Limite di Hamming

Fissata la dimensione n delle parole di un codice a blocchi e la quantità e di errori che si vogliono correggere, il limite di Hamming è un limite massimo al numero di parole di codice (e quindi ai bit di informazione k):

$$|C| = 2^k = 2^{nR_c} \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}$$

La condizione è necessaria ma non sufficiente, cioè potrebbe non esistere un codice con dei parametri n, k, e anche se questi rispettano il limite.

Si può riscrivere come limite inferiore sulle cifre di controllo:

$$2^q \geq \sum_{i=0}^{e} \binom{n}{i}.$$

Un codice che raggiunge esattamente il limite di Hamming è detto *perfetto*.

Dimostrazione

Si possono costruire le sfere $S_i = \{v \mid d(w_i, v) \leq e\}$ $(w_i \in C)$, che contengono le parole ottenibili da w_i con al più e errori.

Vale che,

$$\forall i \ . \ |S_i| = \sum_{i=0}^{e} \binom{n}{i}$$

dove la somma conta tutti i modi in cui possono verificarsi fino ad e errori.

Le sfere complessivamente includono $|C| \sum_{i=0}^{e} \binom{n}{i}$ parole, e visto che sono disgiunte (altrimenti ci sarebbe ambiguità nella correzione) questa quantità non può essere maggiore di 2^n.