Министерство
приборостроения, средств автоматизации и систем управления

Академия Наук
Союза Советских Социалистических Республик

ИНСТИТУТ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ
/технической кибернетики/

Г.М.ТЕНЕНГОЛЬЦ

# НЕКОТОРЫЕ КЛАССЫ КОРРЕКТИРУЮЩИХ КОДОВ

Автореферат
диссертации на соискание ученой степени кандидата технических наук

Научный руководитель
доктор физико-математических наук Р.Р.ВАРШАМОВ

Москва, 1966 г.

Министерство
приборостроения, средств автоматизации и систем управления

Академия Наук
Союза Советских Социалистических Республик

ИНСТИТУТ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ
/технической кибернетики/

Г.М.ТЕНЕНГОЛЬЦ

# НЕКОТОРЫЕ КЛАССЫ КОРРЕКТИРУЮЩИХ КОДОВ

Автореферат
диссертации на соискание
ученой степени кандидата
технических наук

Научный руководитель
доктор физико-математических
наук Р.Р.ВАРШАМОВ

Москва, 1966 г.

Шеннон в своей классической работе о системах связи показал, что ненадежный канал, вообще говоря, не ограничивает надежность, а лишь понижает скорость передачи информации. После опубликования работы Шеннона в 1948 г. резко возрос интерес к теории корректирующих кодов, занимающейся вопросами обеспечения надежности передачи информации за счет введения избыточности кодирования.

С середины 50-х годов для построения корректирующих кодов привлекаются методы современной алгебры - стала глубоко и интенсивно развиваться теория линейного кодирования.

Привлечение аппарата линейной алгебры характеризует качественно новый шаг в теории корректирующих кодов. Из класса линейных кодов был выделен подкласс циклических кодов, допускающих наиболее простую техническую реализацию на регистрах сдвига с обратной связью.

Если первоначально теория кодирования ограничивалась исследованием систем связи с постоянными и независимыми канальными искажениями отдельных символов передаваемого сигнала, то для настоящего времени характерны исследования моделей каналов, наиболее приближающихся к реальным системам связи.

Синтезу кодов для некоторых типов каналов, отличных от наиболее хорошо изученного в теории симметричного канала, и посвящена большая часть настоящей работы. Диссертация состоит из трех глав.

В первой и второй главах рассматриваются коды для несимметрического канала, канала со сбоями типа вставок и выпадений символов, а также канала, в котором символы сигналов принимают значения из разных по мощности алфавитов.

В третьей главе предлагается новый эффективный класс циклических кодов.

В последнее время особое внимание привлекла проблема синтеза кодов, используемых при передаче по несимметрическому каналу.

В отличие от симметрического несимметрическим каналом называется канал с неодинаковыми вероятностями повреждений различных элементарных посылок /импульсов/. В бинарном случае, например, это означает, что вероятность перехода символа " I " в " 0 " в кодовом слове при прохождении его по каналу существенно меньше вероятности перехода " 0 " в " I " или наоборот. В такой ситуации обычно пренебрегают наименьшими вероятностями и пытаются защитить рабочие сигналы только от некоторых частичных ошибок, имеющих в данном случае наибольшую вероятность. Примером реального устройства с несимметрическими искажениями может служить запоминающее устройство на ферритах или на магнитной ленте в больших вычислительных машинах; в релейных же устройствах это искажения типа обрыва или короткого замыкания.

Имеется ряд работ, посвященных теории кодов для несимметрического канала /так называемых несимметрических кодов/. Следует отметить коды Кима-Фреймана, исправляющие одиночные и



кратные несимметрические ошибки, а также небинарный код Кима, исправляющий малые ошибки типа +I или -I по модулю $q$, линейные коды Бернштейна, исправляющие одиночные ошибки в симметричных и несимметричных вычислительных процессах. Пропускная способность двоичного несимметрического канала исследовалась Чангом. Класс разделимых кодов, приспособленных для обнаружения несимметрических ошибок, был предложен Бергером.

Однако в большей части этих работ математические средства, используемые при решении поставленных задач, недостаточно эффективны. Более глубоко математическая структура и характерные особенности несимметрических кодов исследовались Р.Р.Варшамовым. Варшамовым рассматривался канал с $\Omega$ - несимметрическими искажениями, т.е. канал, в котором искажаются не все передаваемые символы, а только некоторая совокупность $\Omega$ из элементов поля $GF(q)$. Им было получено необходимое и достаточное условие существования кодов, исправляющих многократные $\Omega$ - несимметрические ошибки, а также верхняя и нижняя границы максимально возможного числа сигналов. Частным случаем рассмотренного Варшамовым канала является симметрический канал $(\Omega = GF(q))$, а также двоичный полностью несимметрический канал / $\Omega$ состоит из одного элемента "0" или "I"./

В главе I настоящей диссертации рассматривается еще одно обобщение двоичного несимметрического канала, а именно канал, в котором вероятности переходов $0 \to I$ и $I \to 0$ не равны нулю и не равны друг другу. Под несимметрическим бинарным $[n, K_0, K_1]$ - кодом понимается код длины $n$, исправляющий $K_0$ ошибок типа 0 → I и $K_1$ ошибок типа I → 0. В случае строго несимметрического канала $K_0$, либо $K_1$ равны 0.

Введя несимметрическое расстояние между двоичными последовательностями $x$ и $y$ в виде $\bar{\rho}(x,y)=|x-y|+||x|-|y||$, где $|x|$ - норма (число единиц) последовательности $x$, необходимое и достаточное условие существования $[n, K_0, K_1]$ - кодов, получено в виде следующей теоремы.

Теорема I.

Для того чтобы код исправлял $K_0$ ошибок типа 0 → I и $K_1$ ошибок типа I → 0 необходимо и достаточно, чтобы расстояние $\bar{\rho}(x,y)$ между любыми двумя кодовыми словами было не меньше $2(K_0+K_1+1)$.

Из теоремы I следует интересный факт, что $[n, K_0, K_1]$ - код является кодом, исправляющим $K_0+K_1$ строго несимметрических ошибок типа 0 → I /или I 0/ и наоборот.

Таким образом, задача построения $[n, K_0, K_1]$ - кодов сводится к проблеме синтеза кодов, корректирующих многократные несимметрические ошибки. Полученный результат можно использовать при синтезе релейных устройств с несимметрической характеристикой повреждений.

В главах I и П используются сравнения вида:

$$W_{\alpha\beta}=\sum_{i=1}^{n}\beta_i\cdot\gamma(\alpha_i)\equiv a \pmod m, \qquad \text{(I)}$$

где $\beta_i$ - члены заданной последовательности, $a=0,1,\ldots,m-1$

$\alpha_i=0,1,2,\ldots,q_i-1$; $q_i\geq 2$ -



целое, $\gamma(\alpha_i)$ - коэффициенты, зависящие от величины $\alpha_i$. Использование (I) при различных начальных данных позволяет решить ряд технических задач. Автором совместно с Р.Р.Варшамовым было показано, что совокупность всевозможных бинарных решений выражения (I) при $\beta_i=i$, $m=n+1$; $\gamma(\alpha_i)=\alpha_i$ / $n$ - длина сигнала/ образует двоичный код, исправляющий одиночные несимметрические ошибки.

Показано, что при одинаковой длине кодового слова $n$ мощность $M$ наилучшего из предлагаемых кодов x) значительно больше мощности $M_1$ симметрического кода Хэмминга /исключая случай $n=2^k-1$; $k$ - произвольное целое, когда $M=M_1$ и мощности $M_2$ кода Фреймана - Кима /при $n>6$/.

В случае, когда $m=n^2+n+1$; $n=p^k$; $p$ - простое; $k>0$ произвольное целое, $\beta_i$ являются членами последовательности Зингера, обладающей тем свойством, что

$$\beta_i-\beta_j\neq\beta_k-\beta_e \pmod{n^2+n+1},$$

где индексы $i,j,k$ - различны, $\beta_i-\beta_j$ $(i,j=0,1,\ldots,n)$ сравнимы по модулю $n^2+n+1$ с целыми $1,2,\ldots,n^2+n$ в некотором порядке, $\beta_i<n^2+n+1$, $\beta_0=0$, совокупность всевозможных двоичных решений сравнения (I) образует код, исправляющий двойные и одиночные несимметрические ошибки.

В технике связи получают распространение небинарные устройства хранения и передачи информации с несимметрической

---

x) Как показал Р.Р.Варшамов в качестве наилучшего /в смысле мощности/ кода в предлагаемом классе кодов можно взять код, получающийся при $a=0$.

характеристикой повреждений. Поэтому представляет интерес исследование несимметрических систем кодирования с произвольным основанием кода $q \geq 2$.

В этом случае возможны два типа несимметрических ошибок:

I/ малые искажения типа /+I/ /или -I/, когда каждый символ /за исключением символа $q-1$, который не искажается/ может быть подвергнут искажению вида $i \to i+1$ (или $i \to i-1$);

2) большие искажения типа / + / (или / - /), когда все символы (за исключением символа $q-1$) подвержены искажению вида $i \to i+k$ /или $i \to i-k$ $1, k = 1,2,\dots,q-1-i$ $(i=0,1,\dots,q-2)$

Полагая в сравнении (I) $\beta_i = i$, $\gamma(\alpha_i) = \alpha_i = 0,1,2,\dots,q-1$ $m = n+1$,

получаем код, исправляющий малые искажения типа / +I / /или -I/, а выбирая в качестве $p_i$ - члены последовательности, обладающей тем свойством, что для любого $i$ и $j$ $(i \neq j)$ $p_i\alpha_i \neq p_j\alpha_j$ $(i,j = 1,2,\dots,n)$; $\alpha_i, \alpha_j = 1,2,\dots,q-1$, и полагая $m = (q-1)\cdot p_n + 1$, получаем код, исправляющий "большие" искажения типа / + / или / - / .

В главе П предлагается также класс кодов для каналов, в которых допускаются сбои вида $\alpha \to \lambda$, называемые выпадениями, и сбои вида $\lambda \to \alpha$, называемые вставками /здесь $\lambda$ - пустое слово; $\alpha = 0,1,\dots,q-1$; $q \geq 2$ - целое/.

Такого рода искажения, когда полученное сообщение имеет длину /число символов/, отличную от длины посланного сигнала, могут иметь место при нарушении синхронизации работы приемника и



передатчика системы связи.

Проблема синтеза кодов, исправляющих вставки, выпадения и замещения символов в сигнале исследовалась В.И.Левенштейном. Он показал, что двоичный код Варшамова-Тененгольца с исправлением одиночных несимметрических ошибок является кодом с коррекцией одиночных ошибок типа вставок или выпадений символов, причем кодом асимптотически оптимальным.

В настоящей работе предлагается код, исправляющий одиночные вставки или выпадения символов в сигнале, основание которого $q \geq 2$. Этот код получается с помощью сравнения (I), полагая $m = \sum_{v=0}^{q-1} n^v$; $\beta(\alpha_i) = \sum_{t=0}^{\alpha_i - 1} n^t$ /причем по определению $\sum_{t=0}^{-1} n^t = 0$/, $\alpha_i = 0,1,\dots,q-1$.

И, наконец, сравнение (I) используется в диссертации для построения системы кодирования с исправлением одиночных ошибок для канала, в котором символы сигнала принимают значения из неодинаковых по мощности алфавитов.

Из сказанного выше следует как важно знать, при каком $\alpha$ сравнение (I) имеет максимальное число решений.

Задача о выборе оптимального $\alpha$ для случая, когда $\beta_i = i$; $\gamma(\alpha_i) = \alpha_i = 0,1,\dots,q-1$ полностью была решена Варшамовым.

В дальнейшем Б.Р.Гинзбургу удалось найти точную формулу числа решений сравнения (I) для указанного частного случая в точке максимума.

В диссертации исследуется /а именно находится максимальное число решений/ частный случай сравнения (I).

Доказывается следующая

Теорема 5.

Сравнение: $\sum_{i=1}^{n} i\alpha_i \equiv a \pmod{qn}$, где $\alpha_i = 0,1,2,\dots,q-1$; $q$ - произвольное целое, имеет максимальное число решений при значениях $a \equiv 0 \pmod{n}$, причем максимальное число решений

$$\mathcal{M}_{n,qn}^{0,q} = \frac{1}{n}\sum_{\substack{(u,q)=1 \\ u/n}} q^{\frac{n}{u}-1}\cdot\varphi(u)$$

где $\varphi(u)$- функция Эйлера.

Из теоремы 5 следует, что в классе двоичных кодов, исправляющих одиночные симметрические ошибки, получающихся из (I) при $\beta_i = i$, $\gamma(\alpha_i)=\alpha_i$; $m = 2n$, оптимальным будет код при значениях $a=0$ и $a=n$, причем число элементов кода при $a=0$ задается формулой

$$\mathcal{M}_{n,2n}^{0,2} = \frac{1}{n}\sum_{\substack{u/n \\ (u,2)=1}} \varphi(u)\cdot 2^{\frac{n}{u}-1}$$

Третья глава диссертации посвящена исследованию одного эффективного класса линейных циклических $q$-ичных кодов / $q$ -(основание кода) - степень простого числа, получаемых с помощью генератора на регистре сдвига с обратной связью, которой соответствует полином представляющийся в виде произведения примитивных полиномов с попарно взаимно простыми степенями. Выводится конечная формула для кодового расстояния предлагаемо-



го кода.

Доказана следующая.

Теорема

Линейный циклический код длины $\prod_{i=1}^{t}(q^{n_i}-1)$ / $q$ - степень простого/, получаемый с помощью генератора на регистре сдвига с обратной связью, которой соответствует полином $f(x)=\prod_{i=1}^{t} f_i(x)$, где $f_i(x)$ - примитивные полиномы с попарно взаимно простыми степенями $n_i$ $(n_1<n_2<n_3<\dots<n_t)$, имеет кодовое расстояние $d$, задаваемое формулой:

$$d = \begin{cases} \frac{1}{q}\left(q^{n_1+n_2}-q^{n_1}-q^{n_2}\right)\cdot\prod_{i=3}^{t}(q^{n_i}-1), & \text{если } t \geq 2 \\ \frac{1}{q}\cdot q^{n_1}, & \text{если } t=1, \end{cases}$$

где по определению $\prod_{i=3}^{2}(q^{n_i}-1)=1$

Показана оптимальность предлагаемого кода для случая $t \leq 2$ с помощью обобщенной границы Варшамова-Грайсмера. Оптимальный код сравнивается с кодом Соломона-Штиффлера с теми же параметрами, который является наилучшим среди известных в литературе. Схема кодирования и декодирования предлагаемого оптимального кода оказывается проще, чем соответствующего кода Соломона - Штиффлера.

Так как предлагаемый код циклический, то для декодирования можно применить известные схемы декодирования циклических кодов, например схему Меггита.
В случае двоичного кода, получаемого с помощью генератора с соответствующим примитивным полиномом / $t=1$ / можно, как показал Месси, применить мажоритарное декодирование, причем, для реализации /$n,k$/ - кода требуется один мажоритарный элемент и $n$ разрядов регистра сдвига.

Основные результаты диссертации были доложены на I научно-технической конференции молодых ученых и специалистов г.Москвы /Москва,1964г./, Ш Всесоюзном совещании по автоматическому управлению /технической кибернетике/ /Одесса,1965г./, П всесоюзной конференции по теории кодирования и ее приложениям /Баку,1965г./, ХШ конференции молодых ученых Института автоматики и телемеханики /технической кибернетики/ /Москва,1966г./ и опубликованы в следующих печатных материалах.

1. Варшамов Р.Р., Тененгольц Г.М. Код,исправляющий одиночные несимметрические ошибки,
Автоматика и телемеханика т.XXУI, № 2, 1965.

2.Тененгольц Г.М. Об одном классе кодов для несимметрического бинарного канала; сборник "Мир глазами молодого ученого", серия "Кибернетика" /Труды I научно-технической конференции молодых ученых и специалистов Москвы/. Москва, 1966 г.

3.Тененгольц Г.М. Системы кодирования с комбинированным использованием импульсных признаков, сборник "Структурная и абстрактная теория релейных устройств" Изд-во "Наука", Москва, 1966 г.



4. Варшамов Р.Р., Тененгольц Г.М. Математические методы повышения надежности передачи информации по несимметрическому каналу. Труды Ш Всесоюзного совещания по автоматическому управления /технической кибернетике/ Москва, 1966 г.

5. Тененгольц Г.М. Некоторые свойства кодов, исправляющих несимметрические ошибки.
Сборник "Техническая кибернетика", изд-во "Наука" /в печати/