6
А-43

Министерство приборостроения,
средств автоматизации и систем
управления СССР

Академия наук СССР

ОРДЕНА ЛЕНИНА
ИНСТИТУТ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ
(ТЕХНИЧЕСКОЙ КИБЕРНЕТИКИ)

На правах рукописи

В.А.Аракелов

# НЕКОТОРЫЕ ВОПРОСЫ АЛГЕБРАИЧЕСКОЙ СТРУКТУРЫ КОДОВ И ИХ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

(спец. № 255 - техническая кибернетика)

Автореферат
диссертации на соискание ученой степени кандидата
технических наук

Москва - 1969 год

Министерство приборостроения,
средств автоматизации и систем
управления СССР

Академия наук СССР

ОРДЕНА ЛЕНИНА
ИНСТИТУТ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ
(ТЕХНИЧЕСКОЙ КИБЕРНЕТИКИ)

На правах рукописи

В.А.Аракелов

# НЕКОТОРЫЕ ВОПРОСЫ АЛГЕБРАИЧЕСКОЙ СТРУКТУРЫ КОДОВ И ИХ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

(спец. № 255 - техническая кибернетика)

Автореферат
диссертации на соискание ученой степени кандидата
технических наук

Москва - 1969 год

В своей фундаментальной теореме о дискретных каналах с шумом Шеннон показал, что используя достаточно длинные коды, возможно передавать информацию со скоростью, сколь угодно близкой к пропускной способности канала и со сколь угодно малой вероятностью ошибки. Это теоретическое положение послужило началом нового направления науки - теории корректирующих кодов, основным предметом которого является исследование возможностей улучшения связи за счет увеличения избыточности кодирования.

С точки зрения методов различаются два главных направления: метод последовательного декодирования, с использованием принципов вероятностного подхода и алгебраическая теория кодов. Однако, подавляющее большинство работ по кодированию посвящено именно алгебраической теории кодов, основные достижения которой до 1961 г. с исчерпывающей полнотой излагаются в монографии[2] Питерсона.

Привлечение аппарата алгебры характеризует качественно новый шаг в теории корректирующих кодов, логическим результатом которого явилось открытие циклических кодов, образующих подкласс линейных кодов и с точки зрения их технической реализации, являющихся наиболее простыми и удобными. Наиболее важным здесь является результат, полученный Р.К.Боузом и Д.К.Рой-Чоудхури, а также независимо от них А.Хоквингемом, которые сводят задачу построения кодов к задаче отыскания полиномов над конечными полями, имеющих заданное множество корней. Обобщением этих кодов (вообще говоря и всех циклических), очевидно, является случай, когда проверочный полином кода задается произведением произвольных 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, 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. Наконец, более детальное изучение возвратных последовательностей, несомненно, найдет приложение как в вопросах порогового декодирования, так и в конструктивной теории приводимости полиномов над конечными полями.

Структура периодических циклических последовательностей зависит от свойств полиномов обратной связи генератора на регистре сдвига, с помощью которого они могут быть получены. Поэтому исследование полиномов представляющее достаточно самостоятельный интерес, становится важным и в изучении возвратных последовательностей. Кроме того, результаты таких исследований могут быть успешно применены и в ряде других задач.

Основным препятствием на пути широкого, практического применения кодов большой длины, является сложность декодирования. В одних случаях эта сложность связана с большим числом операций и объемом памяти, а в других - с выполнением весьма сложных, с трудом поддающихся автоматизации вычислений, последовательность которых определяется громоздкой логи-



ческой схемой. Этим недостатком, например, обладает алгоритм Питерсона для декодирования кодов Боуза-Чоудхури-Хоквингема. Поэтому, в последнее время, обращено большое внимание на разработку методов декодирования, допускающих простую реализацию. Кроме того, задача построения оптимальных и близких к ним кодов вытесняется задачей построения кодов с простым алгоритмом декодирования, обеспечивающих вместе с тем достаточно хорошее использование избыточности.

В последнее время особое внимание привлекла проблема синтеза кодов, используемых при передаче по несимметричному каналу. В отличие от симметричного несимметричным каналом называется канал с неодинаковыми вероятностями повреждений различных элементарных символов. В данной ситуации обычно пренебрегают наименьшими вероятностями, пытаясь защитить рабочие сигналы только от некоторых частичных искажений, имеющих в настоящий момент наибольшую вероятность. Корректирующие коды, предназначенные для обнаружения и исправления такого рода ошибок называются несимметричными и только с недавнего времени стали предметом систематического изучения.

В системах связи возможна такая ситуация, когда полученное сообщение имеет длину, отличную от длины посланного сигнала. Такого рода искажения могут иметь место при нарушении синхронизации работы приемника и передатчика системы связи. Поэтому представляет интерес исследование каналов, в которых допускаются сбои вида $\alpha \to \Lambda$ ,называемые выпадениями и сбои вида $\Lambda \to \alpha$ , называемые вставками (здесь $\Lambda$ - пустое слово; $\alpha \div 0, I \ldots q - I$, целое $q \geq 2$).

Подводя итоги современному состоянию теории кодирования и её практическому применению, можно по-прежнему, считать актуальным решение следующих вопросов:

I) анализ алгебраической структуры циклических последовательностей, с целью построения новых кодов, а также совершенствования известных методов кодирования и декодирования;

2) задача построения реально осуществимых схем декодирования, а также построение кодов с простым алгоритмом декодирования, обеспечивающих вместе с тем достаточно хорошее использование избыточности;

3) разработка новых, наиболее перспективных методов кодирования и декодирования для широкого класса реальных систем (несимметрических систем, систем с повреждениями типа вставок или выпадений и др.).

Решению указанных задач и посвящена настоящая работа, состоящая из введения и трех глав.

В первой главе проводится исследование математической структуры и характерных особенностей возвратных последовательностей, а также исследуются некоторые полиномы. Периодические последовательности можно получить с помощью генератора на регистре сдвига, обратная связь которого соответствует некоторому нормированному полиному $h(x)$, степени $k$, с коэффициентами из произвольного поля Галуа $GF(q)$. Если $a(0)$, $a(I)$,... $a(K-I)$ первоначальное заполнение накопителя генератора на регистре сдвига, то любой элемент $a(N)$ (целое $N \geq 0$) выходной последовательности генератора можно представить в следующем виде:

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

где коэффициенты $\varphi \in GF(q)$



С целью определения коэффициентов разложения (I) сформулирована и доказана следующая теорема, являющаяся наиболее характерным результатом первой главы.

<u>Теорема.</u> Пусть целое $N \geq k$, $h(x) = \sum_{j=0}^{k} h_j x^j$ полином обратной связи генератора на регистре сдвига, у которого только коэффициенты $h_0, h_{k_1}, h_{k_2}, \dots, h_{k_t}, h_k = 1$ отличны от нуля и пусть $\{z_0^{(i)}, z_1^{(i)}, \dots, z_t^{(i)}\}$, $(i = \overline{1,s})$ системы всевозможных целочисленных неотрицательных решений диофантова уравнения $N-k = \sum_{i=0}^{t} m_i z_i$, тогда

$$\sum_{i=1}^{s} (-1)^{z_0^{(i)} + z_1^{(i)} + \dots + z_t^{(i)}} \cdot h_0^{z_0^{(i)}+1} \cdot h_{k_1}^{z_1^{(i)}} \cdots h_{k_t}^{z_t^{(i)}} \cdot \frac{(z_0^{(i)} + \dots + z_t^{(i)})!}{z_0^{(i)}! \dots z_t^{(i)}!} \equiv \varphi_0(N) \pmod p \qquad (2)$$

полагая $\sum_{i=1}^{0} = 0$.

Другие коэффициенты $\varphi_j(N)$, $(j = \overline{1, k-1})$ разложения (I) можно определить, используя полученную в этой же главе следующую формулу:

$$\varphi_j(N) = \sum_{i=0}^{j} \varphi_0(N-j+i) \cdot h_i \cdot h_0^{-1} \qquad (3)$$

Определение коэффициента $\varphi_0(N)$ из (2) затрудняется вычислением числовой функции

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

где $z_0, z_1, \dots z_t$ целые неотрицательные числа.

Поэтому в дальнейшем исследуется эта функция, в результате чего доказана лемма, устанавливающая необходимое и достаточное условие, при котором указанная функция удовлетворяет следующему сравнению:

$$P(z_0, z_1, \dots z_t) = \prod_{i=0} \frac{\left[\frac{z}{p^i}\right]_p}{\prod\limits_{j=0}^{t} \left[\frac{z_j}{p^i}\right]} \pmod p \quad {}^{*)} \qquad (4)$$

При этом показано, что если условия леммы не выполняются, то тогда $P(z_0, z_1, \dots z_t) \equiv 0 \pmod p$. Все это позволяет в значительной степени упростить вычисление коэффициента $\varphi_0(N)$ из сравнения (2). Следует отметить, что при $q = 2$, приведенные здесь выкладки существенно упрощаются.

Рассматриваемые последовательности являются периодическими и поэтому небезынтересно исследование их периода, т.е. исследование функциии от параметров соответствующего полинома обратной связи генератора на регистре сдвига. Задача определения величины периода в общем случае не решена, поэтому всякий результат в этом направлении представляет интерес и может быть использован не только в теории кодирования, но и в теории приводимости полиномов над конечными полями. В этой связи, в первой главе для функции $T(k, k_1, \dots k_t, 0)$ **) получено аналитическое выражение при довольно широких ее показателях. Таким образом, получена

---

x) Величина $[z]_p = z - p\left[\frac{z}{p}\right]$ — есть наименьший неотрицательный вычет числа $z$ по модулю $p$.

xx) $T(k, k_1, \dots k_t, 0)$ — показатель, которому принадлежит полином $h(x) = x^k + x^{k_1} + x^{k_1} + x^{k_2} + \dots + x^{k_t} + 1$, степени К с коэффициентами из поля $GF(2)$, ($k_i > k_{i+1}$ — натуральные числа. $i = \overline{1, t-1}$).



возможность аналитически определять величину периода, для довольно широкого класса полиномов.

Доказанная основная теорема позволяет в равенстве (I), для произвольного целого $N \geq 0$, определить коэффициенты $\varphi_i(N)$ и тем самым наименьший неотрицательный вычет выражения $x^N$ по модулю полинома $h(x)$. Большой интерес представляет также и обратная задача, когда при заданных коэффициентах требуется определить величину $N$. Несмотря на актуальность этой задачи, автору не известно ни одного результата, полученного в этом направлении. В связи с этим предлагается метод, позволяющий по заданным коэффициентам разложения (I), за ограниченное число шагов $\ell < n$ определить величину $N$, для некоторого класса полиномов над полем $GF(2)$, имеющих вид $h(x) = x^n + x^m + 1$.

Наконец, приведенные в заключении первой главы некоторые замечания о взаимосвязях между корнями полиномов $f(x)$ и $f(1+x)$, позволяют разработать метод, существенно ограничивающий перебор, построения ортогональных соотношений размера два, для класса кодов, проверочный полином которых неприводим в поле $GF(2)$.

Во второй главе приводится метод декодирования линейных кодов, реализация которого предполагает относительно небольшими число операций и объем памяти. Показаны его преимущества над некоторыми известными методами декодирования и, в частности, поэтапным декодированием и методом, "основанным на выборе синдромов". Вторая часть главы посвящена синтезу одного класса линейных кодов, имеющих простые схемы кодирования и декодирования.

Для заданного линейного ( $n,k$ ) кода всякий проверочный символ $b_i$ ( $i = \overline{1, n-k}$ ), представим в виде некоторой линейной комбинации из информационных символов т.е.

$$b_i = \alpha_{i1} a_1 + \alpha_{i2} a_2 + \dots + \alpha_{ik} a_k \qquad (5)$$

Для искаженного вектора

$$V' = (a_1', a_2', \dots a_k', b_1', b_2' \dots b_{n-k}').$$

полученного на приемном конце, справедливы следующие соотношений:

$$b_{p_i} = \alpha_{p_i 1} a_1' + \alpha_{p_i 2} a_2' + \dots + \alpha_{p_i k} a_k', \ (i = \overline{1, g_0}) \qquad (6)$$

$$b_{\ell_i} \neq \alpha_{\ell_j 1} a_1' + \alpha_{\ell_j 2} a_2' + \dots + \alpha_{\ell_j k} a_k', \ (j = \overline{1, g_1}) \qquad (7)$$

$$(p_i + \ell_i = \overline{1, n-k}), \quad (g_0 + g_1 = n-k)$$

Идея предлагаемого алгоритма декодирования основана на исследовании характера размножения ошибок, происшедших в информационной части кодового вектора, и использовании некоторых внутренних закономерностей алгебраической структуры реализуемого кода. Что же касается непосредственной реализации упомянутого метода, то здесь дело фактически сводится к анализу матриц

$A_0 = [\alpha_{p_i, j}]$ размерности $g_0 \times k$, $(i = \overline{1, g_0}, \ j = \overline{1, k})$

$A_1 = [\alpha_{\ell_j, i}]$ размерности $g_1 \times k$, $(j = \overline{1, g_1}, \ i = \overline{1, k})$



элементы $\alpha$ которых, есть соответствующие коэффициенты соотношений (6) и (7). Анализ матриц $A_0$ и $A_1$ предполагает нахождение комбинаций из $\omega \leq t$ векторов-столбцов, для каждой матрицы в отдельности, веса которых удовлетворяют вполне определенным оценкам, зависящим как от числа $t$ исправляемых кодом ошибок, так и от характера искажений. В работе показано, что приведенный алгоритм декодирования легко обобщается также и на случай кодов с основанием $p$ ( $p$ - простое число).

В этой же главе предлагается класс линейных ( $n,k$ ) кодов, имеющих простые алгоритмы кодирования и декодирования. Показано, что к этим кодам применим метод порогового декодирования, который, однако, в данном случае не достаточно эффективен, поскольку эти коды не являются циклическими. Поэтому, в качестве корректирующей схемы предлагается описанный выше алгоритм декодирования, который для данных кодов в силу их некоторых специфических особенностей, существенно упрощается.

Третья глава диссертации посвящена синтезу некоторых классов корректирующих кодов, с произвольным основанием $q \geq 2$, устойчивых к одиночным сбоям типа вставок или выпадений, а также к одиночным несимметрическим искажениям.

Для несимметрического канала рассматриваются "большие" искажения типа "+" (или "-"), т.е. когда произвольный символ может быть подвергнут искажению вида $i \to i + \ell$ (или $i \to i - \ell$ ), где $\ell = 1, 2, \dots q-i-1$ (или $\ell = 1, 2, \dots i$), $i = \overline{0, q-2}$, (или $i = \overline{1, q-1}$ ), целое $q \geq 2$.

Доказаны несколько теорем, позволяющих строить вышеуказанные коды. Эти коды при $q=2$ совпадают с известными. Указанные коды не являются систематическими, поэтому для удобства реализации они видоизменяются так, чтобы получить систематические коды.

Для рассматриваемых в третьей главе кодов приведены алгоритмы кодирования и декодирования, а также схемы соответствующих им устройств. Показано, что рассматриваемая конструкция может быть использована и для синтеза класса кодов, корректирующих одиночные симметрические ошибки, которые также как и коды, исправляющие несимметрические ошибки, могут быть записаны в систематическом виде. Рассмотренные коды используются для построения универсальной системы кодирования с исправлением одиночных несимметрических (симметрических) ошибок или ошибок типа вставок (выпадений). Приведены схемы кодирующего и декодирующего устройств указанной системы, при построении которой использовался тот факт, что большая часть оборудования системы для исправления одиночных несимметрических (симметрических) ошибок и системы с исправлением одиночных вставок (выпадений) общая.

Основные результаты работы.

I. В результате исследования математической структуры возвратных последовательностей предложен метод, позволяющий определять наименьший неотрицательный вычет

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

выражения $x^N$ (целое $N\geq 0$ ) по модулю некоторого нормированного полинома вида $h(x)=\sum h_j\cdot x^j,\ h_0=1$



с коэффициентами из поля Галуа $GF(p^m)$ С алгебраической точки зрения указанная задача сведена к решению диофантова уравнения вида

$$N-k=\sum_{i=0}^{t} m_i z_i\ ,\ \text{где}\quad m_i=k-k_i\ ,\quad (i=\overline{0,t})$$

Кроме того, предлагается метод, для некоторого класса полиномов вида $h(x)=x^n+x^m+1,$ позволяющий по заданным коэффициентам разложения (I) за число шагов $\ell<n$ определить величину $N$ .

2. Для числовой функции $P(z_0, z_1, \dots z_t)$ получено следующее соотношение:

$$P(z_0, z_1, \dots z_t)\equiv\prod_{i=0} \frac{\left[\frac{z}{p^i}\right]_p}{\prod_{j=0}^{t}\left[\frac{z_j}{p^i}\right]_p} \pmod p$$

где $[z]_p$ - наименьший неотрицательный вычет числа по модулю $p$ .

3. Для некоторых классов полиномов получены формулы их периодов.

4. Предлагается метод, существенно ограничивающий перебор, построения ортогональных соотношений размера два, для класса кодов, проверочный полином которых $h(x)$ неприводим в поле $GF(2)$.

5. Предлагается новый метод декодирования линейных кодов, для реализации которого требуются относительно небольшие число операций и объем памяти.

6. Приводится синтез одного класса линейных кодов, с простым алгоритмом декодирования, обеспечивающим вместе с тем достаточно хорошее использование избыточности.

7. Предлагаются классы корректирующих кодов с произвольным основанием $q>2$, устойчивых к одиночным сбоям типа вставок или выпадений, а также к одиночным несимметрическим искажениям. При $q=2$ рассматриваются систематические коды, для которых приводятся алгоритмы кодирования и декодирования, а также схемы соответствующих им устройств.

8. Предлагается универсальная система кодирования с исправлением одиночных несимметрических (симметрических) ошибок или ошибок типа вставок (выпадений). Устройства кодирования и декодирования указанной системы защищены авторскими свидетельствами.

Основные результаты диссертации были доложены на Ш Всесоюзной конференции по теории передачи и кодированию информации (Ужгород, 1967 г.), на Ш Всесоюзном симпозиуме по использованию избыточности в информационных системах (Ленинград, 1968 г.) и опубликованы в следующих работах:

I. Аракелов В.А. "Об одном методе исследования периодических рекуррентных последовательностей". Сборник трудов Ш конференции по теории передачи и кодированию информации, ФАН, Ташкент, 1968 г.

2. Варшамов Р.Р., Тененгольц Г.М., Аракелов В.А. "Устройство для кодирования". Авторское свидетельство № 226 279 от 19 мая 1967 г. Бюллетень изобретений, № 28, 1968 г.

3. Варшамов Р.Р., Тененгольц Г.М., Аракелов В.А., "Устройство для декодирования кодов", Авторское свидетельство № 228338 от 19 мая 1967 г. Бюллетень изобретений № 3I, 1968 г.



4. Аракелов В.А., Тененгольц Г.М. "Метод построения ортогональных проверок". Тезисы докладов к третьему Всесоюзному симпозиуму по использованию избыточности в информационных системах. Ленинград, ЛиАП, 1968 г.

5. Аракелов В.А., Тененгольц Г.М. "Нёкоторые свойства рекуррентных периодических последовательностей". Труды ВЦ АН Арм.ССР "Математические вопросы кибернетики и вычислительной техники". (Теория информации и кодирования), Ереван, 1969 г. (в печати).

6. Аракелов В.А., Тененгольц Г.М. "Некоторые классы корректирующих кодов". Труды ВЦ АН Арм.ССР "Математические вопросы кибернетики и вычислительной техники". (Теория информации и кодирования), Ереван, 1969 г. (в печати).

7. Аракелов В.А., Тененгольц Г.М. "Классы кодов для специальных каналов связи", Сборник "Преобразование и уплотнение телеметрической информации". Изд-во "Илим", Фрунзе, 1969 г. (в печати).

8. Варшамов Р.Р., Аракелов В.А. "К исследованию алгебраической структуры периодических рекуррентных последовательностей". Известия АН Арм.ССР. "Математика", вып.П, Ереван, 1969 г. (в печати).

Т-05714, подп.в печ.9/IУ-69г. Зак.20I, т.I30; Лит.ЦПМ ГТП

Центральная научная
БИБЛИОТЕКА
Академии наук Киргизской ССР