(F29, ti 2 maj 2006)

En (binär) **kod** C är en mängd n-tupler av 0:or och 1:or, dvs

$C \subseteq V^n, \quad (V = \mathbb{Z}_2 = \{0,1\})$

n : kodens **längd**

Minimala avståndet för C :

$\delta(C) = \min\{\partial(\mathbf{x},\mathbf{y}) \mid \mathbf{x},\mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}$

där $\partial(\mathbf{x},\mathbf{y}) =$ antalet i med $x_i \neq y_i$.

C kan **upptäcka** upp till $\delta - 1$ fel

Sats En kod C kan rätta e fel om $\delta(C) \geq 2e+1$.

Sfärpackningssatsen : Om koden C, av längd n, rättar upp till e fel,

$$|C|\left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{e}\right) \leq 2^n \ (= |V^n|)$$

En kod som ger likhet i Sfärpackningssatsen kallas **perfekt**.

C är en **linjär kod** om

$$\mathbf{x},\mathbf{y} \in C \Rightarrow \mathbf{x}+\mathbf{y} \in C$$

dvs C är en **delgrupp** (även delrum) till V^n

$|C| = 2^k$, där k kallas (och är) C:s **dimension**

För en linjär kod är minimala avståndet = **minimala** (nollskilda) **vikten**, dvs

$$\delta = w_{\min} = \min\{w(\mathbf{x}) \mid \mathbf{x} \in C,\ \mathbf{x} \neq 0\}$$

där vikten för $\mathbf{x}$, $w(\mathbf{x})$, är antalet 1:or i $\mathbf{x}$.

Om H är en $r \times n$-matris av full rank så är $C = \{\mathbf{x} \in V^n \mid H\mathbf{x} = \mathbf{0}\}$ en linjär kod av dimension$= n - r$. H kallas kodens **kontrollmatris**.

Sats: Om H:s alla kolumner är olika och $\neq \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, så är $\delta(C) \geq 3$ och C rättar (minst) ett fel.

För att rätta fel : z ett kodord med fel i position $i \ \Rightarrow \ Hz = H$:s i:e kolumn.

Hammingkod ges av en kontrollmatris H med r rader och $2^r - 1$ kolumner, alla olika och $\neq \mathbf{0}$

längd	$n = 2^r - 1$
minimiavstånd	$\delta = 3$
dimension	$k = 2^r - r - 1$

Hammingkoder är **perfekta koder**.