

13 Свойства л.р.п.

13.1 Период л.р.п.

Множество состояний \mathcal{S} конечного автомата конечно и при функционировании автомата рано или поздно встретятся два одинаковых внутренних состояния: $S_t = S_\tau$, $t \neq \tau$. Данное совпадение приведет к совпадениям состояний $S_{t+1} = \varphi(S_t) = \varphi(S_\tau) = S_{\tau+1}$, $S_{t+2} = S_{\tau+2}$, ... и совпадениям выходных символов

$$\gamma_t = \pi(S_t) = \pi(S_\tau) = \gamma_\tau, \quad \gamma_{t+1} = \gamma_{\tau+1}, \quad \gamma_{t+2} = \gamma_{\tau+2}, \dots$$

Таким образом, выходная последовательность всякого конечного автомата оказывается периодической. При использовании автомата для криптографических нужд желательно, чтобы период выходной последовательности был как можно больше (см., напр., задачу S2).

Определение 13.1. Последовательность $\gamma_1, \gamma_2, \dots$ называется *периодической*, если найдутся целые $t_0 \geq 0$ и $r > 0$ такие, что

$$\gamma_{t+r} = \gamma_t$$

для всех $t > t_0$. При этом r называется *периодом* последовательности, а наименьший из всех возможных периодов называется *минимальным периодом*. \square

Определение 13.2. Пусть $\gamma_1, \gamma_2, \dots$ — периодическая последовательность с минимальным периодом r . Наименьшее целое $t_0 \geq 0$ такое, что $\gamma_{t+r} = \gamma_t$ для всех $t > t_0$ называется *предпериодом* последовательности. Периодическая последовательность называется *чисто периодической*, если ее предпериод $= 0$. \square

Пример 13.1. Рассмотрим последовательность десятичных знаков дроби

$$\frac{11}{12} = 0.91666\dots$$

Период данной последовательности — 1, предпериод — 2. \square

Перейдем к анализу периода л.р.п. (s_t) порядка n с неприводимым характеристическим многочленом $f(x)$. При выборе нулевых начальных условий $s_1 = s_2 = \dots = s_n = 0$ вся последовательность (s_t) также оказывается нулевой. Будем отбрасывать данный тривиальный случай и рассматривать только л.р.п. с ненулевыми начальными условиями.

Пример 13.2. Пусть $f(x) = x^4 + x + 1$, $g(x) = x^4 + x^3 + x^2 + x + 1$. Построим л.р.п. порядка 4 с характеристическими многочленами f и g и начальными условиями: $s_1 = s_2 = s_3 = 0$, $s_4 = 1$. Последовательности задаются рекуррентными соотношениями

$$s_{t+4} = s_{t+1} + s_t, \quad s_{t+4} = s_{t+3} + s_{t+2} + s_{t+1} + s_t,$$

выглядят следующим образом:

$$\begin{aligned} &0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, \dots, \\ &0, 0, 0, 1, 1, 0, 0, 0, 1, \dots, \end{aligned}$$

и имеют период 15 и 5 соответственно. Наша ближайшая задача — связать период л.р.п. со свойствами характеристических многочленов f и g . \square

Теорема 13.1 (о периоде л.р.п.). Пусть (s_t) — ненулевая л.р.п. с неприводимым характеристическим многочленом f и пусть $f(0) \neq 0$. Тогда (s_t) является чисто периодической последовательностью с минимальным периодом $\text{ord } \alpha$, где α — корень f в некотором расширении \mathbb{F}_2 .

Доказательство. Пусть M — сопровождающая матрица f (клетка Фробениуса). Поскольку $f(0) \neq 0$, матрица M обратима. Матрица M определяет действие РСЛОС, который генерирует (s_t) : $S_t = S_{t-1}M$, $s_t = S_{t,1}$, $t = 1, 2, \dots$. Обратимость M означает, что последовательность (S_t) является чисто периодической и, следовательно, чисто периодической является последовательность (s_t) .

Пусть r — период (s_t) . Тогда

$$s_{t+r} - s_t = \text{Tr}(b\alpha^t(\alpha^r - 1)) = 0, \quad t = 1, 2, \dots$$

Покажем, что $\alpha^r = 1$. От противного. Если $c = \alpha^r - 1 \neq 0$, то набор $(bc\alpha, bc\alpha^2, \dots, bc\alpha^n) = bc(\alpha, \alpha^2, \dots, \alpha^n)$ является базисом \mathbb{F}_{2^n} над \mathbb{F}_2 . Тогда из $\text{Tr}(bc\alpha^t) = 0$, $t = 1, 2, \dots, n$, следует, что $\text{Tr}(a) = 0$ для всех $a \in \mathbb{F}_{2^n}$. Но это противоречит сюръективности функции «след».

Итак, если r — период (s_t) , то $\alpha^r = 1$. Верно и обратное. Поэтому минимальный период (s_t) совпадает с $\text{ord } \alpha$ — минимальным r таким, что $\alpha^r = 1$. \square

13.2 Порядок многочлена

Определение 13.3. Пусть $f \in \mathbb{F}_2[x]$ и $f(0) \neq 0$. Порядком $\text{ord } f$ многочлена f называется минимальное натуральное e для которого

$$f(x) \mid x^e - 1.$$

Теорема 13.2 (о порядке многочлена). Пусть $f \in \mathbb{F}_2[x]$ — неприводимый многочлен степени n и $f(0) \neq 0$ (т. е. $f(x) \neq x$). Тогда $\text{ord } f = \text{ord } \alpha$, где α — любой из корней f в поле \mathbb{F}_{2^n} . Более того, $\text{ord } f \mid 2^n - 1$.

Доказательство. Первая часть теоремы следует из того, что равенство $\alpha^e = 1$ выполняется тогда и только тогда, когда $f(x) \mid x^e - 1$. Действительно, разделим $x^e - 1$ на $f(x)$:

$$x^e - 1 = f(x)g(x) + r(x), \quad \deg r < n.$$

Подставляя в обе части $x = \alpha$, получаем $r(\alpha) = 0$. Но это возможно тогда и только тогда, когда $r = 0$ (см. доказательство леммы о базисе), т. е. $f(x) \mid x^e - 1$.

Последняя часть теоремы следует из того, что

$$\text{ord } \alpha \mid (\text{порядок } \mathbb{F}_{2^n}^*) = 2^n - 1$$

(по теореме Лагранжа). \square

Упражнение 13.1 (★). Предложить алгоритм определения $\text{ord } f$ при известной факторизации числа $2^{\deg f} - 1$. \square

Определение 13.4. Неприводимый многочлен $f(x) \in \mathbb{F}_2[x]$, отличный от x , называется *примитивным*, если $\text{ord } f = 2^{\deg f} - 1$. \square

Как видим, максимальный период л.р.п. обеспечивается при выборе примитивного f . Ненулевые л.р.п. с примитивным характеристическим многочленом называют *m-последовательностями*.

Пример 13.3. Продолжая предыдущий пример: $\text{ord } f = 15$, $\text{ord } g = 5$, f — примитивный многочлен. \square

Пример 13.4 (числа Мерсенна). Если $2^n - 1$ — простое число, то всякий неприводимый многочлен из кольца $\mathbb{F}_2[x]$ оказывается примитивным. Простые вида $2^n - 1$ получили название *простых Мерсенна*. В октябре 2024 года объявлено о нахождении 52-го (не по порядковому номеру) простого Мерсенна:

$$2^{136\,279\,841} - 1.$$

Это самое большое из известных на сегодняшний день простых чисел (≈ 41 млн. десятичных знаков). Оно найдено в рамках проекта GIMPS (распределенные вычисления). \square

13.3 Постулаты Голомба

Пусть $\gamma = \gamma_1, \gamma_2, \dots$ — выходная последовательность конечного автомата, $\gamma_t \in \mathbb{F}_2$. Как мы уже говорили, последовательность γ является периодической. Пусть r — минимальный период γ . Для простоты полагаем, что предпериод равняется 0.

При решении задачи S2 Виктор пытается прогнозировать символы γ_{T+1}, \dots по известным символам $\gamma_1, \dots, \gamma_T$. Если $T \geq r$, то Виктор может построить точный прогноз:

$$\gamma_t = \gamma_{t-r}, \quad t = T + 1, \dots$$

К сожалению (для Виктора) на практике r велико и $T \ll r$. Однако и в этом случае Виктор может строить нетривиальные (с меньшей чем $1/2$ частотой ошибок) прогнозы, используя статистические особенности γ .

С. Голомб выдвинул три постулата, которым должны удовлетворять последовательности γ :

R1. На отрезке $\gamma_1, \dots, \gamma_r$ число нулей незначительно отличается от числа единиц.

R2. На отрезке периода примерно половина серий имеет длину 1, четверть — длину 2, восьмая часть — длину 3 и далее (серией называется максимальная подпоследовательность из одинаковых символов).

R3. Значения автокорреляционной функции

$$C_\gamma(\tau) = \sum_{t=1}^r \chi(\gamma_t + \gamma_{t+\tau})$$

близки к 0 для всех $\tau = 1, 2, \dots, r-1$. Здесь $\chi: \mathbb{F}_2 \rightarrow \{-1, 1\}$, $a \mapsto (-1)^a$.

Покажем, что m -последовательность $s = (s_t)$ удовлетворяют постулатам Голомба R1 и R3. Период m -последовательности s равняется $r = 2^n - 1$.

R1. Вернемся к первоначальному определению л.р.п. с помощью РСЛОС:

$$S_t = S_{t-1}M, \quad s_t = S_{t,1}, \quad t = 1, 2, \dots$$

Поскольку (s_t) — m -последовательность, период (S_t) равняется $2^n - 1$. Но это значит, что векторы S_1, \dots, S_{2^n-1} различны и, следовательно, пробегают $\mathbb{F}_2^n \setminus \{0\}$. Выходные символы s_1, \dots, s_{2^n-1} являются первыми координатами данных векторов и, таким образом, на отрезке s_1, \dots, s_{2^n-1} встречается 2^{n-1} единиц и $2^{n-1} - 1$ нулей.

R3. Для всякого $\tau \in \{1, \dots, r-1\}$ последовательность

$$s_t^* = s_t + s_{t+\tau}, \quad t = 1, 2, \dots$$

удовлетворяет тому же рекуррентному соотношению, что и исходная m -последовательность (s_t) . Последовательность (s_t^*) не может быть нулевой, так как в противном случае

$$s_1 = s_{1+\tau}, \quad s_2 = s_{2+\tau}, \dots, \quad s_n = s_{n+\tau}, \dots$$

и период (s_t) равняется $\tau < r$, противоречие. Следовательно, (s_t^*) — m -последовательность и

$$C_s(\tau) = \sum_{t=1}^{2^n-1} \chi(s_t^*) = 2^{n-1}\chi(1) + (2^{n-1} - 1)\chi(0) = -1.$$