

Theorem 1.1

1. A code C can detect s errors in any codeword iff $d(C) \geq s+1$.
2. A code C can correct t errors in any codeword if $d(C) \geq 2t+1$.

Proof: Suppose $d(C) \geq s+1$ and consider any codeword \underline{x} of C . If the vector \underline{y} is the result of s errors in \underline{x} , then $d(\underline{x}, \underline{y}) = s < s+1 \leq d(C)$; hence \underline{y} is not a codeword, and therefore the s errors in \underline{x} can be detected.

Suppose $d(C) \geq 2t+1$ and consider any codeword \underline{x} of C . If the vector \underline{y} is the result of t errors in \underline{x} , then $d(\underline{x}, \underline{y}) = t$. Suppose that \underline{x}' is a codeword other than \underline{x} . Then

$d(\underline{x}', \underline{y}) > d(\underline{x}, \underline{y})$, for otherwise

$d(\underline{x}, \underline{x}') \leq d(\underline{x}, \underline{y}) + d(\underline{y}, \underline{x}') \leq 2d(\underline{x}, \underline{y}) = 2t$, which contradicts $d(C) \geq 2t+1$.

Therefore \underline{x} is the unique codeword nearest to \underline{y} , and therefore nearest neighbour decoding corrects the t errors in \underline{x} .

■

Corollary 1.2 If C has minimum distance d , then C can be used either to detect up to $d-1$ errors, or C can be used to correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

Definition 1.7 For any vector \underline{u} in $(F_q)^n$ and any integer $r > 0$, the sphere $S(\underline{u}, r)$ with centre \underline{u} and radius r is the set $\{ \underline{v} \in (F_q)^n : d(\underline{u}, \underline{v}) \leq r \}$.

Lemma 1.3 The sphere $S(\underline{u}, r)$ in $(F_q)^n$ contains $\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \dots + \binom{n}{r}(q-1)^r$ vectors.

Proof: Follow in the notes.

Theorem 1.4 (The Hamming Bound or Sphere Packing Bound.)

For any q -ary $(n, M, 2t+1)$ -code,

$$M \left[\binom{n}{0} + \binom{n}{1}(q-1) + \dots + \binom{n}{t}(q-1)^t \right] \leq q^n.$$

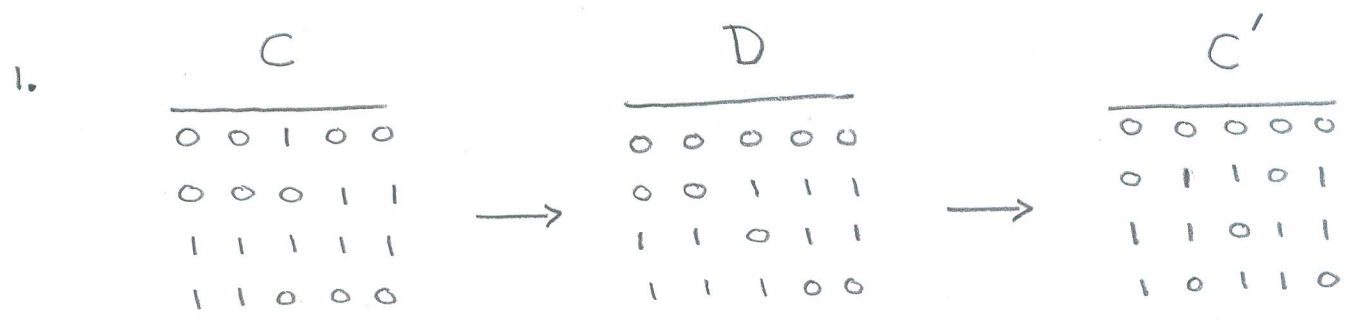
Proof: Follow in the notes.

Corollary 1.5 For any binary $(n, M, 2t+1)$ -code,
 $M \left[\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t} \right] \leq 2^n$.

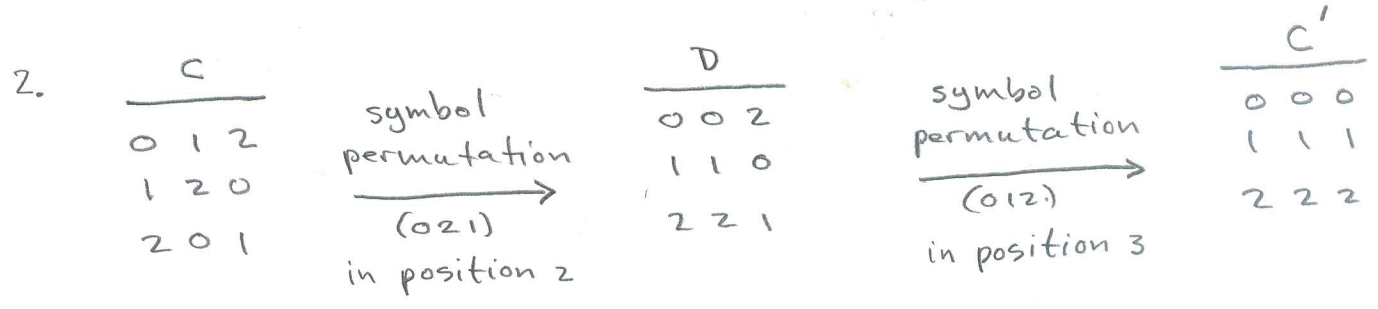
Definition 1.8 A code C' is equivalent to a code C if C' can be obtained from C by a sequence of positional permutations or symbol permutations.

Note that, if C' is equivalent to C , then $d(C') = d(C)$.

Examples:



Do the symbol permutation (01) in column 3 of code C to obtain code D , then do the positional permutation (2,4) — that is, swap columns 2 and 4 — on code D to obtain code C' .



So, C is equivalent to the ternary repetition code C' of length three.

