Matrice di controllo di parità

Per verificare l'integrità di una parola da $n = k + 1$ bit condificata da un codice a controllo di parità singola, si determina se vale

$$y_1 + \cdots + y_n \equiv 0 \mod 2.$$

Con un CCP generale (con $n = k+q$) abbiamo un sistema omogeneo di equazioni modulo 2, che possono essere espresse come una matrice a controllo di parità A di dimensione $q \times n$. La parola y è del codice (non contiene errori rilevabili) se $Ay = 0$; il vettore Ay è detto *sindrome*.

Il rango di A è q, quindi nel sistema ci sono $k = n - q$ cifre che possono essere specificate liberamente (*cifre di informazione*), in base a cui si possono sempre determinare le restanti q (*cifre di controllo*) per rendere vere le congruenze.

Altre proprietà:

- gli errori rilevabili sono le sequenze che non sono parole di codice, quindi $2^n - 2^k$;
- se G è la matrice generatrice, $AG^{\mathsf{t}} = 0_{q \times k}$.

Codici sistematici

Un codice sistematico con generatrice $G = (I_k \mid P)$ ha matrice di controllo di parità $A = (P^{\mathsf{t}} \mid I_q)$.