Доказательство теоремы об исправлении ошибок

Теорема. Если минимальное расстояние кода равно $d_{\min}$, то код позволяет исправлять любые ошибки кратности

$$t \le \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor .$$

Доказательство.

Пусть было передано кодовое слово c, а в результате воздействия канала получено слово y, причём

$$d(c, y) \le t.$$

Предположим, что существует другое кодовое слово $c' \ne c$, которое также находится на расстоянии не более t от y, то есть

$$d(c', y) \le t.$$

Тогда, применяя неравенство треугольника к тройке слов c, y, c', получаем:

$$d(c, c') \le d(c, y) + d(y, c').$$

Следовательно,

$$d(c, c') \le t + t = 2t.$$

По условию на t имеем

$$2t \le 2 \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor \le d_{\min} - 1.$$

Значит,

$$d(c, c') \le d_{\min} - 1 < d_{\min}.$$

Однако по определению минимального расстояния любые два различных кодовых слова удовлетворяют неравенству

$$d(c, c') \ge d_{\min}.$$

Получено противоречие. Следовательно, второго кодового слова c' существовать не может.

Таким образом, при числе ошибок не более t принятое слово однозначно декодируется в исходное кодовое слово c, что и доказывает утверждение.

□