(*) $d(z_1, z_2) \leq d-1 < d = d(C) \overset{\text{def } d(C)}{\Rightarrow} d(z_1, z_2) = 0 \Leftrightarrow z_1 = z_2$

$\Rightarrow d(y, C) \leq d(y, z) \leq e \Rightarrow d(y, C) = d(y, z)$

Proposizione 2.1. *Sia C un codice con $d(C) = d$ e poniamo $e = \lfloor (d-1)/2 \rfloor$. Data una parola $y \in \mathcal{A}^n$ esiste al piú parola $z \in C$ tale che $d(y, z) \leq e$. Se inoltre $d(y, C) = \min\{d(y, x) : x \in C\} \leq e$ allora tale z é tale che $d(y, z) = d(y, C)$.*

Dimostrazione. Supponiamo che $d(y, z_1), d(y, z_2) \leq e$ per $z_1, z_2 \in C$. Allora per la disuguaglianza triangolare $d(z_1, z_2) \leq d(z_1, y) + d(y, z_2) \leq 2e \leq d - 1$ quindi, per definizione di $d = d(C)$ deve essere necessariamente $z_1 = z_2$. Se $z \in C$ é tale che $d(y, z) = d(y, C) \leq e$ allora z é l'unica parola di C con $d(y, z) \leq e$, per quanto provato prima. □

In consequenza al risultato precedente, se usando il codice C si trasmette una parola $x \in C$ e si riceve $y \in \mathcal{A}^n$ con un numero di errori minore od uguale ad $e = [(d(C) - 1)/2]$ allora x quó essere ricostruita univocamente da y. Infatti si avrá $d(y, C) \leq d(y, x) \leq e$ pertanto, applicando la proposizione precedente, x é l'unica parola di C con $d(y, x) \leq e$. Ció giustifica la terminologia *C puó correggere e errori.*

Una nozione correlata a quella di distanza é quella di *peso* di una parola, nel caso che l'alfabeto $\mathcal{A}$ sia un campo finito k, e pertanto l'insieme delle possibili parole sia lo spazio vettoriale k^n.

Definizione 2.5. *Diremo peso di una parola $a \in k^n$ la sua distanza da $0 = (0, \ldots, 0) \in k^n$, ossia il numero $w(a) = \#\{i : a_i \neq 0\}$.*

Notiamo che si puó esprimere la distanza di due parole di k^n tramite il peso, precisamente $d(x, y) = w(x - y)$. Nel caso di una trasmissione di una parola $x \in k^n$, assumendo che la parola ricevuta sia $y = x + e$ allora $w(e)$ é il numero di errori occorsi nella trasmissione.

2.1 Decodifica per massima somiglianza

Il procedimento di decodifica per *massima somiglianza* per un codice $C \subset \mathcal{A}^n$ consiste nel sostituire la parola ricevuta y con una parola $x \in C$ tale che $d(y, x) = d(y, C)$, ossia x é la parola di C di distanza minima da y.
Ad esempio se giá $y \in C$ allora si pone $x = y$. Se $d = d(C)$ ed $e = [(d-1)/2]$ si usa la seguente variante: se $d(y, C) \leq e$ allora si decodifica y con x come sopra, altrimenti, se $d(y, C) > e$ allora y non viene decodificata e si produce un messaggio di errore (avente come consequenza in certi casi una richiesta di ritrasmissione della parola x).

Vediamo attraverso un esempio come la decodifica per massima somiglianza minimizzi la probabilitá di errore nella decodifica, assumendo un canale binario simmetrico privo di memoria. Supponiamo che $C \subset \mathbb{Z}_2^6$, ossia le parole in considerazione sono 6-uple di 0 ed 1.