1. Konspekt lekcii “Osnovnye ponjatiya teorii PK”

Элементы теории помехоустойчивого кодирования

Как уже отмечалось в курсах РТСПИ и ЦСиСРС, повышение помехоустойчивости всегда связано с введением избыточности. Избыточность может вводиться как в аналоговых (например, с ЧМ, ФМ), так и в цифровых системах передачи информации. Введение избыточности в цифровых системах передачи информации называют помехоустойчивым, или избыточным, кодированием. Можно дать такое определение этого термина: помехоустойчивое кодирование – это избыточное преобразование подлежащей передаче двоичной цифровой последовательности в последовательность элементарных сигналов, поступающих непосредственно в канал связи. Зачастую такое преобразование также называют канальным кодированием.

Как говорилось в курсе ЦСиСРС, избыточное кодирование может быть «вертикальным» и «горизонтальным». «Вертикальное» избыточное кодирование осуществляется путем увеличения основания кода при сохранении (или даже уменьшении, если новое основание кода это позволяет) скорости передачи символов цифрового сигнала. «Горизонтальное» избыточное кодирование, напротив, предполагает увеличение скорости передачи, так как к информационным символам добавляются проверочные символы. Основание кода при этом, как правило, не изменяется.

«Вертикальное» кодирование приводит к сокращению полосы частот сигнала и уменьшению межсимвольных помех (МСП), но одновременно снижается помехоустойчивость по отношению к аддитивным помехам (типа флуктуационного, или теплового, шума). Оно применяется в основном на кабельных линиях (для борьбы с МСП) и на радиолиниях с квадратурной фазовой или амплитудной модуляцией (для сокращения полосы частот).

«Горизонтальное» кодирование приводит к расширению полосы частот, при этом увеличивается помехоустойчивость по отношению к аддитивным помехам. Оно применяется, в основном, на УКВ-линиях, например, спутниковых, а также в сотовой связи. В принципе возможно, конечно и комбинированное кодирование – избыточное и «по вертикали» и «по горизонтали», тогда увеличивается и количество подлежащих передаче символов, и основание (позиционность, значность) кода.

Проблема помехоустойчивого кодирования представляет собой обширную область теоретических и прикладных исследований. Ее основными задачами являются:

1) отыскание кодов, позволяющих повысить помехоустойчивость системы передачи информации, обнаруживать или исправлять ошибки требуемого характера;

2) разработка алгоритмов кодирования и способов их реализации;

3) разработка алгоритмов декодирования и способов их реализации.

Рассмотрим основные принципы и идеи “горизонтального” избыточного кодирования. При оценке тех или иных его методов следует учитывать, что кроме полезного эффекта – повышения помехоустойчивости – горизонтальное кодирование вносит определенные трудности:

1) расширение полосы частот;
2) задержку в передаче символов при кодировании;
3) задержку сигнала при декодировании;
4) усложнение (зачастую весьма значительное) передающей (кодеры) и и приемной (декодеры) аппаратуры.

Кодирование

На выходе кодера, осуществляющего горизонтальное избыточное кодирование, образуются комбинации двоичных символов – кодовые комбинации (кодовые группы, кодовые слова). Если кодовое слово состоит из m двоичных символов, то есть является m-разрядным, то m называют длиной кодового слова. Далее рассматриваются только равномерные коды, у которых все кодовые слова имеют одинаковую длину, m=*const*.

Кодирование может быть блочным и неблочным. При блочном кодировании безызбыточный входной сигнал кодера разбивается на блоки, содержащие, например, *к* двоичных символов каждый. Число различных возможных блоков равно, очевидно, 2^k. Каждому такому блоку $A_i, i=1,2,...,2^k$, ставится в соответствие определенная комбинация B_i из $m>k$ двоичных символов на выходе кодера. Таким образом, чтобы не было потерь информации, техническая скорость передачи должна быть увеличена в m/k раз,. Длительность кодового слова $T_c = kT_{\text{вх}} = mT_{\text{вых}}$, где $T_{\text{вх}}$, $T_{\text{вых}}$ – длительности соответственно входных и выходных символов. Отсюда следует, что $T_{\text{вых}} = kT_{\text{вх}} / m$. Поскольку ширина спектра цифрового сигнала обратно пропорциональна длительности одиночного символа, «горизонтальное» кодирование требует соответствующего расширения полосы частот канала

Блочный код с длиной блока m, содержащий в каждом блоке *к* информационных символов и $r=m–k$ избыточных символов, принято обозначать как (m, k) код. Коэффициент избыточности этого кода $R = \frac{m-k}{m} = 1 - \frac{k}{m}$, или $\frac{k}{m} = 1 - R$. Эта величина, называемая скоростью помехоустойчивого кодирования, показывает, какую часть каждого кодового слова составляют информационные символы.

При неблочном кодировании комбинация B_i зависит не только от вида блока A_i, но и от других факторов, например от того, какие информационные блоки предшествовали A_i.

Декодирование

Если с выхода кодера в канал связи поступает сигнал $B(t)$, то на выходе канала из-за действия помех и искажений образуется некоторый другой сигнал $B^*(t)$. Пусть все возможные сигналы $B(t)$ и $B^*(t)$ образуют некоторое множество β. Общие принципы декодирования состоят в следующем:

1. На множестве β вводится метрика, то есть тем или иным образом определяется расстояние $R(B_x, B_y)$ между двумя любыми сигналами B_x и B_y – элементами этого множества.

2. При декодировании принятого сигнала $B^*(t)$ отыскивается такое кодовое слово $B_z(t)$, у которого расстояние $R\left[B_z, B^*(t)\right]$ минимально по всем словам кода. Тогда принимается, что передавался информационный блок, соответствующий кодовому слову $B_z(t)$.

Метрика есть расстояние d, если:

1) $d(x,y)=0$ только при $x=y$;

2) $d(x,y)=d(y,x)$

3) $d(x,y)\le d(x,z)+d(z,y)$ (правило треугольника).

Естественно, что осуществляемое таким образом декодирование иногда приводит к ошибкам. Вероятность ошибки $P_{\text{ош}}$ определяется как структурой кода, так и метрикой, используемой при декодировании. В теории потенциальной помехоустойчивости доказано, что для канала связи, в котором действует только аддитивный белый гауссовский шум (АБГШ) и передача всех информационных блоков равновероятна, наилучшей является среднеквадратическая метрика:

$$R[B(t), B^*(t)] = \frac{1}{T_C}\int_0^{T_c}[B(t) - B^*(t)]^2\, dt.$$

Однако эта метрика требует очень сложных декодеров, поскольку здесь необходимы:

1) точное запоминание принятого сигнала $B^*(t)$;

2) последующее вычисление $R(B, B^*)$ для всех возможных кодовых слов $B(t)$;

3) сравнение результатов вычисления между собой;

4) выбор наименьшего из них Такое декодирование называют «приемом в целом».

Несколько упростить декодер можно, если использовать другую метрику, при которой оценивается расстояние не между функциями времени $B(t)$ и $B^*(t)$, а между их цифровыми эквивалентами. В этом случае каждый двоичный символ сигнала $B^*(t)$ регистрируют независимо от других, то есть осуществляют посимвольный прием, в результате чего формируется некоторое двоичное кодовое слово B^*. Затем определяется так называемое расстояние Хэмминга между B^* и всеми другими возможными (заданными *a priori*) кодовыми словами и выбирается то кодовое слово, до которого расстояние оказалось наименьшим.

Расстоянием Хэмминга $d(x,y)$ между двумя комбинациями равномерного кода B_x и B_y называется количество двоичных разрядов, в которых эти комбинации отличаются друг от друга.

Пример:

$B_x = (11001) \qquad W(x) = 3$

$B_y = (01011) \qquad W(y) = 3$

$d(x,y)=2$

Расстояние Хэмминга $d(0,x)$ между нулевой (то есть состоящей из одних нулей) комбинацией и кодовой комбинацией B_x называется весом $W(x)$ комбинации B_x.

Для каждого блочного кода можно определить *минимальное* расстояние Хэмминга $d_{\min}$, называемое также *кодовым расстоянием*, которое является весьма важной характеристикой кода.

В безызбыточном *к*-значном коде, где разрешены все комбинации, $1 \le d \le k$, $d_{\min} = 1$. Пример показан ниже (первый столбец таблицы).

$A_0 = 000 \qquad 0$

$A_1 = 001 \qquad 1$

$A_2 = 010 \qquad 1$

$A_3 = 011 \quad\quad 0$

$A_4 = 100 \quad\quad 1$

$A_5 = 101 \quad\quad 0$

$A_6 = 110 \quad\quad 0$

$A_7 = 111 \quad\quad 1$

m=4, *k*=3, *r*=1

Поэтому при появлении ошибки в одном или нескольких разрядах получается другая разрешенная комбинация, и такая ошибка не может быть обнаружена при декодировании. Чтобы ошибку можно было обнаружить или даже исправить, необходимо ввести избыточность. Пусть, например, число избыточных символов r=1 (см. последний столбец выше). В этом случае половина четырехзначных комбинаций являются запрещенными, $d_{min} = 2$, и код позволяет обнаружить одну ошибку в каждом кодовом слове. Это простейший помехоустойчивый код (код с проверкой на четность).

В общем случае число обнаруживаемых ошибок $b \leq d_{\min} - 1$, откуда требуемое минимальное расстояние

$$d_{\min} \geq b + 1.$$

В этом случае никакое сочетание из b ошибок не может перевести одну разрешенную кодовую комбинацию в другую.

Если требуется не только обнаруживать, но и исправлять ошибки, то при декодировании используют принцип «максимального сходства». Если принята ошибочная (и, следовательно, неразрешенная) комбинация, то считается истинно переданной та комбинация, которая меньше всего отличается от принятой. Например, для исправления одной ошибки должно быть $d_{min} = 3$, а в общем случае $2c \leq d_{\min} - 1$, откуда

$$d_{\min} \geq 2c + 1,$$

где c – требуемое число исправляемых ошибок.

Поскольку $2c$ всегда четно, $d_{\min}$ должно быть нечетным. В этом случае при появлении c ошибок искаженная комбинация будет отличаться от истинной в c разрядах, а от всех других разрешенных комбинаций – не менее, чем в c+1 разрядах, и для декодирования можно использовать принцип «максимального сходства». Если же $d_{\min}$– четное число, то имеются разрешенные комбинации, одинаково удаленные от неразрешенных (запрещенных).

Коды, исправляющие ошибки, можно одновременно использовать и для обнаружения ошибок (большей кратности). В этом случае необходимое кодовое расстояние определяется соотношением

$$d_{\min} \geq b + c + 1,$$

где обязательно $b \geq c$.

Метрика Хэмминга в принципе очень проста, но и при ее использовании декодер, исправляющий ошибки, может оставаться чрезвычайно сложным: хотя для каждого B_i вычисление расстояния $R(B_i, B^*)$ представляет простую задачу, общее число 2^k таких вычислений может оказаться огромным. Дальнейшее упрощение процедуры декодирования достигается путем использования кодов, обладающих специальной алгебраической структурой, позволяющей отказаться от вычисления расстояния $R(B_i, B^*)$ для всех B_i, и непосредственно по виду B^* определять наиболее близкую к этому слову разрешенную комбинацию. Такие коды называются алгебраическими, или систематическими. К ним принадлежат линейные блочные коды.

Некоторое множество двоичных (или в более общем случае p-ичных, где p – простое число) кодовых слов длины m называется *линейным блочным кодом* тогда и только тогда, когда оно образует аддитивную группу. В общем случае, когда p – не простое число, это определение недостаточно.(см. Питерсон и Уэлдон, стр. 52)

Алгоритмы декодирования и соответствующие декодеры, позволяющие отыскать кодовое слово, наиболее близкое (в смысле принятой метрики) к поступившему на вход декодера сигналу, можно назвать предельными (полными). В некоторых случаях применяемые алгоритмы не всегда позволяют отыскать ближайшее к входному сигналу кодовое слово, и, с целью упрощения декодеров, от предельных алгоритмов отказываются, При этом возникает ситуация, называемая отказом от декодирования (в большинстве систем передачи информации лучше допустить отказ от декодирования, чем неправильный прием кодового слова). К числу таких алгоритмов (которые можно назвать «допредельными», или неполными), относится, например, так называемое последовательное декодирование.