Codici lineari

Un codice è lineare se l'insieme delle parole di codice è chiuso rispetto alla somma bit a bit modulo 2 (XOR), cioè $c_1, c_2 \in C \implies c_1 \oplus c_2 \in C$. Questo implica che la parola nulla è sempre di codice.

I codici lineari con parole di lunghezza $n = k + q$ (q bit di ridondanza) sono sottospazi di dimensione k di $\mathbb{Z}_2^n$.

Possono essere definiti tramite una *matrice generatrice* G di dimensione $k \times n$:

- (def. 1) le righe di G sono una base del codice;
- (def. 2) se la colonna j ha 1 in posizione $i_1, \ldots, i_h$, allora $y_j = x_{i_1} \oplus \cdots \oplus x_{i_h}$;
- $y = xG$ con vettori riga, $y = G^{\mathsf{t}}x$ se sei una persona normale (ma a quel punto avresti definito G bene...);
- se il codice è anche sistematico, $G = (I_k \mid P)$, e la matrice P di dimensione $k \times (n - k)$ è sufficiente a definire il codice. Se $G = (Q \mid P)$ con $Q \neq I$ e $\det Q \neq 0$, il codice non è sistematico ma i bit di informazione sono comunque i primi k;
- per ogni scelta di G si ottiene un codice diverso, quindi quelli possibili sono 2^{nk}, sistematici 2^{qk}, $\frac{2^{qk}}{q!k!}$ se non si contano le permutazioni di righe e colonne di P (che non cambiano la capacità correttiva — codice equivalente);