\{H\}, \tag{10}$$

$$H = \bigcup_{Q_{n-1}} A(q_1, \dots, q_{n-1}; q_0), \tag{11}$$

где

$$A(q_1, \dots, q_{n-1}; q_0) = \{X(t) \equiv q_t - q_{t-1}, t = 1, \dots, n-1, X(n) \equiv q_0 - q_{0-1}\} = \\ = \{S(t) = q_t, t = 1, \dots, n-1, S(n) = q_0\}.$$

Из равенства (11) следует, в частности, что

$$H \subseteq \{S(n) = q_0\}. \tag{12}$$

Из (10) и (12) следует неравенство

$$\mathbf{P}\{q_0 \in C(A_{\text{rand}}, n)\} \le \mathbf{P}\{S(n) = q_0\}.$$

Осталось заметить, что

$$\mathbf{P}\{S(n) = q_0\} = \mathbf{P}\{X(1) + \ldots + X(n) \equiv 0\} = \prod_{i=1}^{r} \Bigg(\sum_{n/l_i \le d_i \le Kn/l_i} B_K(n, d_i l_i) \Bigg).$$

Этим неравенство (4) доказано.

Далее нам понадобится следующее утверждение.

ЛЕММА 2. *Пусть* $n \le 2M$ *и* $(q_1, \dots, q_{n-1}) \in Q^{n-1} \backslash Q_{n-1}$. *Тогда*

$$\mathbf{P}\{A(q_1, \dots, q_{n-1}; q_0)\} = 0. \tag{13}$$

Доказательство леммы 2. Очевидно, что из условий леммы вытекает соотношение

$$A(q_1, \dots, q_{n-1}; q_0) \subseteq \bigcup_{1 \le s < t \le n} \{S(s) = S(t), S(n) = q_0\}, \tag{14}$$

а

$$\{S(s) = S(t), S(n) = q_0\} = \{X(s+1) + \ldots + X(t) \equiv 0,$$
$$X(1) + \ldots + X(s) + X(t+1) + \ldots + X(n) \equiv 0\}, \tag{15}$$

причем обе суммы не пустые. Поскольку $n < 2M$, хотя бы одна сумма в правой части (15) состоит из n', $0 < n' < M$, слагаемых. Но сумма $X(1) + \ldots + X(n')$ такого числа слагаемых не может быть сравнима с нулем, поскольку для координаты с номером $i' = \arg\max\{l_i/K_i\}$ выполняются неравенства

$$\mathbf{P}\{0 < X_{i'}(1) + \ldots + X_{i'}(n') < l_{i'}\} = 1.$$

Поэтому вероятность события в правой части (15) равна нулю. Теперь из (15) и (14) следует (13). Лемма 2 доказана.

Продолжим доказательство теоремы 1. Пусть теперь $n < 2M$. Очевидно, что

$$\mathbf{P}\{H\} = \sum_{Q_{n-1}} \mathbf{P}\{A(q_1, \dots, q_{n-1}; q_0)\}.$$

Кроме этого, согласно лемме 2

$$\sum_{Q_{n-1}} \mathbf{P}\{A(q_1, \dots, q_{n-1}; q_0)\} = \mathbf{P}\{S(n) = q_0\}.$$

Поэтому

$$\mathbf{P}\{H\} = \mathbf{P}\{S(n) = q_0\}.$$

Отсюда и из (10) следует равенство в (4). Теорема 1 доказана.

Доказательство теоремы 2. Оценим факториалы, входящие в выражение (5) с помощью формулы Стирлинга (см., например, [2, с. 72]). Заметим сразу, что все производимые ниже оценки равномерны по z из любого фиксированного конечного интервала. Возьмем

$$n = \frac{2l}{3} + z\sqrt{l}, \quad z = O(1).$$

Тогда при $l \to \infty$

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n = \sqrt{2\pi n}\left(\frac{2l}{3e}\right)^n \left(1 + \frac{3z}{2\sqrt{l}}\right)^{2l/3 + z\sqrt{l}} =$$
$$= \sqrt{2\pi n}\left(\frac{2l}{3e}\right)^n \exp\left\{\left(\frac{2l}{3} + z\sqrt{l}\right)\left(\frac{3z}{2\sqrt{l}} - \frac{9z^2}{8l} + O\left(l^{-3/2}\right)\right)\right\} =$$
$$= \sqrt{\frac{4\pi l}{3}}\left(\frac{2l}{3e}\right)^n \exp\left\{z\sqrt{l} + \frac{3}{4}z^2\right\}(1 + o(1)). \tag{16}$$

Аналогично выводятся формулы

$$(l_i-n)!\sqrt{\frac{2\pi l}{3}}\left(\frac{l}{3e}\right)^{l-n}\exp\left\{(s_i-z)\sqrt{l}+\frac{3}{2}(s_i-z)^2\right\}(1+o(1)), \qquad (17)$$

$$(2n-l_i)!\sqrt{\frac{2\pi l}{3}}\left(\frac{l}{3e}\right)^{2n-l}\exp\left\{(2z-s_i)\sqrt{l}+\frac{3}{2}(2z-s_i)^2\right\}(1+o(1)), \qquad (18)$$

где $i=1,\dots,r$, $s_1=0$. Используя (16)–(18), приходим к равенству

$$\frac{1}{2^{rn}}\prod_{i=1}^{r}\frac{n!}{(l_i-n)!(2n-l_i)!}=$$

$$=\left(\frac{3}{\pi l}\right)^{r/2}\exp\left\{-\frac{27r}{4}\left(z-\frac{2\sigma}{3r}\right)^2+\frac{3}{r}(\sigma-r\sigma_2)\right\}(1+o(1)), \qquad (19)$$

где $\sigma_2=s_1^2+\ldots+s_r^2$. Из формул (5), (19) и равенства

$$\mathbf{E}|C(A_{\mathrm{rand}},n)|=l^r\,\mathbf{P}\{q_0\in C(A_{\mathrm{rand}},n)\}$$

после несложных преобразований получаем (7).

Докажем соотношения (8). Неравенство в (8) очевидно. Чтобы доказать равенство для $\mathbf{E}\zeta$, сложим выражения (7) для всех n от 1 до $m=2l/3+u\sqrt{l}$ и рассмотрим полученное выражение как интегральную сумму (с $\Delta z=1/\sqrt{l}$) для главного члена правой части (19). Тогда в силу гладкости подынтегральной функции и равномерности по z оценки для остаточного члена в (19)

$$\sum_{n=1}^{m}\mathbf{P}\{q_0\in C(A_{\mathrm{rand}},n)\}=$$

$$=\sqrt{l}e^{-3\Sigma/(2r)}\left(\frac{3}{\pi l}\right)^{r/2}\int_{-\infty}^{u}\exp\left\{-\frac{27r}{4}\left(z-\frac{2\sigma}{3r}\right)^2\right\}dz(1+o(1)).$$

Отсюда, используя формулу Стирлинга для оценки факториалов в формуле (5) при $m<n\le 2M-1$, нетрудно вывести равенство

$$\sum_{n=1}^{2M-1}\mathbf{P}\{q_0\in C(A_{\mathrm{rand}},n)\}=$$

$$=\sqrt{l}e^{-3\Sigma/(2r)}\left(\frac{3}{\pi l}\right)^{r/2}\int_{-\infty}^{\infty}\exp\left\{-\frac{27r}{4}\left(z-\frac{2\sigma}{3r}\right)^2\right\}dz(1+o(1))+o(1).$$

Группируя вместе остаточные члены и используя равенство

$$\int_{-\infty}^{\infty}e^{-Hz^2/2}dz=\sqrt{\frac{2\pi}{H}},\quad H>0,$$

получаем

$$\sum_{n=1}^{2M-1}\mathbf{P}\{q_0\in C(A_{\mathrm{rand}},n)\}=\frac{2}{3\sqrt{r}}\left(\frac{3}{\pi l}\right)^{(r-1)/2}e^{-3\Sigma/(2r)}(1+o(1)). \qquad (20)$$

Домножив (20) на l^r, получим выражение для $\mathbf{E}\zeta$ в (8). Теорема 2 доказана.

Автор признателен И. В. Харламову за ряд полезных замечаний.

СПИСОК ЛИТЕРАТУРЫ

1. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. — М.: Наука, 1978.
2. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т.1. — М: Мир, 1984.