**Коды исправления ошибок**

В вычислениях, телекоммуникации, теория информации и теория кодирования, **код исправления ошибок** (ECC) используется для контроля ошибок в данных по ненадежным или зашумленным каналам связи. Основная идея заключается в том, что отправитель кодирует сообщение с помощью избыточной информации в форме ECC. Избыточность позволяет получателю обнаруживать ограниченное количество ошибок, которые могут возникать в любом месте сообщения, и часто исправлять эти ошибки без повторной передачи. ECC контрастирует с обнаружением ошибок. в том, что обнаруженные ошибки можно исправить, а не просто обнаружить. Двумя основными категориями кодов ECC являются блочные коды и сверточные коды.

В теории кодирования **блочные коды** представляют собой большое и важное семейство кодов исправления ошибок, которые кодируют данные в блоках.

**Блочные коды**

Формально, **блочный код** — это инъективное отображение вида:

C: Σk → Σn

Здесь Σ - конечное и непустое множество, а k и n - целые числа.

**Алфавит Σ**

Кодируемый поток данных моделируется как строка над некоторым алфавитом Σ. Размер |Σ| алфавита часто записывается как q. Если q = 2, то блочный код называется двоичным блочным кодом. Во многих приложениях полезно рассматривать q как степень простого числа и определять Σ с конечным полем Fq.

**Длина сообщения k**

Сообщения являются элементами m из Σk, то есть строки длиной k. Следовательно, число k называется длиной сообщения или размером блочного кода.

**Длина блока n**

Длина блока n блочного кода — это количество символов в блоке. Следовательно, элементы c из Σn представляют собой строки длины n и соответствуют блокам, которые могут быть получены получателем. Поэтому их еще называют принятыми словами. Если c = C (m) для некоторого сообщения m, то c называется кодовым словом m.

**Скорость R**

rate блочного кода определяется как отношение длины сообщения к длине блока:

R = k / n

Большая скорость означает, что количество фактического сообщения на переданный блок велико. В этом смысле скорость измеряет скорость передачи, а величина 1 - R измеряет накладные расходы, возникающие из-за кодирования с помощью блочного кода. Скорость не может превышать 1, поскольку данные, как правило, не могут быть сжаты без потерь. Формально это следует из того факта, что код C является инъективным отображением.

**Линейные коды**

**Линейный код длины n и ранга k** является линейным подпространством C размерности k векторного пространства , где — конечное поле из q элементов. Такой код с параметром q называется q-арным кодом (напр. если q = 5 — то это 5-арный код). Если q = 2 или q = 3, то код представляет собой двоичный код, или тернарный соответственно.

**Линейный (блочный) код** — такой код, что множество его кодовых слов образует k-мерное линейное подпространство (назовем его C) в n-мерном линейном пространстве, изоморфное пространству k-битных векторов.

Это значит, что операция кодирования соответствует умножению исходного k-битного вектора на невырожденную матрицу G, называемую **порождающей матрицей**.

**Циклические коды**

Под **перестановкой** произвольного множества подразумевается биекция этого множества на себя. **Цикл** в перестановке – подмножество элементов, которые переставляются циклическим образом. Перестановка называется **циклической** тогда и только тогда, когда она состоит из единственного нетривиального цикла, т. е. цикла длиной больше 1.

**Циклический код** — линейный, блочный код, обладающий свойством цикличности, то есть каждая циклическая перестановка кодового слова также является кодовым словом.

**Код Боуза-Чоудхури-Хоквингема**

**Коды БЧХ** – широкий класс циклических кодов, применяемых для защиты информации от ошибок. Отличается возможностью построения кода с заранее определёнными корректирующими свойствами, а именно, минимальным кодовым расстоянием.

БЧХ-код является циклическим кодом, который можно задать порождающим полиномом. Для его нахождения в случае БЧХ-кода необходимо заранее определить длину кода n (она не может быть произвольной) и требуемое минимальное расстояние d ≤ n. Найти порождающий полином можно следующим образом.

Пусть α — примитивный элемент поля GF(qm) (то есть , αi ≠ 1, i < qm-1), β = αs — элемент поля GF(qm) порядка n, s = (qm - 1) / n. Тогда нормированный полином g(x) минимальной степени над полем GF(q), корнями которого являются d - 1 подряд идущих степеней элемента β для некоторого целого (в том числе 0 и 1), является порождающим полиномом БЧХ-кода над полем GF(q) с длиной n и минимальный расстоянием d0 ≥ d.

**Код Рида-Соломона**

Коды Рида-Соломона – недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки). Очень распространены коды Рида — Соломона, работающие с байтами (октетами).