А. С. Строгалов, О регулярных языках с полиномиальным ростом числа слов, *Дискрет. матем.*, 1990, том 2, выпуск 3, 145–152

Дискретная математика

том 2 выпуск 3 * 1990

УДК 519.95

О РЕГУЛЯРНЫХ ЯЗЫКАХ С ПОЛИНОМИАЛЬНЫМ РОСТОМ ЧИСЛА СЛОВ

А. С. Строгалов

Важной характеристикой регулярных множеств являются функции, описывающие распределение числа слов заданной длины в них и называемые функциями роста этих множеств. Устанавливается, что любой неотрицательный целозначный полином может являться функцией роста некоторого регулярного множества.

Введение

В работе исследуются функции роста регулярных языков, описывающие распределения числа слов заданной длины τ в них. Как установлено в [2], эти функции разделяются на два класса: в первый класс попадают все функции, ограниченные сверху некоторым полиномом от τ; во второй класс — все остальные функции, причем они растут не медленнее, чем экспонента от τ.

Здесь рассматриваются функции роста из первого класса. Основным результатом статьи является доказательство того, что любой неотрицательный целозначный полином является функцией роста.

§ 1. Основные понятия и результаты

Пусть задан алфавит $A=\{\alpha_0, \ldots, \alpha_{n-1}\}$, A^* — множество всех слов $\tilde{\alpha}=\alpha(1)\alpha(2)\ldots\alpha(t)$ над A, где $\alpha(i)\in A$ при $i\in\{1, 2, \ldots, t\}$; число $|\tilde{\alpha}|=t$ называем длиной $\tilde{\alpha}$. Множество $\mathscr{L}\subseteq A^*$ называем *регулярным языком*, если оно распознаваемо некоторым автоматом $\mathfrak{A}_{\mathscr{L}}$ [1].

Пусть $\mathscr{L}(\tau)$ — множество всех слов длины τ из $\mathscr{L}$, тогда $\mathscr{L}=\bigcup\limits_{\tau=1}^{\infty}\mathscr{L}(\tau)$. Обозначая через $|B|$ мощность множества B, рассмотрим функцию $f_{\mathscr{L}}(\tau)=|\mathscr{L}(\tau)|$, которую назовем *функцией роста* языка $\mathscr{L}$.

В работе [2] показано, что эта функция либо не превосходит полинома, либо имеет экспоненциальный рост. В первом случае говорим, что язык имеет *полиномиальный тип* (*рост*), а во втором — *экспоненциальный тип* (*рост*).

В статье [3] описан следующий способ нахождения числа слов длины τ в регулярном языке $\mathscr{L}$. Сначала строится матрица M (называемая *скелетной*) для автомата, распознающего язык $\mathscr{L}$, элементы m_{ij} которой равны количеству дуг, соединяющих в диаграмме переходов i-е состояние с j-м. Затем к ней применяется теорема Гамильтона — Кэли [5] о том, что всякая квадратная матрица удовлетворяет своему характеристическому многочлену, т. е.:

$$M^k + c_1 M^{k-1} + \ldots + c_{k-1} M + c_k E \equiv \Theta. \qquad (1)$$

Здесь E и Θ — единичная (диагональная) и, соответственно, нулевая матрицы, c_i есть i-й коэффициент характеристического многочлена матрицы M, а k — степень характеристического многочлена и одновременно порядок матрицы M, определяемый количеством состояний автомата, распознающего язык $\mathscr{L}$; при этом можно рассматривать только приведенные автоматы.

Умножив обе части тождества (1) на $M^{\tau-k}$, где $\tau \geqslant k$, получим

$$M^\tau + c_1 M^{\tau-1} + \ldots + c_{k-1} M^{\tau-(k-1)} + c_k M^{\tau-k} \equiv \Theta. \qquad (2)$$

Расписав поэлементно (2), имеем

$$m_{ij}^{(\tau)} + c_1 m_{ij}^{(\tau-1)} + \ldots + c_{k-1} m_{ij}^{(\tau-k+1)} + c_k m_{ij}^{(\tau-k)} = 0. \qquad (3)$$

Здесь $m_{ij}^{(l)}$ $(\tau - k \leqslant l \leqslant \tau)$ — соответствующий элемент матрицы M^l. Известно [4], что $m_{ij}^{(\tau)}$ есть число слов длины τ, ведущих из i-го в j-е состояние автомата со скелетной матрицей M. Осталось взять в качестве i номер инициального состояния, а в качестве j — номер финального состояния. Если финальных состояний несколько, то надо просуммировать соответствующие тождества, подобно тому, как это сделано в [2]. В результате мы получим линейное рекуррентное уравнение типа (3).

Структура общего решения линейного рекуррентного уравнения известна и имеет вид

$$m_{ij}^{(\tau)} = \sum_{i=1}^{s} (c_{i1} + c_{i2}\tau + \ldots + c_{ir_i}\tau^{r_i-1}) \lambda_i^\tau,$$

где λ_i — корни характеристического многочлена $\det|M - \lambda E| = 0$, а r_i — кратность соответствующего корня. Коэффициенты c_{ij} определяются из начальных условий для уравнения (3).

Для простоты изложения будем рассматривать случай $A = \{0, 1\}$. Обозначим через $\mathbf{N}$ множество натуральных чисел.

Полином $P_s(\tau)$ называется *целозначным*, если при целых τ его значения целые числа. Например, любой полином с целыми коэффициентами является целозначным, а полином $P_s(\tau) = C_\tau^s$ целозначный, но не целочисленный; его коэффициенты рациональные числа [7]. Далее нас будут интересовать главным образом неотрицательные целозначные полиномы (н. ц. п.) и целозначные полиномы (ц. п.). Имеет место

Теорема 1. *Для любого н. ц. п. $P_s(\tau)$ существует $l \in \mathbf{N}$ такое, что при $\tau \geqslant l$*

$$P_s(\tau) = a_0 + a_1 C_{\tau-l}^1 + \ldots + a_s C_{\tau-l}^s,$$

причем $\sum_{i=0}^{s} a_i \leqslant 2^l$ и $a_i \in \mathbf{N}$ при $i = 0, 1, \ldots, s$.

Отметим, что l зависит только от полинома $P_s(\tau)$. Такое представление н. ц. п. $P_s(\tau)$ позволяет получить основной результат, который для случая, когда $A = \{0, 1\}$ формулируется следующим образом.

Теорема 2. *Для любого н. ц. п. $P_s(\tau)$ существует $l \in \mathbf{N}$ и регулярный язык $\mathscr{L}$ такой, что $f_{\mathscr{L}}(\tau) = P_s(\tau)$ при $\tau \geqslant l$. Здесь l то же, что и в формулировке теоремы* 1.

Если ограничения на мощность входного алфавита A отсутствуют, то теорему 2 можно усилить.

Теорема 3. *Для любого н. ц. п. $P_s(\tau)$ существует регулярный язык $\mathscr{L}$ такой, что $f_{\mathscr{L}}(\tau) = P_s(\tau)$ при $\tau \in \mathbf{N}$.*

Частным случаем регулярных языков полиномиального роста являются те, функция роста которых ограничена сверху константой; их называем *константно-ограниченными*.

Теорема 4. *Класс функций роста константно-ограниченных языков совпадает с классом почти-периодических функций* $f\colon \mathbf{N} \to \mathbf{N} \cup \{0\}$.

§ 2. Доказательство вспомогательных утверждений

Лемма 1. *Существует семейство регулярных языков* $\mathcal{L}_k$, *для которых* $f_{\mathcal{L}_k}(\tau) = C_\tau^{k-1}$.

Доказательство. Заметим, что степень полинома C_τ^{k-1} равна $k-1$. Рассмотрим семейство регулярных языков $\mathcal{L}_k$, распознаваемых автоматами

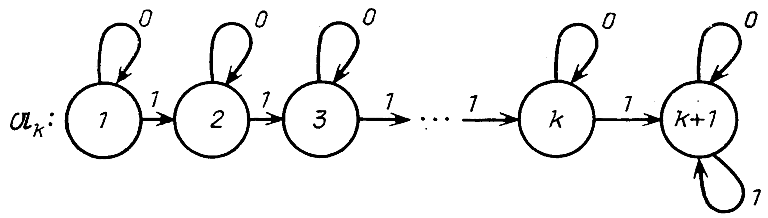

Рис. 1

$\mathfrak{A}_k$, диаграммы которых изображены на рис. 1. Здесь состояние с номером 1 — инициальное, состояние с номером k — финальное. Как следует из работы [2], $f_{\mathcal{L}_k}$ имеет полиномиальный тип. Найдем ее явное выражение. Скелетная матрица размера $(k+1)\times(k+1)$ автомата $\mathfrak{A}_k$ имеет вид

$$M = \begin{pmatrix} 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 1 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & & \dots & 0 & 1 & 1 \\ 0 & 0 & \dots & 0 & 0 & 2 \end{pmatrix}; \quad \det|M - \lambda E| = (\lambda-1)^k(\lambda-2).$$

Следовательно, общее решение уравнения (3) для этой матрицы есть

$$m_{1k}^{(\tau)} = (c_1 + c_2\tau + \dots + c_k\tau^{k-1}) + c_{k+1}2^\tau.$$

В силу того, что $f_{\mathcal{L}_k}$ полиномиального типа, $c_{k+1} = 0$. Отметим, что это верно именно для указанного распределения инициального и финального состояний. Нам остается определить константы $c_1, \dots, c_k$ из начальных условий. Заметим, что из строения диаграммы автомата $\mathfrak{A}_k$ (рис. 1) вытекает, что

$$f_{\mathcal{L}_k}(1) = \dots = f_{\mathcal{L}_k}(k-2) = 0, \quad f_{\mathcal{L}_k}(k-1) = 1, \quad f_{\mathcal{L}_k}(k) = k.$$

Так как $f_{\mathcal{L}_k}(\tau)$ — полином степени $k-1$, то для его построения можно воспользоваться интерполяционной формулой Лагранжа [6] для узлов (x_i, y_i), $1 \leqslant i \leqslant k$, вида $(i, 0)$ при $1 \leqslant i \leqslant k-2$ и $(k-1, 1)$, (k, k). Имеем

$$f_{\mathcal{L}_k}(\tau) = m_{1k}^{(\tau)} = 1\cdot\frac{(\tau-1)\dots(\tau-(k-2))(\tau-k)}{((k-1)-1)\dots((k-1)-(k-2))((k-1)-k)} + $$
$$+ k\cdot\frac{(\tau-1)\dots(\tau-(k-2))(\tau-(k-1))}{(k-1)\dots(k-(k-2))(k-(k-1))} =$$
$$= \frac{(\tau-1)\dots(\tau-(k-2))}{(k-2)!}\left[k-\tau+\frac{k(\tau-(k-1))}{k-1}\right] = \frac{(\tau-1)\dots(\tau-(k-2))\,\tau}{(k-2)!\,(k-1)} = C_\tau^{(k-1)}.$$

Лемма 1 доказана.

Используя формулу интерполяционного многочлена Ньютона [8] (случай равноотстоящих узлов), можно получить следующее представление для ц. п. $P_s(\tau)$:

$$P_s(\tau)=P_s(l)+\sum_{k=1}^{s}\frac{\Delta^k P_s(l)}{k!}(\tau-l)(\tau-l-1)\dots(\tau-l-(k-1))=$$

$$=P_s(l)+\sum_{k=1}^{s}\Delta^k P_s(l)\,C_{\tau-l}^{k}, \qquad (4)$$

где $\Delta^k P_s(l)=\sum_{i=0}^{k}(-1)^{k-i}C_k^i P_s(l+i)$ — k-я разделенная разность. Для нас существенно, чтобы в разложении (4) коэффициенты были целыми числами. Для этого достаточно заметить выполнение следующих очевидных равенств:

$$P_s(l+i)=P_s(l)+\sum_{k=1}^{i}C_i^k\Delta^k P_s(l), \qquad i=0,\ 1,\ \dots,\ s.$$

Учитывая, что $P_s(\tau)$ — целозначный, из этих уравнений последовательно находим величины $\Delta^1 P_s(l)$, $\Delta^2 P_s(l)$, $\dots$, $\Delta^s P_s(l)$ которые, очевидно, целые числа.

Лемма 2. *Для всякого ц. п. $P_s(\tau)$ найдется $l_0\in\mathbf{N}$ такое, что при всех $l\geqslant l_0$ в представлении* (4) *будет выполнено неравенство*

$$\sum_{i=0}^{s}|\Delta^i P_s(l)|\leqslant 2^l.$$

Доказательство. Из определения k-й разделенной разности имеем

$$|\Delta^k P_s(l)|\leqslant\sum_{i=0}^{k}C_k^i|P_s(l+i)|\leqslant 2^k\sum_{i=0}^{k}|P_s(l+i)|\leqslant 2^k kc(l+k)^s,$$

где $c>0$. Далее, для некоторого $c_1>0$ имеем $\sum_{i=0}^{s}|\Delta^i P_s(l)|\leqslant 2^s s^2 c_1(l+s)^s$. Ясно, что при фиксированном s найдется такое l_0, что при всех $l\geqslant l_0$ выполнено $2^s s^2 c_1(l+s)^s\leqslant 2^l$. Лемма доказана.

Лемма 3. *Для любого н. ц. п. $P_s(\tau)$ найдется $l_1\in\mathbf{N}$ такое, что при всех $l\geqslant l_1$ в представлении* (4) *будет выполнено неравенство*

$$\Delta^i P_s(l)\geqslant 0, \quad i=1,\ 2,\ \dots,\ s.$$

Доказательство. Используя интерполяционный многочлен Ньютона, имеем

$$P_s(\tau)=P_s(l)+P_s'(\zeta_1)(\tau-l)+\frac{P_s''(\zeta_2)}{2!}(\tau-l)(\tau-(l+1))+\dots$$

$$+\frac{P_s^{(s)}(\zeta_s)}{s!}(\tau-l)(\tau-(l+1))\dots(\tau-(l+s)),$$

где $P_s^{(i)}(\zeta_i)$ — i-я производная многочлена $P_s(\tau)$ в точке ζ_i, $i=1,\ 2,\ \dots,\ s$. Ясно, что с учетом неотрицательности многочлена можно выбрать такое l_1, что при любых $\zeta_i\in[l_1,\ l_1+s]$ выполнено $P_s^{(i)}(\zeta_i)\geqslant 0$. Теперь остается воспользоваться теоремой Лагранжа для разделенных разностей [8]. Лемма доказана.

§ 3. Доказательство теорем 1—4

Доказательство теоремы 1. Выбрав $l(P_s)$ таким образом, чтобы оно удовлетворяло условиям лемм 2 и 3 как значения l_0 и l_1 соответственно, получим с учетом этих лемм справедливость утверждения теоремы 1.

Доказательство теоремы 2. Рассмотрим автомат $\mathfrak{A}_k$, диаграмма переходов которого изображена на рис. 2. Здесь α_1, $\dots$, $\alpha_l\in\{0,\ 1\}$, $\bar{\alpha}_i$ —

отрицание $\bar{\alpha}_i$, начальное состояние имеет номер 1, финальное состояние имеет номер $l+k$.

Пусть $\mathscr{L}_k$ — язык, распознаваемый этим автоматом, $\tilde{\alpha} \in \mathscr{L}_k$ тогда $\tilde{\alpha} = \alpha_1 \ldots \alpha_l \tilde{\beta}$, где $|\tilde{\beta}| = \tau - l$. Число слов длины $\tau - l$, ведущих из $(l+1)$-го в $(l+k)$-е состояние в силу леммы 1 равно $C_{\tau-l}^{k-1}$. Отсюда следует, что $f_{\mathscr{L}_k}(\tau) = C_{\tau-l}^{k-1}$.

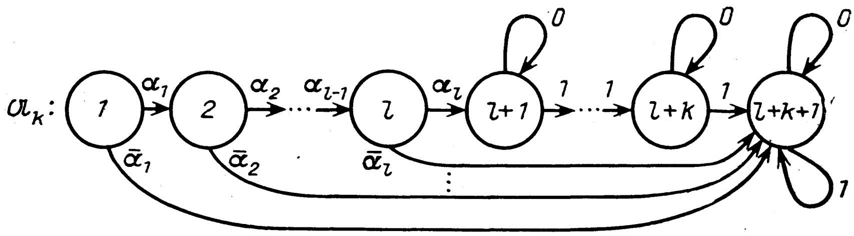

Рис. 2

Возьмем теперь дихотомическое дерево высоты l (l выбирается так, чтобы было выполнено условие теоремы 1) и выделим группы концевых вершин следующим образом (см. рис. 3): 1-я группа содержит a_0 вершин, 2-я группа содержит a_1 вершин, ..., $(s+1)$-я группа содержит a_s вершин. Здесь $a_0, a_1, \ldots, a_s$ — коэффициенты разложения полинома $P_s(\tau)$ из теоремы 1, в силу которой $\sum_{i=0}^{s} a_i \leqslant 2^l$ и, следовательно, числа концевых вершин этого дерева достаточно для образования из них таких групп вершин.

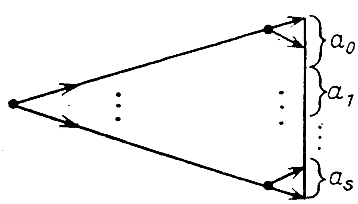

Рис. 3

Вершины группы a_0 объявляются финальными, а к каждой вершине из группы i $(1 \leqslant i \leqslant s+1)$ мы «приклеиваем» автомат, реализующий язык $\mathscr{L}_i$, для которого $f_{\mathscr{L}_i}(\tau) = C_{\tau-l}^{i}$, т. е. фактически мы отождествляем концевые вершины из группы i дерева с соответствующими инициальными состояниями автоматов, реализующих язык $\mathscr{L}_i$. Финальные состояния этих автоматов объявляются финальными состояниями нового автомата. Все свободные ребра дерева подсоединяются к одному поглощающему (нефинальному) состоянию. С этим же состоянием отождествляются поглощающие состояния автоматов, реализующих языки $\mathscr{L}_i$. Из свойства префиксности дерева вытекает, что функция роста этого автомата $\mathfrak{A}$, реализующего язык $\mathscr{L}$, есть

$$f_{\mathscr{L}_i}(\tau) = a_0 + a_1 f_{\mathscr{L}_1}(\tau) + \ldots + a_s f_{\mathscr{L}_s}(\tau) = a_0 + a_1 C_{\tau-l}^{1} + \ldots + a_s C_{\tau-l}^{s},$$

что в свою очередь есть разложение полинома $P_s(\tau)$ из формулировки теоремы 1. Теорема 2 доказана.

Следствие. *Если для $P_s(\tau)$ выполнено при всех $\tau \in \mathbf{N}$ соотношение $0 \leqslant P_s(\tau) \leqslant 2^\tau$, то существует регулярный язык $\mathscr{L}$ такой, что $f_{\mathscr{L}}(\tau) = P_s(\tau)$.*

Следствие вытекает из того, что ограничение $0 \leqslant P_s(\tau) \leqslant 2^\tau$ позволяет при $\tau < l$ «разбросать» по i-му ярусу дерева $P_s(i)$ финальных состояний.

Доказательство теоремы 3. Доказательство теоремы 2 распространяется для этого случая за счет выбора входного алфавита при условии совместности системы неравенств

$$P_s(1) \leqslant |A|, \quad P_s(2) \leqslant |A|^2, \ \ldots, \ P_s(l-1) \leqslant |A|^{l-1}, \quad 2^l \leqslant |A|^l.$$

Доказательство теоремы 4. Пусть $f\colon \mathbf{N} \to \mathbf{N} \cup \{0\}$ — почти-периодическая функция. Тогда целочисленная последовательность $f(1), f(2), \ldots$ ..., $f(\tau), \ldots$ имеет предпериод l и наименьший период T. Введем следующие функции:

$$f_i(\tau)=\begin{cases}1, & \text{если } \tau=l+i+kT, \quad 1\leqslant i\leqslant T, \quad k=0,1,2,\ldots,\\ 0 & \text{в остальных случаях;}\end{cases}$$

$$f_0(\tau)=\begin{cases}f(\tau), & 1\leqslant\tau\leqslant l,\\ 0 & \text{в остальных случаях.}\end{cases}$$

Очевидно следующее представление:

$$f(\tau)=f_0(\tau)+f(l+1)f_1(\tau)+\ldots+f(l+T)f_T(\tau)=\sum_{i=1}^{T}f(l+i)f_i(\tau)+f_0(\tau). \quad (5)$$

Возьмем далее слово $\tilde\beta$ и семейство слов $\tilde\alpha_1^1, \ldots, \tilde\alpha_{f(l+1)}^1; \ldots; \tilde\alpha_1^T, \ldots, \tilde\alpha_{f(l+T)}^T$ над входным алфавитом так, чтобы были выполнены следующие свойства.

1. Ни одно из этих слов (в том числе и $\tilde\beta$) не является префиксом другого слова.

2. Длины слов подчинены следующим соотношениям:

$$|\tilde\alpha_1^i|=\ldots=|\tilde\alpha_{f(l+i)}^i|=l+i; \quad |\tilde\beta|=T, \quad 1\leqslant i\leqslant T. \quad (6)$$

Образуем семейство языков $\mathscr{L}_i=\bigcup_{j=1}^{f(l+i)}\mathscr{L}_{ij}$, где $\mathscr{L}_{ij}=\tilde\alpha_j^i\cup\tilde\alpha_j^i\cdot\{\tilde\beta\}^*$; здесь $\cup$, $\cdot$, $*$ — операции объединения, конкатенации и, соответственно, итерации [1]. Учитывая свойство 2 выбранного семейства слов (6), имеем

$$f_{\mathscr{L}_{ij}}(\tau)=\begin{cases}1, & \text{если } \tau=l+i+kT, \quad k=0,1,2,\ldots,\\ 0 & \text{в остальных случаях.}\end{cases}$$

Значит, $f_{\mathscr{L}_{ij}}(\tau)=f_i(\tau)$, а из свойства 1 (все слова будут разные!) получаем, что

$$f_{\mathscr{L}_i}(\tau)=\sum_{j=1}^{f(l+i)}f_{\mathscr{L}_{ij}}(\tau)=f(l+i)f_i(\tau).$$

В силу свойств 1—2 при $\mathscr{L}^1=\bigcup_{i=1}^{T}\mathscr{L}_i$

$$f_{\mathscr{L}^1}(\tau)=\sum_{i=1}^{T}f_{\mathscr{L}_i}(\tau)=\sum_{i=1}^{T}f(l+i)f_i(\tau).$$

Нам осталось для получения представления (5) реализовать конечный язык $\mathscr{L}_0$, в котором имеется $f(i)$ слов длины i при $i=1, 2, \ldots, l$; это делается с учетом того, что мы можем выбирать входной алфавит из любого конечного числа символов. Положим $\mathscr{L}=\mathscr{L}^1\cup\mathscr{L}_0$ и заметим, что функция роста $f_{\mathscr{L}}(\tau)$ совпадает с $f(\tau)$. Константная ограниченность языка $\mathscr{L}$ вытекает из свойства почти-периодичности функции. Докажем обратное. Пусть дан язык $\mathscr{L}$ такой, что $0\leqslant f_{\mathscr{L}}(\tau)\leqslant c$, где $c\geqslant 0$ — константа. Покажем, что $f_{\mathscr{L}}(\tau)$ — почти-периодическая функция. Для этого рассмотрим производящую функцию $f(\tau)=\sum_{\tau=1}^{\infty}a_\tau x^\tau$, где $a_\tau=f_{\mathscr{L}}(\tau)$. Известно (см., например, [9]), что $f(\tau)$ есть рациональная функция. В силу ограничения $0\leqslant f_{\mathscr{L}}(\tau)\leqslant c$ и того, что $f_{\mathscr{L}}(\tau)$ — целое число, получаем, что коэффициенты степенного ряда $\sum_{\tau=1}^{\infty}a_\tau x^\tau$ принимают конечное число значений. Отсюда с учетом [10] получаем, что, начиная с некоторого номера, эти коэффициенты образуют почти-периодическую последовательность. Теорема 4 доказана.

В заключение автор пользуется случаем выразить признательность проф. В. Б. Кудрявцеву за внимание к работе и полезные замечания, способствовавшие улучшению работы.

СПИСОК ЛИТЕРАТУРЫ

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов.— М.: Наука, 1985.
2. Строгалов А. С. Об одной мере близости для автоматных языков. // Проблемы теоретической кибернетики. Тезисы докладов VIII Всесоюзной конференции, июль 1988, ч. 2.— Горький.— С. 191.
3. Хомский М., Миллер Д. Языки с конечным числом состояний. // Киб. сборник, вып. 4.— М.: ИЛ, 1962.— С. 233—255.
4. Гилл А. Введение в теорию конечных автоматов.— М.: Наука, 1966.
5. Гантмахер Ф. Р. Теория матриц.— М.: Наука, 1988.
6. Бабенко К. И. Основы численного анализа.— М.: Наука, 1986.
7. Полиа Г., Сеге Г. Задачи и теоремы из анализа, ч. 2.— М.: Наука, 1985.
8. Гельфонд А. О. Исчисление конечных разностей.— М.: Наука, 1967.
9. Строгалов А. С. Об ε-моделировании поведения конечных автоматов. // Материалы 1-го Всесоюзного семинара по дискретной математике и ее приложениям.— М.: Изд-во МГУ, 1986.— С. 42—56.
10. Бибербах Л. Аналитическое продолжение.— М.: Наука, 1967.

Статья поступила 01.02.90