56. (n, M, d)-коды. Граница Плоткина

Определение. (n, M, d)-*кодом* называется код, в котором все кодовые слова имеют длину n, d – минимальное расстояние между словами (в смысле расстояния Хэмминга), M – количество кодовых слов.

Теорема (Граница Плоткина)**.** *Пусть задан (n, M, d)-код. Если $2d > n$, то $M \leq \left[\frac{2d}{2d-n}\right]$*

$\blacktriangle$. Пусть $\vec{a_1}, \vec{a_2}, ..., \vec{a_M}$ – все кодовые слова. Запишем их в матрицу следующим образом (каждый вектор представляется в виде строчки):

$$\begin{pmatrix} \leftarrow \vec{a_1} \rightarrow \\ \leftarrow \vec{a_2} \rightarrow \\ ... \\ \leftarrow \vec{a_M} \rightarrow \end{pmatrix}$$

Полученная матрица имеет размер $M \times n$.
Рассмотрим сумму (a_{i_j} – элемент матрицы)

$$S = \sum_{k=1}^{n} \sum_{1 \leq i < j \leq M} I_{\{a_{i_k} \neq a_{j_k}\}}, \text{где } I_{\{a_{i_k} \neq a_{j_k}\}} = \begin{cases} 1, a_{i_k} \neq a_{j_k} \\ 0, a_{i_k} = a_{j_k} \end{cases}$$

S можно рассматривать следующим образом: фиксируем столбец k и смотрим количество несовпадающих пар в этом столбце. Пусть x – число единиц в этом столбце, тогда $M - x$ – число нулей в этом же столбце. Тогда несовпадающих пар в этом столбце ровно $x(M - x) = Mx - x^2$. Максимум этого значения достигается при $x = \frac{M}{2}$, то есть $x(M - x) \leq \frac{M^2}{4}$. Получаем, что $S \leq n \cdot \frac{M^2}{4}$.
Теперь рассмотрим S с другой стороны, переставив знаки суммирования:

$$S = \sum_{1 \leq i < j \leq M} \sum_{k=1}^{n} I_{\{a_{i_k} \neq a_{j_k}\}}$$

Теперь S можно интерпретировать следующим образом: зафиксируем строки i и j (а значит, и соответствующие кодовые слова $\vec{a_i}$ и $\vec{a_j}$). Тогда внутренняя сумма $\sum\limits_{k=1}^{n} I_{\{a_{i_k} \neq a_{j_k}\}}$ – это в точности расстояние Хэмминга $d(\vec{a_i}, \vec{a_j})$. По определению (n, M, d)-кода $d(\vec{a_i}, \vec{a_j}) \geq d$, то есть $S \geq \frac{M(M-1)}{2} \cdot d$, где ($\frac{M(M-1)}{2}$ – количество пар (i, j)).

$$\frac{M(M-1)}{2} \cdot d \leq S \leq n \cdot \frac{M^2}{4}$$

$$(M-1)d \leq n \cdot \frac{M}{2}$$

$$dM - \frac{nM}{2} \leq d$$

$$M(d - \frac{n}{2}) \leq d$$

$$M(2d - n) \leq 2d$$

Так как $2d - n$ – положительное, то можно разделить на него

$$M \leq \frac{2d}{2d - n}$$

Так как M – натуральное, получаем:

$$M \leq \left[\frac{2d}{2d-n}\right]$$

$\blacksquare$