

29 Линейные помехоустойчивые коды, включая коды Хэмминга и циклические коды

Так как помехоустойчивое кодирование выполняется по системе линейных уравнений, помехоустойчивые коды называются линейными. Особенностью являются дополнительные проверочные символы (обычно биты).

Линейные коды, в том числе: коды Хэмминга, циклические коды, БЧХ-коды (коды Боуза-Чоудхури-Хоквингема), РМ-коды (коды Рида-Маллера), итеративные коды, коды на основе матриц Адамара, симплексные коды и некоторые другие.

Коды Хэмминга являются самоконтролирующимися кодами, то есть кодами, позволяющими автоматически обнаруживать ошибки при передаче данных. Для их построения достаточно приписать к каждому слову один добавочный (контрольный) двоичный разряд и выбрать цифру этого разряда так, чтобы общее количество единиц в изображении любого числа было, например, нечётным. Одиночная ошибка в каком-либо разряде передаваемого слова (в том числе, может быть, и в контрольном разряде) изменит чётность общего количества единиц. Счётчики по модулю 2, подсчитывающие количество единиц, которые содержатся среди двоичных цифр числа, дают сигнал о наличии ошибок. При этом невозможно узнать, в какой именно позиции слова произошла ошибка, и, следовательно, нет возможности исправить её. Остаются незамеченными также ошибки, возникающие одновременно в двух, четырёх, и т. д. — в чётном количестве разрядов. Предполагается, что двойные, а тем более многократные ошибки маловероятны.

Пояснение из лектоса

Бинарным кодом Хэмминга **называют** код длины $n = 2m - 1$, $m \geq 2$ с проверочной матрицей H размером $m \times (2m - 1)$, в которой столбцы соответствуют записи $1, 2 \dots 2^m - 1$ в двоичной системе счисления.

Код Хэмминга позволяет исправлять одиночную ошибку и обнаруживать множественные ошибки.

Базовая идея циклического кодирования состоит в том, чтобы в качестве проверочных битов передавать остаток от деления информационных битов на некоторое выбранное число.

После приема снова выполняется деление уже возможно искаженных информационных битов на то же самое число и сравниваются остатки.

Если остатки совпадают, то данные с определенной вероятностью приняты без ошибок

На практике же деление выполняется по правилам арифметики полей Галуа, то есть без учета переносов.

Информационные биты, то есть делимое, соответствуют информационному полиному.

Делитель соответствует порождающему (образующему) полиному.

Частное в процессе кодирования не используется и поэтому «отбрасывается».

Для того чтобы максимально разнообразить остатки в качестве порождающего полинома должен выбираться неприводимый полином.

Существуют два подхода к реализации циклического кода на стороне приемника:

1. Согласно базовой идее, описанной выше.
2. На порождающий полином делится все принятое кодовое слово. Если ошибок не произошло, то остаток будет нулевым.

Оба подхода равноценны.

Источники лектос 4

https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4_%D0%A5%D1%8D%D0%BC%D0%BC%D0%B8%D0%BD%D0%B3%D0%B0#:~:text=%D0%9A%D0%BE%D0%B4%20%D0%A5%D1%8D%CC%81%D0%BC%D0%BC%D0%B8%D0%BD%D0%B3%D0%B0%20%E2%80%94%D1%81%D0%B0%D0%BC%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D0%B9%D1%81%D1%8F%20%D0%B8%20%D1%81%D0%B0%D0%BC%D0%BE%D0%BA%D0%BE%D1%80%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D0%B9%D1%81%D1%8F,%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%20%D0%BA%20%D0%B4%D0%B2%D0%BE%D0%B8%D1%87%D0%BD%D0%BE%D0%B9%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B5%20%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F.&text=%D0%9F%D0%BE%D0%B7%D0%B2%D0%BE%D0%BB%D1%8F%D0%B5%D1%82%20%D0%B8%D1%81%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%8F%D1%82%D1%8C%20%D0%BE%D0%B4%D0%B8%D0%BD%D0%BE%D

1%87%D0%BD%D1%83%D1%8E%20%D0%BE%D1%88%D0%B8%D0%B1%
D0%BA%D1%83%20(%D0%BE%D1%88%D0%B8%D0%B1%D0%BA%D0%
B0,%D0%A5%D1%8D%D0%BC%D0%BC%D0%B8%D0%BD%D0%B3%D0%
B0%20%D0%A0%D0%B8%D1%87%D0%B0%D1%80%D0%B4%D0%B0%20
%D0%A3%D1%8D%D1%81%D0%BB%D0%B8%2C%20%D0%BF%D1%80%
D0%B5%D0%B4%D0%BB%D0%BE%D0%B6%D0%B8%D0%B2%D1%88%D
0%B5%D0%B3%D0%BE%20%D0%BA%D0%BE%D0%B4.