

# Codice di Hamming

Codici lineari a blocchi con

$$q = n - k \geq 3 \quad n = 2^q - 1.$$

Tutti i codici di Hamming sono perfetti.

**distanza minima**  $d_{\min} = 3$ , perciò possono rilevare 2 errori o correggerne 1 — i  $q$  bit di ridondanza possono assumere  $n + 1$  valori, ovvero una per ogni posizione dell'errore (singolo) più una configurazione che ne indica l'assenza;

**costruzione** la matrice di controllo di parità deve contenere tutte le sequenze di  $q$  bit nelle colonne. Questo permette di identificare gli errori singoli, visto che si associa esattamente una posizione ad ogni sindrome. Equivalentemente si può definire  $G = (I \mid P)$  dove tutte le righe di  $P$  sono diverse e hanno peso 2 (spiegazione);

**code rate**  $R_c = \frac{k}{n} = 1 - \frac{q}{2^q - 1}$ . Aumentando  $q$  diminuisce la ridondanza del codice, ma aumenta la probabilità che in una parola di codice si verifichi più di un errore.