Министерство транспорта и связи Украины
Государственный департамент по вопросам связи и информатизации

ОДЕССКАЯ НАЦИОНАЛЬНАЯ АКАДЕМИЯ СВЯЗИ
им. А.С.ПОПОВА

Кафедра теории электрической связи им. А. Г. Зюко

В.Л. Банкет

ДИСКРЕТНАЯ МАТЕМАТИКА В ЗАДАЧАХ ТЕОРИИ ЦИФРОВОЙ СВЯЗИ

Учебное пособие

Одесса 2008

УДК 519.95
ББК 318

Банкет В. Л. Дискретная математика в задачах теории цифровой связи: Учебн. пособие.– Одесса: ОНАС, 2008.– 118 с.

Пособие содержит элементы дискретной математики, необходимые для решения актуальных задач теории цифровой электрической связи. Теоретические положения иллюстрированы примерами. Изложены решения типовых задач теории цифровой связи, на основе которых составлен перечень рекомендуемых тем магистерских и аспирантских научно-исследовательских работ. Пособие предназначено для студентов, преподавателей, стажеров, аспирантов и магистрантов академии связи.

Содержание

Предисловие…… 5
1. Множества…… 7
2. Общая алгебра…… 8
2.1. Группы…… 8
2.1.1. Аксиомы групп…… 8
П.2.1.2. Правила сложения по модулю 2…… 9
2.1.3. Подгруппа. Композиционный ряд…… 11
2.1.4. Разложение группы по подгруппе…… 12
П.2.1.5. Группы в теории корректирующих кодов…… 12
2.1.6. Изоморфизм групп…… 13
2.1.7. Циклические группы…… 13
2.2. Кольца…… 15
2.2.1. Аксиомы колец…… 15
2.3. Поля…… 15
2.3.1. Аксиомы полей…… 15
П.2.3.2. Поле *F*(3) из трех элементов…… 16
2.3.3. Классификация полей…… 16
3. Целые числа. Теория делимости…… 17
4. Пространственные точечные решетки…… 18
4.1. Параметры сферических упаковок…… 19
П.4.2. Примеры решеток…… 20
П.4.3. Сигналы КАМ-16 на базе двумерной решетки…… 21
5. Алгебра степенных многочленов…… 22
П.*5*.1. Многочлены в теории циклических кодов…… 25
П.5.2. Многочленные представления в теории формирователей псевдослучайных последовательностей…… 28
6. ***Многотактные линейные фильтры***…… 31
П**.**6.1.Многотактные линейные фильтры в теории циклических кодов…… 33
….
П.6.2. Модель канала с относительным кодированием на базе теории многотактных линейных фильтров…… 36
П.6.3. ОФМ в системах с ПВК…… 38
7. Графы…… 45
П.7.1. Графы в теории сверточных кодов…… 46
П**.**7.2. Применение метода порождающих функций для анализа помехоустойчивости декодирования СК в каналах с постоянными параметрами…… 47
8. Алгоритмы…… 51
П.8.1. Алгоритм А. Витерби для декодирования сверточных кодов…… 52

9. Задачи теории дискретных сигналов …… 59
9.1. Асимптотические свойства сферических упаковок многомерных сигналов…… 59
9.2.Сигнально-кодовые конструкции……..... 64
9.3. Алгебраические и структурные модели ЧМ сигналов с непрерывной фазой…… 69
10. Задачи теории помехоустойчивого кодирования …….. 75
10.1. Кодовые границы групповых блоковых кодов……..... 75
110.2. Сложность реализации алгоритмов кодирования и декодирования…… 77
10.3. Условия катастрофичности сверточных кодов……..... 79
11. Перспективные методы передачи информации в цифровых телекоммуникационных системах..……. 84
11.1. Турбо-коды и их применение в телекоммуникационных системах…… 84
11.2. Пространственно-временное кодирование в системах беспроводной связи……..... 96
11.3. Помехоустойчивое кодирование в волоконно-оптических системах передачи…… 106
Приложение. Перечень рекомендуемых тем исследовательских работ аспирантов и магистрантов……. 112
Список использованных источников……. 115

Предисловие

В современных телекоммуникационных системах информация, как правило, передается в цифровом виде [1…4] и обрабатывается цифровыми методами [5…6]. Переход в последнее десятилетие к цифровым методам передачи и обработки сигналов существенно отразился на требованиях к содержанию и уровню математической подготовки инженеров. Если популярное в 60-е годы прошлого столетия справочное пособие А. Анго [7] из ”Физико-математической библиотеки инженера” содержало разделы, необходимые инженеру для работы с аналоговой схемотехникой (функции комплексной переменной, анализ и ряды, векторное и матричное исчисление, приближенные вычисления и методы аппроксимации функций), то в последнее время появились пособия, в названия которых введено понятие ”*дискретная математика*” [8...10]. Наиболее остро недостаток математической подготовки ощущается при изучении теоретических вопросов специальных дисциплин (и, в первую очередь, теории электрической связи).

Задача теории электрической связи” (ТЭС) – вооружить будущих специалистов знаниями о перспективных методах передачи информации в цифровых телекоммуникационных системах, сформировать теоретическую базу для усвоения последующих специальных дисциплин. *Теория помехоустойчивого кодирования* [11] посвящена синтезу структуры корректирующих кодов, позволяющих обнаруживать и исправлять ошибки передачи информации. Завершающим разделом дисциплины ТЭС является *теория эффективности систем передачи информации* [12] (анализ эффективности различных методов передачи, как степени использования ресурсов канала связи, расходуемых на единицу передаваемой информации).

Дискретная математика (ДМ) [13] – собирательный термин ряда разделов математики, которые изучают свойства дискретных структур, возникающих как внутри математики, так и в ее приложениях. К числу таких структур могут быть отнесены: *конечные группы, конечные графы, конечные геометрии, конечные автоматы* и др. Часть ДМ, изучающая их, часто называется *конечной математикой*. В отличие от ДМ классическая математика, в основном, занимается изучением свойств объектов непрерывного характера. Использование классической математики или ДМ, как аппаратов исследования, связано с тем, какая модель исследуемого явления рассматривается: дискретная или непрерывная. Само *деление* математики на классическую и дискретную в значительной мере *условно,* поскольку, с одной стороны, происходит активная циркуляция идей и методов между ними, а, с другой стороны, часто возникает необходимость исследования моделей, обладающих как дискретными, так и непрерывными свойствами одновременно. Знания как дискретной, так и классической математики необходимы именно специалистам цифровой связи, в которой информация представлена дискретными моделями и обрабатывается дискретными методами, и, в то же время, дискретные сигналы передаются по аналоговым линиям связи, которые описываются непрерывными моделями. В теории электрической связи широко используются результаты *теории кодирования*. Вместе с тем, в

соответствующих руководствах по теории связи, посвященных изложению основ теории кодирования, необходимые сведения по дискретной математике приводятся в *сокращенном, упрощенном виде,* а изложение теории дискретных сигналов ведется *на описательном уровне*, что не позволяет изучать свойства сигналов с учетом перспектив, вытекающих из свойств сигналов, как дискретных объектов.

Учитывая это, автором была предпринята попытка подготовки и издания учебного пособия [14], которое используется аспирантами и магистрантами ОНАС. Следует отметить, что в имеющихся руководствах по дискретной математике [8…10] отсутствуют *наглядные примеры* решения достаточно сложных и актуальных задач теории связи, которые способны привлечь внимание специалистов по теории связи, аспирантов и магистрантов и *убедить* их *в «полезности»* применения адекватного таким задачам математического аппарата. Автору пособия в последнее время удалось такие примеры разработать. Это и определяет стиль пособия, в котором излагается необходимый теоретический материал и примеры его применения в решении актуальных задач теории связи. Необходимо отметить, что предлагаемый теоретический материал по методам дискретной математики не претендует на полноту и глубину изложения, но приводится лишь в той тематике и в том объеме, которые необходимы для решения ряда актуальных задач теории связи. Для изложения выбран стиль, принятый в последнее время в популярных руководствах [10] и называемый, как «*математика для инженера».* Наряду с основными положениями теории дан ряд иллюстративных примеров, призванных облегчить усвоение материала. Сделано это умышленно, с целью привлечь внимание читателей, не имеющих университетского математического образования, к этой перспективной и не очень простой части современной математики (номера разделов с такими примерами отмечены буквой «П»). Такой стиль изложения существенно облегчит, как надеется автор, преподавателям *введение материалов пособия* в студенческий курс теории связи в инженерном вузе. Более подробную информацию по методам дискретной математики читатель может найти в руководствах, перечисленных в списке литературы. Пособие предназначено для преподавателей (в первую очередь, молодых преподавателей), стажеров, аспирантов и магистрантов. С этой целью разработан перечень рекомендуемых тем научных исследований в сфере теории цифровой связи, которые могут служить «*точками роста»* диссертаций и магистерских квалификационных работ, обозначены индексами «Д» и «М» с соответствующими номерами и помещены в Приложении. С целью расширения кругозора читателей в пособие включены обзоры по перспективным методам передачи информации в телекоммуникационных системах, составленные на основе публикаций в зарубежной печати. Автор признателен заведующему кафедрой высшей математики академии доценту Буслаеву А. Г., сделавшему ряд замечаний по тексту рукописи и проректору академии по учебной работе профессору Захарченко Н.В. за неизменную поддержку этой работы.

1. Множества

Понятие множествапринадлежит к числу простейших математических понятий. Оно не определяется, но может быть пояснено при помощи примеров.

Множество – совокупность элементов, обладающих общим для их всех характеристическим свойством. Например, множество всех действительных чисел, обозначаемое символом ***R.*** Совокупность всех комплексных чисел образует множество, обозначаемое символом ***C.*** Множеством также является совокупность всех решений уравнения $\sin(x)=1$. Множество ***A*** называется *подмножеством* множества ***B***, если всякий элемент из ***A*** является элементом из ***B***. Такая принадлежность обозначается знаком включения $A \subseteq B$.

При этом говорят, что ***B*** содержит или покрывает ***A.*** Множества ***A*** и ***B*** *равны*, если их элементы совпадают, т.е. если выполняются условия

$$A \subseteq B \text{ и } B \subseteq A.$$

Множества могут быть *конечными (*т. е. состоящими из конечного числа элементов) и *бесконечными.* Число элементов в конечном множестве *M* называется *мощностью множества.*

Множество мощности 0 не содержит элементов и называется *пустым* множеством. Понятие пустого множества введено в математике для удобства и единообразия языка.

Множество может быть *задано:*

– перечислением (т.е. списком своих элементов);

– порождающей процедурой;

–описанием характеристических свойств, которыми должны обладать элементы множества.

К примеру, множество четных чисел содержит элементы, кратные числу 2. Порождающая процедура описывает способ получения элементов нового множества из элементов ранее известного множества. Скажем, множество четных чисел можно получить из элементов множества целых чисел путем умножения каждого из них на 2.

В теории рассматриваются следующие *операции* над множествами:

$A \cup B$ *Объединением множеств* ***A*** и ***B*** называется множество, которое состоит из тех и только тех элементов, которые принадлежат хотя бы одному из множеств ***A***, ***B***. Символически объединение обозначается так:

$$A \cup B$$

К примеру, если заданы множества четных и нечетных целых чисел, то полное множество целых чисел является их объединением.

Пересечением множеств ***A*** и ***B*** называется множество, состоящее из тех и только тех элементов, которые принадлежат и ***A*** и ***B***. Символически пересечение обозначается так:

$$A \cap B$$

Пространством называют множество, между элементами которого аксиоматически установлены некоторые *отношения.* Примеры таких множеств (группы, кольца, поля) рассмотрены в следующем разделе.

2. Общая алгебра

Современная *алгебра,* понимаемая как учение об операциях над любыми математическими объектами, является одним из разделов математики, формирующих общие понятия и методы для всей математики. Свойства операций над математическими объектами в разных ситуациях иногда оказываются одинаковыми, несмотря на различие объектов. Отвлекаясь от природы объектов, но, фиксируя определенные свойства операций над ними, приходят к понятию *множества, наделенного алгебраической структурой*, или *универсальной алгебры.* Исследования различных сложившихся типов универсальных алгебр, а также исследования общих свойств универсальных алгебр на теоретико-множественной аксиоматической основе, составляют большое направление в современной алгебре, называемое *общей алгеброй.*

2.1. Группы

2.1.1. Аксиомы групп

Алгебраическая группа – одна из *важнейших* структур дискретной математики.

Определение 2. 1. *Группа G* – совокупность элементов любой природы, для которых определена некоторая операция и справедливы аксиомы ***G*1…*G*4**.

Порядок группы m – количество элементов в группе (далее $G(m)$ – группа порядка m). К примеру, обозначим элементы групп символами *a, b* и *c.*

Операция – однозначная функция двух переменных. Операцию иногда обозначают произвольным символом *(звездочка). К примеру, если символ операции *, то $a*b=c$ есть *двухместная операция*. Если под операцией в группе подразумевают операцию сложения (символ ”+”), то $a+b=c$, и группу с операцией сложения называют *аддитивной группой.* Группу с операцией умножения (т.е. $a \bullet b=c$) называют *мультипликативной группой.* Далее рассматриваются аддитивные группы со следующими аксиомами:

***G*1** *(Замкнутость).* Сложение любых элементов *a* и *b* аддитивной группы *G* дает третий элемент *c*, который принадлежит этой же группе, т.е. $a+b=c \subset G$.

Например, совокупность целых чисел с операцией обычного арифметического сложения удовлетворяет аксиоме замкнутости, так как из школьного курса арифметики известно, что сумма двух целых чисел дает только целое число.

***G*2** *(Ассоциативность).* Для любых элементов *a, b, c* группы *G* справедливо равенство $(a+b)+c=a+(b+c)$.

Свойство ассоциативности известно из школьного курса арифметики, в котором круглые скобки определяют порядок выполнения операций.

***G*3** *(Единичный элемент).* В группе существует такой единичный элемент (иногда называемый *нейтральным элементом)* что выполняются условия:

–в *аддитивной группе* существует нейтральный элемент *0*, причем, для любого элемента *a*: $a+0=a$;

–в *мультипликативной группе* существует нейтральный элемент *1*, причем, $a \bullet 1=a$.

***G*4** *(Обратный элемент).* Каждый элемент группы обладает обратным элементом:

– в аддитивной группе обратный элемент обозначается как «– *a*», причем, $a+(-a)=0$;

– в мультипликативной группе обратный элемент обозначается как(a^{-1}), причем, $a \bullet (a^{-1})=1$.

***G*5** (*Коммутативность).* В группе выполняются условия коммутативности:

– по сложению:$a+b=b+a$;

– по умножению: $a \bullet b=b \bullet a$.

Условие коммутативности известно из школьных правил арифметики («от перестановки мест слагаемых сумма не меняется»). Группы, удовлетворяющие условиям коммутативности, называются *коммутативными группами* или *Абелевыми группами.* Примерами групп могут служить:

–Множество целых чисел (ноль, положительные и отрицательные числа) с операцией арифметического сложения. *Нейтральным элементом* здесь является символ 0. Каждому положительному числу *a* соответствует *обратный элемент*, обозначаемый как(*–a),* так что $a+(-a)=0$;

–Множество положительных рациональных чисел с операцией арифметического умножения. *Нейтральным элементом* здесь является символ 1**.** Каждому положительному числу *a* соответствует обратный элемент(a^{-1}), так что выполняется равенство $a \bullet (a^{-1})=1$. Рассмотрим несколько примеров групп, представляющих интерес для теории кодирования.

П.2.1.2. Правила сложения по модулю 2

В такой группе *G*(2) всего два элемента(m=2). Обозначим их символами *a* и *b* . Для удовлетворения условий аксиомы замкнутости ***G*1** должны выполняться равенства:

(*i*) $a+a=?$;
(ii) $a+b=?$;
(iii) $b+b=?$,

причем, на месте вопроса после знака равенства должен находиться один из элементов группы *G* (2). По аксиоме ***G*3** в данной группе должен содержаться элемент *0*.

Пусть $a=0$ (т.е. элемент *a* играет роль нейтрального элемента в аддитивной группе). Если это так (a=0), то равенства {(*i),(ii)*} будут:

(i) $a+0=a$**,**
(ii) $0+b=b$**.**

Предположим, что третье равенство (*iii*) имеет вид $b+b=a=0$**.** В этом случае получаем набор равенств, не противоречащих аксиомам ***G*1**…***G*5**:

$$\begin{gathered} a+a=0; \\ a+b=b; \\ b+b=0, \end{gathered} \qquad (2.1)$$

где $a=0$, причем обратные элементы $(-a)=a=0$ и $(-b)=b$. Таким образом, аддитивная группа порядка $m = 2$ определена.

На основе изложенного выше нетрудно сформулировать *правила сложения по модулю 2,* которые широко используют в теории кодирования и цифровой технике.

Рассмотрим группу G (2) порядка 2, причем, пусть $a=0$, $b=1$, где 0 и *1*– символы двоичного кода, тогда из набора равенств (2.1) следует:

$$\begin{gathered} 0+0=0, \\ 0+1=1, \\ 1+1=0. \end{gathered}$$

Обозначив символом $\oplus$ операцию *сложения по модулю 2* , получаем:

$$\begin{gathered} 1\oplus1=0, \\ 1\oplus0=1, \\ 0\oplus0=0. \end{gathered} \qquad (2.2)$$

Сложение по правилам *(*2.2*)* в теории кодов используют для вычисления *расстояния* по Хеммингу(*Hamming)* d_H двух кодовых комбинаций.

Определение 2.2. *Расстояние по Хеммингу* d_H двоичных кодовых комбинаций $\overline{U}$ *и* $\overline{V}$ равно числу единиц в результирующей комбинации, определенной при *поразрядном* их *сложении по правилам сложения по модулю 2.*

К примеру:

$$\begin{gathered} \overline{U}=1\ 0\ 1\ 1\ 0\ 1 \\ \overline{V}=1\ 1\ 0\ 0\ 1\ 0 \\ \hline (\overline{U} \oplus \overline{V})=0\ 1\ 1\ 1\ 1\ 1 \Rightarrow d_H=5. \end{gathered} \qquad (2.3)$$

Правила сложения (2.2) широко используют в цифровой технике, поскольку они позволяют установить *совпадение* (либо *несовпадение*) двоичных символов 0 и 1. К примеру:

– сложение *совпадающих* символов $0\oplus0=0$ и $1\oplus1=0$ дает в результате 0;

– сложение *различных* символов $0\oplus1=1$ и $1\oplus0=1$ дает в результате 1.

Пусть аддитивная группа $G(4)$ порядка $m=4$ содержит следующие элементы$\{0,1,2,3\}$, причем, элемент 0 включен в состав группы в соответствии с аксиомой ***G*3.** Требованиям условий аксиомы замкнутости ***G*1** удовлетворяет следующий набор непротиворечивых равенств:

$$0+0=0,\ 0+1=1,\ 0+2=2,\ 0+3=3,\ 1+1=2,$$
$$1+3=0,\ 2+2=0,\ 2+3=1,\ 0+0=0,\ 3+3=2.$$

Обратные элементы определяются набором равенств:

$$0+0=0,\ 1+3=0,\ 2+2=0,\ 3+1=0.$$

На основе изложенного можно составить *правила сложения по модулю 4,* которые приведены ниже в табл.2.1. В левом вертикальном столбце и верхней горизонтальной строке таблицы указаны слагаемые, а в ячейках даны результаты сложения.

Таблица 2.1 – Правила сложения по модулю 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

По аналогии с изложенным выше нетрудно составить *правила сложения по модулю 8*, справедливые в аддитивной группе целых чисел $G(8)$ порядка $m=8$ с операцией сложения, представленной табл.2.2.

Таблица 2.2 – Правила сложения по модулю 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

2.1.3. Подгруппа. Композиционный ряд

В теории групп важную роль играет понятие *подгруппы.*

Определение 2.3. *Подгруппа H* группы *G* – некоторое подмножество элементов группы *G*, удовлетворяющее аксиомам ***G*1**…***G*4**.

Т. е., *всякая подгруппа есть группа.*

Говорят, что *подгруппа H вложена в группу G* (обозначается, как $H \subset G$).

Здесь:$\subset$–знак включения. В свою очередь, подгруппа $H_к$ также может содержать подгруппу $H_{к-1}$ и т.д., т.е. подгруппа $H_{к-1}$ может содержать подгруппу $H_{к-}$

$_2 \subset H_{к\text{-}1}$. Простейшая подгруппа $H_0(1)$ порядка m=1 содержит всего один элемент 0. Вложенные подгруппы образуют *композиционный ряд* группы *G:*

$$H_o \subset H_1 \subset ... H_{k\text{-}1} \subset H_k \subset G \ . \qquad (2.4)$$

Композиционный ряд (2.4) задает структуру группы G и часто используется для синтеза сложных групп более высоких порядков. Группы, не содержащие собственных нормальных подгрупп, называют *простыми группами.* Простые группы являются своеобразными «*кирпичиками*», из которых конструируют группы более сложной структуры.

2.1.4. Разложение группы по подгруппе

Все элементы группы могут быть разбиты на *непересекающиеся* совокупности, называемые *смежными классами*. Подгруппа $H \subset G$ используется для *разложения группы G на смежные классы.* Подгруппа H и смежные классы C совместно с композиционным рядом формируют структуру группы, охватывая в совокупности все элементы группы. Для формирования каждого смежного класса используется *образующий смежного класса h* (или *лидер смежного класса).*

Определение 2.4. *Образующий смежного класса* – элемент группы G, *не входящий в состав подгруппы* $H \subset G$.

Тогда *разложение группы G по подгруппе H* (т. е**.** формирование смежных классов, входящих в состав группы G**,** при котором *подгруппа H является* своеобразным «*штампом*» и, в силу этого, часто задает структурные свойства классов) определяется следующим правилом:

Определение 2.5. Смежный класс *Ch* образован совокупностью элементов, каждый из которых равен сумме (для аддитивной группы) образующего h и каждого элемента подгруппы *H;*

К примеру, рассмотрим аддитивную группу G**,** составленную из совокупности целых положительных и отрицательных чисел (включая 0):

G={...,–12,–11,–10,–9,–8,–7,–6,–5,–4,–3,–2, –1,0,1,2,3,4,5,6,7,8,9,10,11,12,…},

которая состоит из совокупностей четных и нечетных чисел(0– четное).

В группу *G вложена* подгруппа *H,* составленная из четных чисел:

H={...–12,–10,–8,–6,–4,–2,0,2,4,6,8,10,12,…}.

Всем аксиомам группы эта совокупность с операцией арифметического сложения удовлетворяет:

– З*амкнутость*: сумма любых четных чисел есть число четное;

– *Нейтральный элемент:* число 0;

– *Обратный элемент*: каждому числу с произвольным знаком соответствует обратный элемент (такое же число с противоположным знаком).

Выберем в качестве *образующего смежного класса* нечетное число h=1, сложение которого с любым четным числом из подгруппы четных чисел H дает нечетное число, входящее в состав смежного класса нечетных чисел:

C={...,–11,–9,–7,–5,–3,–1,1,3,5,7,9,11,…}.

П.2.1.5. Группы в теории корректирующих кодов

Понятия *группы, подгруппы и смежных классов* играют *фундаментальную роль* в теории линейных корректирующих кодов.

Корректирующие коды позволяют обнаруживать и исправлять ошибки, возникающие в системах передачи и хранения информации.

Процедуру разложения группы на смежные классы по подгруппе используем для пояснения принципа построения кодов, называемых в теории связи *групповыми корректирующими кодами.*

Рассмотрим двоичный трехзначный код, кодовые комбинации которого представлены в левом столбце табл. 2.3. Восемь комбинаций этого кода образуют алгебраическую группу $G(8)$. В качестве *групповой операции* определим поразрядное сложение комбинаций по правилам сложения по модулю 2. Складывая коды различных комбинаций из столбца $G(8)$, можно убедиться в выполнении условий аксиомы ***G.1.*** Нулевым элементом группы $G(8)$ является комбинация (0 0 0), причем каждая комбинация из $G(8)$ имеет свою обратную комбинацию (к примеру, комбинации (0 1 1) обратна комбинация (0 1 1), т.е. комбинация (0 1 1) обратна сама себе). Из состава комбинаций, входящих в группу $G(8)$ выберем комбинации, содержащие *четное число единиц* (которые называют«*разрешенными*»), и образуем из них подгруппу $H(4)$ (*разрешенные комбинации* используются для передачи по каналу). В канале связи происходят *ошибки*. Если ошибка происходит в первом символе, говорят, что действует *вектор ошибки* (1 0 0). Такая ошибка называется *однократной*, т.к. она поражает один символ. В табл. 2.3 показаны три возможные варианта однократной ошибки: (1 0 0), (0 1 0) и (0 0 1), поражающих первый, второй и третий символы, соответственно.

Группа $G(8)$ разложена по подгруппе разрешенных кодовых комбинаций $H(4)$ на смежные классы $C_1(4)$, $C_2(4)$ и $C_3(4)$, причем, образующим каждого класса являются векторы однократных ошибок. Смежные классы в целом охватывают все возможные варианты ошибочных комбинаций с однократной ошибкой, что гарантирует возможность обнаружения однократных ошибок с использованием процедуры определения четности (либо нечетности) числа единиц в полученной из канала кодовой комбинации (что и определяет наименование этого кода).

2.1.6. Изоморфизм групп

Понятие *изоморфизм* является важнейшим понятием современной математики, возникшим сначала в пределах алгебры в применении к таким алгебраическим структурам, как группы, кольца, поля и т.п.

Пусть заданы две аддитивные группы $G_a=\{0,a,b,\ldots c\}$ и $G_A=\{A,B,\ldots C\}$.

Определение 2.6. ГруппыG_a и G_A *изоморфны,* если каждому $x \epsilon G_a$ соответствует $X \epsilon G_A$ и каждой сумме $(x+y)$ $(x,y \epsilon G_a)$ соответствует сумма $(X+Y)$ $(X,Y \epsilon G_A)$. Фактически, изоморфизм есть форма «*эквивалентности*» структур изоморфных групп.

2.1.7. Циклические группы

Определение 2.7. Циклическая группа порождена степенями одного «*образующего элемента»* (обозначаемого, например, как α). Т.е. такая группа содержит элементы $\{\alpha^0,\alpha^1,\alpha^2,\alpha^3,\alpha^4,..\}$. Показатели степеней образующего элемента есть *числа натурального ряда целых чисел.* Здесь элемент $\alpha^0=1$ играет роль *единичного элемента мультипликативной группы* (Аксиома **G3**).

Соответственно, аддитивная циклическая группа $G_{ац}$ содержит элементы $\{0,\alpha,2\alpha,3\alpha,4\alpha,\ldots n\alpha..\}$.

Рассмотрим пример мультипликативной циклической группы с образующим элементом в виде унитарной матрицы

$$\Theta=\begin{bmatrix} Cos(2\pi/M) & Sin(2\pi/M) \\ -Sin(2\pi/M) & Cos(2\pi/M) \end{bmatrix}, \qquad (2.5)$$

где: M – целое.

Мультипликативная Абелева циклическая группа порядка (M+1) в соответствии с Определением 2.7 содержит элементы:

$$G_{цу}(M)=\{\Theta^0,\Theta^1,\Theta^2,..,\Theta^M\}, \qquad (2.6)$$

с операцией умножения матриц.

Учтем, что возведение матрицы (2.5) в целую степень k дает:

$$\Theta^k=\begin{bmatrix} Cos(2\pi k/M) & Sin(2\pi k/M) \\ -Sin(2\pi k/M) & Cos(2\pi k/M) \end{bmatrix}, \qquad (2.7)$$

Таблица 2.3 – Групповая структура кода «с четным числом единиц»

Группа $G(8)$	Смежные классы			
	подгруппа $H(4)$ (разрешенные кодовые комбинации)	$C_1(4)$ образующий класса (вектор ошибки) 1 0 0	$C_2(4)$ образующий класса (вектор ошибки) 0 1 0	$C_3(4)$ Образующий класса (вектор ошибки) 0 0 1
0 0 0	0 0 0	1 0 0	0 1 0	0 0 1
0 0 1				
0 1 0				
0 1 1	0 1 1	1 1 1	0 0 1	0 1 0
1 0 0				
1 0 1	1 0 1	0 0 1	1 1 1	1 0 0
1 1 0	1 1 0	0 1 0	1 0 0	1 1 1
1 1 1				

Анализ четности числа единиц		число единиц ***нечетное***	число единиц ***нечетное***	число единиц ***нечетное***
Ре-зультат		ошибка ***обнаружена***	ошибка ***обнаружена***	ошибка ***обнаружена***

Если $\boldsymbol{S}_0=(s_0, 0)$ – вектор сигнала в двумерном пространстве, то умножение этого вектора на унитарную матрицу (2.5) дает результат $\boldsymbol{S}_0\boldsymbol{\Theta}=(S_0 Cos 2\pi/M),0)$, т. е. модуль вектора $\boldsymbol{S}_0$ остается неизменным, а угол по отношению к горизонтальной оси изменяется на величину $(2\pi/M)$. Можно сказать, что умножение исходного вектора на унитарную матрицу $\boldsymbol{\Theta}$ приводит к *пространственному повороту* на угол $(2\pi/M)$, как показано на рис.2.1.

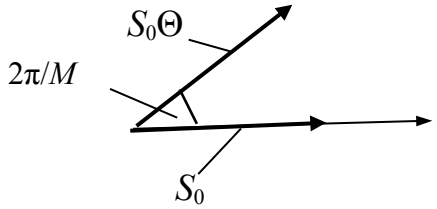


Рисунок 2.1 – Иллюстрация действия матрицы поворота вектора S_0 на угол $2\pi/M$

2.2. Кольца

2.2.1. Аксиомы колец

Определение 2.8. Кольцо **R** – множество элементов, на котором определены две операции: сложение(+) и умножение(•) и справедливы аксиомы:

***R*1.** Множество *R* является аддитивной Абелевой группой.

***R*2.** *(Замкнутость по умножению).* Для любых двух элементов кольца *a* и *b* определено произведение $a•b=c$, где $c \epsilon \boldsymbol{R}$.

R3(*Ассоциативность по умножению*).Для любых элементов кольца *a, b* и *c* справедливо $(a•b)•c=a•(b•c)$.

R4. (*Дистрибутивность*) Для любых элементов кольца *a, b* и *c* справедливо $(a+b)\ •c=a•c+b•c$.

R*5.** *(Единичный элемент по умножению).** В кольце имеется единичный элемент по умножению, такой, что: $a•1=a$.

Следует отметить, что в *кольце обратный элемент по умножению не определен*. Это означает, что *в кольце не определена операция деления* как операция, обратная умножению.

2.3.Поля

2.3.1. Аксиомы полей

F1. *Полем F* называется *коммутативное кольцо с единичным элементом по умножению*, в котором каждый ненулевой элемент имеет обратный элемент по умножению.

Таким образом, в поле *F*:

– определены *две операции* (сложение и умножение);

– имеются *нейтральные элементы:* по сложению 0, и по умножению 1;

– каждому элементу поля *a* определены *обратные элементы*:
по сложению (*–a),* и по умножению (a^{-1})*;*

– выполняются требования *аксиом ассоциативности и дистрибутивности.*

Перечисленный обширный набор свойств элементов поля и операций над ними обуславливает широкое использование теории алгебраических полей в теориях кодирования и обработки цифровых сигналов. В противоположность этому *коды с элементами из алгебраических колец встречаются значительно реже.*

П.2.3.2. Поле *F*(3) из трех элементов

Особенности алгебраического поля рассмотрим на примере поля из трех элементов (*m*=3). В таком поле *F*(3) определены *две операции* (сложение «+» и умножение «(•)») и *нейтральные элементы*: по сложению 0 и по умножению 1. Полагая, что третьим элементом поля *F*(3) будет произвольный элемент *a*, полный набор элементов поля *F*(3) будет {*0,1*, *a}*. Тогда правила сложения в таком поле определяются приведенной ниже табл. 2.4.

Таблица 2.4– Правила сложения в поле *F*(3)

+	0	1	*a*
0	0	1	*a*
1	1	a	0
a	*a*	0	1

Откуда обратные элементы по сложению определяются следующим образом: *(–a*)=1, (–1)=*a*.

2.3.3. Классификация полей

В теории связи (в частности, в теории кодирования) и в теории методов цифровой обработки сигналов математический объект *алгебраическое поле* широко используется, поскольку *допускает весь набор операций,* необходимых для обработки сигналов:

– *сложение* (соответственно, *вычитание*),

– *умножение* (соответственно, *деление* символов).

Если *порядок поля q* задан, то все *поля F(q) изоморфны*, т. е. существует *одно абстрактное поле*, а встречающиеся варианты полей из тех или иных символов называют *представлениями полей.*

Ниже приведены *сведения о существовании абстрактных полей:*

1. Если q – простое число, то существует поле $F(q)$ для любого q;
2. Если p – простое число, то существует поле $F(p)$ с операциями сложения и умножения по модулю p;
3. Если $q=p^m$ (p – простое число, m – любое целое число), то существует поле $F(p^m)$. В этом случае поле $F(p^m)$ называют *расширением поля* $F(p)$. *Число элементов поля* $F(m)$ есть $q=p^m$.

Такое поле обозначается как $GF(p^m)$ и носит название *поля Галуа* (в честь французского математика – основоположника теории групп Э.Галуа). При этом число p называется *характеристикой поля Галуа.*

3. Целые числа. Теория делимости

Теория чисел – один из старейших разделов математики, который занимается изучением свойств целых чисел. *Целыми* называют не только числа натурального ряда 1, 2, 3,...(положительные целые), но также нуль и отрицательные целые:–1, –2, –3, ... и т.д. Таким образом, расположив целые числа в возрастающем порядке, получим ряд, в котором разность между большим и меньшим соседними членами везде равна единице.

Далее, при изложении теоретического материала буквами будут обозначены только целые числа.

Сумма $(a+b)$, разность $(a–b)$ и произведение ab двух целых a и b являются *также целыми*. Но частное a/b от деления a на b (если b не равно нулю) может быть *как целым, так и не целым*. В случае, когда частное a/b от деления a на b есть целое q, получаем $a=bq$, т. е. a представляется произведением b *на целое.* В таком случае говорят, что *a делится на b* или, что *b делит a.* При этом a называем *кратным* числа b, а *b – делителем* числа a.

Справедливы следующие утверждения:

Утверждение 3.1. Если a кратно m, m кратно b, то a кратно b.

Действительно, из $a=ma_1$, $m=bm_1$, следует $a=ba_1m_1$. Таким образом, a представляется произведением b на целое число a_1m_1 и тем самым делится на b.

Утверждение 3.2. Если в равенстве вида $(к+l+…+n=p+q+s)$ относительно всех членов (кроме какого-либо одного) известно, что они кратны b, то и этот один член кратен b.

Действительно, пусть таким одним членом будет $к$. Имеем

$$l=bl_1,\ldots,\ n=bn_1,\ p=bp_1,\ q=bq_1\ \ldots,\ s=bs_1;$$

$$к=p+q+\ldots–s–n=b(p_1+q_1+\ldots+s_1–l_1–\ldots–n_1).$$

Таким образом, $к$ представляется произведением b на целое число $(p_1 + q_1 + +s_1–l_1 – …–n_1)$. и тем самым делится на b.

Утверждение 3.3 *(теорема о делении с остатком).* Всякое целое a представляется *единственным способом* помощью положительного целого b равенством вида

$$a=bq+r,\ 0\le r<b. \qquad (3.1)$$

Действительно, одно представление числа a равенством такого вида получим, взяв bq равным наибольшему кратному числа b, не превосходящему a. Допустив же существование представления числа a еще одним равенством того же вида: $a=bq_1+r_1$, $0\le r_1<b$ и, вычитая почленно это последнее равенство из предыдущего, получим $0=b(q–q_1)+(r–r_1)$.

Отсюда убедимся, что разность $(r–r_1)$ кратна b. С другой стороны, легко видеть, что та же разность, как разность двух неотрицательных чисел, меньших b, сама будет численно меньше b, но числом же, кратным b и численно меньшим b, является лишь число 0. Таким образом, второе представление числа a тождественно первому и теорема доказана.

Число q называется *неполным частным,* а число r – *остатком* от деления a *на* b. Очевидно, что при r=0 понятие «*неполное частное*» и «*частное*» совпадают. В дальнейшем будем рассматривать лишь положительные делители чисел. Всякое целое, делящее одновременно целые $a, b,\ldots,l,$ называется их *общим делителем.* Наибольший из общих делителей называется *общим наибольшим делителем* и обозначается сокращенно ОНД. Если ОНД $(a,b,\ldots,l)$=1, то $a,b,\ldots,l$ называются *взаимно простыми.*

Утверждение 3.4. Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного $b,$ и, в частности,

ОНД$(a, b)=b$.

Для отыскания общего наибольшего делителя применяется ***алгоритм Евклида.*** Он состоит в нижеследующем:

Пусть a и b – положительные целые и $a>b$.

Согласно(3.1) находим ряд равенств:

$$\begin{aligned} a&=bq_1+r_2, \quad 0<r_2<b,\\ b&=r_2q_2+r_3, \ 0<r_3<r_2,\\ r_2&=r_3q_3+r_4, \quad 0<r_4<r_3,\\ &\ldots\ldots\ldots\ldots\\ r_{n-2}&=r_{n-1}q_{n-1}+r_n, \ 0<r_n<r_{n-1},\\ r_{n-1}&=r_nq, \end{aligned} \qquad (3.2)$$

заканчивающийся, когда получается некоторое r_{n+1}=0. Последнее неизбежно, так как ряд b, r_2, r_3..., как ряд убывающих целых , не может содержать более чем b положительных.

Рассматривая равенства (3.2) и идя сверху вниз, убеждаемся, что общие делители чисел a и b одинаковы с общими делителями чисел b и r_2 и, далее, одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4, …, чисел r_{n-1} и r_n , и, наконец, с делителями одного числа r_n, являющегося последним не равным нулю остатком алгоритма Евклида.

4. Пространственные точечные решетки

В математике *решетка* – структура, частично упорядоченное множество. Примерами решеток могут быть:

– Множество всех подмножеств данного множества, упорядоченное по включению;

– Множество всех подпространств векторного пространства, упорядоченное по включению.

– Множество всех неотрицательных целых чисел, упорядоченных по делимости и др.

Понятие *пространственная точечная решетка* возникает в процессе решения *задач упаковки шаров* фиксированного радиуса в заданном объеме. Такие *задачи упаковки* возникают при транспортировке грузов, раскрое материалов, проектировании строительных конструкций шаровидной формы, причем, важным является показатель *плотности упаковки*. Проблему плотной упаковки

блестяще решают пчелы при строительстве сот. За ними интуитивно следуют домохозяйки при раскрое листа теста на вареники. В кристаллографии математический аппарат решеток занимает центральное место. Кроме того, решение задач оптимальных *процедур квантования и дискретизации* в цифровой связи базируется на результатах теории решеток. В теории сигналов и теории кодирования *решетчатые структуры* лежат в основе *синтеза оптимальных сигналов и кодов.*

4.1. Параметры сферических упаковок

Рассмотрим вектор в вещественном n-мерном пространстве $\boldsymbol{R}^n$:

$$\boldsymbol{x} = (\boldsymbol{x}_1 ... \boldsymbol{x}_n) \in \boldsymbol{R}_n , \tag{4.1}$$

с единичной нормой

$$\|x\| = x_1^2 + ... + x_n^2 = 1 \tag{4.2}$$

Теперь можно определить *сферический код* $\boldsymbol{C}_n$ размерности $\boldsymbol{n}$, объема M как множество M векторов вида (4.1) с максимальным скалярным произведением $\boldsymbol{s}$ таким, что:

$$\boldsymbol{x} \cdot \boldsymbol{y} \le \boldsymbol{s}$$

для всех

$$\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{C}_n, \boldsymbol{x} \ne \boldsymbol{y}$$

Проблема поиска наилучших сферических кодов имеет долгую историю и, в первую очередь, поиска лучших кодов для пространств размерности 2 и 3 (иными словами, на плоскости и в заданном объеме). Более подробные сведения по этому вопросу можно найти в фундаментальном руководстве[19].

Местоположение сфер сферического кода в пределах некоторого объема можно изменять, задавая координаты центров сфер вектором

$$\boldsymbol{u}=(u_1,u_2,\ldots,u_n). \tag{4.3}$$

Сфера радиуса ρ в $\boldsymbol{R}_n$ с центром (4.3) состоит из точек $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$, удовлетворяющих равенству:

$$(x_1-u_1)^2+(x_2-u_2)^2+\ldots.+(x_n-u_n)^2=\rho^2 \ . \tag{4.4}$$

Упаковку сфер в пространстве $\boldsymbol{R}_n$ можно *задавать,* указывая набор центров сфер и их радиус. Такая упаковка называется *решетчатой упаковкой*, поскольку она обладает следующими *свойствами*:

а) 0 является центром.

б) Если имеются сферы с центрами $\boldsymbol{u}$ и $\boldsymbol{v}$, то имеются также сферы с центрами $(\boldsymbol{u}+\boldsymbol{v})$ и $(\boldsymbol{u}-\boldsymbol{v})$.

в) Множество центров образует *аддитивную группу*;

г) Каждая решетка может быть задана порождающей матрицей размером $m \cdot n$ элементов:

$$G = \begin{vmatrix} g_1 \\ \cdot \\ \cdot \\ g_m \end{vmatrix} = \begin{vmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \cdot & \cdot & g_{m-1,n-1} & g_{m-1,n} \\ g_{m,1} & g_{n,2} & \cdot & g_{m,n} \end{vmatrix} \qquad (4.5)$$

Строки матрицы (4.5) должны удовлетворять *условию линейной независимости.*
Если $\boldsymbol{p}=(p_1, p_2, \ldots. p_{n-1}, p_n)$ – произвольный вектор с целыми координатами, то все векторы центров решетки определяются произведением матриц вида:

$$\Lambda_n = \boldsymbol{p} \cdot \boldsymbol{G} \qquad (4.6)$$

Иными словами, координаты центров решетки (т.е., собственно, решетка) определяются *линейной комбинацией строк* порождающей матрицы (4.5).
Перечислим параметры сферических упаковок:

Размерность n решетчатой упаковки Λ_n есть максимальное количество линейно независимых центров решетки Λ_n.

Плотность упаковки Δ (любой упаковки, в том числе и решетчатой) определяется *долей пространства* $\boldsymbol{R_n}$, занимаемая сферами упаковки.
Для решетчатой упаковки Λ_n сферами радиуса ρ и размерности решетки n плотность определяется формулой:

, $$\Delta = \frac{V_n \rho^n}{\det \Lambda_n} \quad , \qquad (4.7)$$

где объем сферы единичного радиуса в $\boldsymbol{n}$-мерном пространстве:

$$V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)} \quad , \qquad (4.8)$$

а det Λ_n есть *детерминант решетки* Λ_n, определяемый по матрице (4.5) стандартными методами матричного исчисления.

П.4.2. Примеры решеток

Приведем типичные примеры решеток.

Решетка D_4 плотнейшей паковки четырехмерного пространства $\boldsymbol{R_4}$ определяется порождающей матрицей

. $$\boldsymbol{G}_4 = \frac{1}{\sqrt{2}} \begin{vmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \quad . \qquad (4.9)$$

Такая решетка определяет центры 24 сфер с радиусом ρ= 1/2, упакованных в четырехмерном пространстве с максимальной плотностью $\Delta=\pi^2/16=0{,}61686$.

Плотнейшая решетка A_2 двумерного пространства определяется матрицей

$$\boldsymbol{G}_2 = \begin{vmatrix} 1 & 0 \\ -\frac{1}{2} & \sqrt{\frac{3}{2}} \end{vmatrix} \qquad (4.10)$$

с параметрами ρ=1/2, Δ=0,9069.

Подобные решетки использованы в монографии [3] для синтеза многопозиционных сигналов в двумерных и четырехмерных пространствах.

П.4.3. Сигналы КАМ-16 на базе двумерной решетки

В высокоэффективных телекоммуникационных системах используют *многопозиционные сигналы*. Часто используют ансамбль двумерных сигналов квадратурной амплитудной модуляции КАМ-16, который основан на базе *квадратной решетки двумерного пространства* и обеспечивает высокую плотность упаковки сигналов, простоту их формирования. При этом модулятор формирует сигналы, выбираемые из набора (*ансамбля),* содержащего *M* возможных вариантов сигналов. В этом случае возникает *задача согласования выхода двоичного источника со входом модулят*ора. Задачи согласования решаются с применением *модуляционных кодов.*

Общий принцип построения модуляционного кода состоит в следующем:

1.Передаваемая двоичная последовательность разбивается на блоки длиной $n=log_2M$ символов. Количество всех возможных вариантов таких двоичных блоков длины *n* должно быть равно объему ансамбля $M=2^n$.

2.Процедура модуляционного кодирования состоит в отождествлении блоков двоичных символов и сигналов ансамбля по правилу: каждому сигналу ансамбля ставится в соответствие двоичный блок. *Модуляционный код* есть таблица такого соответствия.

Выбор модуляционного кода зависит от конфигурации ансамбля сигналов и свойств помех, действующих в канале с многопозиционными сигналами.

При демодуляции многопозиционных сигналов на выходе канала с *гауссовскими* помехами наиболее вероятными являются ошибки «*переходов»* передаваемого сигнала в сигналы многопозиционного ансамбля, расположенные от него на *минимальном* расстоянии Евклида.

Ошибка декодирования будет минимальной, если наименьшим расстояниям по Евклиду между сигналами многопозиционного ансамбля будут соответствовать блоки модуляционного кода с наименьшим расстоянием Хэмминга. *Модуляционный код Грея* этим условиям удовлетворяет.

Модуляционный код Грея для сигналов КАМ-16 представлен на рис. 4.1. Сигнальные точки расположены в узлах двухмерной квадратной решетки и результирующий код Грея показан на этом же рисунке. Видно, что расстояния Хэмминга между двоичными комбинациями соседних сигнальных точек равны 1.

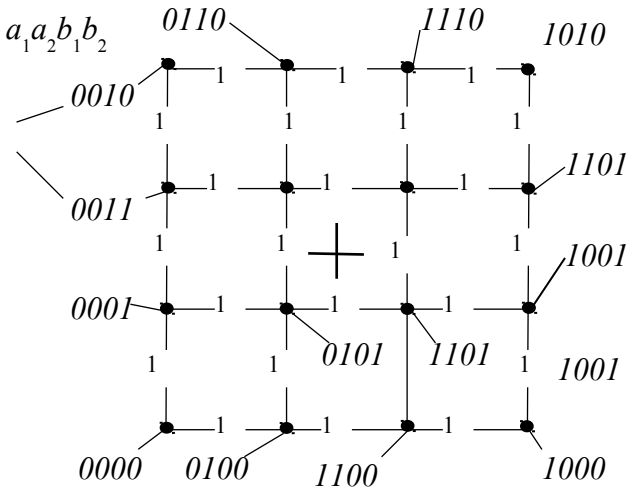


Рисунок 4.1– Модуляционный код Грея ансамбля КАМ-16

5. Алгебра степенных многочленов

В теории кодирования важную роль играют математические объекты – *степенные многочлены*. Далее рассматривается ***A(X)*** – множество степенных многочленов вида:

$$a(X)=a_0+a_1X+a_2X^2+\ldots\ldots a_iX^i\ldots+a_kX^k, i=0,1\ldots k, \qquad (5.1)$$

с коэффициентами a_i, выбираемыми из поля $F(m)$.

Если $a_k \neq 0$, то говорят, что многочлен $a(X)$ имеет *степень* k. (Обычно обозначают $k=deg\ a(X)$). Два многочлена $a(X)=\sum_{i=0}^{k} a_iX^i$ и $b(X)=\sum_{i=0}^{l} b_iX^i$ называются *равными*, если они имеют одну и ту же степень (т.е. $k=l$) и, кроме того, $a^i=b^i$ для всех $i=0\ldots k$. Многочлен, все коэффициенты которого равны 0, называется *нулевым многочленом* и обозначается как 0.

Пример 5.1. *Многочлены степени 2 и менее.* Перечислим все многочлены степени 2 и менее над полем Галуа $GF(2)$ характеристики 2. Результаты приведены в табл.5.1.

Таблица 5.1 – Многочлены степени 2 и менее над полем Галуа ***GF***(2)

Степень многочлена	Многочлен
2	$a_{111}(X)=1+X+X^2$
2	$a_{101}(X)=1+X^2$
2	$a_{011}(X)=X+X^2$
1	$a_{111}(X)=1+X$
1	$a_{110}(X)=X$
0	$a_{100}(X)=1$
Степень не определена	$a_{000}(X)=0$

Из этого примера следует, что число различных многочленов степеней k и меньше над полем порядка q равно $q^{(k+1)}$.

Определим ***операции сложения и умножения многочленов:***

5.1. Для любых двух многочленов $a(X)=\sum_{i=0}^{k} a_i X^i$ и $b(X)=\sum_{i=0}^{l} b_i X^i$ ***сложение*** определяется следующим равенством:

$$a(x)+b(x)=\sum_{i}(a_i+b_i)x^i. \qquad (5.2)$$

5.2. Для любых двух многочленов $a(X)=\sum_{i=0}^{k} a_i X^i$ и $b(X)=\sum_{i=0}^{l} b_i X^i$

умножение определяется следующим равенством:

$$a(X)\cdot b(X)=\sum_{i}(\sum_{j=0}^{i} a_i b_{i-j})X^i. \qquad (5.3)$$

Определив таким образом сложение и умножение в множестве степенных многочленов $F(X)$ вида (5.1) получаем *алгебраическое кольцо многочленов* со следующими свойствами:

1) $a(X)\cdot 0=0$ для любого $a(X)\subset A(X)$;
2) Если $a(X)\neq 0$ и $b(X)\neq 0$, то $a(X)\cdot b(X)\neq 0$;
3) $-[a(X)b(X)]=[-a(X)]b(X)=a(X)[-b(X)]$;
4) $[a(X)+b(X)]c(X)=a(X)c(X)+b(X)c(X)$.

Пример 5.2. *Сложение и умножение многочленов.*

Пусть заданы многочлены с коэффициентами из поля***GF***(2):

$$a(X)=X^3+X^4+X^6 \text{ и } b(X)=1+X^4 \qquad (5.4)$$

Определим их сумму по правилам (5.2), складывая коэффициенты при степенях X по правилам сложения по модулю 2:

$$a(X) = X^3+X^4+X^6;$$

$$b(X) = 1+X^4;$$

$$a(X)+b(X) = 1+X+X^6.$$

Для любых двух ненулевых многочленов $a(X) \in A(X)$ и $b(X) \in A(X)$ существуют, и ,притом , *единственные* многочлены *c(X), r(X)*$\in$ ***F(X)*** такие, что

$$(a(X)=c(X)g(X)+r(X),\ deg\ g(X)>\deg r(X). \qquad (5.5)$$

Здесь
a(X)– многочлен *делимого*;
g(X)– многочлен *делителя*;
c(X)– многочлен *частного*;
r(X)– многочлен *остатка*.

Равенство (5.5) используется для установления *свойств делимости* многочленов.

Пример 5.3. *Деление многочленов.*

Равенство (5.5) используем для иллюстрации практического правила деления многочленов.

Записав многочлены в более удобном виде (со старшими степенями переменной *X* слева):
делимое a(X)=$X^6+X^4+X^3$ и *делитель b(X)*=$X^{4+}1$, производим деление «у*голком*» по алгоритму Евклида:

$a(X)/b(X)\Rightarrow$	$X^6+X^4+X^3$ ← *Делимое*	$X^{4+}1$ ← *Делитель*
+		$X^{2+}1$ ← *Частное*
	X^6+X^2	
	$X^4+X^3+X^2$	
+	X^4+1	
	X^3+X^2+1	← *Остаток*

На основе процедуры деления можно записать равенство:
$(X^6+X^4+X^3)/(X^4+1)=(X^4+1)(X^2+1)+(X^3+X^2+1)$.

В теории циклических кодов широко используют *аналогию* между кодовыми комбинациями и набором коэффициентов при степенях переменной *X* многочленного представления кодовых комбинаций.

Пример 5.4. *Кодовые комбинации и многочлены*.

Пусть задана кодовая комбинация *m*-ичного кода с коэффициентами из поля *F*(*m*) $\boldsymbol{a}=(a_0a_1a_2\ldots\ldots a_i\ldots.a_k)$, $i=0,1\ldots k$,

Составим многочлен вида $\boldsymbol{a}(X)=a_0+a_1X+a_2X^2+\ldots\ldots a_iX^i\ldots+a_kX^k$, $i=0,1\ldots k$.

В случае двоичных кодов некоторые степени переменной *X* могут отсутствовать. К примеру, комбинации $\boldsymbol{a}$=(11001101) соответствует многочлен
$\boldsymbol{a}(X)=1+X+X^4+X^5+X^7$.

Отметим важное ***свойство многочленного представления кодовых комбинаций:***

Если задана комбинация $\boldsymbol{a}=(a_0a_1a_2\ldots\ldots a_i\ldots a_{n-1})$ и соответствующий ей многочлен $\boldsymbol{a}(X)=a_0+a_1X+a_2X^2\ldots+a_{n-1}X^{n-1}$, то справедливо следующее равенство:

$$[X^i\boldsymbol{a}(X)]/(X^n-1)=\boldsymbol{q}(X)+\boldsymbol{a}_i(X)/(X^n+1). \qquad (5.6)$$

Здесь $\boldsymbol{q}(X)$ – ч*астное*,

$\boldsymbol{a}_i(X)=a_iX^i+a_{1+i}X^{1+i}+a_{2+i}X^{2+i}\ldots+a_{n-1+i}X^{n-1+i}$ – *остаток* от деления многочлена $X^i\boldsymbol{a}(X)$ на многочлен (X^n+1). Сопоставляя (5.6) с (5.5), приходим к выводу, что многочлен (X^n-1) имет смысл ***модуля*** $M=(X^n+1)$, а формулу (5.6) можно представить следующим образом:

$$\boldsymbol{a}^{(t)}(X)=[X^t\boldsymbol{a}(X)]\,mod(X^4+1)=X^3+X^2+1. \qquad (5.7)$$

Пример 5.5. *Циклический сдвиг многочлена*.

Проверим справедливость равенства (5.7).

Пусть задан многочлен $\boldsymbol{a}(X)=1+X+X^3$. Ему соответствует двоичная комбинация $\boldsymbol{a}$ =(1101). Установим, что происходит сдвиг комбинации на t=3 символа. В соответствии с (5.7) определим делимое $X^t\mathbf{a}(X)=X^3(1+X+X^3)=X^3+X^4+X^6$, которое необходимо разделить на модуль(X^4+1). Процедура и результаты деления приведены в Примере *5.3*, на основании которых можно записать:

$$\boldsymbol{a}^{(t)}(X)=[X^t\boldsymbol{a}(X)]_{mod\,(X^4+1)}=X^3+X^2+1.$$

Этому остатку соответствует комбинация $\mathbf{a}^{(t)}$=(1011).

Сопоставляя исходную комбинацию $\boldsymbol{a}$ и результат деления на модуль:

$\boldsymbol{a}$=(1101), $\boldsymbol{a}^{(t)}$=(1011),

приходим к выводу, что произошел ***циклический сдвиг*** символов исходной двоичной комбинации на t=3 символа вправо.

Это *свойство многочленного представления кодовых комбинаций широко используется в теории циклических кодов.*

П.5.1. Многочлены в теории циклических кодов

Значительная часть используемых на практике блоковых кодов относится к классу *циклических кодов* (*ЦК*). Это обусловлено *упрощением процедур* кодирования и декодирования на основе использования *циклических свойств* кода.

Если $v=(v_0, v_1,\ldots v_{n-1})$ – разрешенная кодовая комбинация ЦК, то ее *циклический сдвиг* на произвольное число символов также является *разрешенной кодовой комбинацией*.

Например, слово $\boldsymbol{v}^{(1)}=(v_{n-1}, v_0, v_1, \ldots, v_{n-2})$ соответствует циклическому сдвигу комбинации $\boldsymbol{v}=(v_0, v_1,\ldots v_{n-1})$ на один символ вправо. При этом, в соответствии с *правилом циклической перестановки,* символы комбинации $\boldsymbol{v}$ смещаются на один символ вправо, а крайний правый символ v_{n-1} занимает место крайнего левого символа v_0. Свойства ЦК удобно изучать, представляя кодовые слова *в виде многочленов* по степеням формальной переменной X, коэффициенты которых есть символы кодовой комбинации $\boldsymbol{v}(X)=v_0+v_1X+v_2X^2+\ldots+v_{n-1}X^{n-1}$. Математические операции (сложение, умножение и деление многочленов) производят *по правилам алгебры многочленов*, изложенным выше. Если сложение и умножение многочленов производится *по модулю многочлена* (X^n-1), то все возможные многочлены степени $(n-1)$ и меньше образуют ***алгебраическое кольцо многочленов*** $\boldsymbol{R_n}$ со свойствами, изложенными выше в п. 2.2.

Для *построения циклического кода* в кольце $\boldsymbol{R_n}$ выбирают подмножество многочленов – *идеал I*. Многочлен минимальной степени $g(X)$ в этом подмно-

жестве *называется порождающим многочленом ЦК.* В качестве порождающих многочленов ЦК выбирают *неприводимые многочлены.*

Многочлен называется *неприводимым*, если он не может быть представлен в виде произведения других многочленов. Иными словами *неприводимый многочлен делится без остатка на единицу либо сам на себя*. В алгебре многочленов целой степени *неприводимые многочлены* играют такую же роль, какую *простые числа* играют в алгебре целых чисел. Порождающие многочлены коротких циклических кодов приведены в табл.5.2.

Таблица 5.2 – Порождающие многочлены коротких циклических кодов

Максимальная степень порождающего многочлена	Порождающий многочлен $g(X)$.		
3	X^3+X^2+1	X^3+X+1	
4	X^4+X+1	X^4+X^3+1	
5	X^5+X^2+1	X^5+X^3+1	$X^5+X^4+X^2+X+1$
6	X^6+X+1	X^6+X^5+1	$X^6+X^5+X^3+X^2+1$

Все многочлены *идеала I*, соответствующие разрешенным кодовым комбинациям ЦК, делятся на порождающий многочлен $g(X)$ без остатка, что позволяет формулировать *правило кодирования*.

Правило кодирования несистематического ЦК имеет вид:

$$v(X)=u(X)g(X). \qquad (5.8)$$

На практике часто используют *систематические* циклические коды.

Правило кодирования систематического циклического (n,k) ***кода*** имеет вид:

$$v(X)=u(X)X^{n-k}+r(X), \qquad (5.9)$$

где $r(X)$ – остаток от деления $u(X)X^{n-k}$ на $g(X)$.

Правило кодирования (5.9) может быть реализовано таким *алгоритмом* кодирования *систематическим циклическим кодом:*

1. К комбинации первичного кода $u(X)$ дописывается справа($n–k$) нулей, что эквивалентно умножению на X^{n-k}.

2.Произведение $u(X)X^{n-k}$ делится на порождающий многочлен $g(X)$, в результате деления определяется остаток $r(X)$.

3.Вычисленный остаток складывается со смещенной комбинацией $u(X)X^{n-k}$, в результате чего формируется ***разрешенная кодовая комбинация :***

$$v(X)=u(X)X^{n-k}+r(X). \qquad (5.10)$$

Пример 5.6 .*Формирование кодовой комбинации ЦК (7,4).*

Для заданной первичной кодовой комбинации u=1011 сформируем кодовую комбинацию циклического кода (7,4). Многочленное представление заданной комбинации будет $u(X)=(X^3+X^2+1)$.

У заданного ЦК параметры n=7, k=4, r=(n–k)=3. По табл. 5.2 выбираем, например, порождающий многочлен $g(X)=(X^3+X^2+1)$. Выполним математические операции в соответствии с алгоритмом (5.10):

1) $u(X)X^{(n-k)}=(X^3+X^2+1)X^3=X^6+X^4+X^3$;

2) $u(X)\,X^{(n-k)}/\,g(X)$ $= X^6+X^4+X^3$ | X^3+X^2+1

$\oplus$ $X^6+X^5+X^3$ | X^3+X^2

X^5+X^4

$\oplus$ $X^5+X^4+X^2$;

$r(X)=X^2$

3) $v(X)=u(X)X^{n-k}\oplus r(X)=X^6+X^4+X^3+X^2$.

Многочлену $v(X)=X^6+X^4+X^3+X^2$ соответствует комбинация двоичных символов $\boldsymbol{v}$= (1011100), в которой первые четыре символа являются информационными, а остальные – дополнительными.

Свойство делимости разрешенных кодовых комбинаций циклических кодов на порождающий многочлен широко используется для ***обнаружения ошибок*** в телекоммуникационных системах, в которых предусмотрено *исправление ошибок некодовыми методами* (*системы с обратной связью*, например).

Если $z(X)=v(X)+e(X)$ – принятая кодовая комбинация, содержащая многочлен ошибок $e(X)=e_0+e_1X+ \ldots +e_{n-1}X^{n-1}$, то в результате деления получаем:

$$z(X)/g(X)=q(X)+s(X); \qquad (5.11)$$

Здесь $q(X)$ – произвольный многочлен («целое»); $s(X)$ – *многочлен синдрома,* равный остатку от деления $z(X)$ на $g(X)$.

Он имеет степень не выше (n–k–1). *В* ***отсутствие ошибок s(X)=0.***

По виду синдрома можно также установить *местоположение* ошибок в принятой кодовой комбинации и использовать эту информацию для ***декодирования с исправлением ошибок.***

Пример 5.7*. Синдромное декодирование комбинаций циклического кода (7,4).*

Пусть задан ЦК с порождающим многочленом $g(X)=X^3+X^2+1$. Принятая из канала кодовая комбинация имеет вид z=1010101. Используя правило нахождения синдрома (5.11) при синдромном декодировании по виду синдрома можно установить местоположение ошибки (выполнить ***синдромное декодирование****).* Для этого необходимо составить ***таблицу синдромов*** и соответствующих им значений ошибок. Для составления такой таблицы необходимо воспользоваться равенством, вытекающим из (5.11) (при $q(x)=0$):

$$\boldsymbol{s}(X)= \boldsymbol{e}(X)/\boldsymbol{g}(X)\ . \qquad (5.12)$$

В табл. 5.3 представлены результаты вычислений по этой формуле многочленов синдрома $s(X)$ для различных многочленов ошибок. В целях наглядности значения синдромов представлены в виде двоичных комбинаций.

Таблица 5.3 – Соответствие между синдромами и многочленами ошибок

Многочлен ошибок $e(X)$	X^6	X^5	X^4	X^3	X^2	X	1
Многочлен синдрома $s(X)$	X^2+X	$X+1$	X^2+X+1	X^2+1	X^2	X	1
Комбинация синдрома s	110	011	111	101	100	010	001

Представим принятую комбинацию в виде многочлена $z(X)=X^6+X^4+X^2+1$. Выполним операцию деления $z(X)/g(X)$:

$$\begin{array}{l|l} X^6+X^4+X^2+1 & X^3+X+1 \\ \hline \oplus\ X^6+X^4+X^3 & X^3+1 \\ \hline X^3+X^2+1 & \end{array}$$

$$\begin{array}{r} \oplus\ X^3+X+1 \\ \hline \end{array}$$

Синдром $s(X)=X^2+X$

По табл. 5.3 находим, что такому синдрому соответствует многочлен ошибки $e(X)=X^6$. Исправление ошибки состоит в сложении принятой кодовой комбинации с многочленом ошибки:

$v(x)=z(X)+e(X)=X^6+X^4+X^2+1+X^6=X^4+X^2+1$, чему соответствует двоичная комбинация $\boldsymbol{v}$=0010101.

П.5.2. Многочленные представления в теории формирователей псевдослучайных последовательностей

В технике связи широко используются *псевдослучайные последовательности символов* (ПСП). Псевдослучайными их называют потому, что по своим структурным, корреляционным и спектральным свойствам они *подобны случайному шуму*. Ниже, на базе теории многочленных представлений излагаются основы формирования и свойства ПСП.

Рассмотрим типовую схему генератора ПСП (рис.5.1).

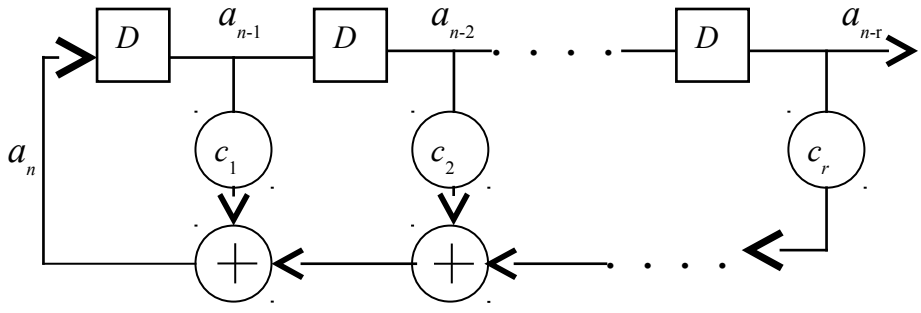


Рисунок 5.1 – Структурная схема линейного регистра сдвигов с обратной связью

Регистр сдвигов состоит из r элементов задержки, обозначаемых символом D. Предполагается, что символы a на входах и выходах элементов регистра *выбираются из поля* $GF(m)$ (m – основание поля Галуа). Под воздействием тактовых импульсов символы a продвигаются по цепочке элементов задержки слева направо и после умножения на коэффициенты c_i ($i=\overline{1,r}$) ($c_i \in GF(m)$) поступают на сумматоры, которые вместе с умножителями образуют *цепь обратной связи*.

Видно, что структура на рис.5.1 представляет собой *автономный конечный автомат,* выходная последовательность которого зависит от *вектора начального состояния* (a_{n-1}, a_{n-2},…a_{n-r}) и *вектора коэффициентов обратной связи* (c_1, c_2, … c_r). Символы на выходе цепи обратной связи

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_r a_{n-r} = \sum_{i=1}^{r} c_i a_{n-1} \qquad (5.13)$$

зависят от r предшествующих символов.

Часто рассматривается формирование двоичных ПСП, когда символы a и c выбираются из поля $GF(2)=\{0, 1\}$. В этом случае при $c_i=1$ символы a поступают на сумматоры *непосредственно*. При $c_i=0$ связь с сумматорами *отсутствует.* В сумматорах реализуется правило сложения по модулю 2. Набор сумматоров и умножители на коэффициенты c_i образуют *линейную цепь обратной связи*. Это дает основание считать структуру на рис.5.1 *линейной*. Рассмотрим линейную комбинацию символов на выходах элементов задержки:

$$F(D) \triangleq a_0 + a_1 D + a_2 D^2 + \ldots = \sum_{n=0}^{\infty} a_n D^n \,. \qquad (5.14)$$

Здесь D – оператор задержки. Комбинируя выражения (5.13) и (5.14) можно получить *рекурсивное* выражение:

$$\begin{aligned} F(D) &= \sum_{n=0}^{\infty} a_n D^n = \sum_{n=0}^{\infty} \sum_{i=1}^{r} c_i a_{n-i} D^n = \\ &\sum_{i=1}^{r} c_i D^i \left[\sum_{n=0}^{\infty} a_{n-1} D^{n-1} \right] = \\ &= \sum_{i=1}^{r} c_i D^i \left[a_{-i} D^{-i} + \ldots + a_{-1} D^{-1} + F(D) \right], \end{aligned} \qquad (5.15)$$

из которого следует равенство, содержащее многочлен $F(D)$:

$$F(D) = \left(1 - \sum_{i=1}^{r} c_i D^i \right) = \sum_{i=1}^{r} c_i D^i \left[a_{-i} D^{-i} + \ldots + a_{-1} D^{-1} \right], \qquad (5.16)$$

и, далее, в виде отношения многочленов конечной степени:

$$F(D)=\frac{\sum_{i=1}^{r} c_i D^i \left(a_{-i} D^{-i} + \ldots + a_{-1} D^{-1}\right)}{1 - \sum_{i=1}^{r} c_i D^i} \triangleq \frac{a_0(D)}{g(D)}, \qquad (5.17)$$

где многочлен $g(D)=1-\sum_{i=1}^{r} c_i D^i$ (5.18)

называется *характеристическим многочленом* данного генератора ПСП. Этот многочлен зависит от *вектора коэффициентов обратной связи* ($c_1 c_2 \ldots c_r$). Многочлен $a_0(D)$ зависит от вектора *начальных условий* ($a_{-r} a_{-r-1} \ldots a_1$), т. е. от состояния регистра в момент, предшествующий генерации члена a_0.

Отметим следующие ***важные свойства*** последовательностей на выходе линейного регистра сдвигов (ЛСР), а именно:

Свойство 5.1. Каждая последовательность на выходе ЛСР периодична с периодом

$$P \le (2^M - 1). \qquad (5.19)$$

Свойство 5.2. (*свойство сдвига).* Любой *циклический сдвиг* псевдослучайной последовательности F(D) вида (5.17) есть также псевдослучайная последовательность.

Свойство 5.3. (*свойство сложения).* Поэлементная сумма по модулю два двух двоичных последовательностей есть псевдослучайная последовательность.

Свойство 5.4.*(свойства сдвига и сложения).* Сумма последовательности F(D) с ее циклическим сдвигом
есть также псевдослучайная последовательность.

Свойство 5.5. (*структура последовательности).* Половина элементов двоичной последовательности есть нули, половина элементов есть единицы.

Обычно в качестве характеристического многочлена выбирают *примитивные* (*неприводимые*) многочлены степени *M.*

Определение 5.1. Степень степенного многочлена равна значению показателя степени *старшего члена* этого многочлена.

$$g(D)=1-\sum_{i=1}^{M} c_i D^i . \qquad (5.20)$$

Многочлен степени *M* называется ***неприводимым***, если он не может быть представлен в виде произведения других многочленов. Иными словами, ***неприводимый многочлен делится без остатка на единицу либо сам на себя.*** При использовании в цепи обратной связи линейного регистра сдвигов многочлена степени *M* вида (5.20) генерируется псевдослучайная последовательность с периодом $P \le (2^M - 1)$. Такие последовательности называют *последовательностями максимального периода* (либо, сокращенно,
***M-последовательностями*).** В алгебре многочленов целой степени *неприводимые многочлены* играют такую-же роль, какую *простые числа* играют в алгебре целых чисел.

6. Многотактные линейные фильтры

В технике помехоустойчивого кодирования широко используются многотактные линейные фильтры (МЛФ).

Многотактный линейный фильтр – устройство, состоящее из элементов задержки, сумматоров, умножителей на скаляры и связей между ними.

Изображение элементов МЛФ на функциональных схемах показано на рис.6.1. Информация в МЛФ представлена *символами из алгебраического поля* $F(m)$. В теории МЛФ вводят оператор задержки D, определяемый для схемы, представленной на рис.6.2. Предполагается, что символы в элементах задержки продвигаются от входа к выходу под действием тактовых импульсов, действующих через равные промежутки времени. Если в $к$-й момент времени на входе элемента задержки D действует символ u_k, то символ $a_к$ на выходе определяется как $a_к=u_{k-1}$.

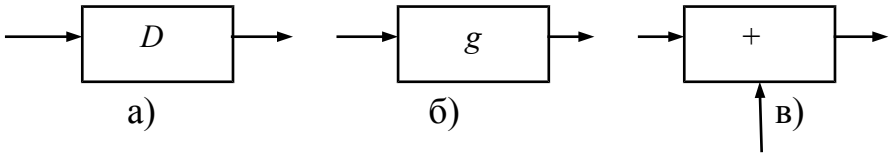


Рисунок 6.1 – Функциональные элементы МЛФ: а) – элемент задержки; б) – умножитель на скаляр g; в) – сумматор;

В теории кодирования рассматривают последовательности вида:

$$u(D)=u_0D^0+u_1D^1+u_2D^2+\ldots+u_iD^i+\ldots\ ;$$

$$a(D)=a_0D^0+a_1D^1+a_2D^2+\ldots+a_iD^i+\ldots\ . \qquad (6.1)$$

При этом действие оператора задержки D для последовательностей символов на входе $u(D)$ и выходе элемента задержки $a(D)$ определяется равенством:

$$a(D)=u(D)\cdot D^1. \qquad (6.2)$$

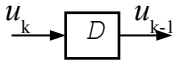


Рисунок 6.2 – К пояснению действия элемента задержки

Аналогично, для последовательного соединения n элементов задержки (рис.6.3) справедливо равенство:

$$a(D) = u(D)\ D^n. \qquad (6.3)$$

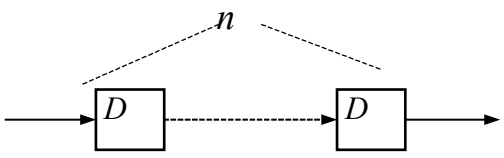


Рисунок 6.3 – Последовательное соединение n элементов задержки

Рассмотрим МЛФ общего вида (рис. 6.4), содержащий, к примеру, r элементов задержки.

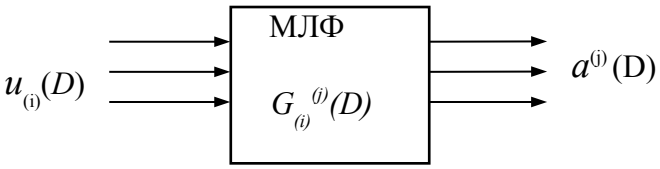


Рисунок 6.4 – К определению передаточной функции МЛФ

Если можно записать связь между последовательностью $u_{(i)}(D)$ на i-м входе МЛФ и последовательностью $a^{(j)}(D)$ на j-м выходе в виде равенства:

$$u_{(j)}(D)G^{(j)}(D)=a^{(i)}(D)G^{(i)}(D), \qquad (6.4)$$

где $$G_{(j)}(D) = \sum_{k=0}^{r} g_{k,(j)} D^k \quad , \qquad (6.5)$$

а коэффициенты g – выбираются из поля $F(m)$.
Из равенства (6.4) можно определить ***передаточную функцию*** МЛФ от j – го входа к i – му выходу:

$$G_{(j)}^{(i)}(D) = \frac{a_{(i)}(D)}{u_{(j)}(D)} = \frac{G^{(j)}(D)}{G^{(i)}(D)}. \qquad (6.6)$$

Рассмотрим простейшие примеры.

Пример 6.1. *Простые формы передаточных функций МЛФ.*

Для схемы на рис. 6.2 ранее было записано $a^{(1)}(D)=u_{(1)}(D)D$. Отсюда передаточная функция

$$G(D) = \frac{a_{(1)}(D)}{u^{(1)}(D)} = D.$$

Аналогично, для схемы на рис. 6.3 получаем $G(D)=D^n$.

Пример 6.2. *Сверточный кодер как МЛФ.*

Сверточный кодер (СК) на рис.6.5 содержит три элемента задержки, два сумматора. СК также может быть рассмотрен как МЛФ с одним входом и двумя выходами.

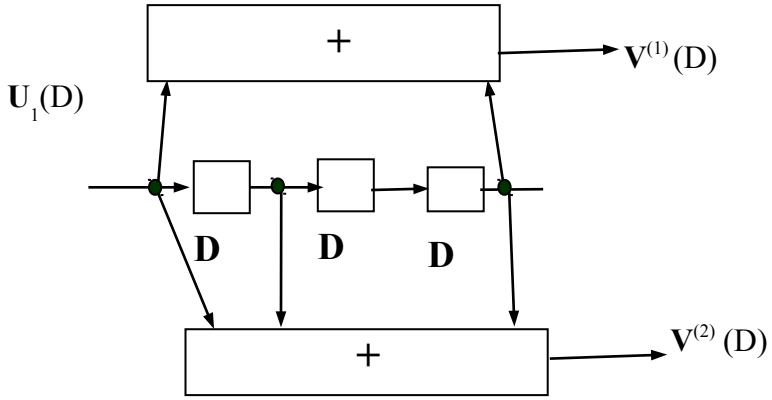


Рисунок 6.5 – Сверточный кодер с порождающими многочленами $(1+D^2)$, $(1+D+D^2)$

По аналогии с предыдущими примерами можно записать передаточные функции СК (называемые в теории СК *порождающими многочленами):*

$$G_{(1)}^{(1)}(D) = \frac{V^{(1)}(D)}{U_{(1)}(D)} = 1 + D^2;$$
$$G_{(1)}^{(2)}(D) = \frac{V^{(2)}(D)}{U_{(1)}(D)} = 1 + D + D^2. \qquad (6.7)$$

П.6.1. Многотактные линейные фильтры в теории циклических кодов

Теория многотактных линейных фильтров, равно как и рассмотренные в разд. 5 многочленные представления, широко используются в теории циклических кодов. Выполним первоначально предварительные построения.

Пример 6.3. *Схема умножения многочлена на многочлен*.

Процедура умножения многочлена $u(\mathrm{D})=u_0D^0+u_1D^1\ldots+u_kD^k$ на многочлен $g(\mathrm{D})=g_0D^0+g_1D^1+g_2D^2+\ldots+g_iD^i+\ldots+g_lD^l$ может быть реализована с использованием МЛФ. Для синтеза структуры перемножителя многочленов рассмотрим их произведение:

$v(D)=u(\mathrm{D})g(\mathrm{D})= g_0D^0\,u(\mathrm{D})+g_1D^1\,u(\mathrm{D})+g_2D^2\,u(\mathrm{D})+\ldots+g_iD^iu(\mathrm{D})+\ldots+g_lD^lu(\mathrm{D})$.

Структура МЛФ с параллельным включением элементов задержки, соответствующая этой формуле, приведена на рис. 6.6.

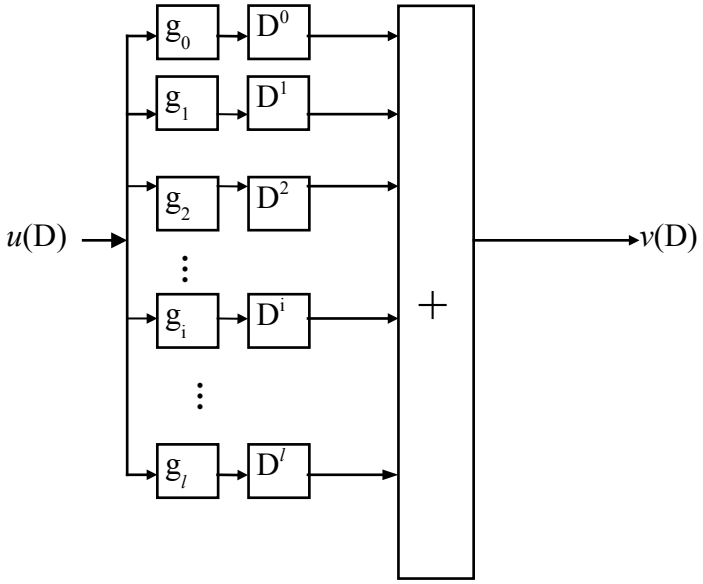


Рисунок 6.6 – Схема для перемножения многочленов (параллельное включение элементов задержки)

Альтернативная структура МЛФ для умножения многочлена на многочлен с последовательным включением элементов задержки, приведена на рис.6.7. Эта схема часто используется на практике в силу *простоты ее реализации.*

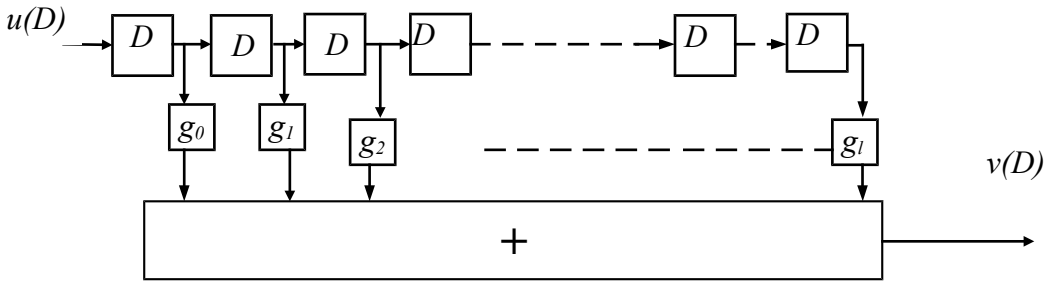


Рисунок 6.7 – Схема для перемножения многочленов (последовательное включение элементов задержки)

Пример *6.4.* *Схема деления многочлена на многочлен.*

Для синтеза схемы для деления многочленов процедуру деления представим следующим образом.

Пусть заданы делимое $u(D)=\sum_{i=0}^{n} u_i D^i$ и делитель $g(D)=\sum_{k=0}^{r} g_k D^k$.

Определим частное $v(D)=\frac{u(D)}{g(D)}$. Это выражение можно переписать в следующем виде: $u(D)=v(D)g_0+v(D)\sum_{k=1}^{r} g_k D^k$. Перенося член с суммой в левую часть равен-

ства получаем $v(D)=\frac{1}{g_0}\left[u(D)+\sum_{k=1}^{r}(-g_k)D^k\right]$. Здесь использованы *обратные элементы* коэффициентов многочлена делителя: по умножению $\frac{1}{g_0}=g_0^{-1}$ и по сложению ($-g_0$). С учетом этого получаем окончательную формулу для частного:

$$\boldsymbol{v(D)}=g_0^{-1}\left[u(D)+v(D)\sum_{k=1}^{r}(-g_k)D^k\right]. \qquad (6.8)$$

Схема МДФ, реализующая функцию деления в соответствии с этим выражением, представлена на рис. 6.8

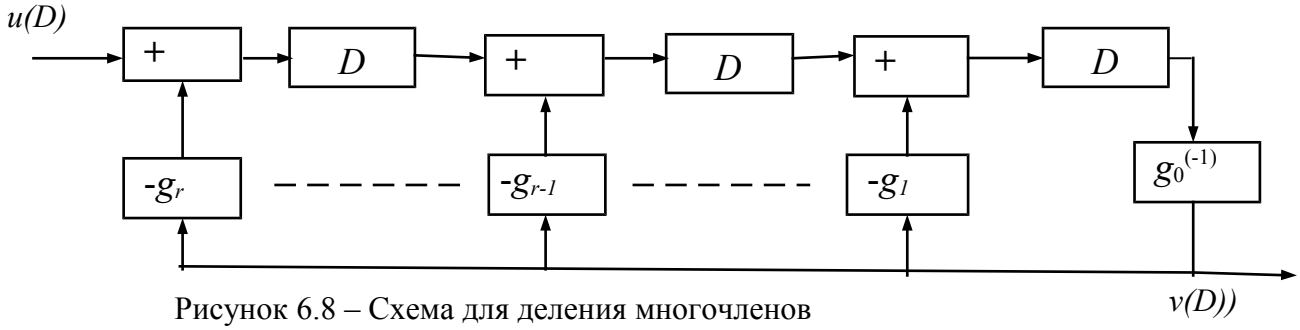


Рисунок 6.8 – Схема для деления многочленов

Пример 6.5. *Структура кодера систематического ЦК.*

Используя алгоритм кодирования систематическим ЦК (5.10) сформируем структурную схему кодера с порождающим многочленом $g(X)=x^4+X+1$. Схема систематического кодера приведена на рис.6.9.

В соответствии с алгоритмом кодирования (5.10) кодер работает следующим образом. Первоначально переключатели $П_1$ и $П_2$ находятся в положении 1. Одиннадцать информационных символов кодируемой комбинации $u(x)$ вводятся слева в цепь деления на многочлен $g(x)=X^4+X+1$. Одновременно они через последовательно соединенные элементы задержки поступают на выход кодера, образуя информационную часть разрешенной кодовой комбинации $u(X)X^{n-k}$. За первые четыре такта в ячейках регистра сдвигов схемы делителя на порождающий многочлен образуется остаток от деления $r(X)$.

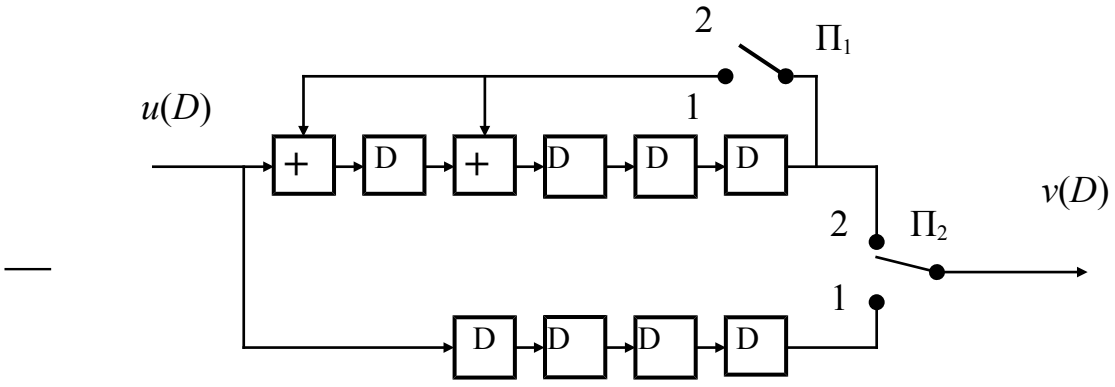


Рисунок 6.9 – Схема кодера систематического ЦК с порождающим многочленом $g(X)=X^4+X+1$; D – элемент задержки на такт; (+) – сумматор по модулю 2.

Затем переключатели $П_1$ и $П_2$ устанавливаются в положение 2, процесс деления прекращается, и остаток считывается с выхода делителя и «*дописывается»* в проверочную часть выходной кодовой комбинации $v(X)=u(X)X^{n-k}+r(X)$.

Пример 6.6. *Структура кодера несистематического ЦК.*

Используя правило кодирования несистематического ЦК (5.5), сформируем структурную схему кодера с порождающим многочленом $g(X)=X^4+X+1$.
Правило кодирования (5.5) предусматривает перемножение многочленов $u(X)$ и $g(X)$. Используя структуру перемножителя многочленов из Примера 6.3 схему кодера представим на рис. 6.10

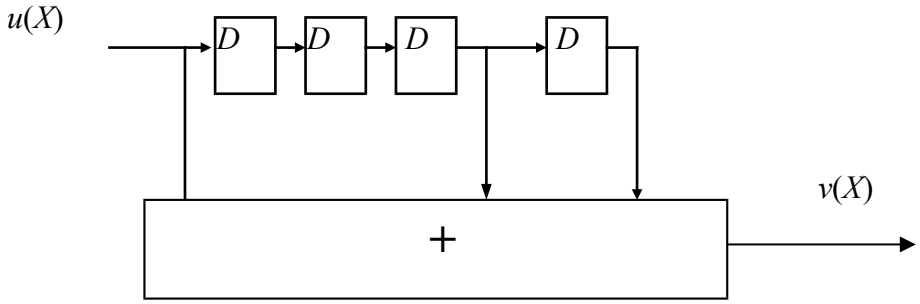


Рисунок 6.10 – Схема кодера несистематического ЦК с порождающим многочленом $g(x)=X^4+X+1$; D – элемент задержки на такт;
(+)– сумматор по модулю 2.

П.6.2. Модель канала с относительным кодированием на базе теории многотактных линейных фильтров

В системах цифровой радиосвязи широко применяются сигналы с фазовой модуляцией (ФМ). Когерентный прием сигналов ФМ сопровождается явлением *неоднозначности фазы* опорного колебания, восстанавливаемого в когерентном демодуляторе. Для передачи информации по каналу с неоднозначностью Н.Т.Петровичем предложен метод *относительной фазовой модуляции* (ОФМ). Метод состоит в *совместном* использовании процессов фазовой модуляции гармонического переносчика и *относительного кодирования (*ОК) информационных символов. Применение рассмотренных выше многочленных представлений и теории многотактных линейных фильтров (см. разд.5 и разд.6) позволяет избежать необходимости использования *эвристических* представлений для пояснения принципа относительного кодирования, выполнить *корректный синтез* метода относительного кодирования и распространить применение ОК на каналы с *пространственно-временным кодированием* (ПВК).

При восстановлении в демодуляторе опорного колебания для когерентного приема ФМ сигналов восстановленная несущая приобретает *дополнительный фазовый сдвиг*, кратный $\Delta\varphi=2\pi/M$ (M – число позиций фазы ФМ сигнала). Если ансамбль передаваемых ФМ-M сигналов содержит набор $\{s_0(t), s_1(t), s_i(t), s_{M-1}(t)\}$ (соответственно, векторы $\{\boldsymbol{S_0}, \boldsymbol{S_1}, \ldots, \boldsymbol{S_{M-1}}\}$ на рис. 6.11), то вследствие *ошибок неоднозначности* при восстановлении фазы несущей к номеру решения на выходе демодулятора S_{i+f} добавляется *произвольное число* $f \in \{0,1..M\}$, что соответствует *ошибке фазы восстановления несущей* $\Delta\varphi_f = f\cdot\frac{2\pi}{M}$.

Изложенное выше, а также *изоморфизм* кольца целых чисел порядка *M* и углов поворота вектора сигналов ФМ-*M* (см.разд.2.1.8) позволяет описать *алгебраическую модель канала с неоднозначностью (*рис. 6.12).

На этом рисунке использованы следующие обозначения:

$\bar{u}(D)$ –последовательность передаваемых символов;

$\hat{\bar{v}}(D)$ –последовательность принятых символов;

$\bar{f}(D)$ –последовательность символов неоднозначности;

⊕ – сумматор по модулю *M*;

ОК – относительный кодер;

ОД – относительный декодер.

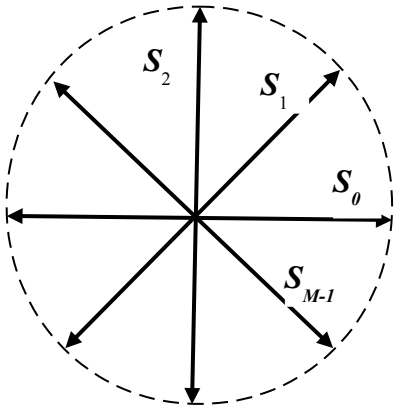


Рисунок 6.11 – Векторная диаграмма ФМ-*M* сигналов

В канале к последовательности передаваемых символов $\bar{u}(D)$ добавляется последовательность символов неоднозначности $\bar{f}(D)$:

$$\hat{\bar{v}}(D) = \bar{u}(D) \oplus \bar{f}(D), \tag{6.9}$$

где: D – оператор задержки;

помеха неоднозначности

$$\bar{f}(D) = fD^0 + fD + fD^2; \tag{6.10}$$

f – *символ неоднозначности*, определяющий фазовый сдвиг несущей

$$\Delta\varphi_f = f \cdot \frac{2\pi}{M}. \tag{6.11}$$

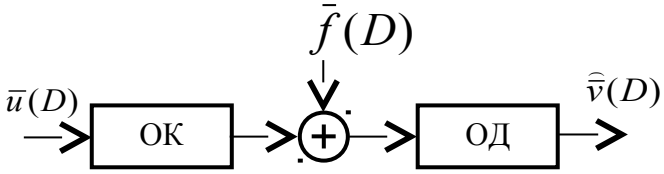


Рисунок 6.12– Модель канала с неоднозначностью

Помеху неоднозначности в выражении (6.11) можно представить так:

$$f(D) = \frac{f}{1 + D}. \tag{6.12}$$

Включение на приемной стороне относительного декодера (ОД) с передаточной функцией

$$K_{\text{ОД}} = 1 + D. \tag{6.13}$$

позволяет "*подавить*" помеху неоднозначности, поскольку на выходе ОД получаем

$$\hat{\bar{v}}(D)=\bar{u}\,(D)(1+D)+f, \qquad (6.14)$$

т. е. в соответствии с выражениями (6.12), (6.13) и (6.14) принимаемая последовательность содержит *только первый символ ошибки неоднозначности* fD^0.
Из выражения (6.13) следует, что для восстановления из принятой последовательности $\hat{\bar{v}}(D)$ переданной последовательности $\bar{u}(D)$ на передающей стороне *необходимо включить относительный кодер* (ОК) с передаточной функцией

$$K_{\text{ОК}}(D)=\frac{1}{1+D}. \qquad (6.15)$$

Тогда последовательность на выходе ОД будет

$$\hat{\bar{v}}(D)=[\bar{u}\,(\mathrm{D})K_{\text{ОК}}(D)+\bar{f}(D)\,]K_{\text{ОД}}(D)=\bar{u}\,(\mathrm{D})+f\mathrm{D}^0, \qquad (6.16)$$

Поскольку $K_{\text{ОК}}(D)\cdot K_{\text{ОД}}(D)=1$.

Представленная выше модель полностью соответствует идеологии относительного кодирования, предложенной Н.Т. Петровичем, при этом структуры ОК и ОД могут быть представлены в соответствии с выражениями (6.13) и (6.15) так, как показано на рис. 6.13, соответственно.

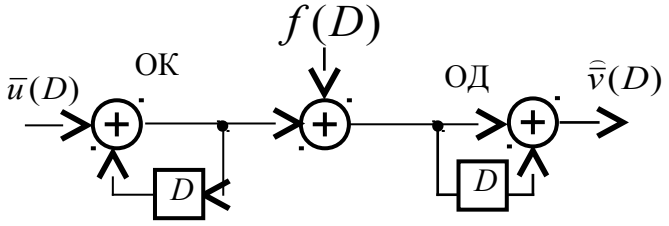


Рисунок 6.13 – Относительный кодер (ОК) и относительный декодер (ОД) в канале с неоднозначностью
(D – элемент задержки, $\oplus$ – сумматор по модулю M).

Из рис.6.13 видно, что помеха на выходе ОД равна

$$\hat{\bar{f}}(D)=f(D)\oplus f(D)D=fD^0=f, \qquad (6.17)$$

что и было отмечено выше (см. (6.16)).

П.6.3. ОФМ в системах с ПВК

Одним из специфических требований к сигналам в системах с ПВК является использование в каналах разнесения *одинаковых* методов модуляции, что упрощает построение приемных устройств. Применительно к рассматриваемому случаю фазовой модуляции в каналах разнесения при ПВК должна использоваться относительная фазовая модуляция (относительное кодирование). Структура ОК (рис. 6.15) позволяет выполнить относительное кодирование без усложнения схемы (рис.6.16). Нетрудно видеть, что передаточная функция такого кодера для первой *ветви разнесения* будет

$$K_{\text{ОД}(1)}(D)=\frac{\bar{v}_1(D)}{\bar{u}(D)}=\frac{1}{1+D}, \qquad (6.18)$$

т.е. последовательность на первом выходе $\bar{v}_1(D)$ также кодируется относительным кодом, при этом в кодированную последовательность вносится задержка D на один такт.

В то же время передаточная функция кодера для второго канала будет

$$K_{\text{ОД(2)}}(D) = \frac{\bar{v}_2(D)}{\bar{u}(D)} = \frac{D}{1+D}, \qquad (6.19)$$

т. е. последовательность на втором выходе также кодируется относительным кодом, при этом в кодированную последовательность вносится задержка D на один такт. При необходимости организации n каналов разнесения целесообразно использовать комбинированный ОК, показанный на рис. 6.16.

В состав ОК для трех каналов разнесения на рис.6.16 входит структура, передаточная функция которой $K_{\text{ОК}}(D)$ может быть определена с учетом равенства

$$(1+D+D^2)(1-D)=1-D^3. \qquad (6.20)$$

Аналогично, представленному на рис.6.13 случаю, кодер на рис. 6.14 формирует относительно кодированные последовательности для трех каналов разнесения (передаточные функции показаны на рис. 6.14 справа). Построение подобного кодера с n выходами можно продолжить по аналогии для любого значения n.

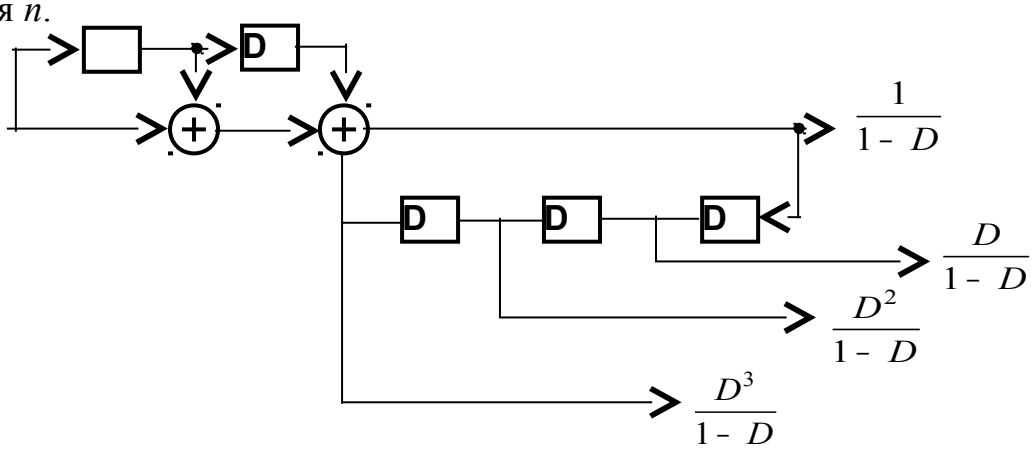


Рисунок 6.14 – Относительный кодер для трех каналов разнесения системы с ПВК

Сверточные коды (СК) находят широкое применение в разнообразных системах передачи цифровой информации. Чаще всего используются *несистематические* СК, обеспечивающие по сравнению с систематическими кодами лучшие характеристики. В частности, несистематические СК в сравнении с эквивалентными им систематическими кодами имеют меньшую длину кодового ограничения при одинаковом минимальном расстоянии. Известно, что процедура формирования синдромов является первым этапом при реализации алгоритма порогового декодирования систематических СК [11]. При использовании несистематических СК формирователи синдромов (ФС) применяются в составе декодеров Витерби для выделения *сигналов синхронизации и оценок неодно-*

значности. Кроме того, ФС могут быть использованы для *идентификации порождающих многочленов* СК.

Преобразователи кодовых последовательностей типа "*инверсных схем"* (ИС) используются для *выделения информационных последовательностей* из принимаемых кодовых последовательностей несистематических СК. Структуры ФС и ИС для систематических кодов хорошо изучены. В настоящем разделе развита теория такого рода преобразователей для несистематических СК, а также приведены сведения о структурах ФС и ИС для типичных примеров СК, используемых на практике.

Рассмотрим линейный несистематический СК со скоростью $R = k/n$ и матрицей порождающих многочленов вида

$$\overline{G}(D) = \begin{vmatrix} \overline{g}_1(D) \\ \overline{g}_2(D) \\ \vdots \\ \overline{g}_k(D) \end{vmatrix} = \begin{vmatrix} g_1^{(1)}(D) & g_1^{(2)}(D) & \ldots & g_1^{(n)}(D) \\ g_2^{(1)}(D) & g_2^{(2)}(D) & \ldots & g_2^{(n)}(D) \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ g_k^{(1)}(D) & g_k^{(2)}(D) & \ldots & g_k^{(n)}(D) \end{vmatrix}, \qquad (6.21)$$

где $g_i^{(j)}(D) = g_{i,0}^{(j)} D^0 + g_{i,1}^{(j)} D^1 + g_{i,2}^{(j)} D^2 + \ldots + g_{i,t}^{(j)} D^t + \ldots + g_{i,\nu_i}^{(j)} D^{\nu_i}$ – элемент матрицы $\overline{G}(D)$, степенной многочлен от формальной переменной D, коэффициенты которого определяют связи i-го входа кодера ($i=\overline{1,k}$) с сумматором на j-ом выходе ($j=\overline{1,n}$); ν_i – количество элементов задержки в i-м регистре СК.

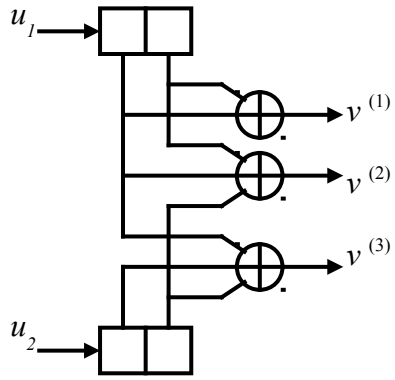


Рисунок 6.15– Кодер СК со скоростью $R = 2/3$

На рис. 6.15 приведен пример СК со скоростью $R=2/3$, $\nu_1=1,\nu_2=1$ и матрицей порождающих многочленов

$$\overline{G}(D) = \begin{vmatrix} 1+D & 1+D & 1 \\ 0 & D & 1+D \end{vmatrix}. \qquad (6.22)$$

Соответствующая ей матрица проверочных многочленов будет

$$\overline{H}(D) = \begin{vmatrix} \overline{h}_1(D) \\ \overline{h}_2(D) \\ \vdots \\ \overline{h}r(D) \end{vmatrix} = \begin{vmatrix} h_1^{(1)}(D) & h_1^{(2)}(D) & \ldots & h_1^{(n)}(D) \\ h_2^{(1)}(D) & h_2^{(2)}(D) & \ldots & h_2^{(n)}(D) \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ h_r^{(1)}(D) & h_r^{(2)}(D) & \ldots & h_r^{(n)}(D) \end{vmatrix}, \qquad (6.23)$$

где $h_l^{(j)}(D)=h_{l,0}^{(j)}D^0+h_{l,1}^{(j)}D+h_{l,2}^{(j)}D^2+\ldots+h_{l,t}^{(j)}D^t+\ldots+h_{l,\nu_l}^{(j)}D^{\nu_l}$ – элемент матрицы $\overline{H}(D)$, многочлен от формальной переменной D, коэффициенты которого определяют связи j-го входа ФС с l-м его выходом ($l=\overline{1,r}$, $r=n-k$).

При заданных последовательностях на входах кодера

$$\overline{u}(D)=|u_1(D)u_2(D)\ldots u_k(D)| \qquad (6.24)$$

кодирование определяется выражением

$$\overline{v}(D)=\overline{u}(D)\overline{G}(D), \qquad (6.25)$$

а порождающая и проверочная матрицы связаны соотношением

$$\overline{G}(D)\,\overline{H}^T(D)=\overline{O}(D), \qquad (6.26)$$

где: $\overline{H}^T(D)$ – транспонированная проверочная матрица;

$\overline{O}(D)$ – матрица многочленов с нулевыми коэффициентами.

При выполнении условия (6.26) многочлены синдромов формируются следующим образом:

$$\overline{S}(D)=\overline{e}(D)\,\overline{H}^T(D). \qquad (6.27)$$

При известной матрице порождающих многочленов $\overline{G}(D)$ многочлены проверочной матрицы $\overline{H}(D)$ могут быть найдены на основе решения уравнения (6.26). При отсутствии ошибок в канале ($\overline{e}(D)=\overline{0}$) на выходе формирователя синдромов последовательности $\overline{S}(D)=\overline{0}$.

При неизвестных порождающих многочленах $\overline{G}(D)$ они могут быть идентифицированы подбором многочленов $\overline{H}(D)$. Пусть кодирование производится в соответствии с выражением (6.25), а формирование синдромов – с использованием проверочной матрицы

$$\overline{H}_0(D)=\overline{H}(D)+\Delta\overline{H}(D). \qquad (6.28)$$

Здесь $\Delta\overline{H}(D)$ – матрица "*несогласованности",* определяющая отличие используемой матрицы $\overline{H}_0(D)$ от матрицы $\overline{H}(D)$, удовлетворяющей условию (6.27). Нетрудно убедиться в том, что на выходе формирователя синдромов в этих условиях будут ненулевые последовательности даже при отсутствии ошибок в канале. Пусть $\overline{S}(D)=\overline{u}(D)\,\overline{G}(D)\,\overline{H}_0^T(D)=\overline{e}(D)\,\overline{H}^T(D)+[\overline{u}(D)+\overline{e}(D)]\Delta\overline{H}^T$ и при $\overline{e}(D)$=О получаем

$$\overline{S}(D) = \overline{u}(D) \cdot \Delta \overline{H}^T. \qquad (6.29)$$

Из столбцов матрицы (6.22) многочленов $\overline{G}(D)$ размером $k \times n$ можно образовать C_n^k квадратных подматриц $\overline{G}_m^*(D)$ (m=$\overline{1, C_n^k}$) размером $k \times k$. Пусть каждая из таких подматриц имеет определитель $\Delta_m(D)$. В работе [54] показано, что информационные последовательности $\overline{u}_i(D)$(i=$\overline{1,k}$), поступающие на k входов сверточного кодера с матрицей порождающих многочленов $\overline{G}(D)$ могут быть восстановлены по кодовым последовательностям на выходе кодера $\overline{v}^{(j)}(D)$ (j = $\overline{1,n}$) с использованием «*инверсной схемы»,* если выполняется условие

$$\text{ОНД}\,(\overline{\Delta}_m(D),\ m = \overline{1, C_n^k}) = D^L. \qquad (6.30)$$

Здесь ОНД – общий наибольший делитель многочленов $\overline{\Delta}_m(D)$;

L– целое положительное число или ноль.

В частности, для кодов со скоростью $R = 1/n$ (k=1) каждая из матриц $\overline{\Delta}_m(D) = g^{(m)}(D)$, m=$\overline{1,n}$ и условие (6.30) упрощаются:

$$\text{ОНД}(g_1^{(1)}(D), g_1^{(2)}(D), \ldots, g_1^{(j)}(D), \ldots, g_1^{(n)}(D)) = D^L. \qquad (6.31)$$

При этом процессы кодирования и "*декодирования*" *(восстановление* информационной последовательности) инверсной схемой в матричной форме описываются следующим образом. Как известно, общий наибольший делитель многочленов может быть определен их линейной комбинацией вида:

$$\text{ОНД}(g_1^{(1)}(D), g_1^{(2)}(D), \ldots, g_1^{(j)}(D), \ldots, g_1^{(n)}(D)) = g_1^{(1)}(D)p^{(1)}(D) + $$
$$+ g_1^{(2)}(D)p^{(2)}(D) + \ldots + g_1^{(j)}(D)p^{(j)}(D) + \ldots + g_1^{(n)}(D)p^{(n)}(D) = D^L. \qquad (6.32)$$

Умножая левую и правую части выражения (6.32) на $u_1(D)$ с учетом того, что $u_1(D) \cdot g_1^{(j)}(D) = v^{(j)}(D)$ получаем

$$v^{(1)}(D) \cdot p^{(1)}(D) + v^{(2)}(D)p^{(2)}(D) + \ldots + v^{(j)}(D)p^{(j)}(D) + $$
$$+ \ldots + v^{(n)}(D)p^{(n)}(D) = u(D)D^L. \qquad (6.33)$$

Таким образом, набор многочленов $p^{(j)}(D)$ образует *матрицу передаточных функций инверсной схемы*

$$\overline{P}(D) = |p^{(1)}(D)\ p^{(2)}(D)\ \ldots\ p^{(n)}(D)|, \qquad (6.34)$$
$$\overline{v}(D) = \overline{u}(D)\ \overline{G}(D), \overline{v}(D)\ \overline{p}(D) = \overline{u}(D)\,D^L. \qquad (6.35)$$

Матрицы передаточных функций кодера и инверсной схемы находятся в соотношении:

$$\overline{G}(D)\,\overline{p}(D)=D^{L}. \qquad (6.36)$$

На рис. 6.18 показаны структуры кодера, формирователя синдрома и инверсной схемы для кода со скоростью $R = 1/2$. При этом многочлены кодера, формирователя синдромов и инверсной схемы удовлетворяют условиям:

$$g_1(D)h_1(D)+g_2(D)h_2(D)=0,$$

$$g_1(D)p_1(D)+g_2(D)p_2(D)=D^{L}.$$

Свойство катастрофичности СК исследовано в разделе 12.2, в котором сформулирован *признак катастрофичности СК в общем виде:*

Признак катастрофичности. Сверточный код с произвольным основанием, скоростью R=1/n и набором порождающих многочленов $\overline{G}(D)=\left|g^{(1)}(D),g^{(2)}(D),...,g^{(n)}(D)\right|$ является *катастрофическим,* если каждый из многочленов можно представить в виде произведения $g^{(j)}(D) = g_0(D)\cdot g^{*(j)}(D)$, где $g_0(D)$ – отличный от единицы общий множитель, $j = \overline{1,n}$.

Отсюда следует

Утверждение 6.1.Общий наибольший делитель порождающих многочленов табличных СК равен единице.

Здесь под табличными подразумеваются многочисленные СК, порождающие многочлены которые найдены различными авторами и помещены в обширных справочных таблицах кодов, предназначенных для практического использования [3].

Как известно, при поиске таких кодов катастрофические коды отбрасывались. Как следует из выражения (6.35) и структур формирователя синдрома и инверсной схемы, представленных на рис. 6.16, прохождение канальных ошибок сопровождается их «*размножением». Коэффициент размножения ошибок* можно определить по виду многочленов *h(D)* или *p(D)*. В частности, единичная ошибка в последовательности $\bar{e}_1$ = 1000000… приведет к появлению комбинации символов (1011011)… на выходе формирователя синдромов кода (133, 171). Несмотря на наличие эффекта «размножения» ошибок, формирователи синдрома позволяют *надежно идентифицировать порождающие многочлены кода*. При отсутствии «*рассогласования»* порождающих многочленов кода и многочленов синдромного формирователя ($\Delta H(D)=0$ в формуле (6.27)) на выходе формирователя будет только *поток синдромных ошибок*. При вероятности ошибки в канале 10^{-4} с учетом их «размножения» *вероятность синдромных ошибок* будет, ориентировочно, на порядок больше (т.е. 10^{-3}).

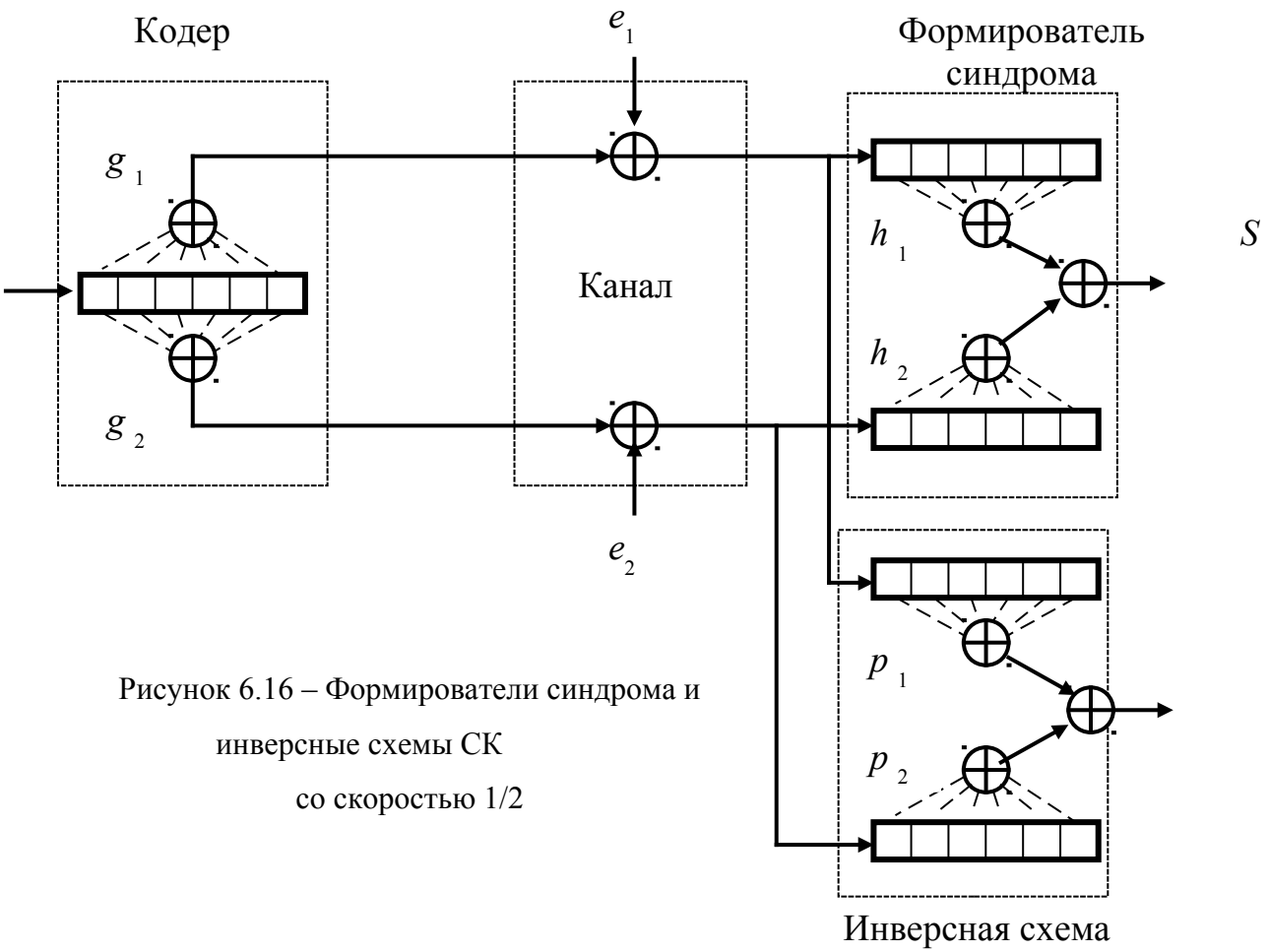


Рисунок 6.16 – Формирователи синдрома и инверсные схемы СК со скоростью 1/2

В то же время при *отсутствии согласования* на выходе синдромного формирователя будет, кроме потока синдромных ошибок, последовательность преобразованных информационных символов с приблизительно равновероятным распределением нулей и единиц. Различение двух описанных выше ситуаций на основе простого *подсчета числа единиц в синдроме* за достаточно длительный промежуток времени легко реализовать. В случае, когда исключена возможность декодирования последовательности символов сверточного кода с исправлением ошибок (например, *декодером Витерби*), применение инверсных схем позволяет *выделить поток информационных символов,* содержащий также «*размноженные»* канальные ошибки. Типичным примером использования инверсных схем является *формирование «зашумленной» копии* принимаемого фазоманипулированного сигнала, которая в демодуляторе используется как *оценка* при формировании опорной несущей для когерентного приема. Наличие достаточно редких ошибок в такой копии мало сказывается на точности восстановления, поскольку петля фазовой автоподстройки обеспечивает высокую помехоустойчивость.

7. Графы

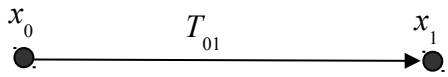
В теории кодирования применяются методы *теории графов.*

Граф представляет собой схему, состоящую из *узлов* (точек), соединенных направленными *ветвями,* и выражающую систему алгебраических уравнений. Узлы графа соответствуют *переменным*, а ветви – *коэффициентам* при этих переменных.

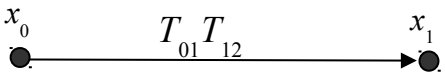
Узел графа – точка, выражающая некоторую переменную величину.

Ветвь – линия, соединяющая два узла. Ветвь *jk* начинается в узле *j* и заканчивается в узле *k,* ее *направление* указывается стрелкой.

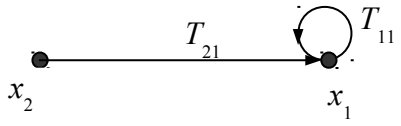
Например, простое алгебраическое уравнение $x_1=T_{01}x_0$ может быть представлено в виде графа:



Граф набора уравнений $x_1=T_{01}x_0$, $x_2=T_{12}x_1$, $x_2=T_{01}T_{12}x_0$ представляется так:

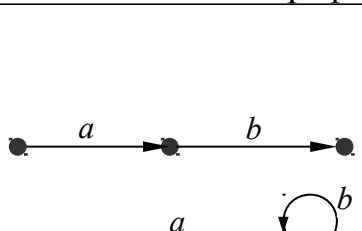
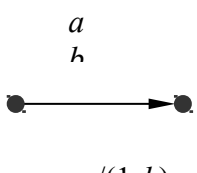
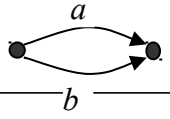


Построим граф, соответствующий уравнению $x_1=T_{11}x_1+T_{21}x_2$, решение которого относительно x_1 имеет вид $x_1 = \frac{T_{21}x_2}{1- T_{11}}$. Этому равенству соответствует граф *с петлей* около узла x_1:



В теории графов широко используют *эквивалентные преобразования*, позволяющие упростить *топологию графа*. Формы простейших эквивалентных преобразований приведены в табл.7.1.

Таблица 7.1 – Простейшие эквивалентные преобразования графов

№	Исходный граф	Эквивалентный граф
1		
2		

П.7.1. Графы в теории сверточных кодов

Сверточные коды образуют *подкласс* непрерывных кодов. Наименование *сверточный код* происходит от того, что результат кодирования на выходе кодера образуется как *свертка* кодируемой информационной последовательности с *импульсной реакцией кодера*.

Кодер сверточного кода содержит один либо несколько *регистров памяти* для хранения определенного числа информационных символов и *преобразователь* информационных последовательностей в кодовые последовательности. Процесс кодирования производится *непрерывно*.

Схема простого кодера показана на рис.7.1.

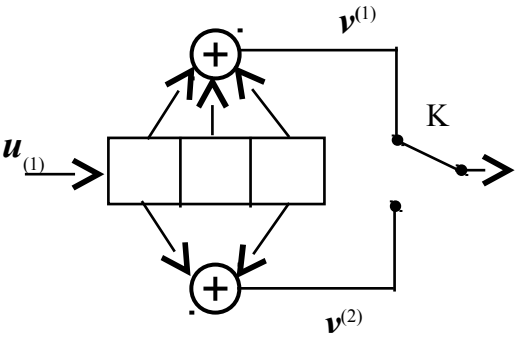


Рисунок 7.1 – Кодер СК

Информационные двоичные символы *и* поступают на вход *регистра сдвигов* с *К* разрядами. Входы сумматоров соединены с определенными разрядами регистра сдвигов. *Коммутатор* К на выходе кодера устанавливает *очередность посылки* кодовых символов в канал. За время одного информационного символа на выходе образуется два кодовых символа. Таким образом, *скорость кода* в этом примере *равна R=1/2*.

Возможно кодирование и с другими скоростями.

Сверточный кодер как *автомат с конечным числом состояний* может быть описан *диаграммой состояний.*

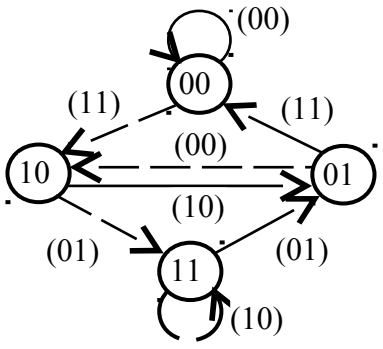


Рисунок 7.2 – Диаграмма состояний СК

Диаграмма состояний представляет собой *направленный граф* и описывает все возможные переходы кодера из одного *состояния* в другое, а также содержит символы выходов кодера, которые сопровождают эти переходы. *Состояния кодера* – содержимое элементов регистра сдвигов кодера. Пример диаграммы состояний кодера, показан на рис.7.2. В кружках указаны четыре возможных *состояния кодера* S_1S_2=00,10,11и0, стрелками – возможные переходы.

Символы около стрелок обозначают символы на выходе кодера $v^{(1)}v^{(2)}$, соответствующие данному переходу. *Сплошными* линиями отмечены переходы, совершаемые при поступлении на вход кодера информационного символа 0, *пунктирными* – при поступлении символа 1.

Первоначально кодер находится в состоянии 00, и поступление на его вход информационного символа u=0 переводит его также в состояние 00. При этом на выходе кодера будут символы ($v^{(1)}v^{(2)}$)=(00). На диаграмме этот переход обозначается *петлей* "00", выходящей из состояния 00 и вновь возвращающейся в это состояние. Далее, при поступлении символа u=1 кодер переходит в состояние 10, при этом на выходе будут символы ($v^{(1}v^{(2)}$)=(11). Этот переход обозначается *пунктирной* линией из состояния 00 в состояние 10. Далее, возможно поступление на вход кодера информационных символов 0 либо 1. При этом кодер переходит в состояние 01(либо 1), а символы на выходе будут 10 (либо 01), соответственно. Процесс построения диаграммы заканчивается, когда будут *просмотрены все возможные переходы* из каждого состояния во все остальные.

Решетчатая диаграмма (решетка) является разверткой диаграммы состояний во времени.

На *графе решетки* состояния показаны *узлами*, а переходы – соединяющими их *линиями.* После каждого перехода из одного состояния в другое происходит *смещение на один шаг вправо*. Пример решетчатой диаграммы показан на рис. 7.3.

Решетчатая диаграмма дает наглядное представление всех *разрешенных путей* (которые являются *аналогами* разрешенных кодовых комбинаций блоковых кодов) и по которым может *продвигаться* кодер при кодировании. Каждой информационной последовательности на входе кодера соответствует *единственный путь* по решетке.

Построение решетчатой диаграммы удобно производить с использованием диаграммы состояний. Исходным является нулевое состояние $S^{(1)}S^{(2)}$=00. Далее, с поступлением очередного информационного символа u=0 либо 1 возможны переходы в состояние 00, либо 10, обозначаемые ветвями 00 и 11, соответственно.

Процесс следует продолжить, причем через 3 шага

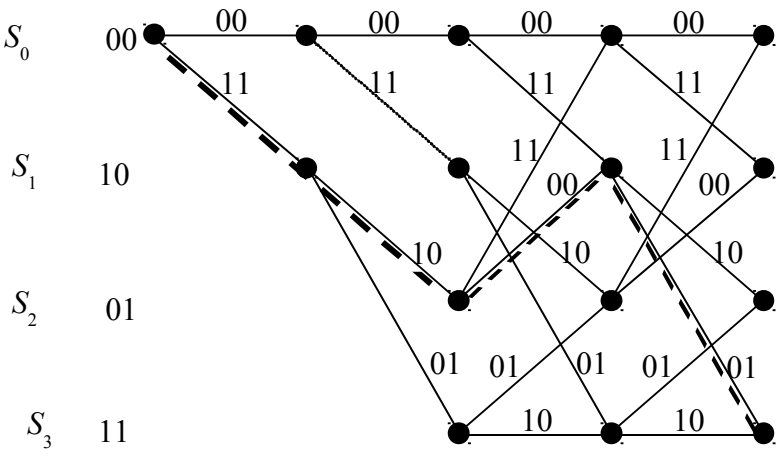


Рисунок 7.3 – Решетчатая диаграмма СК

(см. рис. 7.3) *очередной фрагмент решетки будет повторяться.* Пунктиром показан *путь по решетке* 11100001..., соответствующий поступлению на вход кодера информационной последовательности 1011.... .

П.7.2. Применение метода порождающих функций для анализа помехоустойчивости декодирования СК в каналах с постоянными параметрами

Анализ помехоустойчивости декодирования СК в канале с помехами основан на *использовании групповых свойств* СК, что позволяет рассчитывать вероятность ошибки, используя в качестве передаваемой *любую* из кодовых последовательностей, например, *полностью нулевую.* Для анализа помехоустойчивости используем понятие *ошибочного события*. При декодировании по максимуму правдоподобия ближайшим к передаваемому пути будет путь, который отстоит от него на величину, равную *свободному расстоянию кода*. Если в канале произойдут ошибки, кратность которых превысит исправляющую способность кода, декодер максимального правдоподобия выберет *ошибочный путь*. Такое событие приведет к ошибкам в одном либо нескольких информационных символах на выходе декодера.

При малом уровне шума *ошибочные события происходят редко.* Анализ *структуры ошибочных событий* производят с использованием графа в виде *модифицированной диаграммы состояний* СК. Рассмотрим для примера представленный ранее граф диаграммы состояний кода (7,5) (рис. 7.4 а). Этот граф является *компактным описанием множества путей*, выходящих из состояния S_0 и возвращающихся в него. Расчленим диаграмму в узле S_0, при этом получаем *модифицированную диаграмму* (рис. 7.4 б). Ошибочные события представляются всеми возможными переходами из состояния S_0' в состояние S_0''. Ветви диаграммы маркируем *формальными переменными* D^k, L^l и N^e. Показатель степени k при переменной D равен *весу* (количеству единиц) соответствующего переходу между состояниями. Показатель e переменной N равен числу единиц, поступающих на вход кодера при переходе из предыдущего состояния в последующее. Каждый переход маркируется символом $N^e(e=1)$. Такая маркировка необходима для *подсчета числа шагов* (переходов) по диаграмме. Например, при переходе из состояния S_0 в состояние S_1 на выходе кодера будет пара символов 11, вес которой равен 2 ($n=2$). Этот переход вызван поступлением на вход кодера одного информационного символа 1($l=1$). С учетом этих данных переход из состояния S_0 в состояние S_1 маркируется набором символов D^2LN. *Порождающая функция* СК может быть найдена по правилам нахождения передаточной функции графа, изложенным в табл. 7.1. На рис. 7.4 показана исходная диаграмма кода (7,5), а также ее *модификации*, выполненные по правилам компактной записи передаточных функций ребер графа. В частности, путь из состояния S_1 в состояние S_3 через состояние S_2 состоит из ребер *DLN, DL* и петли *DLN*. Передаточная функция этого пути будет $D^2L^2N/(1\ DLN)$. Последовательно упрощая граф, приходим к выражению для передаточной функции:

$$T(D,L,N) = \frac{D^5L^3N}{1 - DLN(1+L)}$$

. (7.1)

Производя деление по правилам деления многочленов, получаем окончательно:

$$T(D,L,N)=D^3L^3N+D^6L^4(1+L)\,N^2+\ldots.+D^{(5+m)}L^{(3+m)}(1+L)^mN^{(1+m)}+\ldots. \quad . \qquad (7.2)$$

Отсюда следует, что рассматриваемый код содержит один ошибочный путь с весом 5 (D^5), вызванный поступлением на вход кодера последовательности из трех входных символов (L^3), два пути с весом 6 (D^6), вызванных поступлением на вход кодера двух информационных символов 1, причем, один из этих путей соответствует четырем входным символам (L^4), а другой – пяти символам (L^5) и т.д. *Общий член* порождающей функции позволяет вычислить последовательно все возможные наборы таких путей. Для достаточно длинных СК подобные вычисления целесообразно производить с помощью ЭВМ. Производная порождающей функции по N при N=1 будет

$$\left.\frac{dT(D,N)}{dN}\right|_{N=1} = \sum_k C_k D^k \quad ; \qquad (7.3)$$

Набор коэффициентов C_k при $k>d_f$ называют *спектром весов* СК. Спектр показывает суммарное количество ошибок на выходе декодера, когда вместо передаваемого пути выбираются ошибочные пути, отстающие от него на величину d=k. Например, производная функции (7.3) $dT(D,\ N)/dN\,\big|_{N-1} = D^5 + 4D^6+12D^7+...+(1+m)2^mD^{(1+m)}+....$ показывает, что имеется один ошибочный путь веса d=5, выбор которого приводит к одной ошибке в информационной последовательности на выходе декодера. Имеются также ошибочные пути веса d=5, выбор которых дает четыре ошибки на выходе, пути веса d=6 и т.д.

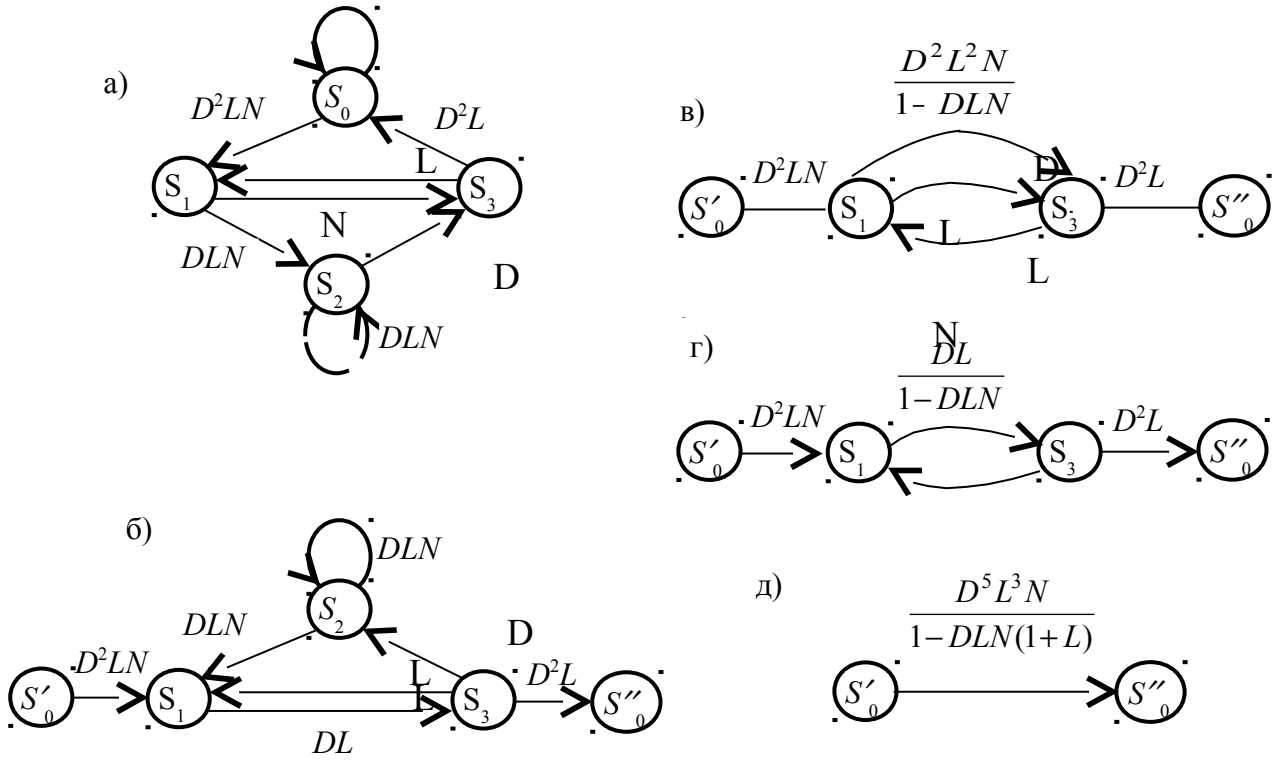


Рисунок 7.4 – К определению порождающей функции кода

При декодировании с *мягким решением* расстояние между различными путями вычисляют *в метрике Евклида*. Если двоичные кодовые последовательности отличаются в k символах, а в канале используют бинарную фазовую модуляцию ФМ-2, то расстояние между путями, соответствующими этим последовательностям, равно

$$d_k = 2k\sqrt{E_k}$$

Учитывая, что энергия каждого кодового символа $E_k=E_б R$, расстояние определим как

$$d_k = 2k\sqrt{E_б R}$$

Суммарная дисперсия отсчетов помех, действующих на k кодовых символов, $\sigma_k^2=kN_0/2$. Ошибка в выборе пути произойдет, когда помеха превысит половину расстояния d_k, т.е.

$$P_k = V((2kE_б/\mathrm{N}_0)^{\frac{1}{2}},$$

где

$$V(x) = \frac{1}{\sqrt{2\pi}}\int_0^{\infty} \exp(-\frac{t^2}{2})dt$$

– дополнение интеграла вероятности до единицы.

Таким образом, расчет вероятности ошибочного воспроизведения двоичного символа на выходе декодера сводится *к вычислению спектра весов*, расчету вероятности ошибочного выбора пути и последующему вычислению вероятности ошибки бита по формуле

$$p \le \sum_{k=d_f}^{\infty} C_k P_k$$

Такая методика достаточно точна при $p \le 10^{-2}$. На рис. 7.5 показаны результаты расчетов вероятности ошибки для кодов с различными скоростями. Кривые помехоустойчивости строятся в зависимости от отношения энергии сигнала, затрачиваемой на передачу одного бита информации, к спектральной плотности мощности шума $E_б/N_0$. В этом случае учитываются затраты энергии каждого двоичного символа, необходимые для передачи по каналу избыточных кодовых символов. Если в этих же координатах отложить зависимость E_b/N_0 для ФМ без кодирования, то легко определить по *разности* требуемых затрат E_b/N_0 (при *p=const)* величину *энергетического выигрыша кодирования* (ЭВК). Видно, что при использовании кода (133, 171) величина ЭВК θ=5,4 дБ. Это означает, что в этом случае в канале с ФМ-2 скорость передачи информации понизится в два раза (скорость кода R=1/2), а отношение сигнал/шум, требуемое для достижения $p=10^{-5}$, может быть уменьшено на 5,4 дБ.

Асимптотический энергетический выигрыш можно определить, сравнивая аргументы для функции V(x) в выражениях для вероятности ошибки, определяющих помехоустойчивость систем с кодированием и без него. Полагая $k=d_f$, получаем АЭВК $\theta_a = 10 lg R d_f$ (дБ). Величина АЭВК показывает *изменение* минимального расстояния при введении кодирования, характеризует ЭВК при $p \to 0$ и является *верхней границей реального* ЭВК.

Анализ кривых рис.7.5 показывает, что применение СК, декодируемых по алгоритму Витерби с мягким решением, позволяет получить ЭВК 4...6 дБ. Переход к жесткому решению снижает ЭВК примерно на 2 дБ. Квантование выхода демодулятора на четыре уровня снижает ЭВК на (0.7...0.8) дБ, а квантование на восемь уровней – на 0.25 дБ. Обычно ограничиваются квантованием на восемь уровней, используя практически полностью возможности мягкого решения.

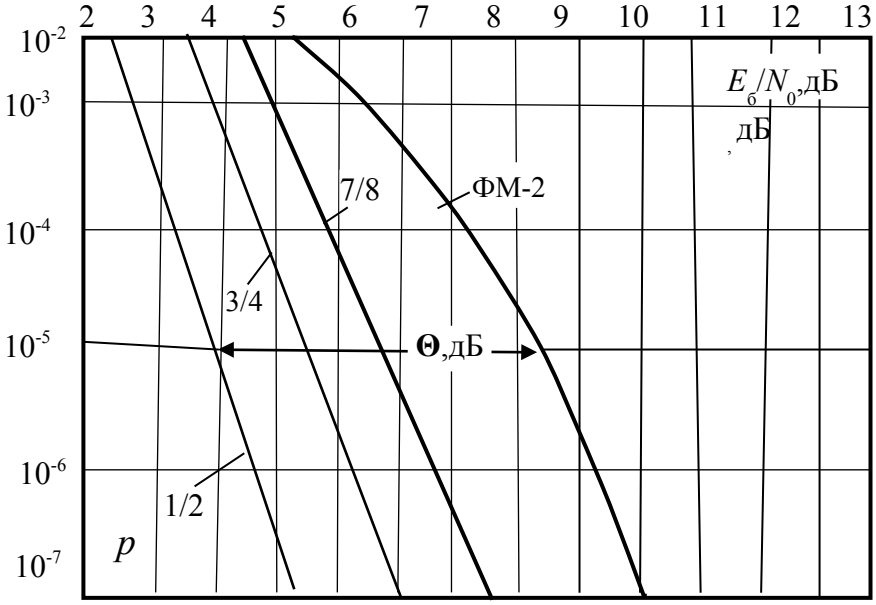


Рисунок 7.5– Помехоустойчивость декодирования СК

8. Алгоритмы

Алгоритм – точное предписание, которое задает вычислительный процес(называемый в этом случае *алгоритмическим*), начинающийся с произвольного *исходного данного,* и направленный на получение полностью определяемого этим исходным данным *результата.* С алгоритмами, т. е. процедурами, однозначно приводящими к результату, математика имела дело всегда. Школьные методы умножения «столбиком» и деления «углом», метод исключения неизвестных при решении системы линейных уравнений, правило дифференцирования сложной функции, способ построения треугольника по трем заданным сторонам – все это знакомые многим алгоритмы.

Перечислим ***основные требования к алгоритмам:***

1. Любой алгоритм применяется к исходным данным и выдает результаты. В привычных технических терминах это означает, что алгоритм имеет *входы* и *вы-*

ходы. Кроме того, в ходе работы алгоритма появляются *промежуточные результаты*, которые используются в дальнейшем. Таким образом, каждый, алгоритм имеет дело с *данными: входными, промежуточными и выходными*. К таким алгоритмическим данным относятся *числа, векторы, матрицы смежностей графов, формулы.*

2. Данные для своего размещения требуют *памяти.* Память обычно считается *однородной и дискретной*, т. е. состоит из одинаковых ячеек, причем каждая ячейка может содержать *один символ* алфавита данных. Таким образом, единицы измерения объема данных и памяти *должны быть согласованы.* При этом память может быть бесконечной. Вопрос о том, нужна ли одна память или несколько и, в частности, нужна ли отдельная память для каждого из трех видов данных, решается по-разному.

3. Алгоритм состоит из отдельных *элементарных шагов,* или *действий,* причем множество различных шагов, из которых составлен алгоритм, *конечно.* Типичный пример множества элементарных действий – система команд ЭВМ. Обычно элементарный шаг имеет дело с фиксированным числом символов, однако, это требование не всегда выполняется. Например, в ЭВМ есть команды типа «память – память», работающие с полями памяти переменной длины.

4. *Последовательность* шагов алгоритма *детерминирована,* т. е. после каждого шага либо указывается, какой шаг делать дальше, либо дается команда остановки, после чего работа алгоритма считается законченной.

5. Естественно от алгоритма потребовать *результативности,* т. е. остановки *после конечного числа шагов* (зависящего от данных) с указанием того, что считать *результатом*. В частности, всякий, кто предъявляет алгоритм решения некоторой задачи, например вычисления функции *f(x),* обязан показать, что алгоритм останавливается после конечного числа шагов (как говорят, *сходится)* для любого *x* из области задания *f.* Однако *проверить сходимость* часто бывает значительно труднее, чем составить собственно алгоритм.

П.8.1. Алгоритм А. Витерби для декодирования сверточных кодов

При оптимальной обработке с целью вынесения решения принятую из канала последовательность символов необходимо сопоставить со всеми возможными передаваемыми последовательностями. Так как число возможных последовательностей n двоичного кода равно 2^n, то при больших длинах последовательностей n декодер становится *неизмеримо сложным (экспоненциальная сложность декодирования),* а оптимальное декодирование – *практически невозможным*. Однако именно при больших n возможно значительное повышение надежности передачи, так как действие шума *усредняется* на длинной последовательности. Поэтому важной является *проблема снижения сложности алгоритмов декодирования*. Известны две группы методов декодирования сверточных кодов.

Алгебраические методы декодирования основаны на использовании *алгебраических свойств* кодовых последовательностей. В ряде случаев эти методы

приводят к простым реализациям кодека. Такие алгоритмы являются *неоптимальными*, так как используемые алгебраические процедуры декодирования предназначены для исправления конкретных (и не всех) конфигураций ошибок в канале. Алгебраические методы отождествляют с *поэлементным приемом* последовательностей, который для кодов с избыточностью, как известно, дает худшие результаты, чем *прием в целом.*

Вероятностные методы декодирования значительно *ближе к оптимальному приему в целом*, так как в этом случае декодер оперирует с величинами, пропорциональными *апостериорным вероятностям*, оценивает и сравнивает *вероятности различных гипотез* и на этой основе выносит решение о передаваемых символах.

Алгебраические алгоритмы оперируют с *конечным алфавитом* входных данных, для получения которых на выходе непрерывного канала необходимо выполнить *квантование.* Чаще всего это *квантование* каждого канального символа *на два уровня* (именуемое в литературе как *жесткое решение* на выходе демодулятора, когда *число уровней L=2*). При этом решение представлено *одним двоичным символом*. Это показано на рис.8.1. При *мягком решении* число уровней квантования *L*>2. При мягком решении выход квантователя *более точно описывает величину отсчета сигнала с помехой*, что повышает помехоустойчивость декодирования.

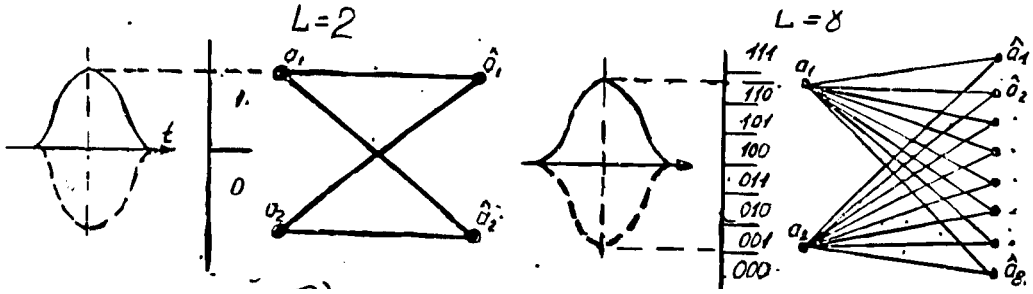


Рисунок8.1 – Жесткое и мягкое решения на выходе демодулятора

Известны два *основных вероятностных алгоритма* декодирования сверточных кодов, а также их различные модификации**.**

Алгоритм последовательного декодирования обеспечивает произвольно малую вероятность ошибки при ненулевой скорости передачи сообщений по каналу. При последовательном декодировании производится *поиск правильного пути* на кодовом дереве, соответствующего переданной информационной последовательности. Последовательное декодирование используется для декодирования *длинных* сверточных кодов.

Другой разновидностью вероятностных алгоритмов является алгоритм, основанный на принципах *динамического программирования* и известный как *алгоритм Витерби*.

Принцип динамического программирования был сформулирован в 1940 г. Р. Беллманом[56]. С тех пор алгоритм нашел широкие приложения в теории управления и теории кодирования. В 1970г. динамическое программирование, в

форме алгоритма декодирования СК (***алгоритма Витерби***), было применено А.Витерби к проблемам телекоммуникации.

Этот алгоритм находит *широкое применение* и *реализует поиск максимально правдоподобного пути* на кодовой решетке с *отбрасыванием части наименее правдоподобных вариантов* путей на каждом шаге декодирования. Алгоритм характеризуется *постоянством вычислительной работы*, однако сложность декодера Витерби *растет*, как при всех переборных алгоритмах, *по экспоненциальному закону* от длины кодового ограничения сверточного кода. *Поэтому алгоритм Витерби используется для декодирования коротких сверточных кодов.*

Рассмотрим алгоритм на примере кода со скоростью 1/*n*.

Пусть, начиная с момента времени t=0, на вход кодера подается информационная последовательность длиной в L символов $\boldsymbol{u_L}=(u_0,u_1,..,u_{L-1})$. На выходе кодера будет последовательность символов $\boldsymbol{a_L}=(a_0,a_1,...,a_{L-1})$. Состояние кодера в момент t определяют как набор из ν информационных символов $\boldsymbol{w_t}=(u_t,u_{t-1},...,u_{L-1})$.

Решетчатая диаграмма кода *однозначно связывает* информационную последовательность $\boldsymbol{u_L}$, последовательность состояний кодера $\boldsymbol{w_t}$ и последовательность символов на его выходе $\boldsymbol{a_L}$.

Каждой ветви $\boldsymbol{a_t}$ в канале соответствует сигнал, который может быть представлен набором координат $\boldsymbol{S_t}=(S_t^{(0)},S_t^{(1)},..,S_t^{(N)})$. В канале действует аддитивная помеха и поступающая на вход декодера последовательность будет $\boldsymbol{X_L}=\boldsymbol{S_L}+\boldsymbol{n_L}$, где $\boldsymbol{S_L}=(S_0, S_1,..., S_{L-1})$, $\boldsymbol{n_L}=(n_0, n_1,.., n_{L-1})$,
где $\boldsymbol{n_L}=(n_t^{(0)},n_t^{(1)},...,n_t^{(N)})$ – N-мерный *вектор помехи.* Декодирование состоит в *прослеживании по кодовой решетке пути с максимальной апостериорной вероятностью.* Декодированный путь можно указать одним из способов:

1. Набором оценок кодовых ветвей $\boldsymbol{S_L}=(S_0, S_1,...,S_{L-1})$, составляющих путь;
2. Последовательностью оценок состояний кодера $\boldsymbol{W_L}=(w_0,w_1, ..., w_{L-1})$;
3. Последовательностью оценок информационных символов на входе кодера $\boldsymbol{U_L}=(u_1,\ldots, u_{L-1})$, которые совпадают с первыми символами оценок состояний $\boldsymbol{S}=(s1,\ldots s_{t-v+1})$. Последовательность $\boldsymbol{X_L}$ будет декодирована с *минимальной вероятностью ошибки*, если из всех возможных путей выбрать оценку $\boldsymbol{S}_L$, для которой *максимальна апостериорная вероятность* $P(\boldsymbol{S_L}/\boldsymbol{X_L})$.

Передачу всех вариантов наборов $\boldsymbol{a_L}$ считают равновероятной. В этом случае декодирование *по критерию максимума апостериорной вероятности равносильно декодированию по критерию максимума правдоподобия,* когда выбирается оценка $\boldsymbol{S_L}$, обеспечивающая выполнение условия $P(\boldsymbol{S}_L/\boldsymbol{X_L})=max$.

В *канале без памяти* условной вероятности $P(\mathbf{S}_L/\boldsymbol{X}_L)$ пропорционально произведение условных плотностей вероятностей суммы сигнала и помехи

$$P(\boldsymbol{X_L}/\boldsymbol{S_L})=\prod_{t=0}^{L-1} p(X_t / S_t) = \prod_{t=0}^{L-1} p(X_t^{(0)}X_t^{(1)}\ldots X_t^{(N)} / S_t^{(0)}S_t^{(1)}\ldots S_t^{(N)}).$$

В *Гауссовском канале* при действии *белого шума* с односторонней спектральной плотностью мощности N_0 каждый сомножитель этого произведения имеет вид:

$$p(X_L / S_L) = (1/\sqrt{\pi N_0})^N \exp\{-[\sum_{i=1}^{N} (X_t^{(i)} - S_t^{(i)})^2]/2N_0\}.$$

Для отыскания максимума прологарифмируем:

$$\ln p(X_L / S_L) = \ln \prod_{t=0}^{L-1} (1/\sqrt{\pi N_0})^N \times$$

$$\times \exp\{-[\sum_{t=1}^{N} (X_t^{(l)} - S_t^{(i)})^2]/2N_0\} = NL \ln(1/\sqrt{\pi N_0}) - \sum_{t=0}^{L-1}\sum_{i=1}^{N} (X_t^{(i)} - S_t^{(i)})^2 / 2N_0.$$

При декодировании выбирают последовательность сигналов $\boldsymbol{S_L}=(S_1,\ldots,S_{L-1})$ и однозначно связанную с ней последовательность ветвей $\boldsymbol{S}_L=(S_0,S_1,\ldots,S_{L-1})$, которая обеспечивает минимум суммы

$$МП = \sum_{t=0}^{L-1}\sum_{i=0}^{N} (X_t^{(i)} - S_t)^2 = \min$$

которая называется *метрикой декодированного пути (*МП*)*. Метрика пути содержит в качестве слагаемых *метрики ветвей*

$$\text{МВ} = \sum_{\text{i-1}}^{\text{N}} (\text{X}_\text{t}^{(\text{i})} - S_t^{(i)})^2.$$

В гауссовском канале *метрика ветви* пропорциональна квадрату Евклидова расстояния между вектором принимаемой суммы сигнала и помехи x_t и вектором сигнала S_t, соответствующего ветви кода a_t. В *дискретном канале* для оценки расстояний используют *метрику Хемминга.*

Периодическая структура решетчатой диаграммы существенно упрощает *сравнение и выбор* путей в соответствии с правилами декодирования. Число состояний на решетке ограничено, и два наугад выбранных достаточно длинных пути имеют, как правило, общие состояния. *Отрезки путей*, входящих в это состояние, *необходимо сравнить* и *выбрать путь с наименьшей метрикой*. Такой путь называется *выжившим.* В соответствии с ***алгоритмом Витерби***, такое сравнение и отбрасывание отрезков путей производится *периодически, на каждом шаге декодирования*. Рассмотрим декодирование кода (7,5), символы которого передаются по дискретному каналу (см. рис. 8.2).

В этом случае метрика ветви (МВ) равна расстоянию Хэмминга между набором символов ($x^{(1)}x^{(2)}$) на входе декодера и набором символов ($a^{(1)}a^{(2)}$), соответствующих данной ветви на решетчатой диаграмме. Если ($x^{(1)}\,x^{(2)}$)=01, то значения МВ для кода (7,5) с решеткой, изображенной на рис.8.2 а, будут МВ(00)=1, МВ(01)=0, МВ(11)=1 и МВ(10)=2.

Метрика пути (МП) есть *сумма метрик ветвей*, образующих некоторый путь на решетчатой диаграмме. Путь конечной длины оканчивается в определенном состоянии. Метрика состояния (МС) равна МП, который заканчивается в данном состоянии.

Шаг декодирования состоит в обработке декодером принимаемых из канала данных в интервале между двумя соседними *уровнями узлов.*

На рис. 8.2 б...8.2 ж показано развитие процесса декодирования символов СК со скоростью 1/2 и длиной кодирующего регистра K=3. На вход декодера поступают пары символов из канала: 11, 10, 00, 11, 01…(декодирование с *жестким решением*). Цифрами около ветвей обозначены метрики ветвей, цифры в кружках обозначают метрики состояний.

В начальный момент времени полагаем, что декодер находится в состоянии 00 и исходная метрика этого состояния МС(00)=0 (рис.8.2 а). Если из канала поступили символы 11, то метрики ветвей 00 и 11, выходящих из этого состояния, будут МВ(00)=2 и МВ(11)=0. Это отмечено на первом шаге декодирования. Так как других ветвей, выходящих из состояния 00 и 11, нет, то метрики этих состояний принимаются равными метриками входящих ветвей МС(00)=2 и МС(10)=2.

——Аналогичная картина имеет место и на следующем шаге декодирования, когда из канала поступает пара символов 10. Здесь МВ(00)=1, МВ(11)=1, МВ(10)=0 и МВ(01)=2. Метрики состояний на этом шаге определяются теперь как суммы метрик входящих ветвей с метриками предыдущих состояний: МС(00)=2+1=3; МС(10)=2+1=3; МС(01)=0+0=0 и МС(11)=0+2=2.

На этом процесс развития решетчатой диаграммы для данного кода заканчивается. Далее алгоритм заключается в *повторении одного основного шага*. На каждой из последующих диаграмм рис. 8.2 этот шаг изображен подробно. К началу *i*-го шага в *памяти декодера* хранятся *метрики состояний*, вычисленных на предыдущем этапе:

$$MC^{i-1}(00),\ MC^{i-1}(10),\ MC^{i-1}(01),\ MC^{i-1}(11).$$

Аналогичная картина имеет место и на следующем шаге декодирования, когда из канала поступает пара символов 10. Здесь МВ(00)=1, МВ(11)=1, МВ(10)=0 и МВ(01)=2. Метрики состояний на этом шаге определяются теперь как суммы метрик входящих ветвей с метриками предыдущих состояний: МС(00)=2+1=3; МС(10)=2+1=3; МС(01)=0+0=0 и МС(11)=0+2=2.

—На этом процесс развития решетчатой диаграммы для данного кода заканчивается. Далее алгоритм заключается в *повторении одного основного шага*. На каждой из последующих диаграмм рис. 8.2 этот шаг изображен подробно. К началу *i*-го шага в *памяти декодера* хранятся *метрики состояний*, вычисленных на предыдущем этапе:

$MC^{i-1}(00),\ MC^{i-1}(10),\ MC^{i-1}(01),\ MC^{i-1}(11).$

По принятым канальным символам производится вычисление метрик ветвей $MB^{i}(00)$, $MB^{i}(11)$, $MB^{i}(10)$ и $MB^{i}(01)$ и формирование четырех новых метрик состояний $MC^{i}(00)$, $MC^{i}(10)$, $MC^{i}(01)$ и $MC^{i}(11)$

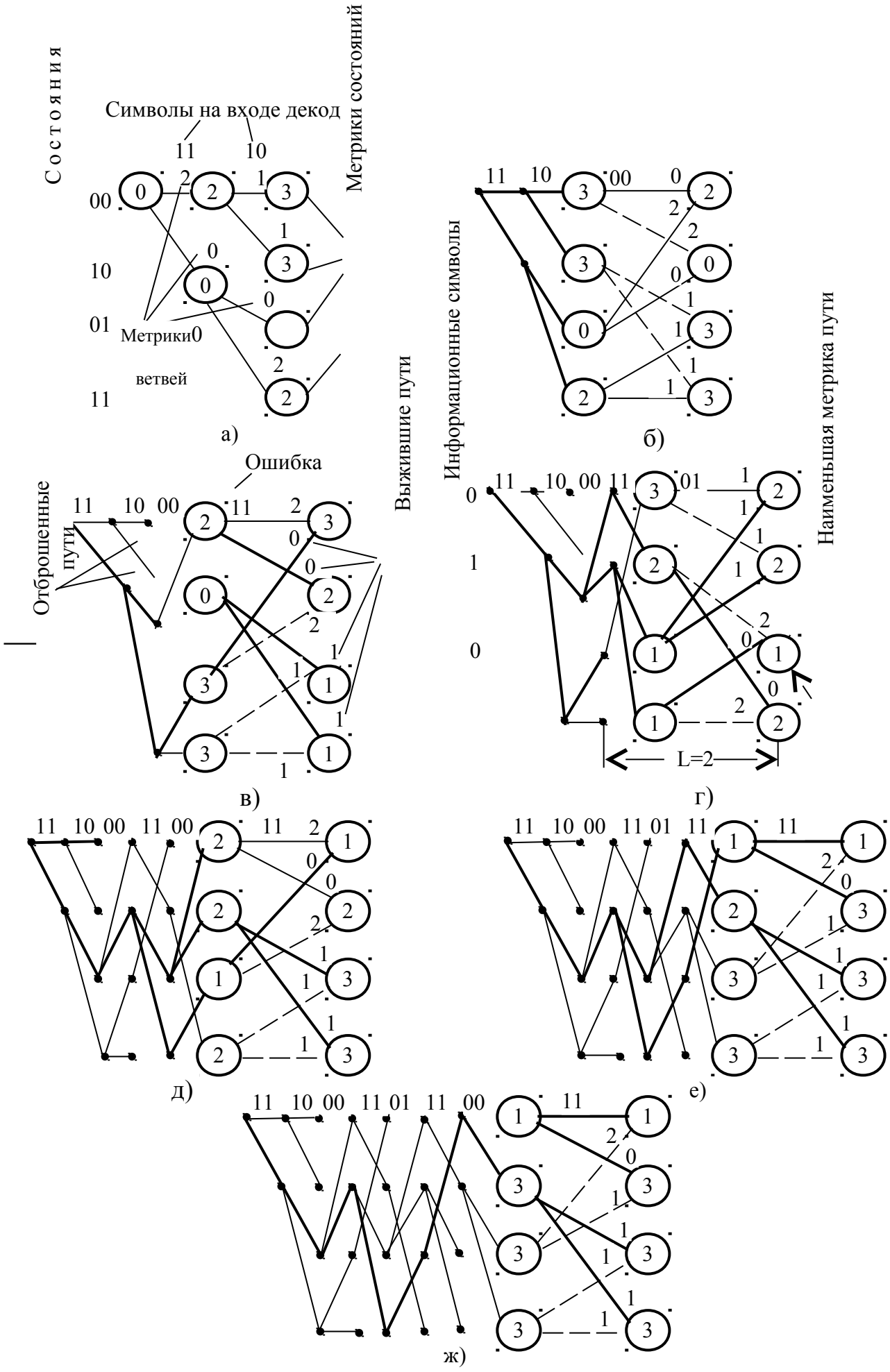


Рисунок 8.2 – декодирование кода (7,5)

К примеру, к состоянию 00 ведут пути из предыдущих состояний 00 и 01. *На i-м шаге декодирования* декодер вычисляет метрики путей как суммы метрик предыдущих состояний и метрик входящих ветвей:

$$MC^i(00)\begin{cases} \text{Мп}^i(00) = MC^{i-1}(00) + MB^i(00) \\ Mn^i(00) = MC^{i-1}(01) + MB^i(11), \end{cases}$$

$$MC^i(01)\begin{cases} Mn^i(01) = MC^{i-1}(10) + MB^i(10) \\ Mn^i(01) = MC^{i-1}(11) + MB^i(01), \end{cases}$$

$$MC^i(10)\begin{cases} Mn^i(10) = MC^{i-1}(00) + MB^i(11) \\ Mn^i(10) = MC^{i-1}(01) + MB^i(00), \end{cases}$$

$$MC^i(11)\begin{cases} \text{Мп}^i(11) = MC^{i-1}(10) + MB^i(01) \\ Mn^i(11) = MC^{i-1}(11) + MB^i(10). \end{cases}$$

Далее производится *попарное сравнение* метрик путей, входящих в каждое из состояний (пары показаны фигурными скобками). В результате сравнения *выбирается меньшая метрика,* и она считается метрикой данного состояния для последующего шага декодирования. Путь, входящий в данное состояние с меньшей метрикой, считается *выжившим.* На рис. 8.2 отрезки выживших путей показаны *сплошной линией*. Пути, входящие в состояния с большими метриками, считаются *отмершими* (*оборванными*). Они показаны на решетчатой диаграмме пунктиром.

Таким образом, на каждом шаге декодирования в соответствии с алгоритмом Витерби, в каждом из состояний решетчатой диаграммы производятся ***однотипные операции*:**

1) ***Сложение метрик*** предыдущих состояний с метриками соответствующих ветвей.

2) ***Сравнение метрик*** входящих путей.

3) ***Выбор путей*** с наименьшими метриками, величины которых используются как метрики состояний на последующем шаге декодирования. Если метрики сравниваемых путей одинаковы, то выбор одного из двух путей производится *случайным образом.*

На каждом шаге декодирования половина возможных продолжений путей *отбрасывается.* Другая половина образует *продолжения путей* для следующего шага декодирования, на котором вновь появляются два варианта продолжения каждого пути. Это обеспечивает *постоянство количества вычислений*, производимых на каждом шаге. Декодер прослеживает по кодовой решетке путь, имеющий *минимальное расстояние от пути,* который порождает кодер.

Таким образом, декодер, выбирающий на решетчатой диаграмме путь с наименьшей метрикой, *минимизирует вероятность ошибки* P_0. Поскольку при декодировании анализу подвергаются последовательности конечной длины *L,* алгоритм *не является строго оптимальным.* Результаты расчетов и моделирова-

ния показывают, что при соответствующем выборе величины $L>(6…7)\nu$ можно получить результаты декодирования, достаточно близкие к оптимальным.

На рис. 8.3 показана структурная схема декодера Витерби, предназначенного для работы с демодулятором сигналов ФМ-4.

Декодер состоит из АЦП в каналах *X* и *Y*, вычислителя метрик ветвей, процессора, устройства памяти путей, которые выжили, и мажоритарного элемента МЕ.

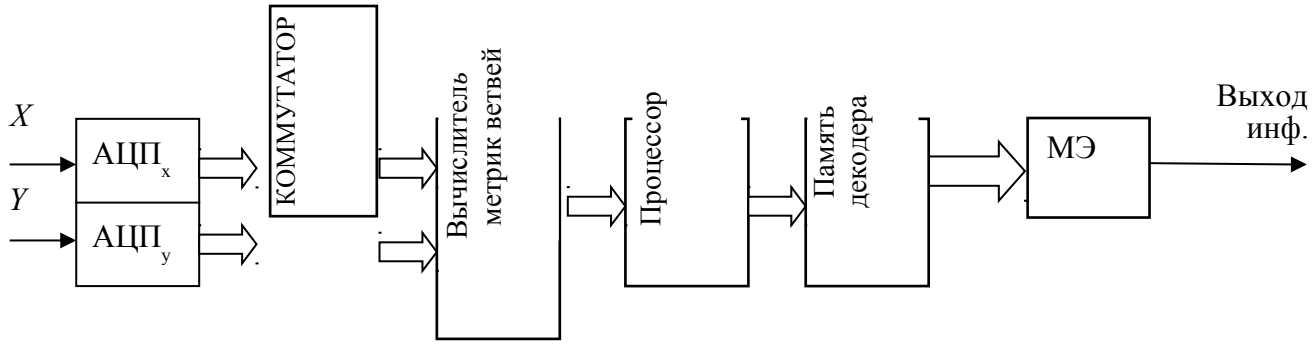


Рисунок 8.3 – Структурная схема декодера Витерби

9.1. Асимптотические свойства сферических упаковок многомерных сигналов

Эффективные методы модуляции и помехоустойчивого кодирования все шире используются в современных телекоммуникационных системах (ТС). Переход к ансамблям многопозиционных сигналов *увеличивает информационную скорость* и обеспечивает передачу больших потоков информации. Современная элементная база позволяет применять достаточно *сложные методы модуляции* и помехоустойчивого кодирования и обеспечивать тем самым *высокую верность передачи.*

Как известно, теория сигналов и теория кодирования длительное время развивались независимо. В последние годы значительно возрос интерес к новому перспективному направлению, возникшему на стыке этих наук. Интенсивно исследуются возможности ТС, в которых для передачи информации используются *ансамбли многопозиционных сигналов* в сочетании с помехоустойчивыми кодами, причем *процедуры модуляции/кодирования* (*демодуляции/декодирования*) осуществляются *совместно.*

При рациональном построении такие *сигнально-кодовые конструкции* (СКК) сочетают в себе положительные качества как многопозиционных ансамблей, так и помехоустойчивых кодов, допускают достаточно простые и реализуемые на практике алгоритмы декодирования и позволяют существенно продвинуться к *теоретическим пределам эффективности.* Вопросы синтеза таких систем модуляции/кодирования, анализа их структуры, помехоустойчивости и эффективности, сложности демодуляции-декодирования составляют основное содержание нового перспективного направления в теории связи – *теории сигнально-кодовых конструкций.* В работе [22] исследован достаточно обширный класс

конструкций, названных *групповыми сигнально-кодовыми конструкциями.* В групповых СКК используются ансамбли *многопозиционных сигналов,* задаваемых множеством элементов, образующих алгебраическую группу и линейные внешние коды. Наличие групповых свойств обуславливает важные структурные особенности последовательностей сигналов СКК. Прежде всего, *групповые СКК обладают набором метрических симметрий,* что, как и в теории линейных кодов, существенно облегчает построение (*синтез)* СКК, анализ их структуры и характеристик, а также разработку алгоритмов декодирования и исследование помехоустойчивости приема СКК. В общем случае целью построения СКК является получение ансамблей (длинных последовательностей) сигналов, обеспечивающих передачу сообщений по каналу с помехами с высокой энергетической эффективностью и большой удельной скоростью, допускающих при этом достаточно простые алгоритмы декодирования. Известно, что достижение этих показателей возможно при увеличении, в общем случае, *размерности пространства сигналов.* Ниже рассмотрены некоторые свойства *многомерных сигналов в пространствах большой размерности.* Рассмотрим передачу сигнала произвольной формы $s(t)$ на фоне аддитивного гауссовского белого шума $n(t)$ со спектральной плотностью мощности N_0. Сигнал и помеху представим в ортонормированном базисе $\{\psi_k(t)\}_{k=1}^{N}$, где $\psi_k(t)$ – базисная функция, N – размерность базиса. Тогда

$$s(t)=\sum_{k=1}^{N} s_k \cdot \psi_k(t), \quad n(t)=\sum_{k=1}^{N} n_k \cdot \psi_k(t). \tag{9.1}$$

Здесь вектор сигнала $\bar{s}=(s_1\ s_2\ \dots\ s_N)$ содержит набор координат сигнала, а вектор помехи $\bar{n}=(n_1\ n_2\ \dots\ n_N)$ содержит набор случайных чисел – координат помехи с дисперсиями $D\{n_k\}=N_0/2$. Геометрическая трактовка задачи различения двух сигналов $\bar{s}_i$ и $\bar{s}_j$ представлена на рис. 9.1. Ошибка при передаче сигнала $\bar{s}_i$ происходит всякий раз, когда проекция n_{ij} вектора помехи $\bar{n}$ превышает половину расстояния d_{ij} , т. е. $n_{ij}>d_{ij}/2$.

Шумовой вектор $\bar{n}$ имеет равновероятное по всем направлениям распределение, окружая точку (конец вектора $\bar{s}$) "*шумовой сферой"*.

Представляет интерес проанализировать изменение параметров этой сферы при $N\to\infty$.

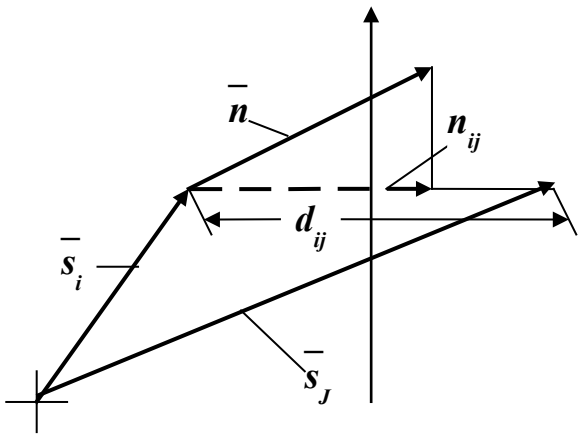


Рисунок 9.1 – Геометрическое представление задачи различения сигналов

Не изменяя стати ıала и помехи (11.1), будем увеличивать размерность пространства N.При этом энергия

сигнала $E_s=\sum_{k=1}^{N} s_k^2$ и энергия помехи $E_n=\frac{N_0}{2}N$ возрастают (векторы $\bar{s}$ и $\bar{n}$ на рис.9.1 удлиняются). Выполним нормировку, перейдя к векторам

$$\tilde{\bar{s}} = \left(\frac{s_1}{\sqrt{N}} \frac{s_2}{\sqrt{N}} \cdots \frac{s_N}{\sqrt{N}} \right) \quad \text{и} \quad \tilde{\bar{n}} = \left(\frac{n_1}{\sqrt{N}} \frac{n_2}{\sqrt{N}} \cdots \frac{n_N}{\sqrt{N}} \right). \tag{9.2}$$

При этом энергии нормированных векторов будут равны

$$\tilde{E}_s = \frac{1}{N}\sum_{k=1}^{N} s_k^2 \quad \text{и} \quad \tilde{E}_n = \frac{N_0}{2}, \tag{9.3}$$

а на векторной диаграмме векторы нормированных сигналов будут иметь постоянную и не зависящую от N длину.

Вектор нормированной помехи $\tilde{\bar{n}}$ случаен и в результате нормировки имеет квадрат нормы, величина которого постоянна и также не зависит от N:

$$\left\|\tilde{\bar{n}}\right\|^2 = \tilde{E}_n = = N_0/2. \tag{9.4}$$

Вместе с тем, дисперсия квадрата нормы зависит от N. Вычислим дисперсию $D\left\{\left\|\tilde{\bar{n}}\right\|^2\right\} = D\left\{\frac{1}{N}\sum_{k=1}^{N} n_k^2\right\} = \frac{1}{N^2}\sum_{k=1}^{N} D\left\{n_k^2\right\}$, поскольку отсчеты помехи при ее представлении в ортогональном базисе независимы.

Дисперсия квадрата каждого отсчета n_k, $k=\overline{1,N}$ будет

$$\mathrm{D}\left\{\mathrm{n_k^2}\right\} = \mathrm{M}\left\{\left[\mathrm{n_k^2} - \mathrm{M}\left\{\mathrm{n_k^2}\right\}\right]^2\right\} = \mathrm{M}\left\{\mathrm{n_k^4}\right\} - 2\mathrm{M}\left\{\mathrm{n_k^2}\cdot\mathrm{M}\left\{\mathrm{n_k^2}\right\}\right\} + \mathrm{M}\left\{\left[\mathrm{M}\left\{\mathrm{n_k^2}\right\}\right]^2\right\}, \tag{9.5}$$

где $M\{\cdot\}$ – знак математического ожидания случайной величины. Отсчеты n_k имеют нормальное распределение с нулевым математическим ожиданием и дисперсией $\sigma^2=N_0/2$. Учитывая, что математическое ожидание четвертой степени гауссовской случайной величины равно

$M\left\{n_k^4\right\} = \frac{1}{\sqrt{2\pi}\,\sigma}\int_{-\infty}^{\infty} x^4 \mathrm{e}^{-\frac{x^2}{2\sigma^2}}\,\mathrm{dx} = 3\sigma^4$, а математическое ожидание квадрата случайной величины есть дисперсия $M\left\{n_k^2\right\}=\sigma^2=N_0/2$, выражение (9.5) можно привести к виду $D\left\{n_k^2\right\} = \frac{N_0^2}{2}$. Тогда дисперсия квадрата нормы вектора $\tilde{\bar{n}}$ будет иметь вид

$$D\left\{\left\|\tilde{\bar{n}}\right\|^2\right\} = \frac{1}{N^2}\sum_{k=1}^{N} D\left\{n_k^2\right\} = \frac{1}{N}\cdot\frac{N_0^2}{2}. \tag{9.6}$$

Таким образом, с ростом размерности пространства N наряду с увеличением длин векторов сигналов возрастают и средние радиусы шумовых сфер, окружа-

ющих каждый из сигналов. Но *флуктуации* размеров шумовых сфер относительно их средних размеров асимптотически *уменьшаются.* Имеет место явление "*затвердевания сферы",* отмеченное еще в монографии [17].

Нетрудно показать, что асимптотически уменьшается также *вероятность выхода* вектора шума за пределы собственной шумовой сферы. Действительно, если $\|\tilde{\tilde{n}}\|^2$ – квадрат нормы случайного вектора шума, создающего шумовую сферу, и $M\{\|\tilde{\tilde{n}}\|^2\}$ – среднее значение квадрата радиуса этой сферы, то вероятность выхода за пределы кольца шириной 2Δ в соответствии с неравенством Чебышева оценивается сверху следующим образом:

$$P\left\{\left|\|\tilde{\tilde{n}}\|^2 - M\{\|\tilde{\tilde{n}}\|^2\}\right| \geq \Delta\right\} \leq \frac{D\{\|\tilde{\tilde{n}}\|^2\}}{\Delta^2} = \frac{1}{N}\cdot\frac{N_0^2}{2\Delta^2}. \qquad (9.7)$$

При конечной "*толщине"* кольца Δ верхняя граница в выражении (9.7), а, следовательно, и вероятность выхода за его пределы с ростом размерности N асимптотически стремится к 0 при любом уровне шума. Рис. 9.2 поясняет общее правило выбора сигналов, обеспечивающих безошибочную передачу при заданном уровне помех. Каждая сигнальная точка окружена *шумовой сферой*, радиус которой R_N определяет половину наименьшего расстояния между ближайшими сигналами.

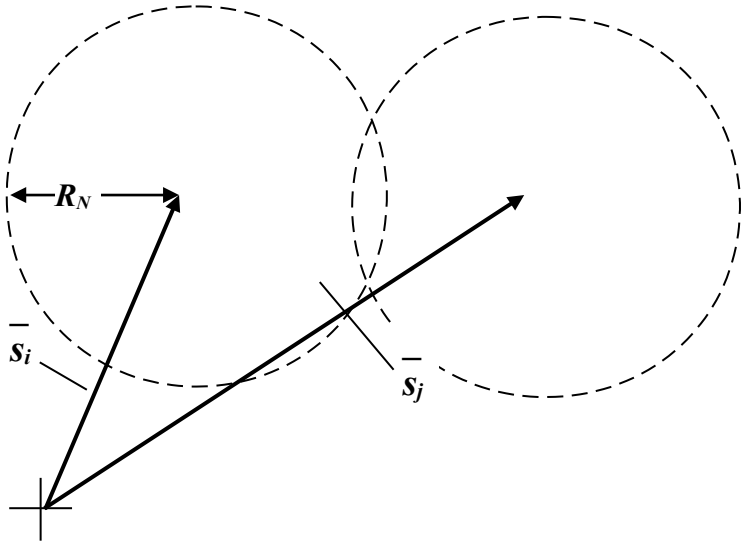


Рисунок 9.2 – Пересечение шумовых сфер

Очевидно, что шумовые сферы соседних сигналов *не должны пересекаться* (на рис. 9.2 сферы пересекаются).Оптимальное расположение шумовых сфер, обеспечивающее размещение наибольшего их числа в заданном объеме N-мерного пространства, формулируется в теории сигналов как ***задача плотнейшей упаковки сфер.***

В теории сигналов известны два вида расположения сигнальных сфер в пространстве сигналов:

1. **ОСУ** – объемно–сферическая укладка, при которой сигнальные сферы располагаются *как на поверхности гиперсферы, так и внутри нее;*

2**. ПСУ** – поверхностно–сферическая укладка, при которой сигнальные сферы располагаются *только на поверхности гиперсферы.*

Объем и площадь поверхности гиперсферы радиуса R в пространстве размерности N определяются выражениями [19]:

$$V_N = (\pi^{N/2}R^N)/\Gamma(N/2+1), \quad S_N = (2\pi^{N/2}R^{(N-1)})/\Gamma(N/2)\,. \qquad (9.8)$$

Анализ показывает, что при больших размерностях пространства сигналов ***объем гиперсферы в основном сосредоточен у ее поверхности.*** На рис. 9.3 в сферу радиуса R вписана сфера с меньшим радиусом $R(1-\Delta)$,
где $0 \le \Delta \le 1$.

Объем вписанной сферы определяется выражением:

$$V_N(\Delta)=(\pi^{N/2}R^N(1-\Delta)^N)/\Gamma(N/2+1).$$

Величина этого объема по сравнению с полным объемом гиперсферы радиуса R определится величиной $\delta_N(\Delta)=(1-\Delta)^N$.

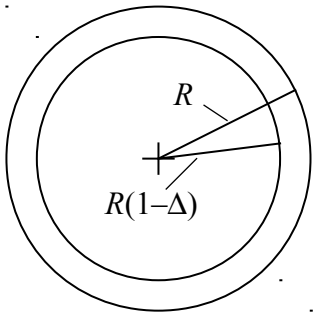


Рисунок 9.3 – Объем сферы N измерений
сосредоточен у ее поверхности

Анализ показывает, что уже при $N>10$ объем вписанной сферы составляет *малую долю* от полного объема гиперсферы. Соответственно, при расположении сигнальных сфер внутри гиперсферы значительная доля сигналов будет располагаться у поверхности, образуя *поверхностно-сферическую укладку.* С ростом размерности пространства *доля сигналов*, дополняющих укладку до объемно-сферической, *будет незначительной*. Вместе с тем, известно, что реализация ансамблей сигналов с поверхностно-сферической укладкой *предпочтительней*, поскольку изменение амплитудного масштаба не изменяет форм областей правильного приема при демодуляции/декодировании СКК. Отмеченное выше свойство расположений сигнальных сфер при больших размерностях гиперсфер подтверждает ***целесообразность использования ПСУ*** в конструкциях большой размерности. При этом потери скорости передачи информации, обусловленные неиспользованием «*внутренней части»* объема гиперсферы будут незначительными и *асимптотически стремятся к нулю* с ростом размерности СКК**.**

9.2. Сигнально-кодовые конструкции

В современных телекоммуникационных системах для повышения скорости передачи информации по каналу связи широко используются *многопозиционные сигналы*. Переход к многопозиционным сигналам позволяет повысить удельную скорость передачи информации. Типичные примеры ансамблей двумерных многопозиционных сигналов показаны на рис.9.5. Однако, при этом снижается помехоустойчивость, поскольку с ростом числа позиций расстояния между сигналами уменьшаются. Для компенсации ухудшения помехоустойчивости *целесообразно использовать корректирующие коды*. Поскольку большинство известных хороших кодов относится к категории двоичных, возникает *задача согласования двоичных корректирующих кодов с недвоичными ансамбями сигналов.* Одним из возможных способов согласования является применение *модуляционного кода Грея*. Однако расчеты и результаты моделирования такого способа согласования показали *низкую его эффективность*. В работах [19…22] был предложен *метод согласования,* положенный в основу построения *сигнально – кодовых конструкций (СКК*). Метод оказался эффективным и в настоящее время *повсеместно используется.*

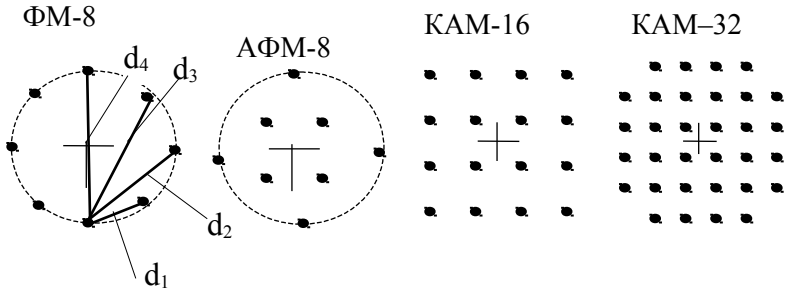


Рисунок 9.4 – Многопозиционные ансамбли неэквидистантных сигналов

Основная концепция построения сигнально-кодовых конструкций основана на использовании *свойств симметрии и групповых свойств* многопозиционных ансамблей сигналов. На рис. 9.4 показаны примеры многопозиционных двумерных ансамблей с числом позиций сигналов M=(8…32):

– Фазовой модуляции ФМ-8.

– Амплитудно-фазовой модуляции АФМ-8.

– Квадратурной амплитудной модуляции КАМ-16, КАМ-32.

Плотное расположение сигнальных точек обеспечивает *высокую удельную скорость.* Однако, *плотные ансамбли не эквидистантны:* в ансамбле ФМ-8.

Евклидовы расстояния между ближайшими сигнальными точками возрастают:$d_1\langle d_2\langle d_3\langle d_4$.

Используем метод *декомпозиции* ансамбля неэквидистантных сигналов, состоящий в том, что исходный ансамбль *раскладывается* на набор *вложенных ансамблей* (подансамблей, каждые точки которых принадлежат исходному ансамблю), причем, расстояния между сигнальными точками в подансамблях d_i должны подчиняться неравенству:$d_{\min}\langle d_i\langle d_{\max}$, где $d_{\max}$,$d_{\min}$ – максимальное и минимальное расстояния ансамбля.

При построении сигнально-кодовых конструкций принадлежность к подансамблям кодируется набором *внешних кодов* с возрастающими кодовыми расстояниями, которые выбираются таким образом, чтобы *выровнять все результирующие расстояния.*

Непременным элементом синтеза новых СКК является *декомпозиция* (разложение) ансамбля канальных сигналов на *набор вложенных подансамблей.* Сказанное иллюстрируется примером разбиения ансамбля ФМ-8, представленном на рис.11.6, где показано разбиение исходного ансамбля $\boldsymbol{A_0}$ на вложенные подансамбли $\boldsymbol{B_0}$ и $\boldsymbol{B_1}$, с последующим разбиением, соответственно, на вложенные ансамбли $\boldsymbol{C_1}$,$\boldsymbol{C_2}$ и $\boldsymbol{C_3}$ (при этом расстояния в ансамблях возрастают $d_A \langle d_B \langle d_C$).

В многочисленных работах по СКК такое разложение производится *эвристически*. В работе [26] отмечено, что декомпозиция может *эффективно выполняться с использованием групповых свойств ансамблей сигналов*. Структура всей СКК имеет вид, представленный на рисунке 9.5 Если исходный ансамбль, содержащий $M=2^m$ сигналов, разложен на 2^n подансамблей, то выбор сигнала подансамбля производится символами сверточного кода со скоростью $R=k/n$, а выбор подансамбля производится (m-n) символами безизбыточного кода.

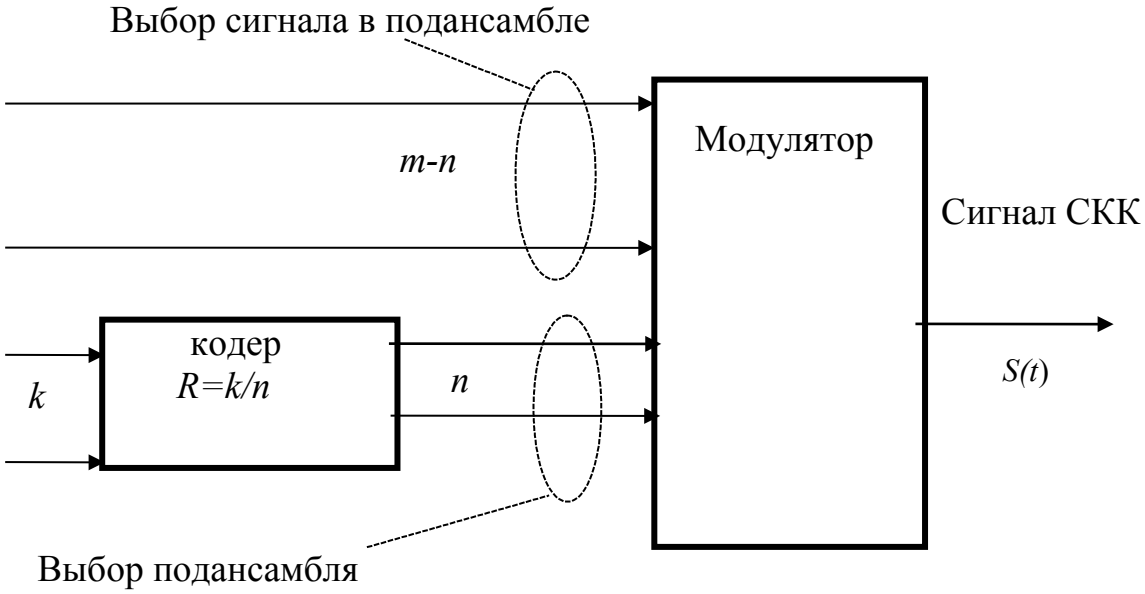


Рисунок 9.5 – Структура СКК

В целом удельная скорость такой СКК оказывается равной

$$\gamma_N=(\log_2 M)/N. \qquad (9.9)$$

Эвристические методы декомпозиции основаны на использовании "очевидных" свойств симметрии многопозиционных ансамблей и на последующем "*прореживании"* ансамблей при переходе к ансамблям более низкого уровня, минимальные расстояния в которых вследствии этого возрастают. Сказанное иллюстрируется примером разбиения ансамбля ФМ-8 из работы [21], представленным на рис.9.6, где показано разбиение исходного ансамбля $\boldsymbol{A_0}$ на вложенные подансамбли $\boldsymbol{B_0}$ и $\boldsymbol{B_1}$, с последующим разбиением, соответственно, на вло-

женные ансамбли $\boldsymbol{C}_1$, $\boldsymbol{C}_2$ и $\boldsymbol{C}_4$ (при этом расстояния в ансамблях возрастают:$d_A\langle \mathrm{d}_B\langle d_C$).

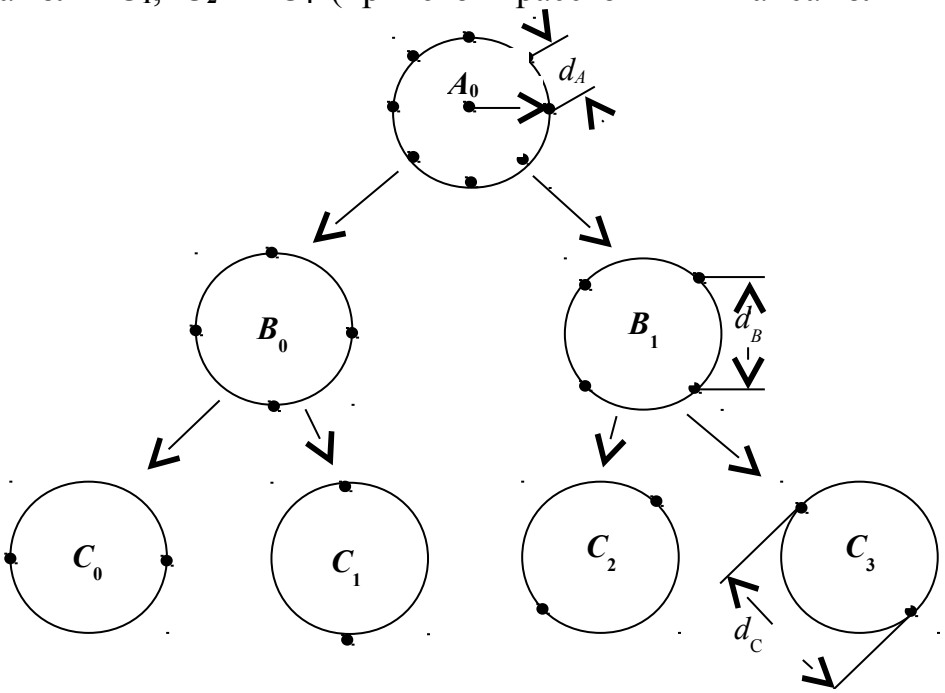


Рисунок9.6 – Разбиение ансамбля ФМ-8 из работы [21]: расстояния в подансамблях *A*,*B*,и *C* возрастают:$\langle \mathrm{d}_A\langle d_B\langle d_C$.

Регулярный метод декомпозиции основан на использовании свойств симметрии групповых ансамблей сигналов. Как показано в работе [22] многие практически важные ансамбли могут быть описаны в терминах *теории алгебраических групп*. Сказанное поясним на примере ансамбля ФМ-8 (рис. 9.7), который задается начальным вектором

$$\boldsymbol{S}_0=(s_{01};s_{02}), \tag{9.10}$$

с кординатами в двухмерном пространстве:$s_{01=E}{}^{1/2}$, s_{02}=0 (*E*–энергия сигнала), и ортогональной матрицей

$$\boldsymbol{M}= \begin{bmatrix} \mathrm{Cos}\theta & \mathrm{Sin}\theta \\ -\mathrm{Sin}\theta & \mathrm{Cos}\theta \end{bmatrix} . \tag{9.11}$$

Умножение начального вектора (11.10) на матрицу(9.11) определяет пространственный поворот вектора сигнала на угол Θ, т.е. $\boldsymbol{S}_0\boldsymbol{M}=\boldsymbol{S}_\Theta=(s_{01}\cos\Theta,0)$, а все возможные сигналы ансамбля ФМ-8 можно получить путем умножения начального вектора (11.10) на набор из степеней матрицы (9.11):

$$\mathbf{G}(M)= \{\boldsymbol{M}^0,\boldsymbol{M}^1\ldots\boldsymbol{M}^i\ldots\boldsymbol{M}^{(M-1)}\}, \tag{9.12}$$

в котором показатель степени *i* при объеме ансамбля *M*=8 изменяется в пределах от 0 до величины (*M*–1)=7. При этом угловой разнос между соседними векторами в ансамбле ФМ-8 будет равен $\Theta=2\pi/M$.

Нетрудно заметить, что набор степеней матрицы $\boldsymbol{M}$ вида (9.12) образует *мультипликативную циклическую алгебраическую группу*, с операцией умножения матриц, степени которых равны целым числам, определяемым сложением

показателей степеней перемножаемых матриц по правилам сложения целых чисел по модулю *M*. Этой группе изоморфна *аддитивная циклическая группа целых чисел* с операцией сложения по модулю *M:*

$$\boldsymbol{G_0}(8)=\{0,1,2..i\ldots(M-1)\}. \qquad (9.13)$$

Изоморфизм групп (9.12) и (9.13) облегчает решение задачи декомпозиции ансамбля сигналов ФМ-8. Алгебраическая группа $\boldsymbol{G_0}$ *(8)* содержит набор вложенных подгрупп, определяемый композиционным рядом:

$$\mathbf{S_H}(8)=\{\boldsymbol{G_0}(8\ э\boldsymbol{H_0}(4)\ э\boldsymbol{H_0}(4)\ э\boldsymbol{H_0}(2)\}, \qquad (9.14)$$

где *э* – символ принадлежности (*вложенности*). Композиционный ряд вида(11.14) задает последовательность декомпозиции. В табл. 9.1 представлены элементы исходной группы $\boldsymbol{G_0}(8)$ и вложенных подгрупп $\boldsymbol{H_0}(4)$ и $\boldsymbol{H_0}(2)$ с порядками 8, 4, 2, соответственно. Кроме этого, в таблице показаны *смежные-классы* этих подгрупп, полученные по правилам разложения группы по подгруппе на смежные классы. Классы этих подгрупп, получены по правилам разложения группы по подгруппе на смежные классы.

Изложенное выше позволяет сформулировать ***алгоритм регулярного метода декомпозиции:***

1.Декомпозиции подлежит ансамбль сигналов, обладающий групповыми свойствами.

2.Отыскивается ***композиционный ряд*** алгебраической группы ансамбля сигналов.

3.Отыскивается *вложеннная подгруппа* (наименьшего порядка) группы сигнального ансамбля, свойства которой и определяют свойства вложенного ансамбля наименьшего объема.

Наглядный пример реализации этого алгоритма показан на рис. 9.7. Вложенная подгруппа наименьшего порядка $H_0(2)$содержит два символа 0 и 4, которые и определяют степени матриц поворота из ряда(9.12) и, соответственно, углы векторов сигналов $0\bullet\Theta=0$ и $4\bullet\Theta=\pi$.

Таблица 9.1 – Разложение группы на смежные классы

$G_0(8)$	$H_0(4)$	$C_1(4)$	$H_0(2)$	$C_1(2)$	$C_3(2)$	$C_6(2)$
0	0	1	0	1	3	6
1						
2	2	3				
3	4	5	4	5	7	2
4						
5						
6	6	7				
7						
8						

Аналогично, подансамбли второго уровня разложения определяются подгруппой $H_0(2)$ и ее смежными классами $C_3(2)$ и $C_6(2)$**,** а ансамбли первого уровня разложения определяются подгруппой $H_0(4)$ и ее смежным классом. Следует отметить, что дистанционные свойства ансамблей на каждом из уровней декомпозиции остаются *одинаковыми,* поскольку образование любого смежного класса производится путем *пространственного поворота ансамбля*, соответствующего подгруппе на угол **l•Θ** , где **l**–образующий смежного класса. Это и доказывает *свойства инвариантности декомпозиции*.

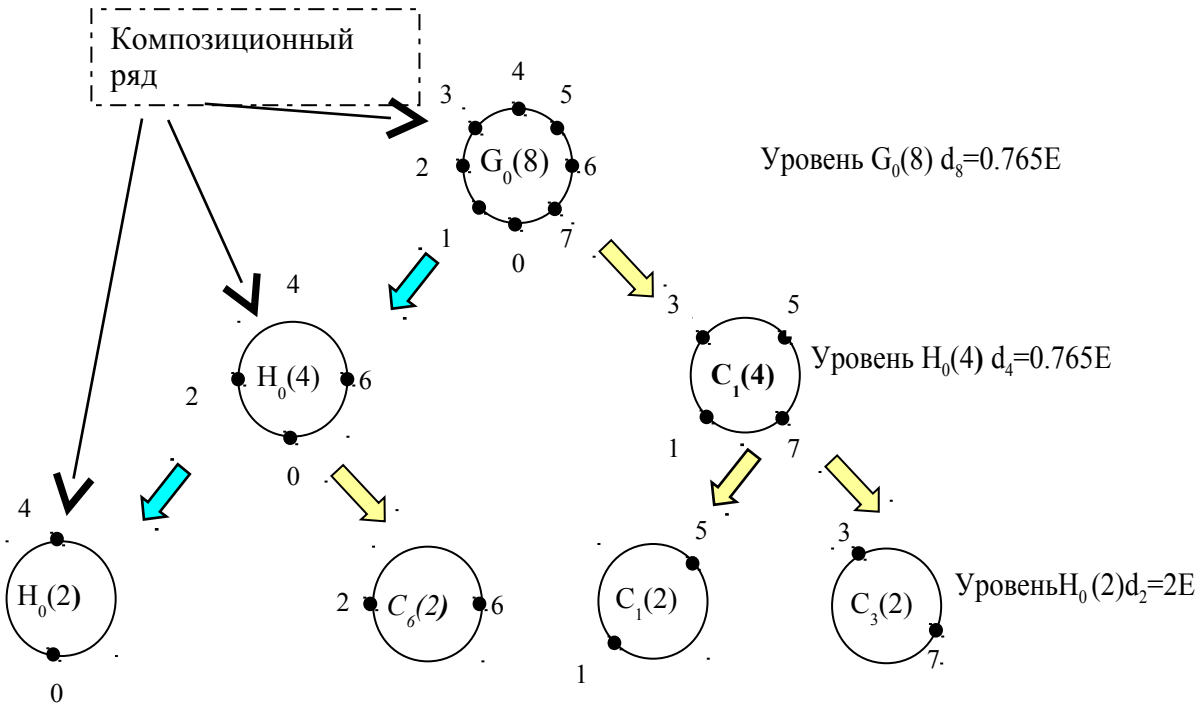


Рисунок 9.7 – Декомпозиция группового ансамбля ФМ-8

На рис. 9.8 приведены результаты расчетов эффективности многопозиционных сигналов и сигнально-кодовых конструкций на их основе[12]. Эффективность систем принято оценивать *показателями эффективности:*
энергетической эффективности

$$\beta = \frac{R}{P_c / N_0}, \qquad (9.15)$$

и удельной скорости γ_N=R/N,
где: R – скорость передачи информации;
P_c – мощность сигнала;
N_0 – спектральная плотность мощности шума;
N –размерность пространства сигналов.

Расчеты произведены для СКК с сигналами, представленными на рисунке 11.5 и количеством сигналов в ансамбле *M*=(4…32). Видно, что применение сигнально-кодовых конструкций описанного выше типа позволяет существенно продвинуться (по сравнению с применением некодированных ФМ и АФМ сиг-

налов) к предельным границам эффективности, определяемым пределом Шеннона.

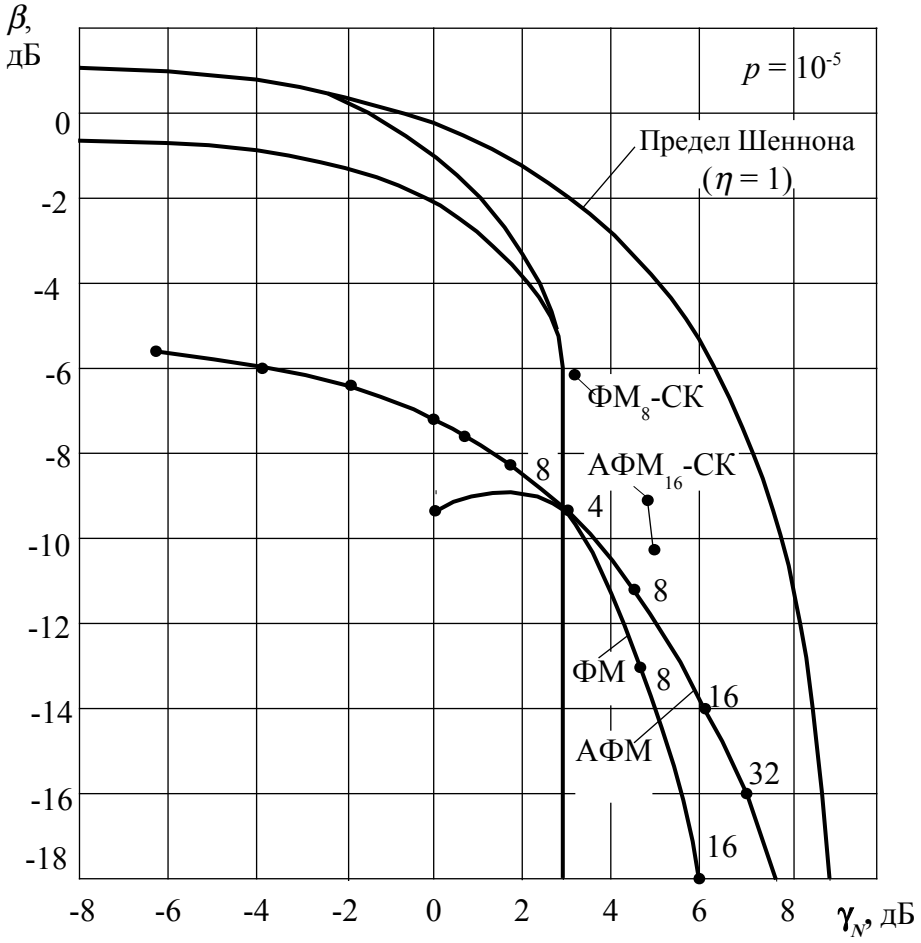


Рисунок 9.8 – Кривые эффективности

9.3.Алгебраические и структурные модели ЧМ сигналов с непрерывной фазой

Дискретные сигналы с частотной модуляцией и непрерывной фазой (ЧМ-НФ) характеризуются постоянной огибающей и отсутствием скачков фазы и применяются в системах наземной и спутниковой мобильной связи. Временные и спектральные свойства ЧМ-НФ сигналов с полным и частичным откликами исследованы в работе [4]. Перспективным является использование ЧМ-НФ сигналов *в сочетании с корректирующими кодами,* что обеспечивает как высокую помехоустойчивость, так и хорошее использование полосы частот. Для согласования модулятора ЧМ-НФ сигнала со свёрточным кодером в [22] разработана *алгебраическая модель ЧМ сигнала* с полным откликом, что позволяет рассматривать кодер-модулятор в виде *единого конечного автомата,* определять характеристики такой сигнально-кодовой конструкции и производить декодирование по единой решетчатой диаграмме. Переход к ЧМ-НФ сигналам *с парциальным откликом* повышает эффективность использования полосы частот, однако неизбежно снижает энергетическую эффективность. В этом случае для *компенсации энергетических потерь* также целесообразно использовать поме-

хоустойчивое кодирование. Однако регулярные методы согласования кодеров и модемов для таких сигналов *не разработаны.*

В разделе представлена алгебраическая модель ЧМ-НФ сигнала с парциальным откликом, которую целесообразно использовать для *синтеза сигнально-кодовых конструкций* со сверточными кодами на внешней ступени и ЧМ-НФ сигналами парциального отклика на внутренней ступени. Модель обобщает ранее изученные случаи ЧМ-НФ сигналов полного отклика.

Дискретный сигнал ЧМ-НФ имеет вид [22]:

$$S(t) = \sqrt{\frac{2E}{T}} \cos\left(2\pi f_0 t + \varphi(t) + \varphi_0\right), \qquad (9.16)$$

где текущая фаза

$$\varphi(t) = 2\pi h \sum_{i=-\infty}^{\infty} (2\alpha_i - m + 1) g_\varphi (t - iT). \qquad (9.17)$$

Здесь E – энергия сигнала длительностью T,; f_0 и φ_0 – частота и начальная фаза; h –индекс модуляции; m –объём алфавита модулирующих символов $\alpha \in \{0,..., m-1\}$.

Из выражений (9.16) и (9.17) следует, что последовательности сигналов S не являются *линейными* функциями последовательностей символов α. По этой причине они не могут быть *описаны в терминах теории линейных кодов.* Вместе с тем, изучение структуры ЧМ-НФ сигналов можно проводить на основе *обобщённой алгебраической модели*, которая впервые была предложена в [22].

Фазу сигнала (9.17) в дискретные моменты времени $t_{k+1}=(k+1)T$, соответствующие окончанию k-го тактового интервала можно представить так:

$$\varphi(t_{k+1}) = 2\pi h \sum_{i=-\infty}^{\infty} (2\alpha_i - m + 1) g_\varphi ((k - i + 1)T). \qquad (9.18)$$

В простейшем случае фазовая функция ЧМ-НФ сигнала с парциальным откликом имеет вид (рис. 9.9).

$$g_\varphi(t) = \begin{cases} 0 & \text{при} \quad t < 0, \\ \dfrac{t}{2LT} & \text{при} \quad 0 \le t \le LT, \\ \dfrac{1}{2} & \text{при} \quad t > LT. \end{cases} \qquad (9.18)$$

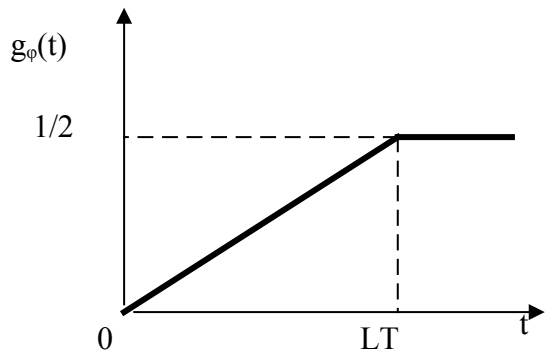


Рисунок 9.9 – Фазовая функция ЧМ-НФ сигнала

Тогда вид фазовой функции, используемой в формуле (9.18) будет

$$g_\varphi(k-i+1)T=\begin{cases}0 & \text{при } i>k+1,\\ \dfrac{k-i+1}{2L} & \text{при } k+1-L\le i\le k+1\\ \dfrac{1}{2} & \text{при } i<k+1-L\end{cases} \qquad (9.19)$$

С учетом выражения (9.19) текущую фазу сигнала можно представить в виде четырех слагаемых:

$$\varphi_1(\alpha_i)=2\pi h\sum_{i=-\infty}^{k-L}\alpha_i,$$

$$\varphi_2(i)=2\pi h\sum_{i=-\infty}^{k-L}\frac{1-m}{2},$$

$$\varphi_3(\alpha_i)=2\pi h\sum_{i=k+1-L}^{k+1}\frac{k+1-i}{L}\alpha_i,$$

$$\varphi_4(i)=2\pi h\sum_{i=k+1-L}^{k+1}\frac{k+1-i}{2L}(1-\overline{m}).$$

Отметим, что слагаемые $\varphi_1(\alpha_i)$ и $\varphi_3(\alpha_i)$ *зависят* от информационных символов и определяют *структуру фазовой решётки* сигнала. Слагаемые $\varphi_2(i)$ и $\varphi_4(i)$ от информационных символов *не зависят* и определяют *регулярное приращение фазы* на каждом такте.

При $L=1$ получаем выражение для текущей фазы ЧМ-НФ сигнала полного отклика, полученное ранее в [22]:

$$\varphi(t_{k+1})=2\pi h\sum_{i=-\infty}^{k}\alpha_i+2\pi h\sum_{i=-\infty}^{k}\frac{1-m}{2}. \qquad (9.20)$$

Нетрудно проверить, что ЧМ-НФ сигнал вида (9.16) удовлетворяет условию инвариантности. Действительно, пусть заданы две последовательности:

$$S'(t)=\sqrt{\frac{2LE}{LT}}\cos\left(2\pi f_0t+2\pi h\sum_{i=-\infty}^{\infty}(2\alpha'_i-m+1)g_\varphi(t-iT)\right),$$

$$S''(t)=\sqrt{\frac{2LE}{LT}}\cos\left(2\pi f_0t+2\pi h\sum_{i=-\infty}^{\infty}(2\alpha''_i-m+1)g_\varphi(t-iT)\right). \qquad (9.21)$$

Полагая, что $\alpha_i'=\alpha_i''$, при $i<0$, определим квадрат расстояния по Евклиду на интервале $(0,...,NT)$. Если выполняется *условие узкополосности* ЧМ-НФ сигнала ($f_0T>>2\pi$), получим

$$\delta_N^2(\overline{S}',\overline{S}'')=2EN\left[1-\frac{1}{NT}\int_0^{NT}\cos(2\pi h\sum_{i=-\infty}^{\infty}2(\alpha'_i-\alpha''_i)g_\varphi(t-iT))dt\right]. \qquad (9.22)$$

Поскольку переход к новым информационным последовательностям $\overline{\alpha}'^*=\overline{\alpha}'+\overline{\alpha}^*$ и $\overline{\alpha}''^*=\overline{\alpha}''+\overline{\alpha}^*$ ($\overline{\alpha}^*$ – произвольная последовательность) расстояние (9.22) не изменяет, сигналы ЧМ-НФ вида (9.16) относятся к категории *инвариантных,* а расстояние $\delta_N^2(\overline{S}',\overline{S}'')$ зависит только от разности фазовых траекторий, определяемых аргументами косинусов в (9.21). Поэтому в последующем целесообразно анализировать приведенную фазовую функцию

$$\tilde{\varphi}(t_{k+1}) = \varphi_1(t_{k+1}) + \varphi_3(t_{k+1}) = \frac{2\pi h}{L}\left(\sum_{i=-\infty}^{k-L} L\alpha_i + \sum_{i=k-L+1}^{k+1} (k+1-i)\alpha_i \right). \quad (9.23)$$

Поскольку выражение для $\tilde{\varphi}(t_{k+1})$ входит в аргумент косинуса, можно перейти к *модифицированной фазовой функции*

$$\tilde{\tilde{\varphi}}(t_{k+1}) = \frac{2\pi h}{L}\left(\sum_{i=-\infty}^{k-L} L\alpha_i + \sum_{i=k-L+1}^{k+1} (k+1-i)\alpha_i \right) \bmod(2\pi). \quad (9.24)$$

Для индекса модуляции $h=p/q$, где p и q – целые числа, выражение (9.24) можно представить в виде

$$\tilde{\tilde{\varphi}}(t_{k+1}) = \left[p\left(L\sum_{i=-\infty}^{k-L} \alpha_i + \sum_{i=k-L+1}^{k+1} (k+1-i)\alpha_i \right) \right] \bmod(Lq). \quad (9.25)$$

Выражению (9.25) соответствует *конечный автомат* (рис.9.9), описывающий поведение фазы на выходе модулятора ЧМ-НФ. На рис. 9.9 и далее по тексту символы сложения и умножения означают операции сложения и умножения по модулю Lq.

Последующие преобразования удобно производить, используя *многочленные представления* последовательностей в виде многочленов от аргумента D, причем задержке на время T соответствует операция умножения на D. Тогда передаточная функция структуры, изображенной на рис. 9.9, будет иметь вид:

$$K(D) = \frac{\tilde{\tilde{\varphi}}(D)}{\alpha(D)} = \left[p\left(1 + 2D + 3D^2 + \ldots + (L-1)D^{L-2} + L\frac{D^{L-1}}{1-D} \right) \right] \bmod(Lq). \quad (9.26)$$

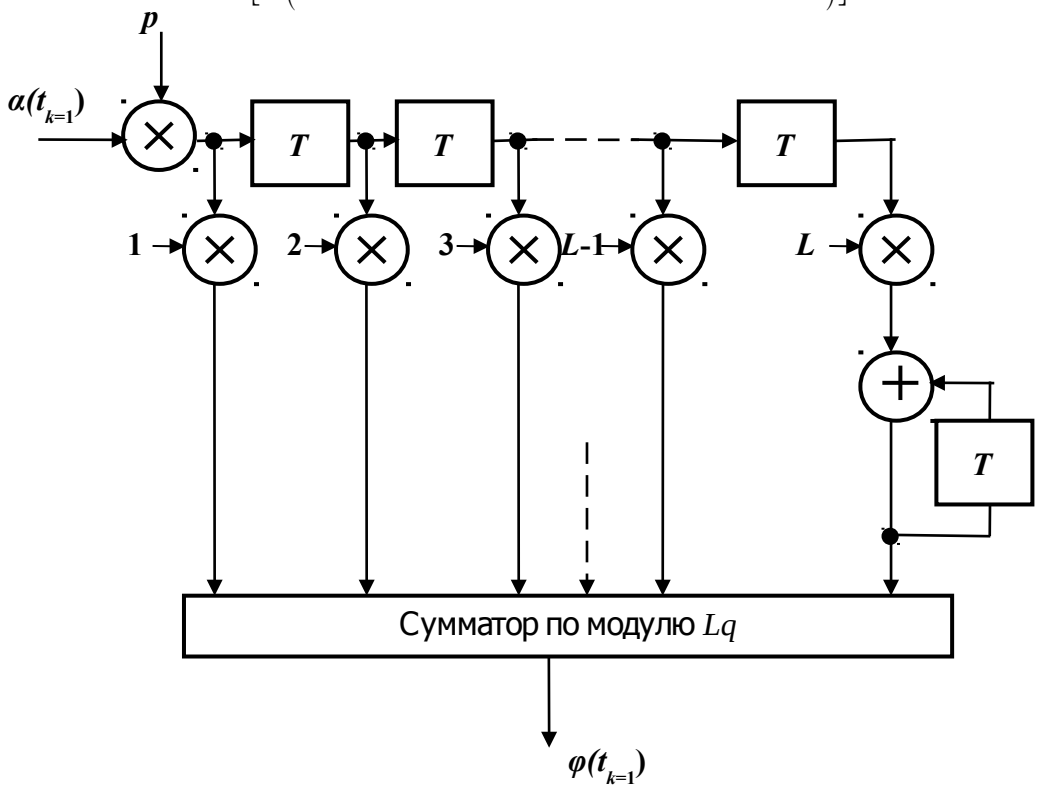


Рисунок 9.9 – Модель модулятора ЧМ-НФ сигнала в виде конечного автомата с памятью

Структура автомата с такой передаточной функцией показана на рис.9.14.

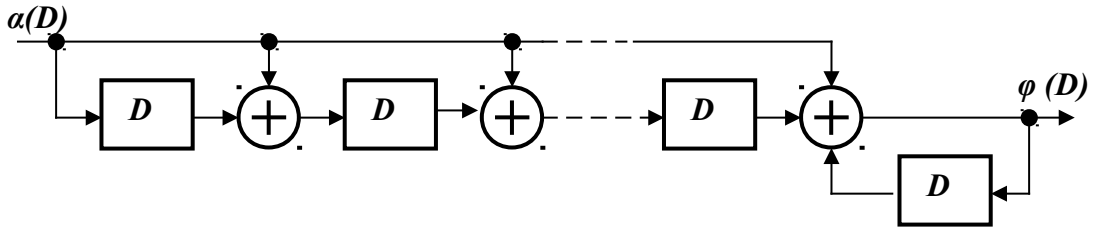


Рисунок 9.10 – Структура автомата

Число состояний конечного автомата определяется полным множеством наборов переменных на входах элементов задержки. Количество элементов задержки и, соответственно, число состояний можно уменьшить, минимизируя структурную схему.

Выражение (9.26) можно преобразовать к виду (9.27):

$$K(D) = \left[p\left(1 + D + D^2 + \ldots + D^{L-2} + D^{L-1}\right) \frac{1}{1 - D} \right] \bmod(Lq). \qquad (9.27)$$

Схема минимального автомата в этом случае принимает вид, изображенный на рис.9.11.

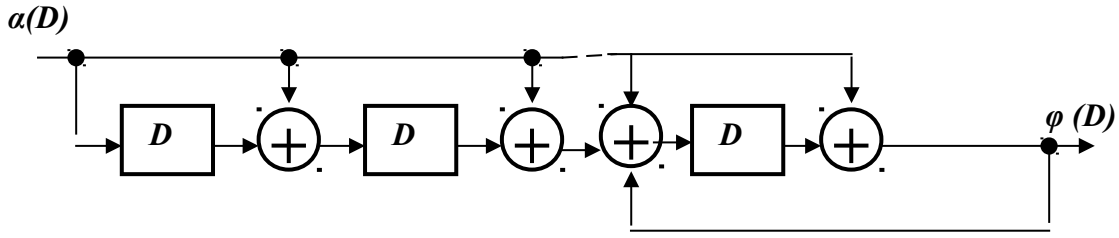


Рисунок 9.11– Структура минимизированного автомата

Из структуры рис. 9.11 следует, что общее число состояний автомата равно $S=q^L L$, причем из них $S_в=q^{L-1}$ – количество *временных* состояний (обусловленных наличием элементов памяти) и $S_ф=qL$ – количество *фазовых* состояний (обусловленных *набегом фазы* сигнала к концу каждого тактового интервала).

При решении задач построения сигнально-кодовых конструкций на основе внутренних ЧМ-НФ сигналов и внешних кодов возникает задача *корректного соединения* нескольких выходов кодера помехоустойчивого кода со входами модулятора с непрерывной фазой. Эта задача ранее была решена для модулятора с непрерывной фазой и длиной отклика $L=1$ [22].

Пусть кодер помехоустойчивого кода имеет v выходов. В этом случае модулятор ЧМ-НФ сигнала также должен иметь v входов и символы поступают на параллельные входы модулятора блоками длиной v. Разобьём последовательность тактовых моментов времени $t_k=kT$ на блоки длительностью vT, т.е. представим текущий индекс как $k=vs+r$. Здесь v – длина блока, s – текущий номер блока, r – текущий номер символа в пределах блока ($0 \le r \le v-1$). Соответственно,

передаточная функция модели модулятора может быть представлена в виде матрицы

$$K(D)=\begin{vmatrix} K_0(D) & K_1(D) & K_2(D) & \dots & K_{\upsilon-1}(D) \\ K_{\upsilon-1}(D) & K_0(D) & K_1(D) & \dots & K_{\upsilon-2}(D) \\ K_{\upsilon-2}(D) & K_{\upsilon-1}(D) & K_0(D) & \dots & K_{\upsilon-3}(D) \\ \dots & \dots & \dots & \dots & \dots \\ K_1(D) & K_2(D) & K_3(D) & \dots & K_0(D) \end{vmatrix} \qquad (9.28)$$

в которой каждый элемент $K_r(D)$ составлен из всех членов ряда (9.28), содержащих переменную D в степени $(vs+r)$, s =1,2,3, ... Для ряда значений L и ν выражения для элементов матрицы приведены в табл. 9.2.

Общее правило построения структурных моделей модуляторов параллельного типа состоит в подстановке элементов $K_r(D)$ в матрицу (9.28), формировании схемы соединений ν входов с ν выходами и последующей минимизацией числа элементов задержки. Пример такой модели приведен на рис. 9.12.

Таблица 9.2– Элементы матрицы многочленов (9.34)

L	v	$K_0(D)$	$K_1(D)$	$K_2(D)$	$K_3(D)$
1	1	$p/(1–D)$	-	-	-
1	2	$p/(1–D^2)$	$pD/(1–D^2)$	-	-
1	4	$p/(1–D^4)$	$pD/(1–D^4)$	$pD^2/(1–D^4)$	$pD^3/(1–D^4)$
2	2	$p(1+D^2)/(1–D^2)$	$2pD/(1–D^2)$	-	-
2	4	$p(1+D^4)/(1–D^4)$	$2pD/(1–D^4)$	$2pD^2/(1–D^4)$	$2pD^3/(1–D^4)$
4	2	$p(1+2D^2+D^4)/(1–D^2)$	$2p(D+D^{3)}/(1–D^2)$	-	-
4	4	$p(1+3D^4)/(1–D^4)$	$2p(D+D^5)/(1-D^2)$	$p(3D^2+D^6)/(1–D^4)$	$4pD^3/(1–D^4)$

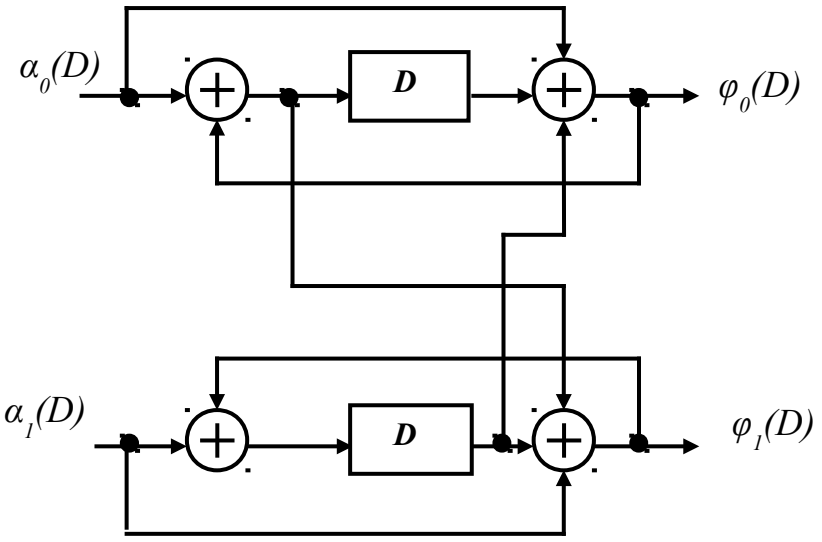


Рисунок 9.12 – Модель модулятора (L=2, ν=2, p=1, q=2, сложение по модулю 4)

Таким образом, разработанные формальные алгебраические и структурные модели *упрощают* изучение свойств частотно-модулированных дискретных сигналов с парциальным откликом. Параллельные схемы модуляторов сочетаются с соответствующими выходами сверточных кодеров. Приведенные результаты справедливы для любых форм фазовых функций, значения которых совпадают со значениями функции (9.19) в точках, кратных интервалу *T*.

10. Задачи теории помехоустойчивого кодирования

В разделе даны решения ряда актуальных задач теории помехоустойчивого кодирования с использованием положений общей алгебры, теории графов и т.п.

10.1. Кодовые границы групповых блоковых кодов

Одна из проблем теории кодирования состоит в поиске кодов, которые при заданной длине блока n и кодовой скорости R обеспечивают наибольшее кодовое расстояние d. Пределы этих параметров определяются *кодовыми границами*, рассмотрение которых приведено ниже.

Нижняя граница Варшамова-Гилберта. Рассмотрим q-ичный блоковый код со скоростью $R=k/n$ и кодовым расстоянием d. Каждую из разрешенных кодовых комбинаций окружим сферой из множества комбинаций, отстоящих на расстоянии Хэмминга (d–1) от данной комбинации. Объем этого множества (объем сферы) равен $\sum_{i=0}^{d-1} C_n^i (q-1)^i$, а общий объем, занимаемый всеми этими сферами равен $\sum_{i=0}^{d-1} C_n^i (q-1)^i \cdot q^k$. Если этот объем меньше объема, содержащего все комбинации кода q^n, то скорость исходного кода может быть увеличена без снижения расстояния d. Действительно, если найдется комбинация, не входящая ни в какую из сфер, то она может быть взята в качестве разрешенной, и поскольку она будет на расстоянии, большем d, то кодовое расстояние улучшенного кода не уменьшится.

Таким образом, скорость кода R всегда может быть повышена, если выполняется неравенство

$$\sum_{i=0}^{d-1} C_n^i (q-1)^i \cdot q^k < q^n,$$

либо, учитывая, что $n - k = n(1 - R)$,

$$\sum_{i=0}^{d-1} C_n^i (q-1)^i < q^{n(1-R)}. \qquad (10.1)$$

Это неравенство определяет *границу Варшамова-Гилберта*[11]. Граница справедлива только для линейных блоковых кодов.

Для двоичных кодов (q=2) из выражения (10.1) получаем

$$\sum_{i=0}^{d-1} C_n^i < 2^{n(1-R)}. \qquad (10.2)$$

В ряде случаев представляет интерес асимптотическая форма границы при $n\to\infty$. Используя неравенство Чернова, можно показать, что скорость кода ограничена сверху:

$$R \le 1 - \varphi_q\left(\frac{d-1}{n}\right), \qquad (10.3)$$

где: $\varphi_q(x)=x\log_q(q-1)-x\log_q x-(1-x)\log_q(1-x)$.

При $q=2$ формула $\varphi_2(x)$ определяет выражение для двоичной энтропии $H_2(x)=\varphi_2(x)= -x\log_2 x-(1-x)\log_2(1-x)$. Асимптотическая формула имеет вид:

$$R \le H_2(d-1/n). \qquad (10.4)$$

График асимптотической границы Варшамова-Гилберта, построенный для двоичных кодов по формуле (10.4) показан на рис. 10.1 (кривая ВГ). Граница *гарантирует* существование кодов, характеристики которых соответствуют точкам, расположенным, по крайней мере, на кривой (или выше ее). Анализ показывает, что большинство используемых на практике кодов конечной длины расположены ниже границы Варшамова-Гилберта, хотя и близко к ней. Поиск кодов, обеспечивающих достаточно высокую скорость R при $n\to\infty$, обеспечивающих в то же время возможность реализации алгоритмов декодирования приемлемой сложности является одной из важных задач теории кодирования.

Верхняя граница Хэмминга. Вывод верхней границы основан на соображениях *сферической упаковки* (граница сферической упаковки). При заданном минимальном расстоянии между разрешенными комбинациями кода d наибольшая скорость может быть достигнута, если сферы радиуса $(d-1)/2$, окружающие каждую комбинацию, будут наиболее плотно упакованы. Объем каждой сферы равен $\sum_{i=0}^{(d-1)/2} C_n^i (q-1)^i$, число сфер (число кодовых комбинаций кода) равно q^k. Для лучшего кода суммарное количество сфер и число всех возможных комбинаций должны совпадать. Равенство достигается для *плотноупакованных* (*совершенных)* кодов. Область каждой кодовой комбинации представляет собой сферу радиуса $(d-1)/2$, и эти области, не пересекаясь, плотно заполняют собой все n-мерное пространство кодовых комбинаций.

Аналогично изложенному выше можно получить асимптотические выражения для границы Хэмминга:

$$R \le 1 - \varphi_q\left(\frac{d-1}{2n}\right), \qquad (10.5)$$

и для двоичных кодов

$$R \le 1 - \varphi_q\left(\frac{d-1}{2n}\right) = \mathrm{H}_2\left(\frac{\delta}{2}\right). \qquad (10.6)$$

График *асимптотической границы Хэмминга* для двоичных кодов показан на рис. 10.1 (кривая Х). Граница Хэмминга справедлива как для линейных, так и для нелинейных кодов. Для малых скоростей эта граница является довольно грубой. Здесь можно получить более плотную границу.

Верхняя граница Плоткина. При выводе этой границы используется тот очевидный факт, что минимальный вес кодовой комбинации не может быть больше среднего веса. Для линейных кодов это эквивалентно тому, что минимальное расстояние между комбинациями не может превышать среднего расстояния. Определив среднее расстояние, можно показать, что

$$\frac{d}{n} \le \frac{(q-1)K}{q(K-1)}. \qquad (10.7)$$

Здесь K – число разрешенных комбинаций кода.

Граница Плоткина справедлива как для линейных, так и для нелинейных кодов.

Коды, параметры которых удовлетворяют равенству в выражении (10.7), характеризуются равенством среднего и минимального расстояний. Это *эквидистантные коды*.

Верхняя граница Элайеса. При средних скоростях кода R можно получить верхнюю границу, которая оказывается лучшей, нежели граница Хэмминга и граница Плоткина. Верхняя граница Элайеса имеет вид

$$\frac{d}{n} < \Delta(R)\left(2 - \frac{q\Delta(R)}{q-1}\right). \qquad (10.8)$$

Здесь Δ(R) – функция, обратная (10.5).

Таким образом, существуют *совершенные коды*, позволяющие исправлять все ошибки веса t и ни одной ошибки большего веса. К ним относятся, например коды Хэмминга. Многие коды отличны от совершенных.

Степень использования корректирующей способности кода зависит от алгоритма декодирования. При полном декодировании используют все возможности исправлять ошибки, вытекающие из свойств кода.

10.2. Сложность реализации алгоритмов кодирования и декодирования

Степень использования корректирующей способности кода зависит от алгоритма декодирования. При *полном* декодировании используют все возможности исправлять ошибки, вытекающие из свойств кода. В соответствии с фундаментальной теоремой К.Шеннона корректирующие коды, используемые для исправления ошибок канала, должны выбираться *достаточно длинными*. Однако

с ростом длины кодовой комбинации *n* возрастает сложность реализации процедур кодирования и декодирования, что обуславливает трудность практической реализации кодеков. В прикладной теории кодирования наряду с оценками корректирующей способности кодов принято *оценивать сложность реализации процедур кодирования/декодирования,* которые могут быть реализованы *программными* либо *аппаратными* средствами. При этом аргументом функции сложности должна выступать длина кодовой комбинации *n.*

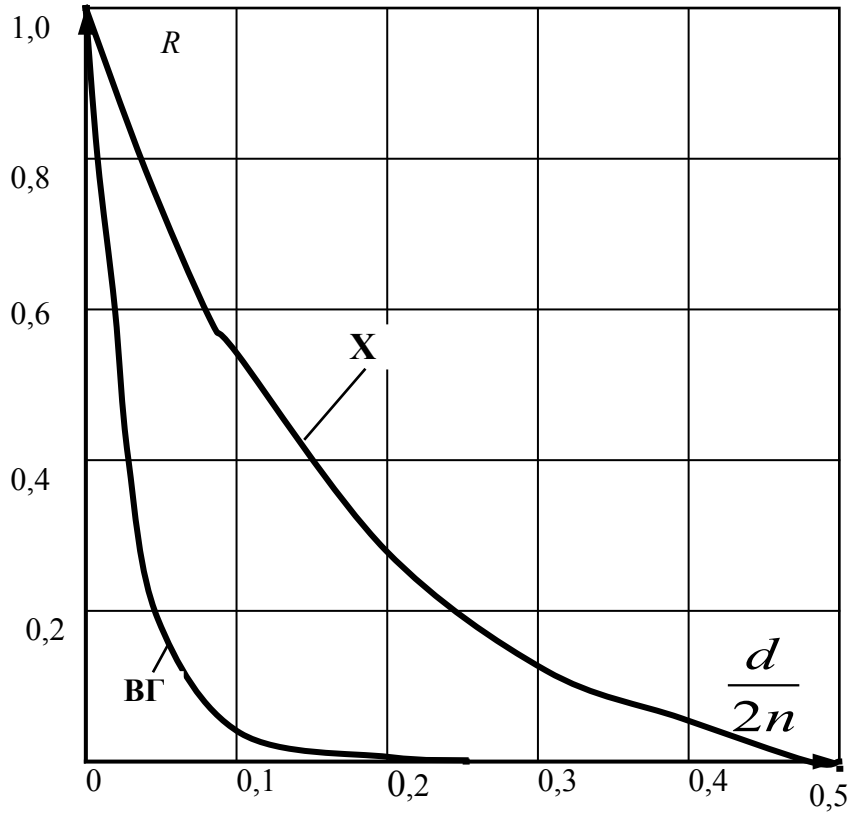


Рисунок 10.1– Кодовые границы блоковых кодов

Сложность кодирования блоковых кодов $C_к$ с использованием порождающей матрицы кода размером $nk=n^2(1–R)$ обычно оценивают величиной, пропорциональной числу элементов порождающей матрицы

$$C_к=nk=n^2(1–R). \qquad (10.9)$$

Алгоритмы декодирования оказываются сложнее. Среди них наиболее сложным алгоритмом принято считать *алгоритм полного перебора,* в соответствии с которым декодер *переборно* сопоставляет принятую кодовую комбинацию с множеством всех возможных комбинаций и выносит решение о передаче той из разрешенных комбинаций, которая оказывается на минимальном расстоянии от принятой комбинации (*декодирование по минимуму расстояния).* Сложность алгоритма переборного декодирования принято считать пропорциональной ко-

личеству всех возможных комбинаций кода (*объему полного перебора)*

$$C_{\text{д-эксп}}=2^{n}. \qquad (10.10)$$

Говорят, что сложность переборного декодирования возрастает «*экспоненциально»* с ростом длины кода. Ясно, что *переборные алгоритмы практически трудно реализовать для длинных кодов.* В связи с этим у специалистов по прикладной теории кодирования бытует жаргонное выражение «*проклятие размерности»:* любая попытка реализовать декодирование длинных кодов оказывается безуспешной из-за *катастрофического роста сложности* программной либо аппаратной реализации алгоритма декодирования. Поэтому *мерилом* реализационных возможностей алгоритмов декодирования блоковых кодов является сопоставление сложности алгоритма с верхней границей сложности (10.10) .Лучшими считаются коды с показателем сложности, *пропорциональным малой степени длины кода*

$$C_{\text{д-степ}}=n^{\kappa}.(k\text{–малое}) \qquad (10.11)$$

В таких случаях говорят, что алгоритм характеризуется «*степенной»* сложностью.

10.3. Условия катастрофичности сверточных кодов

Сверточные коды (СК) широко используются в различных системах передачи дискретной информации для обнаружения и исправления ошибок в канале. Значительная часть таких кодов отыскивается путем *прямого перебора* порождающих многочленов с учетом ряда ограничений. Одним из ограничений является принадлежность кода к классу *катастрофических кодов*, которые в процессе перебора *отбрасываются.*

Изучению *свойств катастрофичности* сверточных кодов посвящен ряд работ. В диссертации [22] обсуждается вопрос о появлении на выходе сверточного кодера последовательности символов конечного веса при подаче на вход кодера последовательности бесконечного веса. В последующем, в ряде монографий упоминаются *признаки катастрофических кодов*. Отмечается, что двоичный код обладает свойством катастрофичности, если двоичное представление каждого порождающего многочлена содержит четное число единиц. Свойства катастрофичности следует учитывать при оптимизации параметров частотно-модулированных сигналов с непрерывной фазой (ЧМ–НФ), поскольку структура таких сигналов родственна структуре сверточных кодов. Условия катастрофичности важны также при анализе свойств *нелинейных* кодов.

В разделе дается наглядное пояснение свойств катастрофичности и явное выражение для порождающих многочленов катастрофических кодов. Приведена таблица многочленов, обладающих *свойством катастрофичности*. Дана оценка катастрофичности сигналов ЧМ-НФ. Сформулирован *общий признак* катастрофических кодов. Свойство катастрофичности поясним на примере ко-

роткого СК (рис.10.2)..Представлен двоичный (основание алфавита m=2) сверточный кодер с длиной кодового ограничения ν=2 и порождающими многочленами $G_1(D)=(1+D^2)$, $G_2(D)=(1+D+D^2)$. Диаграмма состояний такого кодера (обозначаемого в таблицах кодов в восьмеричном представлении как (5, 7)) показана на рис. 10.2 б.

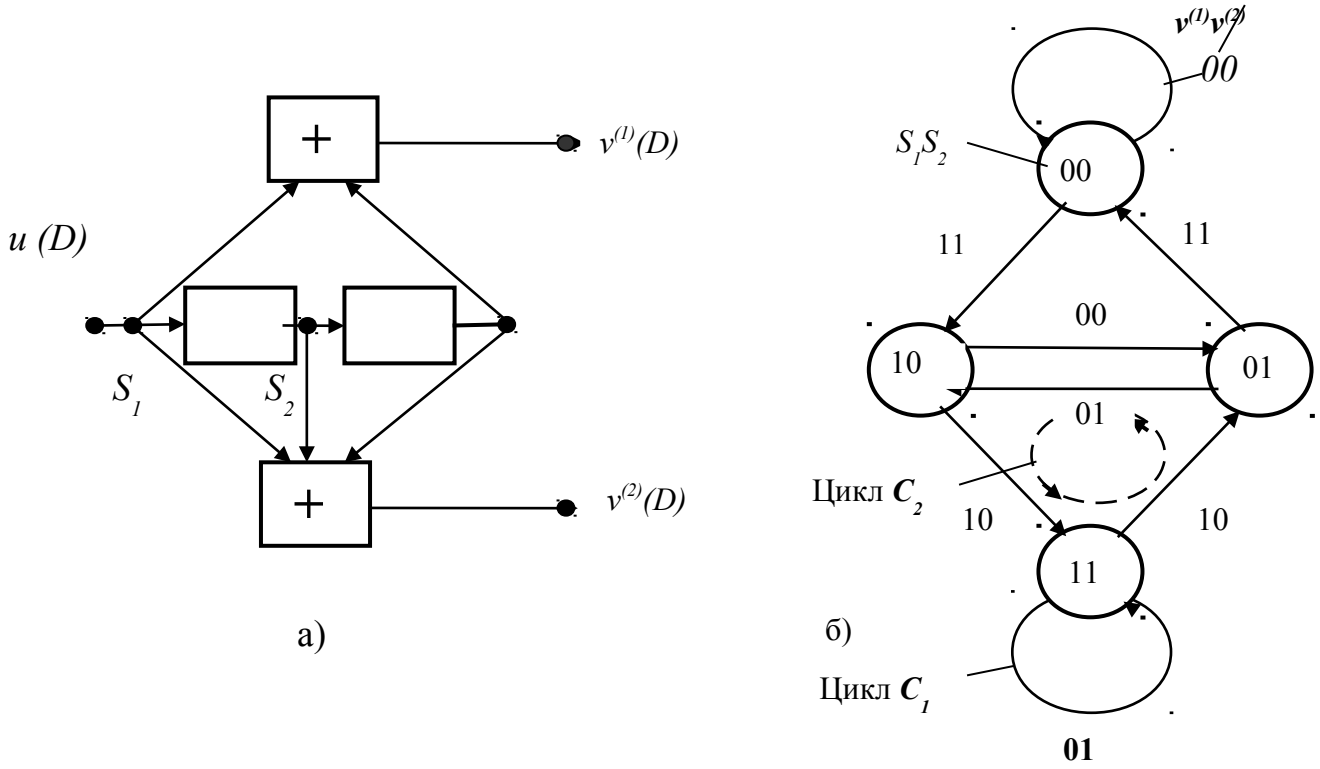


Рисунок 10.2– К иллюстрации свойств катастрофичности

В процессе кодирования кодер под воздействием символов входной последовательности $u(D)$ последовательно изменяет состояния S_1S_2 на диаграмме состояний. При этом в ряде случаев кодер совершает циклы C, последовательно обходя одни и те же наборы состояний.

На рис.10.2 б показаны примеры циклов: цикл C_1 (последовательность состояний 11, 11, 11,…) и цикл C_2 (10, 11, 01, 10, 11, 01,…). Обозначим символом L *длину цикла* (количество различных состояний кодера в пределах одного цикла). В рассматриваемых примерах L_{C1}=1 и L_{C2}=3.

При определенных условиях на выходах кодера в пределах цикла могут располагаться *только нулевые символы*. Так, если на вход двоичного кодера поступает полубесконечная последовательность $u(D)=1+D+D^2+D^3+\ldots$ (двоичная последовательность $\bar{u}$ =1111…), то, как следует из диаграммы рис.10.1 б, цикл C_1 содержит полубесконечную последовательность символов нулевого веса $\bar{v}^{(1)}$ =(0000…). Аналогично, при $u(D)=1+D+D^3+D^4+D^6+D^7+\ldots$ ($\bar{u}$ =11011011…) цикл C_2 содержит полубесконечную последовательность нулевых символов $\bar{v}^{(2)}$ =(0000…).

Определение 10.1. *Цикл нулевого веса* (ЦНВ) – это последовательность состояний ($S_1\ldots S_{v-1}S_v$) вместе с соответствующей последовательностью символов

ветвей $v^{(j)}$, $j=\overline{1,n}$, образующая *замкнутый контур* на диаграмме состояний кодера СК, причем, все символы ветвей $v^{(j)}=0$.

Наличие ЦНВ на диаграмме состояний кодера, очевидно, ухудшает *весовую структуру* СК, поскольку нулевые символы *снижают расстояние* соответствующих путей на от полностью нулевого пути. Однако наиболее опасными являются случаи *совпадения всех циклов нулевого веса* C_j, $j=\overline{1,n}$, когда все символы $v^{(j)}$, $j=\overline{1,n}$ на длине цикла равны нулю. При этом при подаче на вход кодера *ненулевой* полубесконечной последовательности $\bar{u}$ с непрерывно нарастающим весом полубесконечная последовательность $\bar{v}$ на выходе кодера после определенного начального набора ненулевых символов в последующем содержит *полностью нулевые символы*. Вес такой последовательности конечен. Коды, обладающие таким свойством, названы *катастрофическими*, поскольку при их декодировании *конечное число ошибок в канале вызывает бесконечное число ошибок декодирования.*

Замкнутый цикл на решетчатой диаграмме СК образуется при воздействии на входе кодера периодической последовательности символов. Полубесконечная последовательность $u(D)=\frac{1}{1+D^L}=1+D^L+D^{2L}+D^{3L}+\ldots$ периодична с периодом L. Пусть, $u^*(D)=\sum_{i=0}^{L-1} u_i^* \cdot D^i$, где $u_i^* \in \{0,1,2,\ldots,m\text{-}1\}$.

(В нашем случае код двоичный и m=2). Тогда дробь $u^*(D)/(1+D^L)$ также *периодична* с периодом L и определяет один из (m^L–1) всех возможных вариантов ненулевых периодических последовательностей на входе кодера (и, соответственно, (m^L– 1) циклов на диаграмме состояний кодера).

Если $G^{(j)}(D)$ – порождающий многочлен кода по j – му выходу, то последовательность символов на этом выходе будет $v^{(j)}(D)=\frac{u^*(D)G^{(j)}(D)}{1+D^L}$.

Старшие степени многочленов в этом выражении определяются следующим образом:

$$max\ \{deg\ u^*(D)\} \le L-1; \quad max\ \{deg\ G^{(j)}(D)\} \le \nu,$$

где ν: – длина кодового ограничения СК. Следовательно, старшая степень произведения многочленов $max\{deg[u^*(D)\cdot G^{(j)}(D)]\}$ может быть больше длины цикла L и в общем случае результат деления можно представить так:

$$v^{(j)}(D)=\frac{u^*(D)G^{(j)}(D)}{1+D^L}=a(D)+\frac{b(D)}{1+D^L}. \qquad (10.12)$$

Здесь $a(D)$ – многочлен, старшая степень которого $max\ \{deg\ a(D)\} \le (\nu-1)$ (“целое”);

$b(D)$ – многочлен, старшая степень которого $max\ \{deg\ b(D)\} \le (L-1)$ (“остаток”).

Вид остатка $b(D)$ определяет *поведение кодера* СК на цикле периода L. Если $b(D) \neq 0$, то выходная последовательность кодера $v^{(j)}(D)$ содержит начальный фрагмент $a(D)$ длиной не более чем ν символов, вслед за которым начинается

периодическая последовательность $\frac{b(D)}{1+D^L}$, причем, ее вес непрерывно *нарастает*. Такой цикл длины L имеет *ненулевой* вес, а соответствующий порождающий многочлен не принадлежит катастрофическому коду.

Если $b(D)=0$, то результатом деления в (10.12) является только многочлен $a(D)$ ("*целое*") и последовательность $v^{(j)}(D)$ на выходе кодера содержит конечное число ненулевых символов, а все символы на длине цикла L равны нулю.

Таблица 10.1 – Разложение многочленов на неприводимые многочлены

Длина цикла L	Многочлен цикла	Разложение на неприводимые многочлены
1	$1+D$	$(1+D)$
2	$1+D^2$	$(1+D)^2$
3	$1+D^3$	$(1+D)(1+D+D^2)$
4	$1+D^4$	$(1+D)^4$
5	$1+D^5$	$(1+D)(1+D+D^2+D^3+D^4)$
6	$1+D^6$	$(1+D)^2(1+D+D^2)^2$
7	$1+D^7$	$(1+D)(1+D^2+D^3)(1+D+D^3)$
8	$1+D^8$	$(1+D)^8$
9	$1+D^9$	$(1+D)(1+D+D^2)(1+D^3+D^6)$
10	$1+D^{10}$	$(1+D)^2(1+D+D^2+D^3+D^4)^2$

Отсюда следует

Утверждение 10.1. Порождающий многочлен $G_к^{(j)}(D)$, $j=\overline{1,n}$, образующий на решетчатой диаграмме *цикл нулевого веса длины L,* определяется выражением

$$G_к^{(j)}(D) = \frac{a(D)(1+D^L)}{u^*(D)}. \qquad (10.13)$$

Многочлен вида (10.13) назовем *катастрофическим* многочленом. Выражение (10.13) получено из (10.12) при условии $b(D)=0$.

К примеру, при $m=2$, $L=3$ многочлен $(1+D^3)=(1+D)(1+D+D^2)$. Выбирая $a(0)=1$, $u^*(D)=1+D$, получаем $G_к^{(j)}(D)=1+D+D^2$. *Цикл нулевого веса* C_2, порожденный таким многочленом $G^{(2)}(D)$, показан на рис. 10.2.

Рассмотрим свойства многочленов с двоичными коэффициентами вида (10.13), порождающих циклы нулевого веса. В табл.10.1 приведены результаты представления многочленов вида $(1+D^L)$ в виде произведения неприводимых многочленов степеней, меньших L.

Свойства таких разложений сводятся к следующему:

Свойство 10. 1. Если L – простое число, то $(1+D^L)=(1+D)(1+D+D^2+\ldots+D^{L-1})$;

Свойство 10.2. Если L – четное число, то $(1+D^L)=(1+D^{L/2})^2$;

Свойство 10.3. Если L – составное число, используя свойства 10.1 и 10.2, двучлен $(1+D^L)$ можно представить в виде произведения неприводимых многочленов. В таблице 10.1 даны примеры таких разложений для $L\leq 10$.

На основе этих свойств можно сформулировать утверждение:

Утверждение 10.2. Произведение двоичных многочленов $(g_0D^0+g_1D^1+g_2D^2+\ldots+g_kD^k)(1+D)$ всегда содержит *четное число* ненулевых слагаемых (при любых значениях g_i, $i=\overline{0,k}$ и любом k).

Доказательство тривиально и подтверждается, в частности, данными табл. 10.1.

Свойства катастрофичности проявляются на парах "задающий многочлен цикла $u^*(D)$ – порождающий многочлен $G_к(D)$" при известной длине цикла L. Выражение (10.13) удобно для оценки *свойств катастрофичности* конечных автоматов (кодеров) с одним входом и одним выходом.

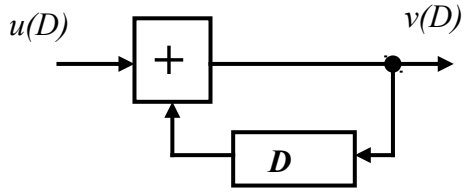


Рисунок10.3 – Модель модулятора ЧМ-НФ сигнала

Например, схема, представленная на рис.10.3, является автоматной моделью как относительного кодера, так и модулятора двоичного ЧМ-НФ сигнала с индексом модуляции 1/2. Передаточная функция такого автомата равна $G(D)=1/(1+D)$. При подстановке этого выражения в формулу (10.13) убеждаемся, что циклы любой длины L на входе порождают ненулевые полубесконечные последовательности на выходе, поскольку в выражении $u^*(D)/[(1+D^L)(1+D)]$ старшая степень многочлена числителя всегда меньше старшей степени многочлена знаменателя. Иными словами, *автомат, представленный на рис.*10.3, *свойством катастрофичности не обладает.*

Изложенное выше позволяет сформулировать *признак катастрофичности в общем виде.* Рассмотрим сверточный код с произвольным основанием алфавита m и скоростью $R=1/n$.Порождающий многочлен этого кода по одному из выходов кодера представим в виде произведения двух многочленов $G^{(j)}(D)=G_0(D)G^{*(j)}(D)$. Если $G^{(j)}(D)$ – неприводимый многочлен, то многочлен $G^*(D)=1$. При известном многочлене $G_0(D)$ выберем многочлен $u^*(D)$ так, чтобы выполнялось равенство $G_0(D)u^*(D)=1+D^L$, где L – некоторое целое число. Нетрудно видеть, что при подстановке выбранных многочленов в формулу (10.12) получим

$$v^{(j)}(D) = \frac{u^*(D)G^{(j)}(D)}{1+D^L} = \frac{u^*(D)G_0(D)G^{*(j)}(D)}{G_0(D)u^*(D)} = G^{*(j)}(D). \quad (10.14)$$

Следует отметить, что если все порождающие многочлены кодера можно представить в виде $G^{(j)}(D)=G_0(D)G^{*(j)}(D)$, $j=1\ldots n$, то они будут одновременно удовлетворять *условиям катастрофичности,* и порождать на всех выходах кодера в пределах совпадающих циклов $u^*(D)/(1+D^L)$ полностью нулевые последовательности и в совокупности задавать *катастрофический сверточный код.*

10.1. Признак катастрофичности. Сверточный код с произвольным основанием, скоростью $R=1/n$ и набором порождающих многочленов $\{G^{(j)}(D)\}$, $j=1\ldots n$ *является катастрофическим,* если каждый из многочленов можно представить в виде произведения многочленов $G^{(j)}(D)=G_0(D)G^{*(j)}(D)$, где $G_0(D)$ – *общий делитель* всех многочленов.

Если $G_0(D)$ – общий наибольший делитель, то длина цикла L – наименьшая.

Сформулированный выше признак легко о*бобщается* на случай кодов с произвольной скоростью $R=k/n$ (k и n – целые числа, $k<n$), когда кодер задается набором порождающих многочленов $\{G_{(i)}^{(j)}(D)\}$, $i=1...k$, $j=1...n$. Такой код будет катастрофическим, если условию катастрофичности удовлетворяет *набор порождающих многочленов* хотя бы по одному из входов кодера $(i=const, j=1...n)$. Отсюда следует:

10.2. Общий признак некатастрофичности двоичных сверточных кодов с произвольной скоростью. Сверточный код с произвольной скоростью $R=k/n$ и набором порождающих многочленов $\{G_{(i)}^{(j)}(D)\}$,i=(1…k),j=(1…n) является *некатастрофическим,* если каждый из многочленов выбирается *из множества неприводимых многочленов.* В соответствии с признаком катастрофичности 10.1 \код будет катастрофическим, если порождающие многочлены *содержат общие множители*. Как известно, любая пара неприводимых многочленов общий множитель не содержит,что и *гарантирует некатастрофичность.*

Используемый в литературе *частный признак катастрофичности* двоичных сверточных кодов (четное число единиц в двоичном представлении каждого из порождающих многочленов СК) вытекает из сформулированного выше общего признака, поскольку, в соответствии с Утверждением 10.2 многочлены с четным числом единиц содержат общий делитель вида $(1+D)$.

11. Перспективные методы передачи информации в цифровых телекоммуникационных системах

В разделе приведены обзоры перспективных методов передачи информации в современных цифровых телекоммуникационных системах. Обзоры составлены по материалам зарубежных публикаций.

11.1. Турбо-коды и их применение в телекоммуникационных системах

В современных цифровых телекоммуникационных системах широко используется помехоустойчивое кодирование, которое является эффективным средством повышения верности передаваемой информации. Наиболее перспективны *сверточные коды,* которые по сравнению с *блоковыми кодами* обеспечивают более высокую помехоустойчивость. К 1990 г. усилиями отечественных и зарубежных ученых и разработчиков аппаратуры были освоены методы корректирующего кодирования, обеспечивающие энергетический выигрыш (5…6) дБ в каналах с постоянными параметрами и гауссовским шумом, что позволяло, например, снизить диаметр спутниковой приемной антенны в (2…3) раза, либо, в сочетании с сигналами *многопозиционной модуляции* довести скорость передачи данных по телефонным каналам до 33,6 кбит/с (Рекомендация *V*.34). Вместе с тем, до теоретического предела оставался нереализованный запас в (5…7) дБ [3]. Из работ К. Шеннона известно, что эффективные коды должны быть *достаточно длинными* со структурой, подобной структуре случайного шума. При этом, с ростом длины кода сложность алгоритма декодирования и аппаратная

сложность декодера *катастрофически* возрастают. Хотя отсутствие в те годы высокопроизводительных ЭВМ и подходящей элементной базы сдерживало поиски и применение новых кодов на базе *теории каскадных кодов*, экспериментально было установлено, что *итеративное (многократное) декодирование* дает определенное улучшение. В 1993г. были предложены *турбо-коды (turbo-codes)*[23], характеристики которых были столь впечатляющими, что реакцией сообщества специалистов по кодированию был скептицизм. Ведущие специалисты по теории кодирования занялись теоретическим обоснованием эффективности турбо-кодирования. Итог этим дискуссиям подвел автор *метода сверточного кодирования* П. Элайес в докладе «Являются ли турбо-коды эффективными в нестандартных каналах?» на международном симпозиуме по теории информации *ISIT*-2001. К настоящему времени исследователи многих стран проверили и в некоторых случаях улучшили первоначальные результаты. Итоги этих работ опубликованы в двух тематических выпусках журнала *Selected Areas in Communications*. На основе имитационного моделирования получен беспрецедентный «*рекордный»* результат (0.0045 дБ до предела Шеннона!).

По утверждению ведущего автора метода турбо кодирования К. Берроу «*… Турбо-коды десять лет спустя вступают на службу…»*. Действительно, высокая эффективность при действии различных помех и простота алгоритмов кодирования-декодирования турбо-кодов быстро привлекли внимание и завоевали симпатии разработчиков и производителей телекоммуникационного оборудования. В настоящее время трудно указать телекоммуникационные системы (от популярных ныне систем мобильной и спутниковой связи до сверхскоростных систем передачи на основе ВОЛС), где не находило бы себе подобающее место турбо-кодирование.

Из общей теории связи известно, что для максимального приближения к пропускной способности канала связи необходим *случайный выбор кодовых комбинаций при их достаточно большой длине*. Практически важной задачей специалистов по кодированию была и остаётся задача поиска и синтеза кодов с высокой исправляющей способностью, и, в то же время, с приемлемой сложностью реализации декодера. Поставленным условиям во многом удовлетворяет метод *последовательного каскадного кодирования-декодирования*, предложенный Д. Форни. Структурная схема кодера, наиболее распространенного последовательного каскадного кода, представлена на рис. 11.1. Он состоит из последовательного соединения *внешнего кодера* кода Рида-Соломона и *внутреннего кодера* свёрточного кода, включенных через *перемежитель*.

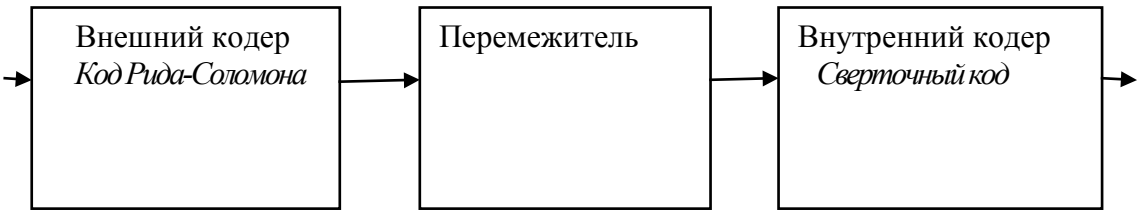


Рисунок 11.1– Структурная схема кодера последовательного каскадного кода

Подобная конструкция стандартизирована для многих приложений передачи информации. Например, последовательный каскадный код с кодом Рида-Соломона (255, 223) и свёрточным кодом (133, 171) используется для передачи телеметрической информации с космических аппаратов [27]. Подобная схема является основным методом помехоустойчивого кодирования стандарта цифрового телевизионного вещания *DVB*[29]. По сравнению со свёрточными кодами использование каскадных кодов приводит к получению *дополнительного энергетического выигрыша* от кодирования (ЭВК) порядка (3..5)дБ при вероятности ошибки двоичного символа (бита) $P_б=10^{-10}$. Вместе с тем, анализ характеристик последовательных каскадных кодов показал, что они на несколько децибел *отстоят от предела Шеннона*. Одна из причин снижения эффективности их использования – *неоптимальное согласование кодов в каскадной конструкции* (кодирование внутренним кодером как информационных, так и проверочных символов внешнего кода ведёт к *нерациональной трате* пропускной способности канала).

Для сравнения методов помехоустойчивого кодирования воспользуемся методикой, описанной в [15]. На рис. 11.2 представлена (β-γ) диаграмма, характеризующая энергетическую эффективность $\beta=RN_0/P_c$ и частотную эффективность $\gamma=R/F$ цифровых систем связи с различными методами помехоустойчивого кодирования. Здесь R – скорость передачи информации по каналу с полосой частот F и мощностью сигнала P_c.

На рисунке точками отмечены характеристики систем со следующими кодами:

1. Блоковый код Рида-Маллера (32, 6).
2. Свёрточный код с длиной кодового ограничения v = 31 и скоростью R = 1/2, последовательное декодирование.
3. Свёрточный код с порождающими многочленами в восмеричном представлении (133, 171) и скоростью R=1/2, декодирование по алгоритму Витерби.
4. Каскадный код: {свёрточный код (133,171)+код Рида-Соломона (255,223)};
5. Длинный свёрточный код с длиной кодового ограничения v = 14 и скоростью R=1/4 – декодер *BVD* (*Big Viterbi Decoder – большой декодер Витерби.*
6. Каскадный код: {“*BVD*”+код Рида-Соломона (255, 223)}.
7. Турбо-код со скоростью R=1/2 и объемом перемежителя 65536 символов, предложенный в оригинальной работе К. Берроу [23]. Алгоритм декодирования *MAP*, 18 итераций, компонентные свёрточные коды в восьмеричном представлении (1,21/37).

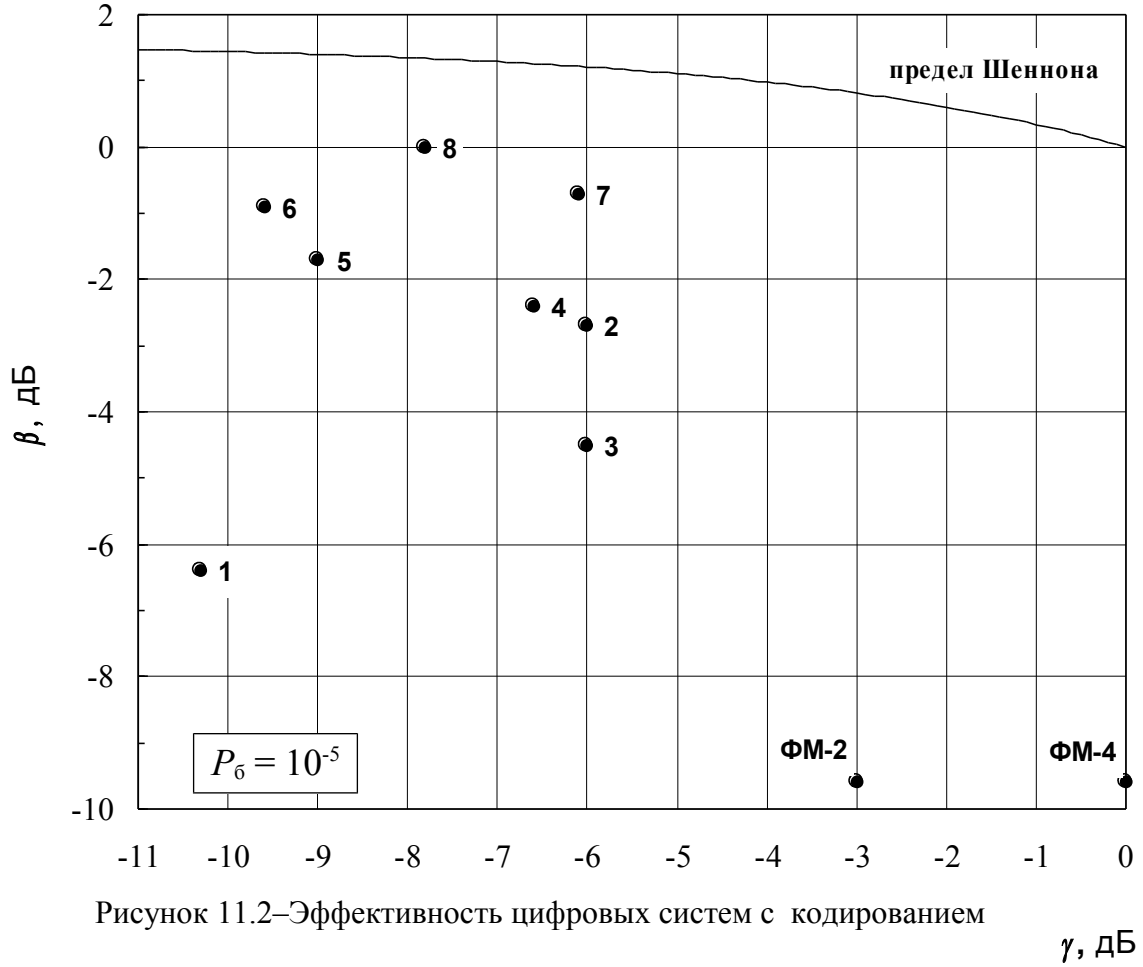


Рисунок 11.2–Эффективность цифровых систем с кодированием

Сравнение на рис. 11.2 ведется с эффективностью систем с некодированной двоичной фазовой модуляцией (ФМ-2) либо с двукратной ФМ (ФМ-4).

Как видно из рис. 11.2, турбо-коды являются *наиболее эффективными* из рассмотренных кодов. При одинаковой частотной эффективности дополнительный ЭВК, по сравнению с последовательными каскадными конструкциями (т.4 и 6) у систем с турбо-кодами (т. 7 и 8), составляет 1 дБ и более.

Наиболее распространенной является схема кодера турбо-кода с двумя идентичными *компонентными кодерами* и одним перемежителем, изображённая на рис. 11.3.

Рассмотрим структуру и роль компонентных кодов в составе турбо-кодов. В оригинальной работе К. Берроу [23] в качестве компонентных предложено использовать *рекурсивные систематические свёрточные коды (РССК).*

Показано, что использование РССК при прочих равных условиях гарантирует турбо-коду наилучшие характеристики.

Вероятность ошибочного декодирования турбо-кода пропорциональна выражению

$$\frac{N}{C_N^{i_{\min}}} \approx N^{1-i_{\min}} \cdot i_{\min}, \text{ при } N >> i_{\min}. \qquad (11.1)$$

Здесь $i_{\min}$ – минимальный вес информационной последовательности, порождающей слившийся путь на решётчатой диаграмме компонентного кодера, N – размер информационного блока турбо-кода.

Из анализа выражения (11.1) видно, что чем больше $i_{\min}$, тем меньше вероятность ошибочного декодирования. Таким образом, параметр $i_{\min}$ является ключевым при выборе компонентных кодов. У стандартных свёрточных кодов без обратной связи $i_{\min} = 1$.

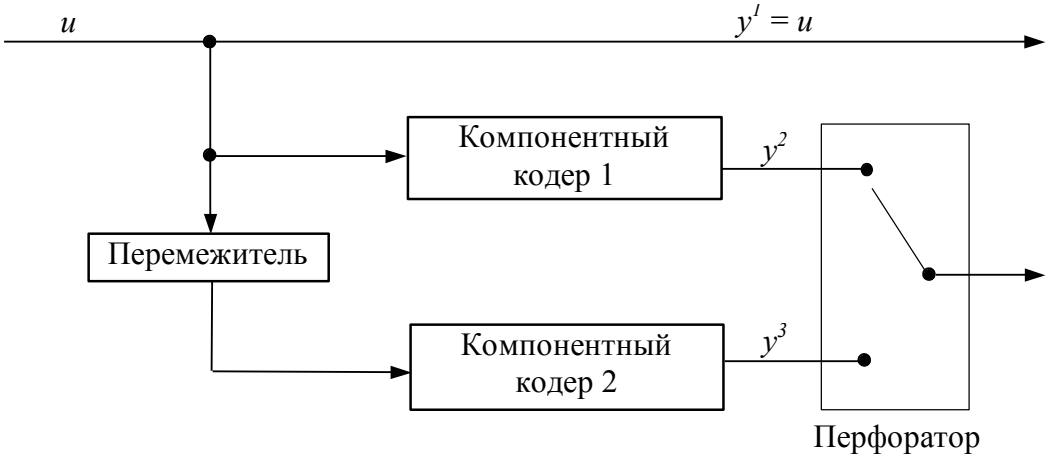


Рисунок 11.3 – Кодер турбо-кода

При этом из (11.1) следует, что с ростом оъема перемежителя характеристики турбо-кода практически не изменяются(отсутствует *выигрыш перемежителя*). Если же в роли компонентных использовать рекурсивные свёрточные коды, у которых $i_{\min}$ всегда больше 1 (в частности, для кодов со скоростью $1/n$ $i_{\min} = 2$), то вероятность ошибочного декодирования турбо-кода уменьшается обратно пропорционально N, т.е. появляется *выигрыш перемежителя.*

В процессе кодирования *начальные состояния* компонентных кодеров чаще всего нулевые. Предпочтительным является окончание кодирования информационного блока также при нулевых состояниях кодеров, так как многочисленные результаты моделирования показывают существенное преимущество характеристик помехоустойчивости турбо-кодов с такими параметрами. Процедуру *принудительного заполнения* кодирующего регистра нулями называют *обнулением кодеров* либо *обнулением решётчатой диаграммы* компонентных кодеров.

Можно выделить следующие *методы обнуления* компонентных кодеров:

1. *Принудительное зацикливание*. Идея данного метода обнуления заключается в независимом принудительном зацикливании кодирующих регистров (см.рис. 11.4), при котором после кодирования блока данных на вход кодера подаётся последовательность, порождённая полиномом обратной связи кодера. Это приводит регистр в нулевое состояние за время, меньшее или равное v тактовых интервалов.

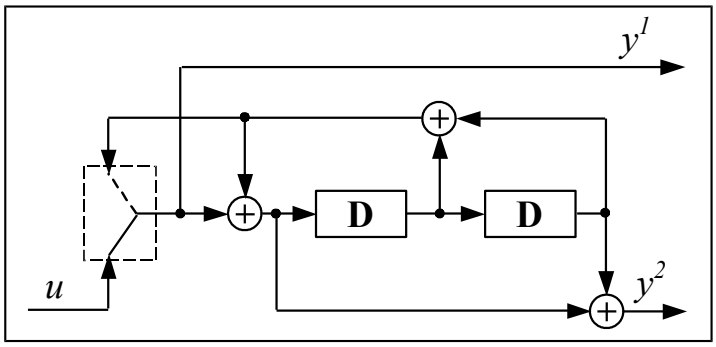


Рисунок 11.4 – Схема кодера свёрточного кода с принудительным зацикливанием

Преимуществом данного метода является *простота реализации* (минимум дополнительных аппаратных затрат). Недостаток – несколько худшие характеристики турбо-кода по сравнению с другими методами обнуления. Это объясняется тем, что некоторые информационные последовательности с малым весом (в частности, с единичным весом) порождают кодовые слова турбо-кода с небольшим весом, так как для таких последовательностей "*выигрыш перемежителя"* отсутствует.

2. Метод "*нейтрализации хвоста*" (*tail-biting*). В данном случае начальные состояния компонентных кодеров подбираются так, чтобы поданная на вход информационная последовательность вводила кодеры в состояния, идентичные начальным. Применение данного метода ко всем компонентным кодерам влечёт за собой увеличение *вычислительной сложности* кодирующего устройства турбо-кода приблизительно на 50%.

3. *Обнуление дополнительной "хвостовой" последовательностью*. В соответствии с данной методикой, для обнуления одного компонентного кодера на его вход необходимо подать дополнительную последовательность из v символов ("*хвостовик")*, зависящую от текущего состояния и порождающего полинома обратной связи кодера. Это приводит к некоторому уменьшению скорости кодирования, однако обычно размер информационного блока значительно больше v, и *уменьшение скорости несущественно*. Путём поиска "*хвостовика*" возможно *обнуление* либо только первого компонентного кодера, либо всех компонентных кодеров.

4. *Использование самообнуляемого перемежителя*. Накладывая ограничение на структуру перемежителя, можно добиться того, что "*хвостовая"* последовательность, обнуляющая первый компонентный кодер, будет обнулять и все остальные кодеры. Это ограничение записывается в виде:

$$\pi(t) = t(\mathrm{mod}\, L), \qquad (11.2)$$

где $t = 1, 2, ..., N$ – порядковый номер символа на входе перемежителя;

$\pi(t)$ – номер этого же символа на выходе перемежителя; а L – период импульсной реакции компонентного кодера ($L \le 2^v - 1$). Недостатком данного метода является то, что ограничение, наложенное на перемежитель, ведёт к невоз-

можности полноценной оптимизации структуры перемежителя, и, как следствие, характеристики декодирования турбо-кода оказываются хуже ожидаемых.

Следующим важным звеном турбо-кодов является *перемежитель*.

Перемежитель – устройство, осуществляющее перестановку символов внутри блока по определенному закону. Этот закон может определяться математической формулой, табличной формой записи либо описанием закономерности построения перемежителя. За счёт наличия перемежителя процесс формирования кодовых комбинаций турбо-кода достаточно б*лизок к случайному*. Поэтому турбо-код с большим размером блока можно характеризовать как *длинный случайный код*. В соответствии с теоремами Шеннона именно такие коды и нужны для передачи информации со скоростями *максимально близкими* к пропускной способности канала связи.

Перемежитель играет важную роль в *формировании распределения весов* турбо-кода. Основной задачей его синтеза является *максимизация минимального кодового расстояния* турбо-кода $d_{\min}$ и, после этого, *минимизация числа кодовых слов* с весом $d_{\min}$. Если входная последовательность порождает на выходе первого компонентного кодера проверочную последовательность с малым весом, то перемежитель должен так изменить *порядок следования символов*, чтобы *вес проверочной последовательности* на выходе второго компонентного кодера был достаточно большим. При этом общий вес кодового слова турбо-кода, состоящего из двух практически независимых частей, будет заметно больше свободного расстояния компонентного свёрточного кода.

В отличие от свёрточных кодов, корректирующие способности турбо-кодов в большей степени зависят от количества кодовых слов, отстающих от других на расстояние d (т.е. от *спектра расстояний*). Таким образом, для корректной оценки эффективности турбо-кодов необходимо располагать достаточно полным описанием *функции распределения весов,* хотя знание только $d_{\min}$ всё же позволяет сделать предварительные выводы.

Как и при свёрточном кодировании, в схеме кодера турбо-кода (рис. 11.4) для повышения относительной скорости кода R возможно применение процедуры *перфорации* (периодического «в*ыкалывания*» части символов кодовых слов по определённому правилу). В случае итеративного декодирования предпочтительным является *выкалывание* только *проверочных символов* кодера турбо-кода, хотя такая техника перфорации не гарантирует, что минимальное кодовое расстояние будет максимально. Так например, для повышения скорости турбо-кода с 1/3 до 1/2 перфоратор обычно *удаляет* символы с чётным номером на выходе первого компонентного кодера и с нечётным номером на выходе второго кодера или наоборот. Показано, что при этом перемежитель должен формироваться так, чтобы символы с чётным номером на входе перемежителя отображались также в символы с чётным номером на его выходе, а символы с нечётным номером на входе – в символы с нечётным номером на выходе. Совсем не обязательно производить *равнодолевое* выкалывание – для каждого компонентного кодера выкалывание может осуществляться в различных про-

порциях. При определённых условиях, это может *улучшить* характеристики декодера турбо-кода. Так в работе К. Берроу [23] на один удалённый символ с выхода первого компонентного кодера приходится три удалённых символа на выходе второго кодера.

Перфорация позволяет устанавливать *произвольное значение кодовой скорости*, *адаптируя* таким образом параметры турбо-кода к свойствам канала. Если в канале возрастает уровень шумов, то уменьшение степени перфорации вносит в кодированный блок дополнительную *избыточност*ь, т.е. повышает корректирующие способности кода, хотя и снижает его скорость.

Высокая эффективность использования турбо-кодов во многом обязана разработанным для них алгоритмам декодирования. В первую очередь следует отметить, что в основе декодирования любых корректирующих кодов лежит *сравнение вероятностных характеристик* различных кодовых слов, а применительно к свёрточным кодам – различных путей на решётчатой диаграмме. Если есть некоторое предварительное знание о надёжности принятого сообщения до его декодирования, то такая информация называется *априорной* и ей соответствует *априорная вероятность*. В противном случае имеет место только *апостериорная информация*. При декодировании турбо-кодов существенным является использование обоих видов информации.

Из практики помехоустойчивого кодирования хорошо известно, что использование нескольких *повторных циклов декодирования (итераций)* одного и того же принятого сообщения может значительно улучшить корректирующие способности кода. Одной из главных особенностей декодирования турбо-кодов является использование принципа *повторного* или *итеративного декодирования*. При этом экспериментально установлено, что наилучшие результаты получаются в схеме *с обратной связью,* когда информация в *мягком виде* с выхода последнего элементарного декодера поступает на вход первого.

На рис. 11.5 приведена структурная схема декодера турбо-кода, состоящего из двух *элементарных* декодеров (каждый из них осуществляет декодирование своего компонентного свёрточного кода), двух перемежителей и двух *деперемежителей*. Перемежители аналогичны тому перемежителю, который использовался в кодере. Деперемежители осуществляют *операцию, обратную перемежению*.

Первый декодер в схеме на рис. 11.5 имеет только один выход, на который поступает *внешняя информация*, полученная этим декодером в процессе декодирования. Внешняя информация, вырабатываемая декодером для каждого принятого символа, представляет собой непрерывную величину, модуль которой пропорционален *надёжности* этого символа (его *правдоподобию*), а знак соответствует значению символа (–1) или (+1).

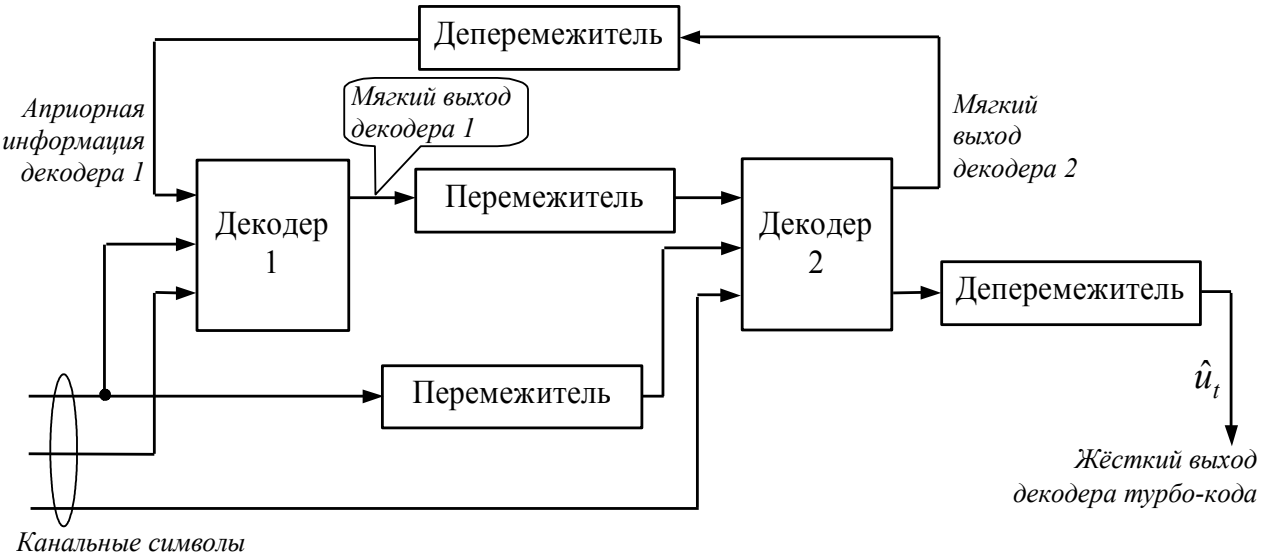


Рисунок11.5 – Структурная схема декодера турбо-кода со скоростью 1/3

Практически найдено, что в итеративном декодере удобнее использовать *логарифм отношения правдоподобия:*

$$L(\hat{u}_t) = \ln \frac{P(\hat{u}_t = +1 \mid \overline{X})}{P(\hat{u}_t = -1 \mid \overline{X})} \quad , \tag{11.3}$$

где $\hat{u}_t$ – текущая оценка информационного символа;

$\overline{X}$ – последовательность на входе декодера турбо-кода.

После выполнения определённого числа итераций, декодер 2 выносит решение, с учётом операции деперемежения, о декодированных символах по правилу:

$$\hat{u}_t = sign[L(\hat{u}_t)]. \tag{11.4}$$

Важным является то, что внешняя информация о каждом декодируемом символе, вырабатываемая элементарным декодером с использованием сведений, содержащихся только в проверочной группе данного компонентного кода, поступая на вход следующего элементарного декодера, подвергается *перестановке.* Таким образом, она оказывается некоррелированной с мягкими канальными символами на входе декодера, и может быть использована в качестве *априорной.*

На рис. 11.6 приведены результаты моделирования характеристик декодирования турбо-кода со скоростью 1/3 и компонентными РССК (1, 17/15) при использовании различного числа итераций*. Из графиков видно, что при увеличении числа итераций помехоустойчивость кода *значительно улучшается*, особенно в области малых и средних значений $E_б/N_0$. При $E_б/N_0$>2,5 дБ количество итераций более 3 уже *не даёт ожидаемого выигрыша.*

* Моделирование выполнено аспирантом С.Д. Прокоповым

Алгоритмы декодирования компонентных кодов в составе турбо-кодов используют *мягкое решение как по входу, так и по выходу*. По этой причине они получили название алгоритмов с *мягким входом – мягким выходом SISO* (*Soft Input – Soft Output*). К их числу относятся алгоритм Витерби с мягким выходом *SOVA* (*Soft Output Viterbi Algorithm*), алгоритм декодирования по максимуму апостериорной вероятности *MAP* (*Maximum Aposteriori Probabilities*), который иногда называют алгоритмом *BCJR* (*Bahl-Cocke-Jelinek-Raviv*) либо алгоритмом Баля, а также упрощённые алгоритмы *max-log-MAP* и *log-MAP*. Алгоритм *SOVA* осуществляет декодирование по максимуму правдоподобия, минимизируя вероятность ошибочного декодирования последовательности принятых символов. Из всех перечисленных выше алгоритмов типа *SISO* этот алгоритм *наиболее прост в реализации*, однако обладает несколько худшими характеристиками декодирования. Алгоритм *MAP* сформулирован для линейных кодов и позволяет *минимизировать вероятность ошибки* информационного символа (бита). Долгое время алгоритм *MAP* оставался невостребованным ввиду значительно большей вычислительной сложности по сравнению с алгоритмом Витерби. Однако с появлением турбо-кодов интерес к алгоритму *MAP* возобновился. Это объясняется особенностями итеративного декодирования турбо-кодов, при котором незначительное превосходство алгоритма *MAP* перед алгоритмом *SOVA* на каждом шаге декодирования позволяет получить *существенный дополнительный* ЭВК при многократном повторении итераций.

Как отмечалось выше, главным *достоинством* турбо-кодов является наибольшая энергетическая эффективность систем с их использованием. Турбо-коды позволили максимально приблизиться к пределу Шеннона, причем, нереализованный запас составляет менее 1 дБ. При этом, в связи с тем, что турбо-коды состоят из *стандартных* свёрточных кодов, многие вопросы кодирования-декодирования хорошо решены на практике.

Однако турбо-кодам, как и всем другим корректирующим кодам, свойственны некоторые реализационные *особенности*, о которых следует упомянуть. Типичные кривые вероятности ошибочного декодирования имеют так называемую область "*порога ошибок*" (*error floor*), в которой их наклон резко уменьшается (см. рис.11.6). При этом, для достижения малых вероятностей ошибки ($P_б$=10^{-8}…10^{-11}) необходимы значительные затраты энергетических ресурсов (большое значение $E_б/N_0$).

Это объясняется относительно малым минимальным кодовым расстоянием турбо-кодов, которое начинает доминировать при средних и больших значениях отношения $E_б/N_0$.

К методам снижения влияния порога ошибок следует отнести:

1. *Оптимизацию* компонентных кодов и *структуры перемежителя*. Эти методы позволяют достичь вероятность ошибки декодирования бита (10^{-8}…10^{-11}) до появления явно выраженной области "*порога ошибок*".

2. *Последовательное каскадирование* турбо-кодов стандартными блоковыми кодами (БЧХ, циклическими кодами либо кодами Рида-Соломона). Данный метод практически полностью устраняет эффект "*порога ошибок*" взамен на снижение кодовой скорости и увеличение сложности.

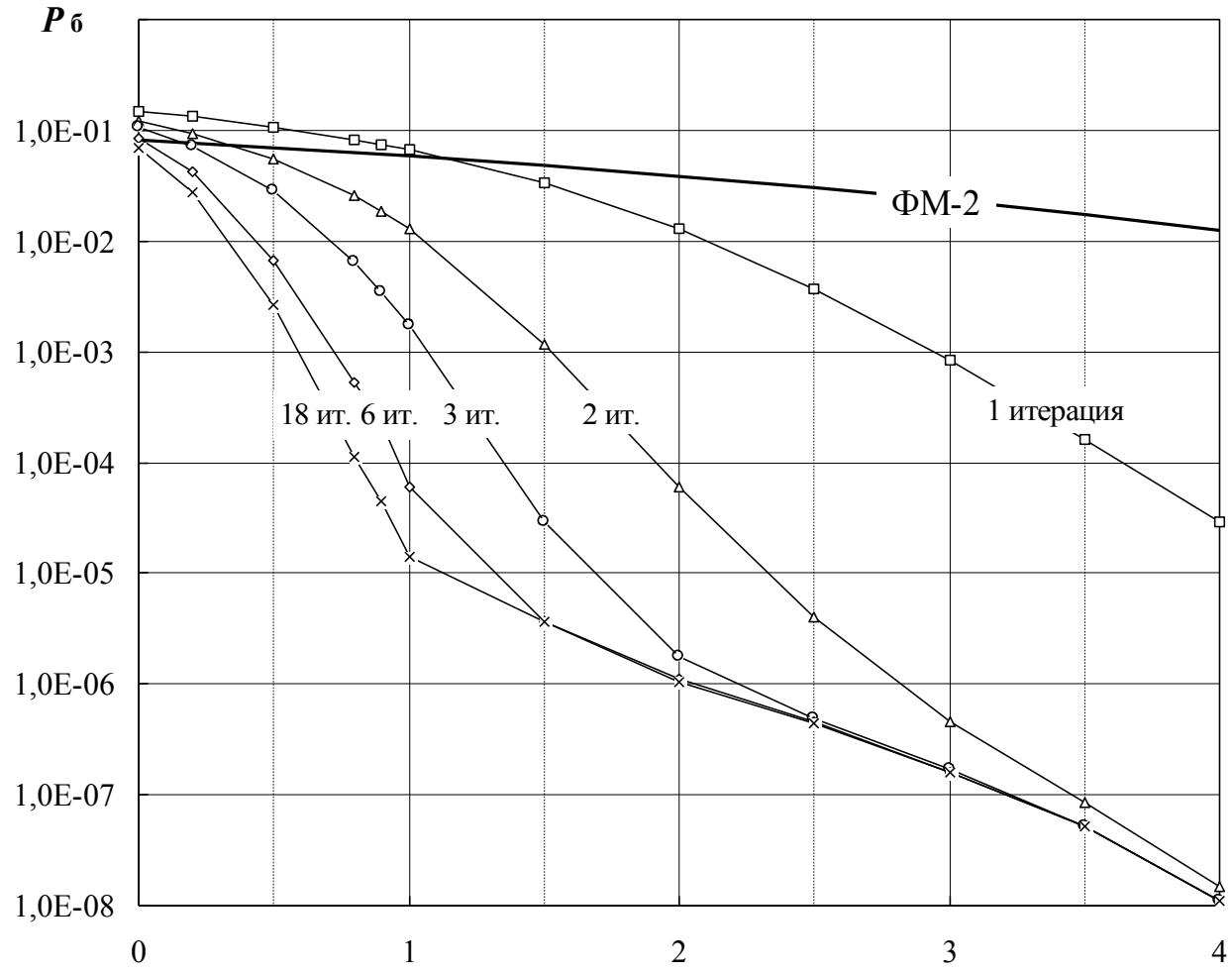


Рисунок 11.6 – Влияние числа итераций на помехоустойчивость турбо-кода $E_б/N_0$, (дБ) R=1/3 и длиной перемежителя 1000 символов. Алгоритм декодирования компонентных кодов *log-MAP*

Известно, что с увеличением длины перемежителя улучшаются характеристики турбо-кода. Однако это приводит к еще одному *существенному недостатку* – увеличивается *время декодирования*. Общую задержку на обработку принятого сообщения $T_з$ можно определить, используя выражение:

$$T_з = \frac{2 \cdot N}{R_и} + 2 \cdot T_{дек} \cdot Q + T_р, \qquad (11.5)$$

где N – длина перемежителя;

$R_и$ – скорость информационного потока;

$T_{дек}$ – задержка, вносимая одним элементарным декодером;

Q – число итераций;

$T_р$ – время распространения сигнала в канале связи.

На практике для уменьшения задержки обработки у*меньшают размеры перемежителя и число итераций,* а также уменьшают задержку, вносимую элементарным декодером путём оптимизации алгоритмов декодирования и *повышения тактовой частоты вычислительного устройства*.

При разном значении $E_б/N_0$ в канале связи эффективное число итераций декодера турбо-кода различно, что подтверждают графики на рис. 11.6.

Одновременно с появлением в научной печати первых публикаций по турбо-кодам начались широкие исследования возможностей применения принципа турбо-кодирования в перспективных телекоммуникационных системах. Ниже приведены примеры таких реализаций.

*1.Модем CMD–550T с турбо-кодированием для спутниковых каналов***.** Системы цифровой спутниковой связи являются типичной сферой для внедрения разработок теории кодирования. Это обусловлено тем, что получение энергетического выигрыша от кодирования позволяет существенно ослабить требования к энергетике спутникового канала, которая ограничена энергоресурсами бортового ретранслятора и малыми размерами приемной антенны. Традиционным здесь является использование сверточных кодов(СК в табл.11.1) с различными скоростями (1/2, 3/4, 7/8), последовательных каскадных конструкциях с внутренним СК, внешним кодом Рида-Соломона(РС). На рынке модемов для спутниковой связи предлагаются модемы, параметры которых приведены в табл. 11.1. В силу большого энергетического выигрыша за счет применения турбо-кодов, модем *CMD–550T,* по сравнению с предыдущей модификацией *CMD–550*, обеспечивает дополнительный ЭВК=2.7 дБ при 40% экономии полосы.

Таблица 11.1 – Низкоскоростные спутниковые модемы

Наименование	*CM*—601	*DMD*24011	*CDM*–550	*CDM*–550 T
Призводитель	*Com Stream*	*Com Stream*	*Comtech*	*Comtech*
Диапазон частот, МГц	52–88	950–1450	52–88, 104–176	52–88, 104–176
Скорость, кбит/с	4,8–512	9,6–2048	2,4–512	2,4–512
Модуляция Внешний код Внутренний код	ФМ–2, ФМ–4 РС СК(1/2, 3/4, 7/8)	ФМ–2, ФМ–4 (СФМ–4) РС СК(1/2, ФМ–2) СК(1/2, 3/4, 7/8, ФМ–4)	ФМ–2, ФМ–4, СФМ–4 РС СК(1/2, ФМ–2) СК(1/2, 3/4, 7/8, ФМ–4)	ФМ–2,ФМ–4, СФМ–4, ФМ8 Турбо-код РС СК(1/2, ФМ–2) СК(1/2, 3/4, 7/8, ФМ–4) СК(2/3, ФМ–8)
Величина $E_б/N_0$, необходимая для обеспечения вероятности ошибки10^{-7}			6.7 *dB*	4.0 *dB*

Обозначения в таблице:

ФМ-2 – двоичная фазовая модуляция;

ФМ-4 – четверичная фазовая модуляция;

ФМ-8 – фазовая модуляция с числом позиций фазы 8.

2. Применение турбо-кодов в оптической системе передачи цифровой информации методом импульсной позиционной модуляции (*PPM – Pulse Position Modulation*) с кодовым разделением источников пользователей (*CDMA*). Описанный в работе [48] проект *CDMA-PPM* является примером применения турбо-кодов в системах волоконно-оптической связи для исправления случайных ошибок.

3. В последние годы международные организации проводят работы по стандартизации турбо-кодов в качестве метода канального кодирования в *системах передачи телеметрической информации с космических аппаратов* по рекомендации *CCSDS* (*Consultative Committee for Space Data Systems*) [28]. В данном документе рекомендовано использование турбо-кодов со скоростями R=1/2, 1/3, 1/4, 1/6 и компонентными РССК с длиной кодового ограничения $\nu = 4$. Выбраны следующие длины информационного блока: 1784, 3568, 7136, 8920 и 16384 символов.

4. Применение турбо-кодов предусмотрено в системах подвижной радиосвязи третьего поколения по стандарту *UMTS* (*Universal Mobile Telecommunications System*).

5. Рекомендацией Европейского института по стандартизации *ETSI* (*European Telecommunications Standards Institute*) [29] определены следующие параметры турбо-кода: скорость кода 1/3, компонентные РССК (1, 13/15) с $\nu = 3$, длина информационного блока (40…5114) символов. Для декодирования используется алгоритм *log-MAP*.

6. Системы *цифрового телевизионного вещания стандарта DVB-RSC* (*Digital Video Broadcasting Reverse Satellite Channel*)[29].

Высокая эффективность турбо-кодирования вызвала поток исследований по оценке эффективности применения турбо-кодов в различных телекоммуникационных приложениях. Перечислим основные из них:

– применение параллельной каскадной схемы кодирования (турбо-кодов) в каналах с межсимвольной интерференцией;

– применение турбо-кодов в системах разнесенного приема с пространственно временным кодированием;

– оценка возможности турбо-кодирования в системах авиационной связи;

– анализ алгоритма совместного декодирования турбо-кодов и восстановления несущей;

– применение турбо-кодов в системах с высокой частотной эффективностью на основе решетчатой модуляции.

11.2. Пространственно-временное кодирование в системах беспроводной связи

В каналах радиосвязи, в частности, в каналах систем мобильной связи действует комплекс помех и искажений. В первую очередь, необходимо учитывать влияние многолучевости в среде распространения радиоволн, частотно-селективные замирания, сдвиги частоты и фазы несущей за счет эффекта Допплера, а также интерференционные помехи от сигналов других пользователей. Сильные

з*амирания* сигнала в канале затрудняют оценку переданных сообщений и приводят к *ухудшению качества* передачи информации. Традиционным методом повышения помехоустойчивости таких систем является *разнесение.*

В прежние годы сфера применения *разнесенного приема* ограничивалась коротковолновой радиосвязью, где использовались хорошо апробированные методы и техника. Идея разнесенного приема была реализована в 1927 г. для организации радиотелефонной коротковолновой связи. С 1931 г. разнесенный прием начал применяться в радиотелеграфной связи. Впервые методы теории вероятностей к разнесенному приему были применены в конце 30-х годов прошлого столетия. Потребовалось, однако, еще 15-20 лет для разработки основных теоретических положений *статистической теории разнесенного приема*.

В последнее время, в связи с широким внедрением систем сотовой и мобильной спутниковой радиосвязи, потребовалось вернуться к этой проблематике. Хотя общая идеология разнесенного приема осталась прежней, изменились как характеристики каналов (переход в новые диапазоны частот, прием сигналов в более сложных условиях переотражений, наличие большого числа мешающих сигналов и т.д.), так и *методы* передачи сигналов по радиоканалам. Не менее важным является и то, что появилась возможность реализации более эффективных, но и более *сложных методов разнесения.*

Идея разнесения для борьбы с замираниями заключается в *совместном использовании* на приеме нескольких сигналов, несущих одну и ту же информацию, но пришедших *различными путями.* Разнесение должно выбираться таким образом, чтобы *вероятность одновременных замираний* всех используемых сигналов была много меньше, чем какого-либо одного из них. Иными словами, эффективность разнесения тем выше, чем менее *коррелированы замирания в парциальных каналах*.

Классический подход к реализации метода разнесения состоит в использовании одного передатчика и нескольких, *разнесенных в пространстве* приемных антенн с последующим *весовым суммированием* либо *автовыбором сигналов* с целью повышения качества приема. В условиях мобильной связи для участка «базовая станция – мобильный абонент» такая реализация *неприемлема*, поскольку использование нескольких приемных антенн и устройства комбинирования принимаемых сигналов делает мобильную станцию громоздкой и дорогой. Однако, возможна организация разнесенных каналов за счет использования *нескольких разнесенных антенн на передаче* (на базовой станции). Базовая станция обслуживает сотни и тысячи мобильных абонентов и более целесообразно усложнение аппаратуры небольшого числа базовых станций, нежели множества мобильных терминалов. При этом на участке «*мобильный абонент – базовая станция*» может осуществляться прием на те же разнесенные антенны базовой станции, но работающие в режиме приема. В некоторых существующих сотовых системах уже используются на базовых станциях две приемные антенны для разнесенного приема. Эти же антенны могут быть использованы для *разнесенной передачи.*

Системы с разнесенной передачей теоретически *исследованы значительно меньше*, чем системы с разнесенным приемом. Среди различных методов разне-

сения на передаче перспективным является ***пространственно-временное кодирование,*** реализация которого предполагает не только передачу информационных сигналов через несколько антенн, но и соответствующее их кодирование, что с учетом адекватной обработки их в приемнике, по сравнению с некодированной передачей через одну антенну, должно обеспечить *выигрыш*, как от *разнесения*, так и от *кодирования*.

Одной из основных целей внедрения систем мобильной связи третьего и четвертого поколений является предоставление абоненту услуг *широкополосного доступа*. Передача мультимедийных сообщений в реальном масштабе времени требует больших скоростей, в десятки раз превышающих скорости в существующих системах мобильной связи. Методы *пространственно-временного кодирования* обеспечивают лучший *обмен между частотной и энергетической эффективностью* и приняты во внимание при формировании стандартов третьего поколения систем мобильной радиосвязи (*CDMA*-2000*, W-CDMA*), других *служб беспроводной связи.* Рассмотрим классификацию и особенности методов разнесения.

Повышение качества связи в условиях многолучевости – сложная задача. В канале с постоянными параметрами и гауссовским шумом с помощью обычных методов помехоустойчивого кодирования можно *на порядок* понизить вероятность ошибок за счет увеличения отношения сигнал/шум (ОСШ) на (1...2) дБ. В каналах с замираниями добиться подобных результатов можно увеличением ОСШ примерно на 10 дБ. Однако простое увеличение мощности как абонентских, так и базовых станций в системах мобильной связи *нельзя признать конструктивным решением*, поскольку в этом случае чаще всего нарушаются требования по электромагнитной совместимости.

Адаптивное регулирование мощности передатчика является одним из возможных методов работы в каналах с замираниями. Если состояние канала, наблюдаемое на приемной стороне, известно и на передаче, в передатчике можно повысить уровень излучаемого сигнала с тем, чтобы *преодолеть влияние замираний*. В этом случае существуют две проблемы. Во-первых, необходим дополнительный динамический диапазон в передатчике. Во-вторых, на передающей стороне должно быть известно текущее состояние канала. Исключение составляют случаи, когда прямая и обратная передачи организованы на одной частоте, как это имеет место при *временном дуплексном разделении* (*TDD*) прямого и обратного каналов связи. По этой причине режим *TDD* рассматривается как перспективный для будущих поколений мобильных систем. В иных случаях необходимость обратного канала усложняет систему и приводит к снижению скорости передачи

В зависимости от способов формирования разнесенных каналов различают *несколько вариантов методов разнесения.*

Частотное разнесение. Информационные сигналы, передаваемые на разных частотах, подвергаются при многолучевом распространении воздействию *различных искажений*. Для получения выигрыша несущие частоты должны быть достаточно разнесены, чтобы замирания в ветвях были *некоррелированными.* Платой за повышение помехоустойчивости является *расширение занимаемой*

полосы частот. При этом также возможно применение кодирования с исправлением ошибок в сигналах парциальных частотных каналов, которые могут возникать вследствие *частотно-селективных замираний*. Известный метод частотного мультиплексирования и передачи информации по разнесенным по частоте узкополосным подканалам (*OFDM*) можно также использовать в режиме частотного разнесения.

Временное разнесение. Когда одно и то же сообщение посылается по каналу в разные отрезки времени, замирания принимаемых сигналов могут быть некоррелированными, если *достаточен временной разнос* между ними. Если передаваемые сигналы разнесены на время, большее *времени когерентности* канала, то вероятность того, что сигналы в разных ветвях подвержены действию одних и тех же *глубоких замираний,* достаточно мала. Для повышения помехоустойчивости дополнительно может быть использовано к*анальное кодирование в сочетании с перемежением во времени.* Эффективность временного разнесения зависит от *скорости перемещения* мобильной станции. Когда параметры канала изменяются во времени медленно, необходимо перемежение с большой памятью, что приводит к большим задержкам в передаче сообщений. По этой причине кодирование с перемежением *эффективно* лишь в каналах с быстрыми замираниями (в условиях «б*ыстрой*» мобильности) и малоэффективно в каналах с медленными замираниями («*медленная*» мобильность или *фиксированная беспроводная связь*). В среднем *временной разнос* каналов обратно пропорционален скорости передвижения мобильного терминала.

Пространственно-разнесенный прием. Нередко *параллельные каналы* образуются в результате особенностей механизма распространения радиоволн. При многолучевом распространении один и тот же сигнал приходит к месту расположения приемной антенны по нескольким путям. Применяя ряд *остронаправленных приемных антенн*, можно *разделить лучи* по углам прихода и рассматривать информационные сигналы как пришедшие по *параллельным каналам.* Если энергетический спектр сигнала достаточно широк по сравнению с величиной, обратной запаздыванию соседних лучей, то, как известно, эти лучи можно *разделить* в приемнике, т.е. осуществить *разнесенный прием по лучам.* Другой способ образования параллельных пространственно разнесенных каналов заключается в том, что сигнал принимается несколькими антеннами, находящимися на значительном расстоянии друг от друга. При этом каждая из антенн принимает сумму всех приходящих лучей. Однако вследствие различных фазовых соотношений между ними интерференционные замирания в различных антеннах оказываются слабо коррелированными. Благодаря этому сигналы в различных антеннах дополняют друг друга и их совместный анализ позволяет существенно повысить верность приема. Можно осуществить также **поляризационно-разнесенный прием**, используя антенны, принимающие волны с различными векторами поляризации. Возможно также *комбинирование* перечисленных выше методов.

Перечисленные выше методы разнесенного приема характерны тем, что передатчик излучает один сигнал (как при обычной одноканальной передаче), а

различные образцы принимаемого сигнала формируются в процессе распространения или приема.

Несмотря на все разнообразие методов разнесенного приема, принципы, положенные в их основу, ничем *существенно не отличаются*. Это позволяет построить единую теорию разнесенного приема, результаты которой одинаково применимы ко всем перечисленным выше системам. Разумеется, необходимо учитывать и некоторые особенности различных методов разнесения. Так, например, при разнесении по углу прихода или по лучам средние значения мощностей сигнала и интенсивностей помех в различных каналах, как правило, различны, тогда как в других системах разнесения они чаще всего одинаковы.

При различных видах разнесения мощность сигнала различным образом распределяется по отдельным каналам. Тем не менее, теория разнесенного приема может быть сделана достаточно *общей*, охватывающей все указанные случаи.

Помехоустойчивость приема разнесенных сигналов зависит от метода их *объединения (комбинирования) на приеме.* Все известные методы комбинирования подразделяются на три группы:

1.*Весовое сложение сигналов* отдельных ветвей по критерию максимума отношения сигнал/шум на выходе схемы сложения.

2.*Автовыбор канала с наибольшим отношением сигнал/шум.*

3.*Линейное сложение сигналов парциальных каналов.*

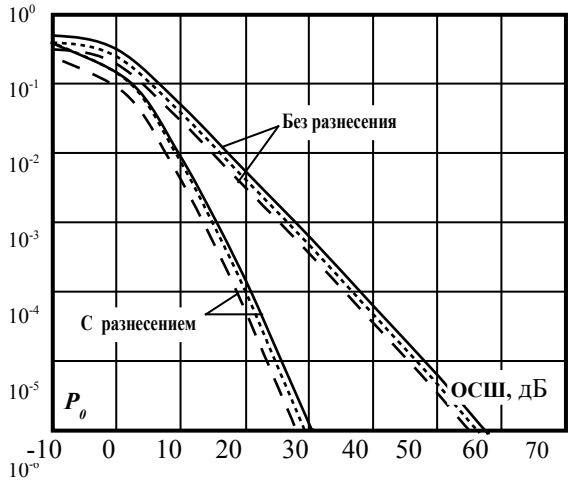


Рисунок 11.7 – помехоустойчивость разнесенного приема

Первый метод дает наилучшую помехоустойчивость, тогда как последний метод комбинирования наиболее просто реализуется. Кроме того, помехоустойчивость разнесенного приема зависит также от используемого *метода детектирования.* На рис. 11.7 приведены результаты расчетов вероятности ошибки приема двоичных символов P_0 при двухканальном разнесенном приеме сигналов минимальной частотной модуляции (*MSK)* в каналах с релеевскими замираниями и весовым сложением принимаемых сигналов. В интересной для практики области вероятностей ошибки ($10^{-5}…10^{-6}$) энергетический выигрыш за счет разнесения на приеме составляет (20…25) дБ.

Как отмечалось выше, известны методы разнесения, при которых параллельные каналы формируются при передаче. Рассмотрим эти методы более подробно.

На рис. 11.8 представлена *базовая структура* классической системы передачи сигналов по каналам с замираниями с двумя ветвями разнесения на приеме. Используется комбинирование сигналов по критерию максимального отношения сигнал/помеха.

Сигнал S_0 посылается передатчиком через передающую антенну. Передаточные функции каналов включают учет влияния цепей на передающей и приемной стороне, искажения сигналов в радиоканале и моделируются как функции следующего вида:

$$h_0 = \alpha_0 e^{j\theta_0},$$
$$h_1 = \alpha_1 e^{j\theta_1},$$

где α_0, α_1 – модули передаточных функций на участке «передающая антенна – приемная антенна» (приемные антенны с номерами 0 и 1, соответственно).

На входах приемников действуют аддитивные смеси сигналов $h_0 s_0\,(h_1 s_0)$ и шумов совместно с интерференцией n_0 (n_1, соответственно):

$$r_0 = h_0 s_0 + n_0,$$
$$r_1 = h_1 s_1 + n_1. \qquad (11.6)$$

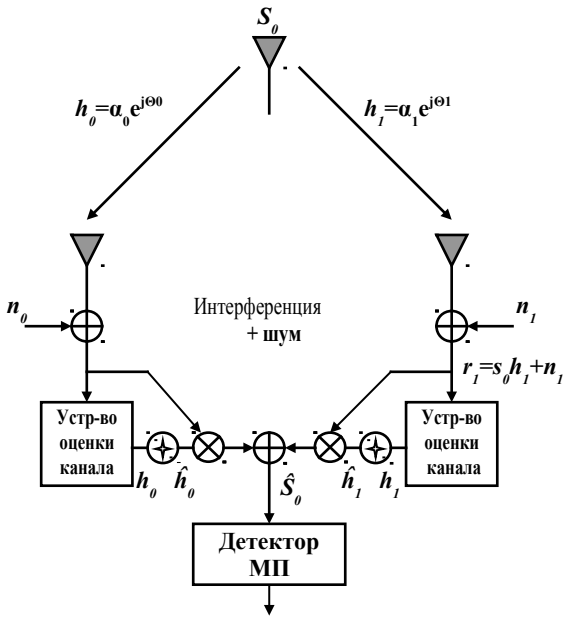


Рисунок 11.8 – Передача сигналов по каналам с замираниями и разнесением приемных антенн

Полагая, что аддитивные помехи n_0 и n_1 распределены по гауссовскому закону, можно сформулировать в общем виде *решающее правило* максимально правдоподобного приема сигнала s_i:

$$d^2(r_0, h_0, s_i) + d^2(r_1, h_1, s_i) \le d^2(r_0, h_0, s_k) + d^2(r_1, h_1, s_k),\ i \ne k, \qquad (11.7)$$

где $d^2(x, y)$ есть евклидово расстояние между x и y. Вычисление (11.7) приводит к следующему результату:

$$(\alpha_0^2 + \alpha_1^2)|s_i|^2 - \tilde{s}_0 s_i^* - \tilde{s}_0^* s_i \le (\alpha_0^2 + \alpha_1^2)|s_k|^2 - \tilde{s}_0 s_k^* - \tilde{s}_0^* s_k,\ i \ne k \qquad (11.8)$$

Для сигналов с одинаковыми энергиями выражение (11.8) упрощается:

$$d^2(\tilde{s}_0, s_i) \le d^2(\tilde{s}_0, s_k),\ i \ne k. \qquad (11.9)$$

Детектор максимального правдоподобия (рис.11.8) работает по правилу(11.9).

На рис.11.9 представлена структура системы, в которой функции разнесения реализованы *на передающей стороне.*

На приемной стороне используется *одна антенна* и реализуется решающее правило приема по максимуму правдоподобия. Передача сигналов организована следующим образом (см. табл. 11.2). В момент времени t через антенну с номером 0 передается сигнал s_0, а через антенну с номером 1 – сигнал s_1. В следующий момент $(t+T)$ передается, соответственно, сигнал $-s_1^*$ и s_0^* (* – знак комплексного сопряжения).

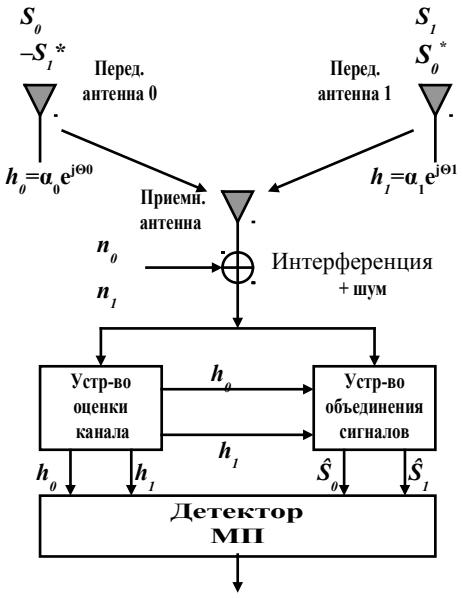


Рисунок 11.9 – Передача сигналов с разнесением передающих антенн

Таблица11.2 – Порядок передачи символов

	Антенна 0	Антенна 1
Момент t	s_0	s_1
Момент $t+T$	$-s_1^*$	s_0^*

Предполагается, что условия замираний остаются неизменными на интервале двух соседних символов, т. е.

$$h_0(t) = h_0(t+T) = \alpha_0 e^{j\theta_0}, \qquad (11.10)$$
$$h_1(t) = h_1(t+T) = \alpha_1 e^{j\theta_1}.$$

Принимаемые сигналы могут быть выражены следующим образом:

$$r_0 = r(t) = h_0 s_0 + h_1 s_1 + n_0; \qquad (11.11)$$
$$r_1 = r(t+T) = -h_0 s_1^* + h_1 s_0^* + n_1.$$

Формируемые на приеме оценки сигналов (см. рис. 11.10) определяются как:

$$\tilde{s}_0 = h_0^* r_0 + h_1 r_1^*; \qquad (11.12)$$

$$\tilde{s}_1 = h_1^* r_0 - h_0 r_1^*.$$

С учетом этого получаем

$$\tilde{s}_0 = (\alpha_0^2 + \alpha_1^2)s_0 + h_0^* n_0 + h_1 n_1^*. \qquad (11.13)$$

Нетрудно убедиться в том, что решающее правило совпадает с таким же правилом для схемы с разнесением на приеме, причем, поворот фазы в шумовом компоненте не влияет на величину отношения сигнал/шум. Следовательно, по помехоустойчивости *схемы* с разнесением на приеме (рис. 11.8) и разнесением на передаче (рис. 11.9) *эквивалентны.*

Результаты моделирования различных вариантов описанных выше систем разнесения показаны на рис.11.10. Рассмотрены варианты разнесения только на передаче, только на приеме и одновременное разнесение передающих и приемных антенн:

1 – без разнесения.

2 – одна передающая антенна, две приемных антенны.

3 – одна передающая антенна, четыре приемных антенны.

4 – две передающих антенны, одна приемная антенна.

5 – две передающих антенны, две приемных антенны.

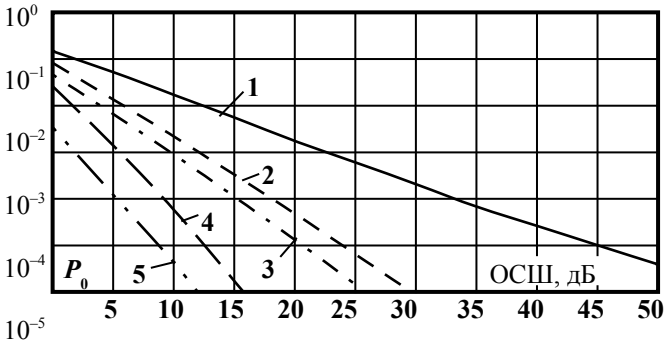


Рисунок 11.10 – Сравнение помехоустойчивости методов разнесения:

1 – без разнесения;

2 – одна передающая антенна, две приемных антенны;

3 – одна передающая антенна, четыре приемных антенны;

4 – две передающих антенны, одна приемная антенна;

5 – две передающих антенны, две приемных антенны

Моделирование подтверждает высокую эффективность разнесения как на приеме, так и на передаче. Наилучшие результаты получены для сочетания разнесения на передаче и на приеме. Одним из перспективных методов разнесения является **пространственно - временное кодирование.**

Используемые во многих современных системах передачи информации методы корректирующего кодирования реализуют, по существу, *разнесение во времени*. При одноканальной передаче (одна передающая и одна приемная антенны) пакет ошибок можно трактовать как результат действия сильного замирания сигнала. Даже короткие блоковые либо сверточные коды в сочетании с эффективными перемежителями позволяют исправлять достаточно длинные пакеты ошибок в каналах. Поэтому сочетание рассмотренных в предыдущем разделе методов разнесения и методов корректирующего кодирования вполне *целесообразно.*

Идеи пространственно–временного кодирования (ПВК) возникли на базе результатов и как развитие методов разнесения на передаче. По существу, простейший короткий блоковый код уже был представлен выше в табл. 11.2, кото-

рую можно трактовать как кодовую таблицу. При традиционном корректирующем кодировании вводится *избыточность во временной области.*

В системах с ПВК вводится *избыточность* и в *пространственной области*, образованной несколькими приемными и передающими антеннами (рис. 11.11). При ПВК возможно получение дополнительного выигрыша за счет усложнения методов передачи и обработки сигналов на приеме.

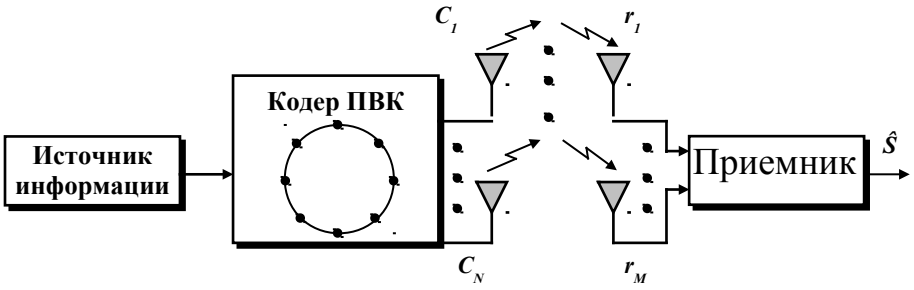


Рисунок11.11 – Модель системы с пространственно - временным кодированием

На рис. 11.12 представлен простой пример кодера на передаче, конфигурации сигнального созвездия и решетчатой диаграммы ПВК.

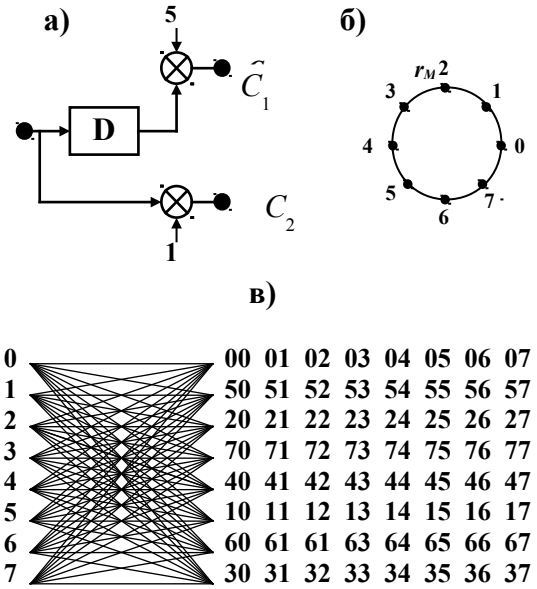


Рисунок 11.12 – Кодер (а), сигнальное созвездие (б) и решетчатая диаграмма (в) ПВК

Кодирование производится в алфавите алгебраического кольца $Z(8)$ (кольцо целых чисел с операциями сложения и умножения по модулю 8).

Порождающие многочлены кодера ПВК отыскиваются на основе *перебора* по критерию максимизации энергетического выигрыша в канале с замираниями. Количество передающих и приемных антенн $N=M=2$. Выходы кодера C_1 и C_2 подключены к соответствующим входам передатчиков разнесенных передающих антенн. С целью повышения удельной скорости передачи информации в

модуляторах используется фазовая модуляция ФМ-8. Соответствующее сигнальное созвездие показано на рис.11.12 б. Число состояний ПВК определяется структурой кодера и равно S=8. Порождающие многочлены кодера в восьмеричной форме записи имеют вид (5D, 1) (*код с единичной памятью*).

Один шаг решетчатой диаграммы ПВК (рис. 11.12 в) содержит наборы предыдущих и последующих состояний (1…7) и соединяющих их ветвей. Каждая ветвь маркируется парой символов на выходе кодера C_1C_2. В правой части диаграммы показаны строки с парами символов, маркирующими ветви, выходящие из конкретного состояния в порядке их перечисления сверху вниз. К примеру, пара символов (C_1C_2)=(52), расположенная во второй строке на втором месте слева маркирует ветвь, соединяющую предыдущее состояние «1» с последующим состоянием «2». Предполагается, что обработка сигналов на приеме производится путем декодирования по решетке ПВК на основе *алгоритма Витерби.*

На рис. 11.13 приведены результаты моделирования ПВК в канале с замираниями.

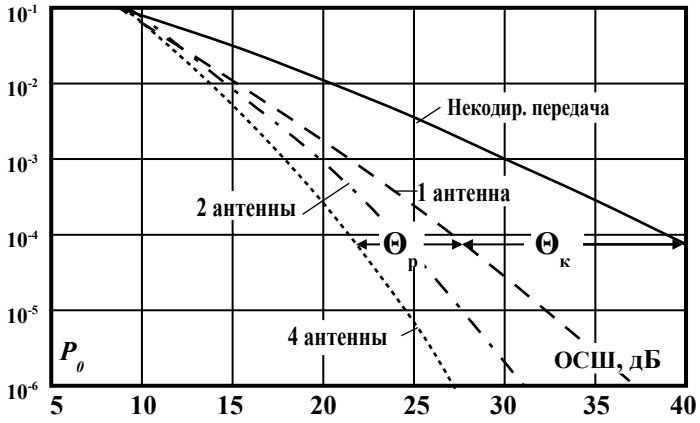


Рисунок 11.13 – Помехоустойчивость ПВК

При использовании одной антенны на передающей и одной антенны на приемной стороне величину $\Theta_к$ можно трактовать как энергетический выигрыш за счет помехоустойчивого кодирования.

Увеличение количества передающих антенн (2 либо 4 антенны) при одной приемной антенне дает дополнительный выигрыш $\Theta_р$ за счет *разнесения на передаче*. Величины этого выигрыша не очень велики, поскольку используется короткий помехоустойчивый код.

Методы пространственно-временного кодирования обладают большой *гибкостью* и позволяют применять различные методы помехоустойчивого кодирования, в том числе и эффективные *недвоичные коды Рида–Соломона*.

В сочетании с сигнальными созвездиями и плотной укладкой сигнальных точек применение ПВК обеспечивают не только высокую помехоустойчивость, но и высокую удельную скорость передачи информации по каналам с ограниченной полосой частот. К примеру, использованием созвездия КАМ-16 в системе с двумя передающими и двумя приемными антеннами достигается скорость

передачи 74,4 Кбит/с с при ОСШ, равном 16 дБ. Эта скорость в 2,6 раза выше скорости передачи в системе на базе стандарта *IS*-136 (28,8 Кбит/с).
Анализ показывает, что применение ПВК дает хорошие результаты, даже когда имеется корреляция между сигналами передающих антенн. Однако при реализации выигрыша необходимо применять *многоканальные корректоры.*

11.3. Помехоустойчивое кодирование в волоконно-оптических системах передачи

Успех модернизации существующих и создания новых волоконно-оптических систем передачи (ВОСП) определяется эффективностью используемых методов формирования сигнала, его передачи и приема. Под эффективностью телекоммуникационных систем понимают степень использования ресурсов, затрачиваемых на единицу передаваемой информации [15]. Под э*ффективностью* ВОСП будем понимать отношение скорости информационного потока, передача которого на заданное расстояние обеспечивается системой, к объёму затрат на ее создание и эксплуатацию. Эффективность таких ВОСП можно *повысить двумя путями*:

1.Повышением *степени использования физической среды* распространения сигнала, т.е. оптического волокна. Этот способ известен и реализуется технологией *волнового* (по длине волны) *мультиплексирования* (*WDM*).

2.*Увеличением длины* волоконно-оптической линии передачи при заданной вероятности ошибки, которое может быть обеспечено при применении *помехоустойчивого кодирования* передаваемого цифрового потока, и последующего *декодирования с исправлением ошибок.* При этом возможно снижение отношения сигнал/шум на входе приёмной части ВОСП и адекватное *увеличение длины линии передачи*.

Теория помехоустойчивого кодирования предлагает широкий набор методов кодирования [11]. Каждый метод характеризуется величиной *энергетического выигрыша кодирования* Θ, скоростью кода R, сложностью алгоритма кодирования/декодирования и, соответственно, сложностью и быстродействием декодера. В разделе дан анализ эффективности применения методов помехоустойчивого кодирования в ВОСП.

Энергетический выигрыш кодирования (ЭВК). Применение корректирующих кодов, исправляющих ошибки, возникающие в канале с шумами, позволяет снизить вероятность ошибок в потоке символов на выходе декодера и получить определенный энергетический выигрыш. Если зависимость вероятности ошибки p на выходе системы передачи без кодирования от отношения сигнал/шум ОСШ(дБ) на входе приемника ВОСП характеризуется кривой 1 на рис.11.14, то при использовании помехоустойчивого кодирования с исправлением ошибок вероятность ошибки снижается, как показано стрелками на рис. 11.14 (кривая 2-КК – корректирующий код).

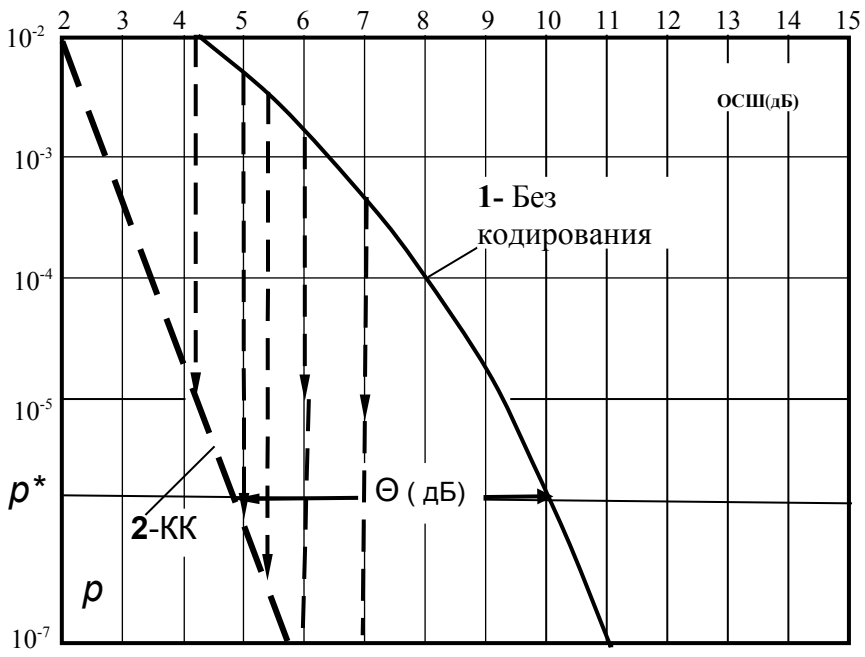


Рисунок 11.14 – К определению ЭВК

Видно, что для обеспечения заданной вероятности ошибки p^* система с кодированием требует *меньших значений* отношения сигнал/шум (ОСШ), обеспечивая определенный *энергетический выигрыш* Θ, обычно измеряемый в дБ. Значения энергетического выигрыша для конкретного метода кодирования устанавливают расчетным путем, на основе имитационного моделирования, либо с использованием прямого эксперимента.

Величина отношения сигнал/шум ОСШ на входе приемной части волоконно-оптической системы передачи определяется *уровнем мощности оптического сигнала* $P_{о,с}$ и приведенным ко входу приемника ВОСП *уровнем шумов* $P_{о,ш}$ всего тракта передачи (включая шумы электронно-оптического преобразователя (лазера) на передающей стороне, тепловые шумы резистора нагрузки оптико-электронного преобразователя(ОЭП) и следующего за ним электронного усилителя[44]). Мощность оптического сигнала на входе ОЭП $P_{о,с}$(дБм)=$P_{о,пер}$(дБм) – α(дБ) определяется уровнем мощности оптического сигнала, вводимого в волокно на передающей стороне $P_{о,пер}$(дБм) и суммарным затуханием волоконно-оптического канала передачи α(дБ), которое при длине оптического волокна L(км) и усредненном коэффициенте затухания α_0(дБ/км) определяется выражением[44]: α(дБ)=α_0(дБ/км)L(км). При проектировании цифровых ВОСП обычно задают величину вероятности ошибки на бит в передаваемом цифровом потоке p^*.

Рассмотрим энергетические соотношения в ВОСП с длиной оптического волокна L(км). Пусть, в системе без кодирования с заданными параметрами $P_{о,пер}$(дБм), $P_{о,ш}$(дБм) и α_0(дБ/км) для обеспечения вероятности ошибки p^* необходимо отношение сигнал/шум, равное

ОСШ*(дБ)=$P_{о,с}$(дБм)–$P_{о,ш}$(дБм) =$P_{о,пер}$(дБм)–$P_{о,ш}$(дБм) – α_0(дБ/км)L(км).

Для выяснения роли помехоустойчивого кодирования положим, что длина оптического волокна увеличена на величинуΔL. В этих условиях возрастет суммарное затухание волоконно-оптического канала передачи α(дБ) до значения α(дБ)=α_0(дБ/км)($L+\Delta L$)(км), вследствие чего отношение сигнал/шум на входе приемной части ВОСП понизится на величину ΔОСШ(дБ)=α_0(дБ/км)ΔL(км). Это снижение ОСШ можно *скомпенсировать* применением помехоустойчивого кодирования с энергетическим выигрышем Θ(дБ)=ΔОСШ(дБ)=α_0(дБ/км)ΔL(км). Отсюда следует простое выражение для длины участка, на которую можно *увеличить протяженность волоконно-оптической линии передачи* в системе с помехоустойчивым кодированием:

$$\Delta L(км) = \frac{\Theta\ (дБ)}{\alpha_0(дБ/км)}, \qquad (11.14)$$

где Θ(дБ) – энергетический выигрыш, обеспечиваемый прменением помехоустойчивого кодирования при заданной вероятности ошибки p*;

α_0(дБ/км) – коэффициент затухания применяемого оптического волокна.

Значения коэффициента затухания современных оптических волокон при длинах волн оптического излучения λ=(850…1550)нм составляют α_0=(0,01…0,03)дБ/км, соответственно. Значения коэффициента затухания оптических волокон, выпускаемых ОАО «Одескабель» удовлетворяют нормам, которые определяются Рекомендациями Международного Союза Электросвязи (табл. 11.3).

Таблица 11.3 –Значения коэффициента затухания оптических волокон

Рекомендация		*G*.652	*G*.652.*B*	*G*.652.*C*	*G*.652.*D*	*G*.653.*A*
Коэф.затухания оптического волокна в кабеле α_0(дБ/км) (на соответствующей длине волны λ)	λ=1310 нм	≤ 0.5	≤ 0.4	–	–	–
	λ=1550 нм	–	≤ 0.4	–	–	–
	λ=1625 нм	≤ 0.35	≤ 0.3	≤ 0.3	≤ 0.3	≤ 0.35
	λ=(1310-1625)нм	–	–	≤ 0.4	≤ 0.4	–
	λ=1383 нм	≤ 0.4	≤ 0.4	–	–	–

Возможность увеличения длины оптического волокна за счет применения помехоустойчивого кодирования привлекла внимание ведущих производителей оптических кабелей и оборудования для особенно длинных волоконно-оптических систем передачи (например, трансконтинентальные магистрали). По данным мирового лидера в этой области фирмы *Alcatel* зависимость протяженности волоконно-оптической линии передачи с оптическим кабелем с коэффициентом затухания оптического волокна α_0=0,2 (дБ/км) от энергетического выигрыша кодирования имеет вид, показанный на рис. 11.15 [43]. Зависимость рассчитана для ВОСП с суммарной скоростью 68х 10(Гбит/с). Применение кода с ЭВК порядка 10 дБ позволяет увеличить протяженность ВОЛП от 2500км (без кодирования) до 8000км.

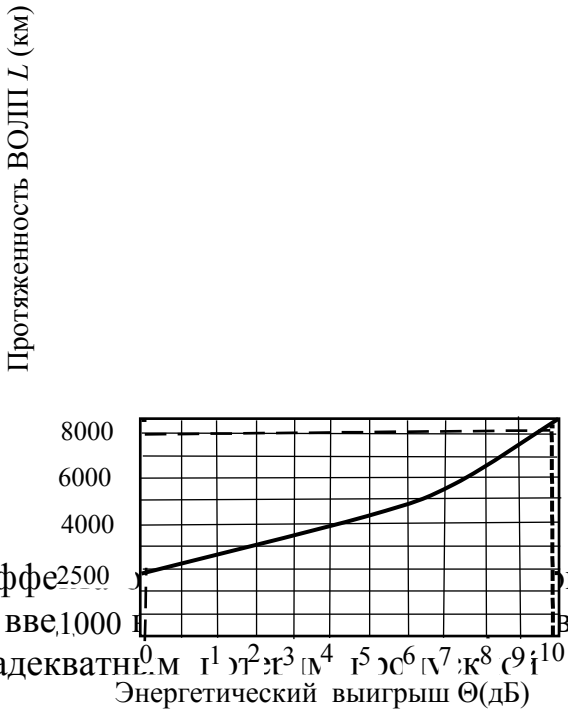


Рисунок 11.15 –Зависимость протяженности волоконно-оптической линии передачи от величины энергетического выигрыша

Такие величины эффе[illegible]йчивого кодирования достижимы благодаря вве[illegible]ваемый цифровой поток, что приводит к адекватн[illegible] пособности системы передачи.

Избыточность вы[illegible]

1.Необходимост[illegible]ми корректирующего кода [illegible]ировании на приемной сто[illegible] длиной кодового блока *n* символов в состав блока включают *k* информационных символов(остальные (*n–k)* – дополнительные символы). Для таких кодов определяют кодовую скорость $R_к=\frac{k}{n}$ и избыточность кода $\eta_к=\frac{n-k}{n}$.

2.Необходимостью введения в поток передаваемых символов ВОСП с кодированием специальных синхровставок («*уникальных слов*»), необходимых для синхронизации работы кодера на передаче и декодера на приемной стороне. При этом избыточность $\eta_с$ зависит от конкретной реализации кодера-декодера.
Результирующая избыточность с учетом этих двух факторов будет

$$\eta=\eta_к+\eta_с-\eta_к\eta_с . \qquad (11.15)$$

Величина избыточности η позволяет определить потери в скорости передачи цифровой информации в ВОСП с помехоустойчивым кодированием. Так, при известных избыточности η и скорости передачи цифрового потока в ВОСП *R «полезная»* скорость передачи информации по ВОСП с кодированием будет равной

$$R_и=R(1-\eta) \qquad (11.16)$$

В целом, значения энергетического выигрыша Θ и избыточности η находятся в *противоречии* и зависят от конкретного метода кодирования/декодирования.

Методы помехоустойчивого кодирования для ВОСП. При выборе помехоустойчивых кодов для ВОСП проблема *сложности реализации* оборудования для кодирования/декодирования (кодеков) является весьма трудной, поскольку от элементной базы требуется *высокое быстродействие*. Здесь находят при-

менение *циклические коды*, алгоритм декодирования которых упрощается в силу циклических свойств кодовых комбинаций. Наиболее популярным классом циклических кодов являются коды БЧХ(*BCH – Bose-Chaudhuri-Hochquenghem codes*), сочетающие высокие корректирующие свойства с простотой алгоритма декодирования[41]. Рассмотрены возможности применения следующих кодов[38,39].

Коды Рида-Соломона (*RS–Reed-Solomon codes*) – популярный вид блоковых циклических кодов, оптимальных в своем классе[42]. Применение таких кодов в ВОСП предусмотрено Рекомендацией *G*975/*G*709 [45] Международного Союза Электросвязи. Код *RS* обеспечивает ЭВК Θ=6,7дБ (Вероятность ошибки декодирования $p^*=10^{-13}$) при избыточности η=0,07. Вместе с тем, среди специалистов такие показатели считаются неудовлетворительными, и предпринимаются попытки поиска более эффективных методов кодирования.

Последовательный каскадный код [*RS* (1023,1007)/*BCH* (2047,1952)]. При каскадном построении систем кодирования достигается лучшее соотношение между корректирующими свойствами кода и сложностью алгоритма декодирования[41]. Втаком варианте каскадного кода в качестве «в*нутреннего*» кода выбран код *BCH* (2047,1952). В качестве «*внешнего*» используется код – *RS* (1023,1007), эффективно исправляющий пакеты ошибок, возникающие на выходе декодера «*внутреннего*» кода в процессе декодирования. *Порождающие многочлены* циклических кодов:

Код *RS* (1023,1007): $g_{RS}(X)=X^{10}+X^3+1$;

Код *BCH (*2047,1952): $g_{BCH}(X)=X^{11}+X^2+1$.

Такая комбинация кодов обеспечивает ЭВК Θ=8,03дБ при коэффициенте избфточности η=0,07.

Коды с малой плотностью проверок на четность *LDPC*(*Low-Density Parity-Check codes*) были предложены с целью снижения сложности алгоритма декодирования[46]. Их длительное время игнорировали разработчики помехоустойчивых кодеков.В настоящее время структура таких кодов является наиболее подходящей для реализации в условиях современной технологии высокоскоростных ИМС. К примеру, для декодирования двоичного систематического *LDPC* кода с длиной кодового блока 32640 символов требуется реализация блока памяти в виде двумерной матрицы размером
(112х 293) двоичных ячеек. Простая процедура декодирования этого кода обеспечивает ЭВК Θ=7,43дБ (Вероятность ошибки декодирования $p^*=10^{-13}$) при избыточности η=0,07.

Турбо-коды. 1993-й год отмечен важным событием в сфере телекоммуникаций – группа французских ученых(*C. Berrou, A. Glavieux, P. Thitimajshima*) представила новый подход к решению проблемы построения систем помехоустойчивого кодирования (*турбо-коды*).

Анализ темпов и результатов исследований в области помехоустойчивого кодирования позволяют утверждать, что в ближайшие годы кодеки турбо-кодов станут стандартными в системах телекоммуникаций, постепенно вытеснят и заменят существующие каскадные конструкции на базе кодов Рида-Соломона, так как в силу псевдослучайной структуры турбо-кодов они обеспечивают

большую помехозащищённость для широкого класса каналов и помех. Подробная информация о турбо-кодах содержится в обзорных статьях автора [24, 25].

На выставке, посвященной международной конференции по вопросам волоконно-оптической связи *OFC* анонсирована реализация *турбо-кодека для ВОСП* со скоростью 12,4 Гбит/с, обеспечивающего ЭВК порядка 10,1 дБ (избыточность η=0,14)[48] .

Новые итеративно-декодируемые *LDPC* коды для ВОСП предложены в работе [49]. Основная трудность построения *LDPC* кодов состоит в отыскании формы проверочной матрицы двоичного блокового кода, содержащей минимум единиц в столбцах.

В цитируемой статье предложено правило построения такой матрицы с использованием взаимно *ортогональных латинских квадратов* на базе теоремы *MacNeich–Mann* из теории чисел. Такие коды имеют высокую кодовую скорость, допускают простое в реализации итеративное (поэтапное) декодирование при высокой помехоустойчивости. Результаты моделирования (ЭВК Θ=12,6 дБ при избыточности η=0,14) выдвигают такие коды в число лидеров из выше рассмотренных.

Как следует из выражений (11.15) и (11.16) *лучшим* следует считать такой способ кодирования, который обеспечивает *наибольший* энергетический выигрыш при *минимальной* избыточности.

Сравнение методов помехоустойчивого кодирования для ВОСП. Сравнительные данные рассмотренных выше методов помехоустойчивого кодирования сведены в табл.11.4.

Таблица11.4 – Сравнительные характеристики методов кодирования для ВОСП

Метод кодирования	ЭВК Θ(дБ) (при вероятности ошибки $p^*=10^{-13}$)	Избыточность η
Код Рида-Соломона *RS*(2720,2550)	6,7	0,07
Код *LDPC* (с малой плотностью проверок на четность)	7,43	0,07
Последовательный каскадный код [*RS*(1023,1007)/*BCH* (2047,1952)]	8,03	0,07
Блоковый турбо-код(с гибким решением(*экспериментальные результаты)*	10,1	0,14
Итеративно-декодируемые *LDPC* коды (основанные на теореме*Mac-Neish-Mann*)	12,6	0,092

Приложение

Перечень
тем исследовательских работ в области теории цифровой связи, рекомендуемых магистрантам и аспирантам

Перечень составлен на базе материалов настоящего пособия. Наименование каждой темы (**М** – для магистрантов, **Д** – для аспирантов) сопровождается кратким комментарием. Указаны также рекомендуемые номера разделов пособия и ссылки на литературу.

М.1. *Анализ групповой структуры блокового линейного корректирующего кода с заданной порождающей матрицей*. (Разд. П. 2.1.5, [11, 14, 18]).

Разработать методику анализа групповой структуры линейного корректирующего кода(над полем Галуа), порождающая матрица которого задана. Показать возможность применения этой методики для анализа дистанционных свойств кода. Применить методику к известным классам линейных кодов.

М.2. *Анализ групповой структуры блокового линейного корректирующего кода с заданной проверочной матрицей*. (Разд. П.2.1.5, [11, 14, 18]).

Разработать методику анализа групповой структуры линейного корректирующего кода(над полем Галуа), проверочная матрица которого задана. Показать возможность применения этой методики для анализа дистанционных свойств кода. Применить методику к известным классам линейных кодов.

М.3. *Исследование возможностей применения теории пространственных точечных решеток для синтеза практически важных ансамблей многопозиционных сигналов*. (Разд. 4, [3, 18]).

Выполнить классификацию известных из литературы пространственных точечных решеток с указанием порождающих матриц и показателей плотности упаковки.

На этой основе разработать рекомендации по синтезу эффективных ансамблей дискретных сигналов для цифровых систем.

М.4. *Исследование возможностей реализации методов формирования и оптимальной демодуляции многопозиционных решетчатых сигналов для практически важных структур модемов. (*Разд. 4, [3, 15, 18]).

Методы формирования и демодуляции решетчатых многопозиционных сигналов базируются на использовании групповых свойств пространственных точечных решеток. Показать пути упрощения алгоритмов формирования и демодуляции, пригодных для практического применения.

М.5. *Исследование возможностей применения алгебры многочленов для построения недвоичных циклических кодов* (Разд. 5, 5.1, 6.1, 11.1 [4, 11]).

Широко используемые на практике блоковые корректирующие коды Рида-Соломона относятся к классу циклических недвоичных совершенных кодов. Задача состоит в исследовании алгоритмов работы кодера кода Рида-Соломона, основанных на использовании циклических свойств многочленного представления кодовых комбинаций и в разработке на этой основе структуры кодера, пригодной для аппаратной либо программной реализации.

М.6. *Разработка методики анализа статистики ошибок на выходе декодера ОФМ*(Разд., 6.2, [3, 4]).

Алгебра степенных многочленов и теория многотактных линейных фильтров составляют основу математического аппарата для решения поставленной задачи.

Необходимо получить в замкнутом виде выражения для многочленов ошибок на выходе декодера ОФМ высокой кратности и на этой основе составить данные о распределении ошибок при действии в канале потока независимых ошибок.

Разработать программу для экспериментальной проверки теории.

М.7. *Дифференциальный метод анализа дистанционных свойств неинвариантных сигнально-кодовых конструкций. (*Разд. 4, [3, 15, 18]).

Многие классы сигнально-кодовых конструкций относятся к классу неинвариантных СКК. Разработать численный метод и программу, позволяющие выполнять расчет минимального расстояния таких СКК с последующим вычислением верхней границы вероятности ошибки декодирования. *(*Разд. 9.3, [3]).

М.8. *Методика численного расчета спектра расстояний сверточного кода произвольных длины и скорости. (*Разд. П. 7.1, П. 7.2 [3, 4]).

Аналитический метод определения спектра расстояний СК основан на применении теории графов и алгебры многочленов. Такой метод требует значительного объема «ручной» работы. Предлагается разработать методику и программу, позволяющие выполнять расчет спектра расстояний линейных СК с произвольными параметрами.

Применить результаты для вычисления верхней границы вероятности ошибки декодирования.

М.9. *Методика переборного поиска порождающих многочленов СК*. *(*Разд. П. 2, 1.5 [3, 4]).

Для синтеза СКК необходимо применять внешние СК, удовлетворяющие заданным требованиям по скорости и дистанционным свойствам. Имеющиеся таблицы СК в руководствах по теории кодирования содержат ограниченное количество сведений о кодах, подходящих для синтеза СКК. Предлагается разработать методику и программу для переборного поиска порождающих многочленов СК при наперед заданных параметрах скорости и расстояния (и тем самым пополнить таблицы СК).

М.10. *Методика декомпозиции групповых ансамблей многопозиционных сигналов плотнейшей упаковки. (*Разд. 2.1, 3, 9.2 [3, 4]).

На базе теории групп разработать композиционные ряды ансамблей многопозиционных сигналов. На этой основе дать рекомендации по синтезу эффективных СКК.

Д.1.*Метод модификации решетчатых диаграмм сверточных кодов.* (Разд. 7.1 [3, 4]).

Теория графов представляет широкие возможности для модификации(преобразования) решетчатых диаграмм СК, направленной на снижение сложности реализации алгоритма Витерби для декодирования СК. Задача состоит в разработке формальных методик модификации, в оценке обменных соотношений «сложность/быстродействие» и в разработке на этой основе рекомендаций по реализации процессора Витерби в виде ИМС.

Д.2. *Рекурсивные сверточные коды.* [3,4].

Исследуется новый, перспективный класс СК.

Д.3.*Сигнально-кодовые конструкции для систем беспроводного доступа с пространственно-временным кодированием*.

Исследуется эффективность СКК в каналах с пространственно-временным кодированием радиосистем беспроводного доступа к сети общего пользования.

Д.4. *Эффективность применения помехоустойчивого кодирования в каналах с модуляцией парциального отклика.*

Помехоустойчивое кодирование применяется для компенсации энергетических потерь, обусловленных применением модуляции парциального отклика.

Д.5. *Пространственно-временное кодирование в системах с расширенным спектром сигнала.*

Новый метод кодирования (ПВК)применяется к синтезу СКК с внутренними сигналами с расширенным спектром.

Д.6. *Методы сокращения сложности декодирования сигнально-кодовых конструкций.*

Проблема снижения сложности декодирования СКК решается с использованием свойств симметрии групповых СКК.

Д.7. *Сигнально-кодовые конструкции с внутренними ансамблями широкополосных сигналов.*

Идеи групповых СКК применяются к синтезу СКК с внутренними сигналами с расширенным спектром.

Д.8. *Эффективность применения кодов с малой плотностью проверок на четность в высокоскоростных системах цифровой связи (на базе ВОЛС).* (Разд. 11.13 [11, 47].

Коды с малой плотностью проверок на четность обеспечивают высокую помехоустойчивость при приемлемых показателях сложности и быстродействия кодеков и потому перспективны для применения в аппаратуре волоконно-оптической связи.

Д.9. *Сигнально-кодовые конструкции с внутренними сигналами с компактным спектром.*

Д.10. *Сигнально-кодовые конструкции с внутренними сигналами ЧМ-НФ*. (Разд. 9.4 [4].

Сигналы частотной модуляции с непрерывной фазой широко применяются в радиосистемах с жесткими требованиями к эффективности использования выделенного радиоспектра (мобильная связь).

Список использованных источников

1. *Довгий С.О., Савченко., О. Я., Воробієнко П. П.* Сучасні телекомунікації: мережі, технології , економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавничий Центр, 2002.– 520 с.
2. *Радіотехніка:* Енциклопедичний навчальний довідник: Навч. Посібник / За ред. Ю.Л. Мазора,Є.А. Мачуського, В.І. Правди. - К.: Вища шк., 1999. – 838с.
3. *Помехоустойчивость и эффективность систем передачи информации*/А.Г. Зюко, А. И. Фалько, И. П. Панфилов, В. Л. Банкет, П. В. Иващенко; Под ред. А. Г. Зюко. – М.: Радио и связь, 1985. – 272 с.
4. *Банкет В. Л., Дорофеев В. М.* Цифровые методы в спутниковой связи. – М.: Радио и связь, 1988. – 240 с.
5. *Цифровые фильтры в электросвязи и радиотехнике*/ А.В. Брунченко, Ю.Т. Бутыльский., Л.М Гольденберг. и др.; Под ред. Л.М. Гольденберга.- М.: Радио и связь, 1982. – 224 с.
6. *Голд Б., Рэйдер Ч.* Цифровая обработка сигналов/ Пер. с англ. под. ред. А.М. Трахтмана. – М.: Советское радио, 1973. - 370 с.
7. *Анго А.* Математика для электро и радиоинженеров: Пер. с франц; Под ред.
К. С. Шифрина.М:Наука, 1965. – 780 с.
8. *Яблонский С.В.* Введение в дискретную математику: Учеб. пособие для вузов. - 2-е изд. перераб. и доп. – М.: Наука. Гл. ред. физ.-мат. лит. – 384 с.
9. *Дискретная* математика и математические вопросы кибернетики. - Т. 1 / Под общей редакцией С. В. Яблонского и О. Б. Лупанова. – М.: Наука, 1974. – 312 с.
10. *Кузнецов О. П., Адельсон-Вельский Г.М.* Дискретная математика для инженера. – 2-е изд., перераб. и доп. – М.: Энергоатомиздат, 1988. - 480 с.
11. *ПитерсонУ., УэлдонЭ*. Коды, исправляющие ошибки: Пер. с англ.; Под ред.. Добрушина Р. Л и Самойленко С. И. – М.:Мир, 1976. – 380 с.
12. *Банкет В.Л.* Развитие теории эффективности систем передачи информации // Наукові праці УДАЗ ім. О. С. Попова. – Одесса. – 2000. – № 2.– С. 20-30.
13. *Математический энциклопедический словарь*; Гл. ред. Ю. Прохоров. – М.: Сов. энциклопедия, 1988. – 847 с.
14. *Банкет В.Л.* Использование положений дискретной математики в теории электрической связи: Учебн. пособие.– Одесса: ОНАС, 2005. – 36 с.
15. *Банкет В. Л.* Эффективные системы передачи дискретных сообщений // Труды НИИР.– Москва. – 1981. – № 2. – С. 22-30.
16. *Банкет В. Л., Дорофеев В. М.* Цифровые методы в спутниковой связи. - М.: Радио и связь, 1988. - 240 с.
17. *Возенкрафт Дж., Джекобс И.* Теоретические основы техники связи. – М.: Мир, 1969. – 640 с.
18. *Конвей Дж., Слоэн Н.*Упаковки шаров, решетки и группы: в 2-х томах. Пер. с англ. – М.: Мир, 1990. – 415 с.

19. *Игнатьев Н. К.* Геометрические основания оптимального кодирования // Сб. ГосНИИ Министерства связи СССР. – 1958. – Вып. 8. – С. 85 – 145.
20. *Imai H., HirakawaS.* A new multilevel coding method using error –correcting codes // IEEE Transactions on Information Theory. 1977–Vol. IT –23, – № 3,. –P. 371 – 377.
21. *Ungerboeck G.* Channel coding with multilevel / phase signals//IEEE Transactions on Communications. –Vol. Com – 28, Jan.1982.–P.55 – 67.
22. *Банкет В.Л.,* Теория групповых сигнально – кодовых конструкций и ее применения в системах передачи информации. Дис… д-ра техн. наук. – М.: 1980 – 433 с.
23. *Berrou C., Glavieux A., Thitimajshima P.* Near Shannon limit error-correcting coding and decoding: turbo-codes // *In Proc. Int. Conf. On Commun., ICC-93*. – 1993. – Geneva. – Switzerland. – May. – P. 1064-1070.
24. Банкет В.Л., Прокопов С.Д., Постовой А.Г., Топорков Ф.В. Турбо-коды и их применение в телекоммуникационных системах// Зв'язок–2004.–№3,С. 45-47.
25. *Прокопов С. Д., Постовой А. Г.* Перспективы использования турбо-кодов в спутниковых системах связи// Праці УНДІРТ–№4(28).–2001.–. 30-36.
26. *Банкет В.Л., Прокопов С.Д., Постовой А.Г., Топорков Ф.В.* Алгоритмы кодирования/декодирования турбо-кодов//Зв'язок.– 2004.– №4,С. 45-46.
27. *Consultative Committee for Space Data Systems* "Recommendations for space data systems, telemetry channel coding" // *BLUE BOOK*. – 1998. – May.
28. *III-rd Generation Partnership Project* "*Multiplexing and channel coding (FDD*)" // R*ecommendation* 3*G TS* 25.212 *V*3.1.1 (1999-12). – 1999. – *June.*
29. *Digital Video Broadcasting (DVB):* Interaction channel for satellite distribution systems (*DVB-RCS*) // *ETSI EN 301 790 V1.2.1 (2000-07)*. – 2000. – *February.*
30. *Forney G. D., Jr.* Maximum-Likelihood Sequence Estimation of Digital Sequences in the Presence of Intersymbol Interference// *IEEE Trans. Inform. Theory, vol. IT*-18, p.363-378, May 1972
31. *Douillard C., Jezequel M., Berrou C., Picart A., Didier P., Glavieux A.* Iterative correction of intersymbol interference: turbo equalization// Eur. Trans. Telecommun., vol. 6, p. 507-511, Sept.-Oct. 1995
32. *Tarokh V., Jatarkani H., Caldenbank A. R.* Space-Time Block Codes from Orthogonal designs // IEE Transactions on Information Theory. V. 45. - № 5. – July 1999. – p. 1455 .
33. *Банкет В.Л., Эль-Дакдуки А. С.* Анализ методов разнесения в системах беспроводной связи // Труды УНИИРТ.Одесса:–№3(27).–2001.– С.15-22.
34. *V.L.Banket,A.S. Dakdouki,N.K.Myckhailov, A.A. Skopa.* Downlink Processing Algorithms for Multi-Antenna Wireless Communications *IEEE Communications Magazine***,** January 2005.
35. *Banket V.L., Dakdouki A.S., Mikhailov N.K., Janoudi B.A.* On the Signal-to-Code Construction of Space-Time codes//Сборник докладов 6-й международной НТК «Телеком –2003». Одесса. ОНАС.–2003.–С.154-157.

36. *В.Л.Банкет,Н.А. Ищенко, А.С.Эль-Дакдуки.* Пространственно-временное кодирование – эффективный способ помехоустойчивой передачи цифровой информации в системах мобильной связи //Зв'язок–2004, –№8,С.40-42.
37. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение.изд.2-е,испр.:Пер с англ.–М.:Издательский дом «Вильямс»,2003.–1104 с.
38. *БанкетВ.Л.*Достижения теории связи и прогресс радиотехнологий.//Робочі Матеріали III науково- практичної конференції "НПК РТ-99".–Одеса - Київ. –Червень 1999 – С.83-88.
39. *Банкет В.Л.,Топорков Ф.В* Возможности повышения эффективности волоконно-оптических систем передачи при использовании помехоустойчивого кодирования//Доклад на международной конференции"Сучасний стан та перспективи використання ВОЛЗ. Первинні мережі, як транспортна основа телекомунікаційної інфраструктури України" Київ.–9-10 грудня.–2003.
40. *BanketV., ToporkovF.* The Efficiency of Forvard Error Correction Methods for Optical Telecommunications// Proceedings of International Congress on Optics and Optoelectronics. Warsaw. Sept.2005.Vol.5956 Manuscript #5956-36.(p.12.1-12.4).
41. *Gautheron O.,* Submarine optical networks at the threshold of Tbit/s per fiber capability// Alcatel Telecommunications Review –3rd Quarter 2000, –P.171 – 179
42. *Корнейчук В.Н.,Мосорин П.Д*. Расчет энергетических параметров волоконно-оптической линии передачи//Наукові праці ОНАЗ ім О. С. Попова, №2.– 2001.– С.68-72.
43. I*TU Telecommunication Standartization Sector*. Forward Error Correction for High Bit Rate DWDM Submarine Systems."Tech. Recommendation G 975/G709
44. *S.Lin and J.Costello*. Error Control Coding:Fundamentals and Applications.Englewood Cliffs, NJ:Prentice-Hall,1983
45. *Mizuochi T., Ouchi K,* Kobayashi T, and others. Experimental Demonstration of Net Coding Gain of 10.1 dB using 12.4 Gb/s Block Turbo Code with 3-bit Soft Decision, OFC-2003, PD21-1.
46. *Yang M., Ryan W.E.,Li Y.* Design of Efficiently Encodable Moderate -Length High-Rate Irrequlal LDPC Codes//*IEEE Transactions on Communications*.Vol.52.№4, April 2004. pp. 564-570.-
47. *Chung S.-Y., ForneyG. D., Richardson T. J., Urbanke R*.On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit// *IEEE Communications Letters*. Vol.5, №2, February 2001.pp.58-60
48. K. *Balachandran, J. B.Anderson*. Mismatched Decoding of Intersymbol Interference Using a Parallel Concatenaned Sheme//IEEE Journal on Selected Areas in Communications.–Vol.16.–No. 2.–February1998.P.256-259.
49. *H.Michel,N.When*. Turbo-Decoder Quantization for UMTS//IEEE Communications Letters –Vol. 5.–No.2.February 2001.–p.55-56.
50. E.*Yeo, B. Nicolich, V.Ananheram*. Iterative Decoder Architectures//IEEE Communications Magazine.–Vol.41.–No.8.August, 2003.–P.132-140
51. *W.Oh., K.Cheun*. Joint Decoding and Carrier Phase Recovery Algorithm for Turbo Codes // IEEE Communication Letters, Vol 5, № 9, Sept. 2001, P. 375 – 377.

52. *Forney G. D., Jr.* Maximum-Likelihood Sequence Estimation of Digital Sequences in the Presence of Intersymbol Interference// IEEE Trans. Inform. Theory, vol. IT-18, May 1972.P.363-378,.

53. *Douillard C., Jezequel M., Berrou C., Picart A., Didier P., Glavieux A.* Iterative correction of intersymbol interference: turbo equalization// Eur. Trans. Telecommun. vol. 6.Sept.-Oct. 1995. – P. 507-511

54. *Massey J. L., Sain M. K.* Inverses of Linear Sequential Circuits// IEEE Trans. on Computers. 1968– V. C–17.–№4.–P. 330–337.

55. *Банкет В. Л., Жануди Б. А.* Условия катастрофичности сверточных кодов // Праці УНДІРТ.– Одеса: – № 1 (25). –2001. – С. 19–23.

56. *R.E.Bellman.*Dynamic Programming, – N.Y.:Princeton Princeton Univ. Press, 1957.

57. *Вентцель Е. С.* Элементы динамического программирования /– М: Наука, 1964.– 175с.