ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ՏԵՂԵԿԱԳԻՐ
ИЗВЕСТИЯ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

Մաթեմատիկա VI, № 5, 1971 Математика

В. А. АРАКЕЛОВ, Р. Р. ВАРШАМОВ

К ИССЛЕДОВАНИЮ АЛГЕБРАИЧЕСКОЙ СТРУКТУРЫ ПЕРИОДИЧЕСКИХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Широкое распространение в последнее время получили циклические корректирующие коды. Это объясняется тем, что они имеют простые правила кодирования, допускающие относительно несложную реализацию, и тем, что свойство цикличности приводит к определенной алгебраической структуре кодов, которая может быть использована не только для предсказания их корректирующих свойств, но и для нахождения относительно простых алгоритмов декодирования.

Циклическим кодам посвящено довольно большое число исследований. Хорошо изученными являются циклические коды максимальной длины [1]. Найден новый класс циклических кодов, проверочный полином которых представим в виде произведения примитивных полиномов с попарно взаимно простыми степенями [2]. Естественным обобщением этих кодов, очевидно, является случай, когда проверочный полином задается произведением неприводимых полиномов. Задача исследования таких кодов фактически сводится к анализу распределения весов кодовых векторов и определению конечной формулы кодового расстояния, которая, в свою очередь, может быть получена в результате более глубокого анализа алгебраической структуры циклических последовательностей. Кроме того, более детальное изучение циклических возвратных последовательностей несомненно найдет приложение как в вопросах порогового декодирования [3], так и в конструктивной теории приводимости полиномов над конечными полями. Поэтому данная работа посвящена исследованию математической структуры и характерных особенностей рекуррентных периодических последовательностей.

Известно [4], что периодические последовательности получаются с помощью генератора на регистре сдвига, обратная связь которого соответствует некоторому нормированному полиному $h(x)=\sum_{l=0}^{k} h_l x^l$, $h_0 \neq 0$ степени k, с коэффициентами из поля Галуа $GF(q)$.

Если в первоначальный момент работы генератора накопитель его заполнен комбинацией $a(0), a(1), \cdots, a(k-1)$, то выходная последовательность, снимаемая с первого разряда регистра сдвига, будет иметь вид

$$a(0), \quad a(1), \cdots, a(k-1), a(k), \cdots.$$

Полином $h(x)$ определяет рекуррентное соотношение

$$a(i+k) = -\sum_{j=0}^{k-1} h_j a(i+j) \quad (i=0, 1, \cdots), \tag{1}$$

в силу которого любой элемент $a(N)$ $(N \geqslant 0)$ выходной последовательности можно представить в виде некоторой линейной комбинации первоначального заполнения с коэффициентами φ из поля $GF(q)$:

$$a(x) = \varphi_0(x)\, a(0) + \varphi_1(x)\, a(1) + \cdots + \varphi_{k-1}(x)\, a(k-1). \tag{2}$$

В настоящей статье предлагается метод определения коэффициентов разложения (2) для всякого $N \geqslant k$ (случай $N < k$ тривиален). Попытаемся вначале вычислить первый коэффициент $\varphi_0(x)$ выражения (2). Если $k=N$, то, согласно (1), будем иметь соотношение

$$a(k) = -h_0 a(0) - h_1 a(1) - \cdots - h_{k-1} a(k-1),$$

позволяющее непосредственно определить $\varphi_0(k) = -h_0$. Если $N > k$, то, рассматривая диофантово уравнение

$$N - k = m_0 z_0 + m_1 z_1 + \cdots + m_t z_t, \tag{3}$$

где $m_l = k - k_l$, k_l — номера всех* отличных от нуля коэффициентов полинома $h(x) = x^k + \sum_{l=0}^{t} h_{k_l} x^{k_l}$, можно показать, что оно имеет непосредственное значение при вычислении коэффициентов разложения (2). Так, например, выяснилось, что для всех значений N, для которых уравнение (3) не разрешимо в целых неотрицательных значениях z_l, коэффициент $\varphi_0(N)=0$. А поэтому ясно, что выражение $\varphi_0(x)$ может быть отлично от нуля лишь в случае, когда (3) имеет хотя бы одно целочисленное решение. Именно этот случай в дальнейшем и будет нами рассмотрен.

Условимся преобразование, в результате которого $a(x)$ переходит в $a(x+1)$, т. е. $a(x) \to a(x+1)$, называть шагом функции $a(x)$, а преобразование из, соответственно, $m_l = k - k_l$ $(i = \overline{0, t})$ последовательных шагов — i-переходом. Тогда преобразование $a(k) \to a(N)$, состоящее из $N - k$ последовательных шагов, в зависимости от (3), можно будет осуществлять различными i-переходами, содержащими, соответственно, по m_l шагов каждый. В самом деле, пусть $\{z_0^{(i)}, z_1^{(i)}, \cdots, z_t^{(i)}\}$ $(i=\overline{1, s})$ означает множество всевозможных различных решений (3), а $z_0^{(u)}, z_1^{(u)}, \cdots, z_t^{(u)}$ — некоторый его произвольный элемент. Тогда, применяя к функции $a(k)$ вначале, соответственно, $z_0^{(u)}$ раз 0-переход, затем $z_{(1)}^{u}$ раз 1-переход и т. д., $z_t^{(u)}$ раз t-переход, получим некоторое выражение $\bar{a}^{(u)}(N)$, которое, в свою очередь, может быть записано в виде

$$\bar{a}^{(u)}(N) = \bar{\varphi}_0^{(u)}(N)\, a(0) + \bar{\varphi}_1^{(u)}(N)\, a(1) + \cdots + \bar{\varphi}_{k-1}^{(u)}(N)\, a(k-1),$$

---

* Исключая старший коэффициент.

где

$$\bar{\varphi}_0^{(u)}(N) = (-1)^{z_0^{(u)}+\cdots+z_t^{(u)}+1} h_0^{z_0^{(u)}} h_1^{z_1^{(u)}} \cdots h_{k_t}^{z_t^{(u)}}.$$

Причем, если указанные преобразования осуществлять без учета порядка переходов, то общее число различных вариантов $P(z_0^{(u)}, z_1^{(u)}, \cdots \cdots, z_t^{(u)})$ определится формулой

$$P(z_0^{(u)}, z_1^{(u)}, \cdots, z_t^{(u)}) = \frac{(z_0^{(u)} + z_1^{(u)} + \cdots + z_t^{(u)})!}{z_0^{(u)}!\, z_1^{(u)}! \cdots z_t^{(u)}!},$$

а поэтому в выражении

$$a^{(u)}(N) = \sum \bar{a}^u(N) = \varphi_0^{(u)}(N)\, a(0) + \cdots + \varphi_{k-1}^{(u)}(N)\, a(k-1) \qquad (4)$$

коэффициент

$$\bar{\varphi}_0^{(u)}(N) = \varphi_0^{(u)}(N) \frac{(z_0^{(u)} + z_1^{(u)} + \cdots + z_t^{(u)})!}{z_0^{(u)}!\, z_1^{(u)}! \cdots z_t^{(u)}}.$$

Сопоставляя между собой (2) и (4) и принимая во внимание также, что $a(N) = \sum_{u=1}^{s} a^{(u)}(N)$, окончательно получим

$$\varphi_0(N) = \sum_{u=1}^{s} \bar{\varphi}_0^{(u)}(N) = \sum_{u=1}^{s} (-1)^{z_0^{(u)}+\cdots+z_t^{(u)}+1} h_0^{z_0^{(u)}+1} \cdots h_{k_t}^{z_t^{(u)}} \times$$

$$\times P(z_0^{(u)}, \cdots, z_t^{(u)}).$$

Таким образом, нами установлен следующий факт.

Теорема. *Пусть целое* $N \geqslant k$, $h(x) = \sum_{s=0}^{k} h_l x^l$ *— произвольный нормированный полином над полем* $GF(q)$, *порождающий периодическую последовательность, у которого только коэффициенты* $h_0, h_{k_1}, \cdots, h_{k_t}, h_k$ *отличны от нуля, и пусть* $\{z_0^{(i)}, z_1^{(i)}, \cdots, z_t^{(i)}\}$ $(i = \overline{1,s})$ *— непустая система всевозможных неотрицательных решений диофантова уравнения* $N - k = \sum_{l=0}^{t} (k - k_l) z_l$. Тогда

$$\varphi_0(N) \equiv \sum_{i=1}^{s} (-1)^{z_0^{(i)}+\cdots+z_t^{(i)}+1} h_0^{z_0^{(i)}+1} \cdots h_{k_t}^{z_t^{(i)}} \frac{(z_0^{(i)}+\cdots+z_t^{(i)})!}{z_0^{(i)}!\cdots z_t^{(i)}!} \pmod{p},$$

где p *— характеристика основного поля.*

Опираясь далее на очевидное соотношение $\varphi_{k-1}(N)\, h_0 = \varphi_0(N)$, нетрудно получить соотношение

$$\varphi_j(N) = \frac{1}{h_0} \sum_{l=0}^{l} \varphi_0(N - j + i)\, h_l, \qquad (5)$$

справедливое для любых натуральных N и j.

Это соотношение позволяет по найденным значениям $\varphi_0(N)$ определять остальные коэффициенты $\varphi_1(N), \varphi_2(N), \cdots, \varphi_{k-1}(N)$ разложения (2).

Примеры:

1. Пусть $q=3$, $h(x)=x^3+x+1$ и $N=13$. Подставляя эти данные в (3), получим

$$10=3z_0+2z_1. \tag{6}$$

Уравнение (6) имеет два решения:

$$z_0^{(1)}=0, \quad z_1^{(1)}=5 \text{ и } z_0^{(2)}=2, \quad z_1^{(2)}=2,$$

и поэтому, согласно теореме, будем иметь

$$2\cdot 2^5\cdot\frac{5!}{5!}-2^3\cdot 2^2\frac{4!}{2!\,2!}\equiv 1 \pmod 3,$$

т. е. $\varphi_0(13)=1$.

Аналогичным образом определим коэффициенты $\varphi_0(12)=2$, $\varphi_0(11)=1$, которые, согласно (5), позволят получить $\varphi_1(13)=\varphi_2(13)=0$, а, следовательно, и $\alpha(13)=\alpha(0)$. Таким образом, выяснилось, что 13 является кратным периоду полинома $h(x)$. А это означает, так как 13 является простым числом, что период полинома x^3+x+1 равен 13, и поскольку $13|3^3-1$, то полином x^3+x+1 неприводим в поле $GF(3)$.

2. Пусть $q=2^4$, $h(x)=x^4+\alpha x+1$, где α — примитивный элемент поля $GF(2^4)$, являющийся корнем полинома x^4+x+1. В данном случае $h_0=-1=1$, $h_1=-\alpha=\alpha$, $h_2=h_3=0$ и следовательно, уравнение (3) примет вид

$$N-4=4z_0+3z_1.$$

Пусть $N=15$, тогда уравнение $11=4z_0+3z_1$ будет иметь единственное решение $z_0=2$, $z_1=1$ и, согласно теореме, получим $\alpha\frac{3!}{2!\,1!}=\alpha^3 \pmod 2$, т. е. $\varphi_0(15)=\alpha$. Аналогичным образом определим $\varphi_0(14)=\alpha^2$, $\varphi_0(13)=\alpha^3$ и $\varphi_0(12)=1$. Используя (5), получим $\varphi_1(15)=\varphi_2(15)=0$, $\varphi_3(15)=\alpha$, т. е. $\alpha(15)=\alpha\cdot\alpha(0)+\alpha\cdot\alpha(3)$.

Как видно из теоремы определение коэффициентов упирается в вычисление выражения $P(z_0, z_1, \cdots, z_l)$. Нетрудно показать, что

$$P(z_0, z_1, \cdots, z_l)\equiv p^F R \pmod p,$$

где

$$F=\sum_{\nu=1}^{\infty}\left[\frac{z_0+\cdots+z_l}{p^\nu}\right]-\left[\frac{z_0}{p^\nu}\right]-\cdots-\left[\frac{z_l}{p^\nu}\right]^*,$$

а R — некоторая числовая функция от $z_0, z_1, \cdots, z_l$, удовлетворяющая условию $R\not\equiv 0 \pmod p$. Поэтому, если $F>0$, то $P(z_0, \cdots, z_l)\equiv 0 \pmod p$; если $F=0$, то $P(z_0, \cdots, z_l)\equiv R\not\equiv 0 \pmod p$.

Пусть

---

* $[z]$ — наибольшее целое число, не превосходящее z.

$$z=\sum_{j=0}^{n}\beta_{n-j}\,p^{n-j},$$

$$z_i=\sum_{j=0}^{n}\beta_{n-j}^{(i)}\,p^{n-j}\quad(i=\overline{0,t}) \tag{7}$$

являются представлением чисел $z=\sum_{i=0}^{t} z_i$; $z_0, z_1, \cdots, z_t$, в p-ичной системе счисления. Тогда справедлива

Лемма. Для того чтобы функция $F=\sum_{\nu=1}\left[\frac{z}{p^\nu}\right]-\left[\frac{z_0}{p^\nu}\right]-\cdots-\left[\frac{z_t}{p^\nu}\right]$ *была равна нулю, необходимо и достаточно, чтобы* $\beta_i=\sum_{i=0}^{n}\beta_j^{(i)}$ $(j=\overline{1,n})$.

Доказательство. Необходимость. Действительно, используя (7), функцию F можно представить в следующем виде:

$$F=A_0+A_1+\cdots+A_{n-1},$$

где

$$A_0=(\beta_n-\beta_n^{(0)}-\cdots-\beta_n^{(t)}),$$

$$\cdots\cdots\cdots\cdots$$

$$A_{n-1}=(\beta_n-\beta_n^{(0)}-\cdots-\beta_n^{(t)})\,p^{n-1}+$$

$$+(\beta_{n-1}-\beta_{n-1}^{(0)}-\cdots-\beta_{n-1}^{(t)})\,p^{n-2}+\cdots+(\beta_1-\beta_1^{(0)}-\cdots-\beta_1^{(t)}),$$

причем $A_j\geqslant 0$.

Поэтому, если $F=0$, то $A_j=0$ и $\beta_j=\sum_{i=0}^{t}\beta_j^{(i)}$, что и требовалось показать. Достаточность очевидна.

Можно также показать, что в случае, если $F=0$, будет иметь место сравнение

$$P(z_0,\cdots,z_t)\equiv\prod\frac{\left[\frac{z}{p^i}\right]_p}{\left[\frac{z_0}{p^i}\right]\cdots\left[\frac{z_t}{p^i}\right]}\pmod p,$$

где $\left[\frac{z}{p}\right]_p=z-p\left[\frac{z}{p}\right]$,

позволяющее в значительной степени упростить вычисление $P(z_0,\cdots,z_t)$, а следовательно, согласно теореме, и коэффициентов $\varphi_0(N)$.

В заключение следует отметить, что рассмотренный метод, устанавливающий тесную связь между структурой периодических последовательностей и соответствующими диофантовыми уравнениями, оказывается весьма полезным и при решении ряда актуальных задач теории

приводимости полиномов над конечными полями. Так, например, при исследовании арифметической функции $T(h(x))$*, определении вычетов функции высоких степеней по модулю заданного полинома $h(x)$ и др. В самом деле, умножая выражение (3) на произвольное натуральное число λ и исследуя его затем, можно получить одно из важнейших свойств функции $T(h(x))$, а именно

$$T(h(x^{\lambda})) = \lambda T(h(x)).$$

Или же, используя добавочно некоторые вспомогательные средства, можно также для $T(h(x))$ получить ряд интересных соотношений, справедливых в поле $GF(2)$. Приведем без доказательства некоторые из них

1. $$T(x^{2^k}+x+1) = 2^{2^k}-1,$$

2. $$T\left(\sum_{\nu=0}^{m} x^{\frac{1}{2^k-1}(2^{\nu k}-1)}\right) = 2^k\left(\frac{2^{mk}-1}{2^s-1}\right)+1,$$

где m и k — любые целые положительные числа.

Вычислительный центр АН АрмССР
и Ереванского государственного
университета

Поступило 20.VII.1968

Վ. Ա. ԱՌԱՔԵԼՈՎ, Ռ. Ռ. ՎԱՐՇԱՄՈՎ. Ռեկուրենտ պարբերական հաջորդականությունների ճառագայթական կառուցվածքի ուսումնասիրության շուրջը *(ամփոփում)*

Երկու մասից բաղկացած աշխատանքը նվիրված է Գալուայի $GF(q)$, $(q=p^n)$ դաշտից վերցված գործակիցներով K աստիճանի նորմավորված $h(x)$ բազմանդամին համապատասխանող հետադարձ կապով տեղաշարժի ռեգիստրով գեներատորի օգնությամբ ստացվող ռեկուրենտ պարբերական հաջորդականությունների մաթեմատիկական կառուցվածքի և բնորոշ հատկությունների ուսումնասիրմանը։

Եթե ռեգիստրի սկզբնական պարունակությունն է $a(0),\cdots,a(k-1)$, ապա ելքի հաջորդականության ցանկացած $a(N)$, $(N\geqslant 0)$ անդամ կարելի է ներկայացնել հետևյալ տեսքով.

$$a(N) = \varphi_0(N)\,a(0)+\varphi_1(N)\,a(1)+\cdots+\varphi_{k-1}(N)\,a(k-1),$$

որտեղ $\varphi_l(N)$ դործակիցները $GF(q)$ դաշտից են։

Առաջին մասի հիմնական արդյունքը հետևյալն է։

Թեորեմ. Դիցուք $N\geqslant k$, ամրողջ թիվ է, $h(x)=\sum_{j=0}^{k} h_j x^j$, $h_j\in GF(q)$ տեղաշարժի ռեգիստրով գեներատորի հետադարձ կապի բազմանդամն է, որի միայն $h_0, h_{k_1},\cdots,h_{k_t}, h_{k_t}=1$ դործակիցներն են զերոյից տարբեր և $\{x_0^{(l)},\cdots x_l^{(l)}\}$ $(l=\overline{1,s})$, $N-k=\sum_{l=1}^{t}(k-k_l)\,z_l$ հավասարման բոլոր հնարավոր ամրողջաթիվ ոչ բացասական լուծումների բազմությունն է։ Այդ դեպքում՝

* $T(h(x))$ есть показатель, которому принадлежит полином $h(x)$, т. е. наименьшее натуральное число, удовлетворяющее условию $x^T\equiv 1 \pmod{h(x)}$.

$$\sum_{l=1}^{s} (-1)^{z_0^{(l)}+\cdots+z_t^{(l)}+1} \cdot h_0^{z_0^{(l)}+1} \cdot h_{k_1}^{z_1^{(l)}} \cdots h_{k_t}^{z_t^{(l)}} \frac{(z_0^{(l)}+\cdots+z_t^{(l)})!}{z_0^{(l)}!\cdots z_t^{(l)}!} \equiv \varphi_0(N) (\mathrm{mod}\ p),$$

ընդունելով $\sum_{l=1}^{0} = 0$:

Երկրորդ մասում հետազոտվում է հետևյալ թվային ֆունկցիան՝

$$P(z_0, \cdots, z_t) = \frac{(z_0+z_1+\cdots+z_t)!}{z_0!z_1!\cdots z_t!}.$$

V. A. ARAKELOV, R. R. VARSHAMOV. *On the research of algebraic strvcture of periodical recurrent sequencies* (summary)

The paper is devoted to investigation of mathematical structure and of characteristic peculiarities of recurrent periodic sequencies, received by means of the generator on shift register with feedback, corresponding to a monic polinomial $h(x)$, of degree k, with factors from the Galua field $GF(q)$ $(q=p^n)$.

If $a(0)$, $a(1)\cdots$, $a(k-1)$ is the initral filling of generator storage on the shift register, any element $a(N)$ $(N>0)$, of output generator's sequence can be represented by:

$$a(N) = \varphi_0(N)\, a(0) + \varphi_1(N)\, a(1) + \cdots + \varphi_{k-1}(N)\, a(k-1)$$

where factors $\varphi_i(N)$ are elements of field $GF(q)$.

Theorem (§ 1). Let integer $N \geq k$, $h(x) = \sum_{j=0}^{k} h_j x^j$, $h_j \in GF(q)$ be the polinomial of generator feedback on shift register, with nonsero factors $h_0, h_{k_1}, \cdots, h_{k_t}$, $h_{k_t}=1$, and let $\{z_0^{(l)}, z_1^{(l)}, \cdots, z_t^{(l)}\}$ $(l=\overline{1,s})$ be a system of all integer non-negative solutions of equation $N-k = \sum_{l=0}^{t} (k-k_l)\, z_l$.

Then

$$\sum_{l=1}^{s} (-1)^{z_0^{(l)}+\cdots+z_t^{(l)}+1} \cdot h_0^{z_0^{(l)}+1} \cdot h_{k_1}^{z_1^{(l)}} \cdots h_{k_t}^{z_t^{(l)}} \cdot \frac{(z_0^{(l)}+\cdots+z_t^{(l)})!}{z_0^{(l)}!\cdots z_t^{(l)}!} \equiv \varphi_0(N)(\mathrm{mod}\,p),$$

assuming $\sum_{l=1}^{0} = 0$.

In § 2 numerical function $P(z_0, \cdots, z_t) = \frac{(z_0+\cdots+z_t)!}{z_0!\cdots z_t!}$ is considered.

ЛИТЕРАТУРА

1. *J. H. Green*, R. L. Sr. San Souce. An error correcting encoder and decoder of high Efficiency, Proc. IRE, 46, 1958.
2. *Р. Р. Варшамов, Г. М. Тенениольц.* Об одном классе циклических кодов, Проблемы кибернетики, Изд-во „Наука", вып. 22, 1970, 157—166.
3. *Дж. Месси.* Пороговое декодирование, Изд-во Мир, М., 1964.
4. *У. Питерсон.* Коды, исправляющие ошибки, Изд-во Мир, М., 1964.
5. *В. А. Аракелов.* Об одном методе исследования периодических рекуррентных последовательностей, Сборник трудов III Всесоюзной конференции по теории передачи и кодирования информации, Изд-во ФАН, 1967.