Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon : S \to C$ codificación

es inyectiva (y podemos asumir que sea sobre)

$\delta : F^n \to C$ decodificación

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Códigos lineales

S: mensajes

C: código

F: alfabeto

$\varepsilon : S \to C$ <u>codificación</u>

es inyectiva (y podemos asumir que sea sobre)

$\delta : F^n \to C$ <u>decodificación</u>

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

<u>Def</u>: Sea F un campo finito. El código C es un <u>código lineal</u> si es un subespacio del F-espacio vectorial F^n

Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon : S \to C$ codificación

es inyectiva (y podemos asumir que sea sobre)

$\delta : F^n \to C$ decodificación

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

Def: Sea F un campo finito. El código C es un código lineal si es un subespacio del F-espacio vectorial F^n

Dada una palabra w, definimos su peso como

$wt(w)$ = número de coordenadas de w distintas de 0

$wt(11010) = 3$

Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon: S \to C$ codificación

es inyectiva (y podemos asumir que sea sobre)

$\delta: F^n \to C$ decodificación

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

Def: Sea F un campo finito. El código C es un código lineal si es un subespacio del F-espacio vectorial F^n

Dada una palabra w, definimos su peso como

$wt(w)$ = número de coordenadas de w distintas de 0

$wt(11010) = 3$

El peso mínimo de un código C es el mínimo peso dentre las palabras código distintas del 0.

Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon: S \to C$ codificación

es inyectiva (y podemos asumir que sea sobre)

$\delta: F^n \to C$ decodificación

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

Def: Sea F un campo finito. El código C es un código lineal si es un subespacio del F-espacio vectorial F^n

Dada una palabra w, definimos su peso como
$wt(w)$ = número de coordenadas de w distintas de 0

$wt(11010) = 3$

El peso mínimo de un código C es el mínimo peso dentre las palabras código distintas del 0.

Prop: El peso mínimo de un código lineal es igual a su distancia mínima.

Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon: S \to C$ <u>codificación</u>

es inyectiva (y podemos asumir que sea sobre)

$\delta: F^n \to C$ <u>decodificación</u>

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

<u>Def</u>: Sea F un campo finito. El código C es un <u>código lineal</u> si es un subespacio del F-espacio vectorial F^n

Dada una palabra w, definimos su <u>peso</u> como $wt(w)$ = número de coordenadas de w distintas de 0

$wt(11010) = 3$

El <u>peso mínimo</u> de un código C es el mínimo peso dentre las palabras código distintas del 0.

<u>Prop</u>: El peso mínimo de un código lineal es igual a su distancia mínima.

Sigue de $d(v,w) = wt(v-w)$.

Códigos lineales

S: mensajes
C: código
F: alfabeto

$\varepsilon: S \to C$ codificación

es inyectiva (y podemos asumir que sea sobre)

$\delta: F^n \to C$ decodificación

Usualmente: $\delta(w) = c$, donde c es la palabra código más cercana a w.

Si F es un campo finito, como $\mathbb{F}_2$, F^n es un espacio vectorial sobre F con dimensión n.

Def: Sea F un campo finito. El código C es un código lineal si es un subespacio del F-espacio vectorial F^n

Dada una palabra w, definimos su peso como

$wt(w)$ = número de coordenadas de w distintas de 0

$wt(11010) = 3$

El peso mínimo de un código C es el mínimo peso dentre las palabras código distintas del 0.

Prop: El peso mínimo de un código lineal es igual a su distancia mínima.

Sigue de $d(v,w) = wt(v-w)$.

Si transimitimos c y recibimos $w = c+e$, $wt(e)$ es el número de errores que han occurrido.

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix} \quad \text{es una matriz } k \times n \text{ en } F$$

<u>matriz</u> <u>generadora</u> de C [si $c \in C$, existe un $x \in F^k$ t.q.:

$$\underset{\underset{x_1 c_1 + \cdots + x_k c_k}{\parallel}}{xG} = c$$

]

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix} \quad \text{es una matriz } k \times n \text{ en } F$$

<u>matriz</u> <u>generadora</u> de C si $c \in C$, existe un $x \in F^k$ t.q.:

$$\begin{array}{c} xG = c \\ \shortparallel \\ x_1 c_1 + \cdots + x_k c_k \end{array}$$

En este formalismo:

$$S = F^{k}$$

$$\begin{aligned} \varepsilon : S &\to C \qquad\qquad (\text{lineal!}) \\ x &\mapsto xG \end{aligned}$$

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$$ es una matriz $k \times n$ en F

<u>matriz</u> <u>generadora</u> de C ⌜si $c \in C$, existe un $x \in F^k$ t.q.:

$$\begin{aligned} xG &= c \\ &\| \\ x_1 c_1 &+ \cdots + x_k c_k \end{aligned}$$ ⌟

En este formalismo:

$$S = F^k$$

$$\begin{aligned} \varepsilon : S &\to C \\ x &\mapsto xG \end{aligned}$$ (lineal!)

Podemos hacer manipulaciones en las líneas y las columnas de G para que quede en la <u>forma estándar</u> $G = (I \; A)$

I: $k \times k$ identidad

$$\varepsilon(x) = (x \;\; xA)$$

los primeros k dígitos son de <u>información</u>
los $n-k$ que quedan son de <u>control</u>

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$$ es una matriz $k \times n$ en F

<u>matriz</u> <u>generadora</u> de C ⌜si $c \in C$, existe un $x \in F^k$ t.q.:

$$x G = c$$
$$\shortparallel$$
$$x_1 c_1 + \cdots + x_k c_k$$
⌟

En este formalismo:

$$S = F^{k}$$

$$\begin{aligned} \varepsilon : S &\to C \\ x &\mapsto xG \end{aligned}$$ (lineal!)

Podemos hacer manipulaciones en las líneas y las columnas de G para que quede en la <u>forma estándar</u> $G = (I \ A)$

I: $k \times k$ identidad

$$\varepsilon(x) = (x \ \ xA)$$

los primeros k dígitos son de <u>información</u>
los $n-k$ que quedan son de <u>control</u>

<u>Ejemplo</u> (Código (7,4) de Hamming)

Sea $F = \mathbb{F}_2$ y

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$ $|C| = 2^4 = 16$

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$$ es una matriz $k \times n$ en F

<u>matriz generadora</u> de C ⌐si $c \in C$, existe un $x \in F^k$ t.q.:

$$\begin{gathered} xG = c \\ \| \\ x_1 c_1 + \cdots + x_k c_k \end{gathered}$$
⌟

En este formalismo:

$$S = F^k$$

$$\begin{aligned} \varepsilon : S &\to C \\ x &\mapsto xG \end{aligned} \qquad \text{(lineal!)}$$

Podemos hacer manipulaciones en las líneas y las columnas de G para que quede en la <u>forma estándar</u> $G = (\underset{\substack{\uparrow \\ k\times k \text{ identidad}}}{I} \ A)$

$\varepsilon(x) = (x \ \ xA)$

los primeros k digitos son de <u>información</u>
los $n-k$ que quedan son de <u>control</u>

<u>Ejemplo</u> (Código (7,4) de Hamming)

Sea $F = \mathbb{F}_2$ y

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad |C| = 2^4 = 16$$

$$xG = (x_1, x_2, \ldots, x_7) \qquad \left.\begin{aligned} x_5 &= x_2 + x_3 + x_4 \\ x_6 &= x_1 + x_3 + x_4 \\ x_7 &= x_1 + x_2 + x_4 \end{aligned}\right] \Rightarrow \begin{array}{l} \text{mín wt} = 3 \\ C \text{ es 1-corrector} \end{array}$$

Siendo C un subespacio de F^n podemos elegir una base de C formada de $k = \dim C$ palabras de longitud n.

$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$ es una matriz $k \times n$ en F

matriz generadora de C ⌜si $c \in C$, existe un $x \in F^k$ t.q.:

$$x G = c$$
$$\shortparallel$$
$$x_1 c_1 + \dots + x_k c_k$$
⌟

En este formalismo:

$$S = F^k$$
$$\varepsilon : S \to C \qquad \text{(lineal!)}$$
$$x \mapsto xG$$

Podemos hacer manipulaciones en las líneas y las columnas de G para que quede en la forma estándar $G = (\underset{\substack{\uparrow \\ k\times k \text{ identidad}}}{I} \; A)$

$\varepsilon(x) = (x \;\; xA)$

los primeros k dígitos son de información
los $n-k$ que quedan son de control

Ejemplo (Código (7,4) de Hamming)

Sea $F = \mathbb{F}_2$ y

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad |C| = 2^4 = 16$$

$xG = (x_1, x_2, \dots, x_7)$ $\left.\begin{array}{l} x_5 = x_2 + x_3 + x_4 \\ x_6 = x_1 + x_3 + x_4 \\ x_7 = x_1 + x_2 + x_4 \end{array}\right] \Rightarrow$ mín wt $= 3$, C es 1-corrector

C es perfecto: $16 = |C| = 2^7 / (1 + 7(2-1))$