Лекция 2

Для линейного кода минимальное расстояние $d_{\min}$ может быть найдено непосредственно по его проверочной матрице $\mathbf{H}$. Поскольку кодовое слово $\mathbf{c}$ удовлетворяет условию $\mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0}$, то наличие ненулевого кодового слова веса w эквивалентно существованию линейной комбинации w столбцов матрицы $\mathbf{H}$, дающей нулевой вектор. Таким образом, минимальное расстояние $d_{\min}$ равно наименьшему весу ненулевого кодового слова, что в терминах проверочной матрицы означает наименьшее число столбцов $\mathbf{H}$, которые являются линейно зависимыми. Следовательно, для определения $d_{\min}$ необходимо найти минимальную мощность множества линейно зависимых столбцов проверочной матрицы.

Сформулируем соответствующую теорему. Для линейного (n, k)-кода с проверочной матрицей $\mathbf{H}$ минимальное расстояние равно d тогда и только тогда, когда любые $d-1$ столбцов матрицы $\mathbf{H}$ линейно независимы, и существует набор из d столбцов, которые линейно зависимы. Иными словами, код имеет минимальное расстояние d в точности тогда, когда d — это наименьшее число столбцов проверочной матрицы, образующих линейно зависимую систему. Это свойство часто используется как для оценки корректирующей способности кода, так и для построения кодов с заданным минимальным расстоянием.

Важную роль в теории кодирования играет понятие дуального кода. Пусть C — линейный (n, k)-код над полем $\mathbb{F}_2$. Его дуальным кодом $C^{\perp}$ называется множество всех векторов длины n, ортогональных каждому кодовому слову из C относительно стандартного скалярного произведения. Иными словами, $C^{\perp} = \{\mathbf{v} \in \mathbb{F}_2^n \mid \forall \mathbf{c} \in C,\ \mathbf{c} \cdot \mathbf{v} = 0\}$. Размерность дуального кода равна $n-k$, а его порождающей матрицей служит проверочная матрица исходного кода. Примером может служить код Хэмминга $(7, 4)$: его дуальным кодом является $(7, 3)$-код, известный как симплекс-код, все ненулевые слова которого имеют одинаковый вес 4.

Двоичные коды Хэмминга обладают свойством оптимальности. Для заданной длины $n = 2^r - 1$ и минимального расстояния 3 максимально возможное число кодовых слов в любом (не обязательно линейном) коде ограничено сверху границей Хэмминга: $M \leq \frac{2^n}{1+n}$. Коды Хэмминга $(2^r - 1,\ 2^r - r - 1)$ достигают этого равенства, то есть являются совершенными. Это означает, что никакой код (в том числе нелинейный) с длиной n и расстоянием 3 не может содержать больше кодовых слов, чем код Хэмминга. Таким образом, коды Хэмминга оптимальны по отношению к границе Хэмминга.

Как уже было сказано, дуальные коды к кодам Хэмминга представляют собой важный класс кодов — симплекс-коды. Для параметра r код Хэмминга имеет длину $2^r - 1$ и размерность $2^r - r - 1$, а дуальный к нему код имеет длину $2^r - 1$ и размерность r. Этот код называется симплекс-кодом и замечателен тем, что все его ненулевые кодовые слова имеют одинаковый вес 2^{r-1}. Например, для $r = 3$ код Хэмминга $(7, 4)$ и дуальный ему симплекс-код $(7, 3)$ состоит из восьми слов, ненулевые из которых имеют вес 4.

Расширенные коды Хэмминга получаются из исходных добавлением общей проверки на четность. Если исходный код Хэмминга имеет параметры $(2^r - 1, 2^r - r - 1, 3)$, то расширенный код $(2^r, 2^r - r - 1, 4)$ строится путем добавления одного дополнительного символа, равного сумме всех символов кодового слова по модулю два. Это увеличивает минимальное расстояние до 4, что делает код пригодным для одновременного обнаружения двух ошибок или исправления одной ошибки и обнаружения двух. Примером может служить расширенный код Хэмминга $(8, 4, 4)$, который широко используется в системах обнаружения ошибок и является самодуальным (совпадает со своим дуальным кодом).