

⊗ ovvero, $\{H_1, \dots, H_n, h\}$ non gode più della proprietà di avere i settori a due a due non proporzionali; se $h \notin \{H_1, \dots, H_n\}$.

4 Alcune classi di codici

4.1 Codici di Hamming

Definizione 4.1. I codici di Hamming sono quei codici $C \subset \mathbb{F}_q^n$ che amettono una matrice di controllo H le cui colonne $H_1, \dots, H_n$ formino un insieme massimale di vettori di $\mathbb{F}_q^n$ a due a due non proporzionali, ⊗

Spiegheremo meglio questa definizione, fornendo anche un metodo per costruire tali codici. Richiamiamo la definizione di spazio proiettivo su un campo.

Definizione 4.2. Lo spazio proiettivo $r - 1$ dimensionale $\mathbb{P}^{r-1}(k)$ su un campo k è l'insieme dei sottospazi vettoriali 1-dimensionali di k^r .

Def 4.2.1 Un punto di $\mathbb{P}^{r-1}(k)$ è pertanto un sottospazio $\langle v \rangle = \{\lambda v \mid \lambda \in k\}$ di k^r generato da un vettore non nullo $v \in k^r$. Per due vettori non nulli $v, w \in k^r$ si ha $\langle v \rangle = \langle w \rangle$ se e solo se v e w sono proporzionali, ossia esiste $\lambda \in k^*$ tale che $w = \lambda v$. Pertanto possiamo rappresentare $\mathbb{P}^{r-1}(k)$ anche come l'insieme delle classi di equivalenza $\bar{v}$ della relazione di equivalenza su $k^r \setminus \{0\}$ definita da $v \equiv w$ se e solo se esiste $\lambda \in k^*$ tale che $w = \lambda v$:

$$\mathbb{P}^{r-1}(k) = (k^r \setminus \{0\}) / \equiv$$

Se $k = \mathbb{F}_q$ allora in ogni classe di equivalenza $\bar{v}$ vi sono $q - 1$ elementi, precisamente tutti i vettori λv con $\lambda \neq 0$. Poiché in $k^r \setminus \{0\}$ vi sono $q^r - 1$ elementi, segue la formula

$$\#\mathbb{P}^{r-1}(k) = \frac{q^r - 1}{q - 1}$$

Se un elemento $\langle v \rangle \in \mathbb{P}^{r-1}(k)$ è determinato da un vettore $v \in k^r \setminus \{0\}$, allora le coordinate di $v = (x_0, \dots, x_{r-1})$ rispetto alla assegnata base di k^r sono per definizione *coordinate omogenee* di $\langle v \rangle$, il quale viene spesso indicato con $(x_0 : \dots : x_{r-1})$. Da quanto detto sopra $(x_0, \dots, x_{r-1})$ e $(y_0, \dots, y_{r-1})$ sono coordinate omogenee dello stesso punto di $\mathbb{P}^{r-1}(k)$ se e solo se $y_i = \lambda x_i$ per ogni $i = 0 \dots r - 1$, per un dato $\lambda \in k^*$. Notiamo infine la seguente decomposizione di $\mathbb{P}^{r-1}(k)$ nell'unione disgiunta di uno spazio affine ed un iperpiano proiettivo

$$\mathbb{P}^{r-1}(k) = \mathbb{A}^{r-1}(k) \cup \mathbb{P}^{r-2}(k)$$

dove $\mathbb{A}^{r-1}(k) = \{(x_0 : \dots : x_{r-2} : 1)\}$ e $\mathbb{P}^{r-2}(k) = \{(x_0 : \dots : x_{r-2} : 0)\}$. Tale decomposizione fornisce evidentemente un metodo induttivo per elencare tutti i punti di $\mathbb{P}^{r-1}(k)$.