

# Insinöörimatematiikka 3

Mika Hirvensalo  
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos  
Turun yliopisto

2022

## Määritelmä

Olkoon  $V$  kompleksinen vektoriavaruus. Kuvaus  $V \times V \rightarrow \mathbb{C}$ , on *Hermiten sisätulo*, jos se toteuttaa seuraavat ehdot:

## Määritelmä

Olkoon  $V$  kompleksinen vektoriavaruus. Kuvaus  $V \times V \rightarrow \mathbb{C}$ , on *Hermiten sisätulo*, jos se toteuttaa seuraavat ehdot:

- $(\mathbf{x}, \mathbf{x}) \geq 0$  ja  $(\mathbf{x}, \mathbf{x}) = 0$  tarkalleen silloin kun  $\mathbf{x} = \mathbf{0}$  (epänegativisuus ja epädegeneratiivisuus).

## Määritelmä

Olkoon  $V$  kompleksinen vektoriavaruus. Kuvaus  $V \times V \rightarrow \mathbb{C}$ , on *Hermiten sisätulo*, jos se toteuttaa seuraavat ehdot:

- $(\mathbf{x}, \mathbf{x}) \geq 0$  ja  $(\mathbf{x}, \mathbf{x}) = 0$  tarkalleen silloin kun  $\mathbf{x} = \mathbf{0}$  (epänegativisuus ja epädegeneratiivisuus).
- $(\mathbf{x}, \mathbf{y}) = \overline{(\mathbf{y}, \mathbf{x})}$  (vinosymmetria).

## Määritelmä

Olkoon  $V$  kompleksinen vektoriavaruus. Kuvaus  $V \times V \rightarrow \mathbb{C}$ , on *Hermiten sisätulo*, jos se toteuttaa seuraavat ehdot:

- $(\mathbf{x}, \mathbf{x}) \geq 0$  ja  $(\mathbf{x}, \mathbf{x}) = 0$  tarkalleen silloin kun  $\mathbf{x} = \mathbf{0}$  (epänegativisuus ja epädegeneratiivisuus).
- $(\mathbf{x}, \mathbf{y}) = \overline{(\mathbf{y}, \mathbf{x})}$  (vinosymmetria).
- $(a\mathbf{x} + b\mathbf{y}, \mathbf{z}) = a(\mathbf{x}, \mathbf{z}) + b(\mathbf{y}, \mathbf{z})$  (lineaarisuus 1. argumentin suhteen).

## Määritelmä

Olkoon  $V$  kompleksinen vektoriavaruus. Kuvaus  $V \times V \rightarrow \mathbb{C}$ , on *Hermiten sisätulo*, jos se toteuttaa seuraavat ehdot:

- $(\mathbf{x}, \mathbf{x}) \geq 0$  ja  $(\mathbf{x}, \mathbf{x}) = 0$  tarkalleen silloin kun  $\mathbf{x} = \mathbf{0}$  (epänegativisuus ja epädegeneratiivisuus).
- $(\mathbf{x}, \mathbf{y}) = \overline{(\mathbf{y}, \mathbf{x})}$  (vinosymmetria).
- $(a\mathbf{x} + b\mathbf{y}, \mathbf{z}) = a(\mathbf{x}, \mathbf{z}) + b(\mathbf{y}, \mathbf{z})$  (lineaarisuus 1. argumentin suhteen).

## Määritelmä

Vektoreiden  $\mathbf{x} = (x_1, \dots, x_n)$  ja  $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{C}^n$  *Hermiten pistetulo* määritellään  $\mathbf{x} \cdot \mathbf{y} = x_1 \overline{y_1} + \dots + x_n \overline{y_n}$ .

## Määritelmä: Kulma vektoriavaruudessa

Nollasta poikkeavien vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  välinen kulma  $\theta$  määritellään

$$\cos \theta = \frac{(\mathbf{x}, \mathbf{y})}{\|\mathbf{x}\| \|\mathbf{y}\|}.$$

## Määritelmä: Kulma vektoriavaruudessa

Nollasta poikkeavien vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  välinen kulma  $\theta$  määritellään

$$\cos \theta = \frac{(\mathbf{x}, \mathbf{y})}{\|\mathbf{x}\| \|\mathbf{y}\|}.$$

Nollavektorin välinen kulma toiseen vektoriin määritellään aina suoraksi kulmaksi.

## Määritelmä: Kulma vektoriavaruudessa

Nollasta poikkeavien vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  välinen kulma  $\theta$  määritellään

$$\cos \theta = \frac{(\mathbf{x}, \mathbf{y})}{\|\mathbf{x}\| \|\mathbf{y}\|}.$$

Nollavektorin välinen kulma toiseen vektoriin määritellään aina suoraksi kulmaksi.

## Huomautus

Cauchyn-Schwarzin epäyhtälön perusteella

$$|(\mathbf{x}, \mathbf{y})|^2 \leq (\mathbf{x}, \mathbf{x})(\mathbf{y}, \mathbf{y}) = \|\mathbf{x}\|^2 \cdot \|\mathbf{y}\|^2,$$

joten

$$|(\mathbf{x}, \mathbf{y})| \leq \|\mathbf{x}\| \|\mathbf{y}\|$$

## Esimerkki

### Esimerkki 82

## Esimerkki

### Esimerkki 82

## Määritelmä

Olkoon  $(\mathbf{x}, \mathbf{y})$  jokin sisätulo. Vektorit  $\mathbf{x}$  ja  $\mathbf{y}$  ovat *ortogonaalit* eli *kohtisuorat* jos  $(\mathbf{x}, \mathbf{y}) = 0$ .

## Esimerkki

### Esimerkki 82

## Määritelmä

Olkoon  $(\mathbf{x}, \mathbf{y})$  jokin sisätulo. Vektorit  $\mathbf{x}$  ja  $\mathbf{y}$  ovat *ortogonaalit* eli *kohtisuorat* jos  $(\mathbf{x}, \mathbf{y}) = 0$ .

## Määritelmä

Vektorijoukko  $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$  on *ortogonaali*, jos  $(\mathbf{x}_i, \mathbf{x}_j) = 0$  aina kun  $i \neq j$ . Ortogonaali joukko  $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$  on *ortonormaali*, jos lisäksi  $(\mathbf{x}_i, \mathbf{x}_i) = 1$ .

## Huomautus

- Jokaisesta ortogonaalista joukosta joka ei sisällä nollavektoria voidaan helposti saada ortonormaali kertomalla kukin  $\mathbf{x}_i$  norminsa käänteisluvulla  $\|\mathbf{x}_i\|^{-1}$ .

## Huomautus

- Jokaisesta ortogonaalista joukosta joka ei sisällä nollavektoria voidaan helposti saada ortonormaali kertomalla kukin  $\mathbf{x}_i$  norminsa käänteisluvulla  $\|\mathbf{x}_i\|^{-1}$ .
- $\mathbb{R}^n$ :n luonnollinen kanta  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  on ortonormaali kun sisätuloksi valitaan tavallinen pistetulo.

## Huomautus

- Jokaisesta ortogonaalista joukosta joka ei sisällä nollavektoria voidaan helposti saada ortonormaali kertomalla kukin  $\mathbf{x}_i$  norminsa käänteisluvulla  $\|\mathbf{x}_i\|^{-1}$ .
- $\mathbb{R}^n$ :n luonnollinen kanta  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  on ortonormaali kun sisätuloksi valitaan tavallinen pistetulo.

## Lause

Olkkoon  $V$  vektoriavaruus ja  $A = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$  joukko, joka ei sisällä nollavektoria ja on ortogonaali jonkin sisätulon  $(\mathbf{x}, \mathbf{y})$  suhteen. Tällöin  $A$  on lineaarisesti riippumaton.

## Koordinaattivektorin etsiminen

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on jokin kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

## Koordinaattivektorin etsiminen

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on jokin kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

## Koordinaattivektorin etsiminen

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on jokin kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

Koordinaattivektori  $(x_1, \dots, x_n)$  voidaan löytää Gaussin-Jordanin prosessilla (Yleensä työläs prosessi)

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

Koordinaattivektori  $(x_1, \dots, x_n)$  voidaan löytää laskemalla sisätulo  $(\mathbf{x}, \mathbf{b}_i)$ , jolloin

$$(\mathbf{x}, \mathbf{b}_i) = x_1(\mathbf{b}_1, \mathbf{b}_i) + \dots + x_i(\mathbf{b}_i, \mathbf{b}_i) + \dots + x_n(\mathbf{b}_n, \mathbf{b}_i)$$

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

Koordinaattivektori  $(x_1, \dots, x_n)$  voidaan löytää laskemalla sisätulo  $(\mathbf{x}, \mathbf{b}_i)$ , jolloin

$$\begin{aligned} (\mathbf{x}, \mathbf{b}_i) &= x_1(\mathbf{b}_1, \mathbf{b}_i) + \dots + x_i(\mathbf{b}_i, \mathbf{b}_i) + \dots + x_n(\mathbf{b}_n, \mathbf{b}_i) \\ &= x_i(\mathbf{b}_i, \mathbf{b}_i) \end{aligned}$$

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

Koordinaattivektori  $(x_1, \dots, x_n)$  voidaan löytää laskemalla sisätulo  $(\mathbf{x}, \mathbf{b}_i)$ , jolloin

$$\begin{aligned}(\mathbf{x}, \mathbf{b}_i) &= x_1(\mathbf{b}_1, \mathbf{b}_i) + \dots + x_i(\mathbf{b}_i, \mathbf{b}_i) + \dots + x_n(\mathbf{b}_n, \mathbf{b}_i) \\ &= x_i(\mathbf{b}_i, \mathbf{b}_i) = x_i \|\mathbf{b}_i\|^2,\end{aligned}$$

## Koordinaattivektorin etsiminen, Ortonormaali kanta

Jos  $B_1 = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$  on ortonormaali kanta, on jokaiselle  $\mathbf{x} \in \mathbb{R}^n$  olemassa kantaesitys:

$$\mathbf{x} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n,$$

ja vektoria  $(x_1, \dots, x_n)$  kutsutaan vektorin  $\mathbf{x}$  koordinaattivektoriksi kannan  $B_1$  suhteen.

Koordinaattivektori  $(x_1, \dots, x_n)$  voidaan löytää laskemalla sisätulo  $(\mathbf{x}, \mathbf{b}_i)$ , jolloin

$$\begin{aligned}(\mathbf{x}, \mathbf{b}_i) &= x_1(\mathbf{b}_1, \mathbf{b}_i) + \dots + x_i(\mathbf{b}_i, \mathbf{b}_i) + \dots + x_n(\mathbf{b}_n, \mathbf{b}_i) \\ &= x_i(\mathbf{b}_i, \mathbf{b}_i) = x_i \|\mathbf{b}_i\|^2,\end{aligned}$$

siis

$$x_i = \frac{(\mathbf{x}, \mathbf{b}_i)}{\|\mathbf{b}_i\|^2}$$

## Määritelmä

Olkoot  $\mathbf{x}$  ja  $\mathbf{y} \neq \mathbf{0}$  avaruuden  $\mathbb{R}^n$  vektoreita. Tällöin *vektorin  $\mathbf{x}$  projektio vektorilla  $\mathbf{y}$*  tarkoittaa sitä origon ja pisteen  $\mathbf{y}$  kautta kulkevan suoran  $L(\mathbf{y})$  pistettä  $\mathbf{x}'$ , jolle  $\mathbf{x} - \mathbf{x}'$  on kohtisuorassa vektoria  $\mathbf{y}$  vastaan.

## Määritelmä

Lineaarikuvaus  $f : V \rightarrow V$  säilyttää etäisyyden, jos  $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$  aina, kun  $\mathbf{x}, \mathbf{y} \in V$ .

## Määritelmä

Lineaarikuvaus  $f : V \rightarrow V$  säilyttää etäisyyden, jos  $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$  aina, kun  $\mathbf{x}, \mathbf{y} \in V$ . Kuvaus  $f$  säilyttää normin, jos  $\|f(\mathbf{x})\| = \|\mathbf{x}\|$ .

## Määritelmä

Lineaarikuvaus  $f : V \rightarrow V$  säilyttää etäisyyden, jos  $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$  aina, kun  $\mathbf{x}, \mathbf{y} \in V$ . Kuvaus  $f$  säilyttää normin, jos  $\|f(\mathbf{x})\| = \|\mathbf{x}\|$ . Kuvaus  $f$  säilyttää sisätulon, jos  $(f(\mathbf{x}), f(\mathbf{y})) = (\mathbf{x}, \mathbf{y})$ .

## Määritelmä

Lineaarikuvaus  $f : V \rightarrow V$  säilyttää etäisyyden, jos  $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$  aina, kun  $\mathbf{x}, \mathbf{y} \in V$ . Kuvaus  $f$  säilyttää normin, jos  $\|f(\mathbf{x})\| = \|\mathbf{x}\|$ . Kuvaus  $f$  säilyttää sisätulon, jos  $(f(\mathbf{x}), f(\mathbf{y})) = (\mathbf{x}, \mathbf{y})$ .

## Lause

Olcoon etäisyys normin ja tämä puolestaan sisätulon indusoima. Jos lineaarikuvaus  $f : V \rightarrow V$  säilyttää sisätulon, säilyttää se myös normin ja etäisyyden.

# Etäisyyden säilyttävät kuvaukset

## Määritelmä

Matriisi  $A$  on ortogonaali, jos  $A^T = A^{-1}$ , siis  $A^T A = A A^T = I$ .

# Etäisyyden säilyttävät kuvaukset

## Määritelmä

Matriisi  $A$  on ortogonaali, jos  $A^T = A^{-1}$ , siis  $A^T A = A A^T = I$ .

## Lause

Jos lineaarikuvauksen  $f : V \rightarrow V$  matriisi  $A_f$  on ortogonaali, niin kuvaus  $f$  säilyttää pistetulon (ja siis myös tämän indusoiman normin ja etäisyyden)

# Etäisyyden säilyttävät kuvaukset

## Määritelmä

Matriisi  $A$  on ortogonaali, jos  $A^T = A^{-1}$ , siis  $A^T A = A A^T = I$ .

## Lause

Jos lineaarikuvauksen  $f : V \rightarrow V$  matriisi  $A_f$  on ortogonaali, niin kuvaus  $f$  säilyttää pistetulon (ja siis myös tämän indusoiman normin ja etäisyyden)

## Määritelmä

Matriisin  $A$  *adjugaatti* määritellään  $A^* = \overline{A}^T$ . Matriisi  $A$  on *unitaarinen*, jos  $A^* = A^{-1}$ , siis  $A^* A = A A^* = I$ .

# Etäisyyden säilyttävät kuvaukset

## Määritelmä

Matriisi  $A$  on ortogonaali, jos  $A^T = A^{-1}$ , siis  $A^T A = A A^T = I$ .

## Lause

Jos lineaarikuvauksen  $f : V \rightarrow V$  matriisi  $A_f$  on ortogonaali, niin kuvaus  $f$  säilyttää pistetulon (ja siis myös tämän indusoiman normin ja etäisyyden)

## Määritelmä

Matriisin  $A$  *adjugaatti* määritellään  $A^* = \overline{A}^T$ . Matriisi  $A$  on *unitaarinen*, jos  $A^* = A^{-1}$ , siis  $A^* A = A A^* = I$ .

## Lause

Jos lineaarikuvauksen  $f : V \rightarrow V$  matriisi  $A_f$  on unitaarinen, niin  $f$  säilyttää Hermiten pistetulon (ja siis myös sen indusoiman normin ja etäisyyden)

# Vektoriavaruuksien geometriaa

## Kulma avaruudessa $\mathbb{R}^n$

Vektoreiden  $\mathbf{x}$  ja  $\mathbf{y} \in \mathbb{R}^n$  välinen *kulma* tarkoittaa kulmaa  $\theta \in [0, \pi]$ , joka muodostuu origosta (pisteestä  $\mathbf{0}$ ) pisteeseen  $\mathbf{x}$  ja origosta pisteeseen  $\mathbf{y}$  kulkevien janojen välille.

# Vektoriavaruuksien geometriaa

## Kulma avaruudessa $\mathbb{R}^n$

Vektoreiden  $\mathbf{x}$  ja  $\mathbf{y} \in \mathbb{R}^n$  välinen *kulma* tarkoittaa kulmaa  $\theta \in [0, \pi]$ , joka muodostuu origosta (pisteestä  $\mathbf{0}$ ) pisteeseen  $\mathbf{x}$  ja origosta pisteeseen  $\mathbf{y}$  kulkevien janojen välille.

Huomaa, että kolme pistettä  $\mathbf{x}$ ,  $\mathbf{y}$  ja  $\mathbf{0}$  kuuluvat aina samalle tasolle, joten vektoreiden välinen kulma on aina *tason* ominaisuus.

# Vektoriavaruuksien geometriaa

## Kulma avaruudessa $\mathbb{R}^n$

Vektoreiden  $\mathbf{x}$  ja  $\mathbf{y} \in \mathbb{R}^n$  välinen *kulma* tarkoittaa kulmaa  $\theta \in [0, \pi]$ , joka muodostuu origosta (pisteestä  $\mathbf{0}$ ) pisteeseen  $\mathbf{x}$  ja origosta pisteeseen  $\mathbf{y}$  kulkevien janojen välille.

Huomaa, että kolme pistettä  $\mathbf{x}$ ,  $\mathbf{y}$  ja  $\mathbf{0}$  kuuluvat aina samalle tasolle, joten vektoreiden välinen kulma on aina *tason* ominaisuus.

## Määritelmä

Jos  $\theta$  on vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  välinen kulma, niin

$$\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\| \cdot \|\mathbf{y}\| \cos \theta.$$

# Vektoriavaruuksien geometriaa

## Kulma avaruudessa $\mathbb{R}^n$

Vektoreiden  $\mathbf{x}$  ja  $\mathbf{y} \in \mathbb{R}^n$  välinen *kulma* tarkoittaa kulmaa  $\theta \in [0, \pi]$ , joka muodostuu origosta (pisteestä  $\mathbf{0}$ ) pisteeseen  $\mathbf{x}$  ja origosta pisteeseen  $\mathbf{y}$  kulkevien janojen välille.

Huomaa, että kolme pistettä  $\mathbf{x}$ ,  $\mathbf{y}$  ja  $\mathbf{0}$  kuuluvat aina samalle tasolle, joten vektoreiden välinen kulma on aina *tason* ominaisuus.

## Määritelmä

Jos  $\theta$  on vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  välinen kulma, niin

$$\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\| \cdot \|\mathbf{y}\| \cos \theta.$$

## Huomautus

Jos kumpikaan  $\mathbf{x}$  tai  $\mathbf{y}$  ei ole nollavektori, on

$$\cos \theta = \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|}$$



## Esimerkki

- "Pysäyttäkää auto JBN-372"

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"
- Redundantti informaatio parantaa luotettavuutta

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"
- Redundantti informaatio parantaa luotettavuutta

## Tiedonsiirto

- Sähkömagneettinen säteily

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"
- Redundantti informaatio parantaa luotettavuutta

## Tiedonsiirto

- Sähkömagneettinen säteily
- Ääniaallot

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"
- Redundantti informaatio parantaa luotettavuutta

## Tiedonsiirto

- Sähkömagneettinen säteily
- Ääniaallot
- Analoginen ↔ digitaalinen

## Esimerkki

- "Pysäyttäkää auto JBN-372"
- "Pysäyttäkää auto IPM-372"
- JBN → "Jaakko – Bertta – Niilo"
- IPM → "Ilmari – Pekka – Mika"
- Redundantti informaatio parantaa luotettavuutta

## Tiedonsiirto

- Sähkömagneettinen säteily
- Ääniaallot
- Analoginen ↔ digitaalinen
- Digitaalisessa muodossa informaation suojaaminen virheiltä on helpompaa.

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$
- 74 minuuttia vaatii  $74 \cdot 60 \cdot 172,266 \text{ KB} \approx 746 \text{ MB}$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$
- 74 minuuttia vaatii  $74 \cdot 60 \cdot 172,266 \text{ KB} \approx 746 \text{ MB}$

## 4K kuvaformaatti

- $3840 \times 2160 = 8294400 \text{ pikseliä}$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$
- 74 minuuttia vaatii  $74 \cdot 60 \cdot 172,266 \text{ KB} \approx 746 \text{ MB}$

## 4K kuvaformaatti

- $3840 \times 2160 = 8294400$  pikseliä
- Joka pikseliä varten RGB-komponentit vaativat  $3 \cdot 8 = 24$  bittiä.

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$
- 74 minuuttia vaatii  $74 \cdot 60 \cdot 172,266 \text{ KB} \approx 746 \text{ MB}$

## 4K kuvaformaatti

- $3840 \times 2160 = 8294400$  pikseliä
- Joka pikseliä varten RGB-komponentit vaativat  $3 \cdot 8 = 24$  bittiä.
- Yhteensä  $24 \cdot 8294400 \text{ bit} \approx 23 \text{ MB}$

## Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200 \text{ bit/s} = 172,266 \text{ KB/s}$
- 5 minuuttia vaatii  $5 \cdot 60 \cdot 172,266 \text{ KB} \approx 50 \text{ MB}$
- 74 minuuttia vaatii  $74 \cdot 60 \cdot 172,266 \text{ KB} \approx 746 \text{ MB}$

## 4K kuvaformaatti

- $3840 \times 2160 = 8294400$  pikseliä
- Joka pikseliä varten RGB-komponentit vaativat  $3 \cdot 8 = 24$  bittiä.
- Yhteensä  $24 \cdot 8294400 \text{ bit} \approx 23 \text{ MB}$
- 25 kuvaa sekunnissa vaatii n.  $593 \text{ MB/s}$

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.

Laajempia symbolijoukkoja voidaan esittää bittijonoilla.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.

Laajempia symbolijoukkoja voidaan esittää bittijonoilla.

Esimerkiksi kahden bitin jonoilla voidaan esittää neljä erilaista symbolia: 00, 01, 10, ja 11.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.

Laajempia symbolijoukkoja voidaan esittää bittijonoilla.

Esimerkiksi kahden bitin jonoilla voidaan esittää neljä erilaista symbolia: 00, 01, 10, ja 11.

## Digitaalinen tiedonsiirto

Monenlaiset häiriötekijät voivat aiheuttaa virheitä tiedonsiirtoon, jolloin digitaalinen viesti 1110100111010111 voi muuntua esim. muotoon 1110100111010101.

## Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.

Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.

Laajempia symbolijoukkoja voidaan esittää bittijonoilla.

Esimerkiksi kahden bitin jonoilla voidaan esittää neljä erilaista symbolia: 00, 01, 10, ja 11.

## Digitaalinen tiedonsiirto

Monenlaiset häiriötekijät voivat aiheuttaa virheitä tiedonsiirtoon, jolloin digitaalinen viesti 1110100111010111 voi muuntua esim. muotoon 1110100111010101. Virheellinen viesti pitäisi voida tunnistaa ja siitä pitäisi voida päätellä alkuperäinen.

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen.

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ .

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ . Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

# Virheitä korjaavat koodit

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ . Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

## Esimerkki: Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ , jolloin esimerkiksi

$01001 \mapsto 000111000000111$ .

# Virheitä korjaavat koodit

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ . Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

## Esimerkki: Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ , jolloin esimerkiksi

$$01001 \mapsto 000111000000111.$$

Tällöin yksi virhe muuntaa viestin esim. muotoon

$$000111000000101,$$

# Virheitä korjaavat koodit

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ . Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

## Esimerkki: Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ , jolloin esimerkiksi

$$01001 \mapsto 000111000000111.$$

Tällöin yksi virhe muuntaa viestin esim. muotoon

$$000111000000101,$$

joka voidaan dekodata viestiksi  $000111000000111$

# Virheitä korjaavat koodit

## Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi  $0010100 \mapsto 00101000$  ja  $0101100 \mapsto 01011001$ . Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

## Esimerkki: Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ , jolloin esimerkiksi

$$01001 \mapsto 000111000000111.$$

Tällöin yksi virhe muuntaa viestin esim. muotoon

$$000111000000101,$$

joka voidaan dekodata viestiksi  $000111000000111 \rightarrow 01001$ .

## Toistokoodi

$0 \rightarrow 000, 1 \rightarrow 111.$

## Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ . Hintana kolminkertainen lähetysaika,

## Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ . Hintana kolminkertainen lähetysaika, 1 virhe  
korjattavissa / 3-pituinen lohko

## Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ . Hintana kolminkertainen lähetysaika, 1 virhe korjattavissa / 3-pituinen lohko

## Esimerkki

Koodaus  $00 \mapsto 00000$   $01 \mapsto 00111$ ,  $10 \mapsto 11100$ ,  $11 \mapsto 11011$ .

# Virheitä korjaavat koodit

## Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ . Hintana kolminkertainen lähetysaika, 1 virhe korjattavissa / 3-pituinen lohko

## Esimerkki

Koodaus  $00 \mapsto 00000$   $01 \mapsto 00111$ ,  $10 \mapsto 11100$ ,  $11 \mapsto 11011$ .  
hintana 2,5-kertainen lähetysaika,

## Toistokoodi

$0 \rightarrow 000$ ,  $1 \rightarrow 111$ . Hintana kolminkertainen lähetysaika, 1 virhe korjattavissa / 3-pituinen lohko

## Esimerkki

Koodaus  $00 \mapsto 00000$   $01 \mapsto 00111$ ,  $10 \mapsto 11100$ ,  $11 \mapsto 11011$ .  
hintana 2,5-kertainen lähetysaika, 1 virhe korjattavissa / 5-pituinen lohko.

## Määritelmä

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$  on kahden alkion kunta.

## Määritelmä

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$  on kahden alkion kunta.
- $\bar{0} = 0 + 2\mathbb{Z}, \bar{1} = 1 + 2\mathbb{Z}$ .

## Määritelmä

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$  on kahden alkion kunta.
- $\bar{0} = 0 + 2\mathbb{Z}$ ,  $\bar{1} = 1 + 2\mathbb{Z}$ .
- Esim.  $\bar{0} + \bar{1} = \bar{1}$ ,  $\bar{1} + \bar{1} = \bar{0}$

## Määritelmä

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$  on kahden alkion kunta.
- $\bar{0} = 0 + 2\mathbb{Z}$ ,  $\bar{1} = 1 + 2\mathbb{Z}$ .
- Esim.  $\bar{0} + \bar{1} = \bar{1}$ ,  $\bar{1} + \bar{1} = \bar{0}$
- Jätetään yläviivat pois ja merkitään  $\mathbb{F}_2 = \{0, 1\}$ , missä  $1 + 1 = 0$ .

## Määritelmä

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$  on kahden alkion kunta.
- $\bar{0} = 0 + 2\mathbb{Z}$ ,  $\bar{1} = 1 + 2\mathbb{Z}$ .
- Esim.  $\bar{0} + \bar{1} = \bar{1}$ ,  $\bar{1} + \bar{1} = \bar{0}$
- Jätetään yläviivat pois ja merkitään  $\mathbb{F}_2 = \{0, 1\}$ , missä  $1 + 1 = 0$ .
- $n$ -ulotteinen vektoriavaruus  $\mathbb{F}_2^n$  yli kunnan  $\mathbb{F}_2$  koostuu  $n$ -pituisista järjestetyistä kunnan  $\mathbb{F}_2$  jonoista (bittijonoista):  
 $\mathbb{F}_2^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{F}_2\}$ , jossa yhteenlasku ja skalaarikertolasku on määritelty kuten reaalisessa.

## Määritelmä

Vektoreiden  $\mathbf{x} = (x_1, \dots, x_n)$  ja  $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_2^n$

*Hamming*-etäisyys on

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|$$

## Määritelmä

Vektoreiden  $\mathbf{x} = (x_1, \dots, x_n)$  ja  $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_2^n$

*Hamming*-etäisyys on

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|$$

Vektorin  $\mathbf{x}$  Hamming-paino määritellään  $w_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$ .

## Määritelmä

Vektoreiden  $\mathbf{x} = (x_1, \dots, x_n)$  ja  $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_2^n$

*Hamming*-etäisyys on

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|$$

Vektorin  $\mathbf{x}$  Hamming-paino määritellään  $w_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$ .

## Esimerkki

$$d_H(00000, 00111) = 3, d_H(00000, 11100) = 3,$$

$$d_H(00111, 11100) = 4, d_H(11100, 11011) = 3$$

$$d_H(00111, 11011) = 3 \text{ ja } d_H(00000, 11011) = 4$$

## Huomautus

- Hamming-etäisyys toteuttaa metriikan aksioomat

## Huomautus

- Hamming-etäisyys toteuttaa metriikan aksioomat
- $\mathbf{e}_i = (0, \dots, 1, \dots, 0)$

## Huomautus

- Hamming-etäisyys toteuttaa metriikan aksioomat
- $\mathbf{e}_i = (0, \dots, 1, \dots, 0)$
- Jos  $d_H(\mathbf{x}, \mathbf{y}) \geq 3$  on  $\mathbf{x}' = \mathbf{x} + \mathbf{e}_i$  edelleen lähempänä vektoria  $\mathbf{x}$  kuin vektoria  $\mathbf{y}$ , joten virhe  $\mathbf{x} \mapsto \mathbf{x}' = \mathbf{x} + \mathbf{e}_i$  voidaan korjata dekoodaamalla  $\mathbf{x}'$  vektoriksi  $\mathbf{x}$ .

## Huomautus

- Hamming-etäisyys toteuttaa metriikan aksioomat
- $\mathbf{e}_i = (0, \dots, 1, \dots, 0)$
- Jos  $d_H(\mathbf{x}, \mathbf{y}) \geq 3$  on  $\mathbf{x}' = \mathbf{x} + \mathbf{e}_i$  edelleen lähempänä vektoria  $\mathbf{x}$  kuin vektoria  $\mathbf{y}$ , joten virhe  $\mathbf{x} \mapsto \mathbf{x}' = \mathbf{x} + \mathbf{e}_i$  voidaan korjata dekodeamalla  $\mathbf{x}'$  vektoriksi  $\mathbf{x}$ .
- Yleistys: Jos  $d_H(\mathbf{x}, \mathbf{y}) \geq 2t + 1$ , voidaan  $t$ :n virheen jälkeen saatu  $\mathbf{x}'$  palauttaa vektoriksi  $\mathbf{x}$ , sillä  $\mathbf{y}$  on silti vielä kauempana.

# Virheitä korjaavat koodit

## Määritelmä

$C \subset \mathbb{F}_2^n$  on  $t$  virhettä korjaava koodi, jos  $d_h(\mathbf{x}, \mathbf{y}) \geq 2t + 1$  aina kun  $\mathbf{x} \neq \mathbf{y} \in C$ .

# Virheitä korjaavat koodit

## Määritelmä

$C \subset \mathbb{F}_2^n$  on  $t$  virhettä korjaava koodi, jos  $d_h(\mathbf{x}, \mathbf{y}) \geq 2t + 1$  aina kun  $\mathbf{x} \neq \mathbf{y} \in C$ .

## Periaate

Viestit  $\mathbf{x} \in \mathbb{F}_2^m$  (pituus  $m$ ) koodataan *koodisanoiksi* (pituus  $n > m$ ), jotka ovat etäällä toisistaan.

# Virheitä korjaavat koodit

## Määritelmä

$C \subset \mathbb{F}_2^n$  on  $t$  virhettä korjaava koodi, jos  $d_h(\mathbf{x}, \mathbf{y}) \geq 2t + 1$  aina kun  $\mathbf{x} \neq \mathbf{y} \in C$ .

## Periaate

Viestit  $\mathbf{x} \in \mathbb{F}_2^m$  (pituus  $m$ ) koodataan *koodisanoiksi* (pituus  $n > m$ ), jotka ovat etäällä toisistaan. Mikäli tiedonsiirtokanava aiheuttaa virheitä koodisanoissa, on toivottavaa että muuttuneet viestit yhä muistuttaisivat eniten lähetettyjä koodisanoja ja voitaisiin täten dekoddata.

# Virheitä korjaavat koodit

## Määritelmä

$C \subset \mathbb{F}_2^n$  on  $t$  virhettä korjaava koodi, jos  $d_h(\mathbf{x}, \mathbf{y}) \geq 2t + 1$  aina kun  $\mathbf{x} \neq \mathbf{y} \in C$ .

## Periaate

Viestit  $\mathbf{x} \in \mathbb{F}_2^m$  (pituus  $m$ ) koodataan *koodisanoiksi* (pituus  $n > m$ ), jotka ovat etäällä toisistaan. Mikäli tiedonsiirtokanava aiheuttaa virheitä koodisanoissa, on toivottavaa että muuttuneet viestit yhä muistuttaisivat eniten lähetettyjä koodisanoja ja voitaisiin täten dekoddata.

## Määritelmä

Koodia  $C$  sanotaan  $(n, M, d)$ -koodiksi, jos koodisanojen pituus on  $n$ ,  $|C| = M$ , ja erisuurten koodisanojen Hamming-etäisyys on vähintään  $d$ .

## Periaate

Kuvataan lyhyemmät jonot (pituus  $m$ ) bijektiivisesti pidemmiksi jonoiksi (pituus  $n$ ),

$$\mathbb{F}_2^m \rightarrow C \subset \mathbb{F}_2^n$$

siten että kaikkien  $\mathbf{x} \neq \mathbf{y} \in C$  Hamming-etäisyys on ainakin  $2t + 1$ .

## Periaate

Kuvataan lyhyemmät jonot (pituus  $m$ ) bijektiivisesti pidemmiksi jonoiksi (pituus  $n$ ),

$$\mathbb{F}_2^m \rightarrow C \subset \mathbb{F}_2^n$$

siten että kaikkien  $\mathbf{x} \neq \mathbf{y} \in C$  Hamming-etäisyys on ainakin  $2t + 1$ . Mikäli kuvavektorin lähetys tiedonsiirtokanavassa  $\mathbf{x} \mapsto \mathbf{x}' \notin C$  tuottaa korkeintaan  $t$  virhettä, voidaan alkuperäinen vektori  $\mathbf{x}$  saada yksikäsitteisesti lähimpänä Hamming-etäisyyden vektorina jolle  $\mathbf{x} \in C$ .

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .
- Miten laskea koodaus  $\mathbb{F}_2^m \rightarrow C$  tehokkaasti?

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .
- Miten laskea koodaus  $\mathbb{F}_2^m \rightarrow C$  tehokkaasti?
- Miten laskea dekkoodaus  $\mathbb{F}_2^n \rightarrow C$  tehokkaasti?

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .
- Miten laskea koodaus  $\mathbb{F}_2^m \rightarrow C$  tehokkaasti?
- Miten laskea dekkoodaus  $\mathbb{F}_2^n \rightarrow C$  tehokkaasti?
- Miten laskea kuvaus  $C \rightarrow \mathbb{F}_2^m$  tehokkaasti?

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .
- Miten laskea koodaus  $\mathbb{F}_2^m \rightarrow C$  tehokkaasti?
- Miten laskea dekodaus  $\mathbb{F}_2^n \rightarrow C$  tehokkaasti?
- Miten laskea kuvaus  $C \rightarrow \mathbb{F}_2^m$  tehokkaasti?

## Ongelmia

- Monissa sovelluksissa dekodaus  $\mathbb{F}_2^n \rightarrow C$  on hankalinta toteuttaa tehokkaasti.

## Ongelmia

- Miten valita *koodisanojen* joukko  $C \subseteq \mathbb{F}_2^n$  siten että  $d_H(\mathbf{x}, \mathbf{y})$  olisi suuri aina kun  $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^m$ .
- Miten laskea koodaus  $\mathbb{F}_2^m \rightarrow C$  tehokkaasti?
- Miten laskea dekodaus  $\mathbb{F}_2^n \rightarrow C$  tehokkaasti?
- Miten laskea kuvaus  $C \rightarrow \mathbb{F}_2^m$  tehokkaasti?

## Ongelmia

- Monissa sovelluksissa dekodaus  $\mathbb{F}_2^n \rightarrow C$  on hankalinta toteuttaa tehokkaasti.
- Osoittautuu, että informaatio suhde paranee lohkon pituutta kasvatettaessa, mutta laskennalliset ongelmat kasvavat myös.

# Virheitä korjaavat koodit

## Esimerkki: Taulukointi

Koodi: {00000, 00111, 11100, 11011}, dekooodaus

00000 → 00000

00001 → 00000

00010 → 00000

00011 → 00111

...

01001 → 00000 tai 11011

...

11110 → 11100

11111 → 11011

# Virheitä korjaavat koodit

## Esimerkki: Taulukointi

Koodi: {00000, 00111, 11100, 11011}, dekooodaus

00000 → 00000

00001 → 00000

00010 → 00000

00011 → 00111

...

01001 → 00000 tai 11011

...

11110 → 11100

11111 → 11011

Bittijonon pituuden ollessa  $n \geq 30$  on taulukoinnin mahdollisuus suljettu käytännössä pois:  $2^{30} = 1\,073\,741\,824$

## Määritelmä

Koodi  $C \in \mathbb{F}_2^n$  on *lineaarinen*, jos  $C \subseteq \mathbb{F}_2^n$  on aliavaruus.

## Määritelmä

Koodi  $C \subseteq \mathbb{F}_2^n$  on *lineaarinen*, jos  $C \subseteq \mathbb{F}_2^n$  on aliavaruus. Tällöin  $\alpha \mathbf{x} + \beta \mathbf{y} \in C$  aina, kun  $\mathbf{x}, \mathbf{y} \in C$  ja  $\alpha, \beta \in \mathbb{F}_2 = \{0, 1\}$ .

## Määritelmä

Koodi  $C \in \mathbb{F}_2^n$  on *lineaarinen*, jos  $C \subseteq \mathbb{F}_2^n$  on aliavaruus. Tällöin  $\alpha \mathbf{x} + \beta \mathbf{y} \in C$  aina, kun  $\mathbf{x}, \mathbf{y} \in C$  ja  $\alpha, \beta \in \mathbb{F}_2 = \{0, 1\}$ .

## Huomautus

Jos  $C$  on avaruuden  $\mathbb{F}_2^n$   $m$ -ulotteinen aliavaruus ( $m < n$ ), on sillä kanta  $\{\mathbf{c}_1, \dots, \mathbf{c}_m\} \subset \mathbb{F}_2^n$  ja jokainen  $\mathbf{c} \in C$  voidaan esittää yksikäsitteisesti muodossa

$$\mathbf{c} = x_1 \mathbf{c}_1 + \dots + x_m \mathbf{c}_m = (x_1, \dots, x_m) \begin{pmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_m \end{pmatrix} = (x_1, \dots, x_m) G.$$

## Määritelmä

Koodi  $C \in \mathbb{F}_2^n$  on *lineaarinen*, jos  $C \subseteq \mathbb{F}_2^n$  on aliavaruus. Tällöin  $\alpha \mathbf{x} + \beta \mathbf{y} \in C$  aina, kun  $\mathbf{x}, \mathbf{y} \in C$  ja  $\alpha, \beta \in \mathbb{F}_2 = \{0, 1\}$ .

## Huomautus

Jos  $C$  on avaruuden  $\mathbb{F}_2^n$   $m$ -ulotteinen aliavaruus ( $m < n$ ), on sillä kanta  $\{\mathbf{c}_1, \dots, \mathbf{c}_m\} \subset \mathbb{F}_2^n$  ja jokainen  $\mathbf{c} \in C$  voidaan esittää yksikäsitteisesti muodossa

$$\mathbf{c} = x_1 \mathbf{c}_1 + \dots + x_m \mathbf{c}_m = (x_1, \dots, x_m) \begin{pmatrix} \mathbf{c}_1 \\ \dots \\ \mathbf{c}_m \end{pmatrix} = (x_1, \dots, x_m) G.$$

Matriisia  $G = \begin{pmatrix} \mathbf{c}_1 \\ \dots \\ \mathbf{c}_m \end{pmatrix}$  kutsutaan koodin *generoijamatriisiksi*.

## Huomautus

Lineaarisen koodin *koodausfunktio*  $\mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$  voidaan esittää matriisikertolaskuna

$$\mathbf{c} = \mathbf{x}G,$$

missä  $\mathbf{x} \in \mathbb{F}_2^m$  on lähetettävä viesti (esitetään rivivektorina),  $G$  on  $m \times n$ -matriisi yli kunnan  $\mathbb{F}_2$ , ja  $\mathbf{c} \in C \subset \mathbb{F}_2^n$  on koodattu viesti.

## Huomautus

Lineaarisen koodin *koodausfunktio*  $\mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$  voidaan esittää matriisikertolaskuna

$$\mathbf{c} = \mathbf{x}G,$$

missä  $\mathbf{x} \in \mathbb{F}_2^m$  on lähetettävä viesti (esitetään rivivektorina),  $G$  on  $m \times n$ -matriisi yli kunnan  $\mathbb{F}_2$ , ja  $\mathbf{c} \in C \subset \mathbb{F}_2^n$  on koodattu viesti. Tällöin kyseessä on  $(n, 2^m, d)$ -koodi, jossa minimietäisyys  $d$  riippuu generoijamatriisin ominaisuuksista.

## Huomautus

Lineaarisen koodin *koodausfunktio*  $\mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$  voidaan esittää matriisikertolaskuna

$$\mathbf{c} = \mathbf{x}G,$$

missä  $\mathbf{x} \in \mathbb{F}_2^m$  on lähetettävä viesti (esitetään rivivektorina),  $G$  on  $m \times n$ -matriisi yli kunnan  $\mathbb{F}_2$ , ja  $\mathbf{c} \in C \subset \mathbb{F}_2^n$  on koodattu viesti. Tällöin kyseessä on  $(n, 2^m, d)$ -koodi, jossa minimietäisyys  $d$  riippuu generoijamatriisin ominaisuuksista.

## Määritelmä

Lineaarikoodia, jonka pituus on  $n$  ja dimensio  $m$  ja minimietäisyys  $d$ , sanotaan  $[n, m, d]$ -koodiksi. Jos minimietäisyyttä ei ilmoiteta, sanotaan koodia  $[n, m]$ -koodiksi.

## Lause

Jos  $C \subseteq \mathbb{F}_2^n$ , on  $[n, m]$ -koodi, on olemassa sellainen  $(n - m) \times n$ -matriisi  $H$ , että

$$C = \{\mathbf{x} \in \mathbb{F}_2^n \mid H\mathbf{x}^T = 0\}.$$

Matriisia  $H$  kutsutaan koodin  $C$  tarkistusmatriisiksi.

## Lause

Jos  $C \subseteq \mathbb{F}_2^n$ , on  $[n, m]$ -koodi, on olemassa sellainen  $(n - m) \times n$ -matriisi  $H$ , että

$$C = \{\mathbf{x} \in \mathbb{F}_2^n \mid H\mathbf{x}^T = 0\}.$$

Matriisia  $H$  kutsutaan koodin  $C$  tarkistusmatriisiksi. Jos  $G$  on koodin generoijamatriisi, on  $GH^T = O$  nollamatriisi.

## Lause

Jos  $C \subseteq \mathbb{F}_2^n$ , on  $[n, m]$ -koodi, on olemassa sellainen  $(n - m) \times n$ -matriisi  $H$ , että

$$C = \{\mathbf{x} \in \mathbb{F}_2^n \mid H\mathbf{x}^T = 0\}.$$

Matriisia  $H$  kutsutaan koodin  $C$  tarkistusmatriisiksi. Jos  $G$  on koodin generoijamatriisi, on  $GH^T = O$  nollamatriisi.

## Huomautus

Tarkistusmatriisi voidaan muodostaa generoijamatriisista ja päinvastoin.

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Lineaariset koodit

Jos  $\mathbf{c} \in C$  ja  $\mathbf{x} = \mathbf{c} + \mathbf{e}$  on "virheellinen", on kuitenkin  $H\mathbf{x}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$ .

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Lineaariset koodit

Jos  $\mathbf{c} \in C$  ja  $\mathbf{x} = \mathbf{c} + \mathbf{e}$  on "virheellinen", on kuitenkin  $H\mathbf{x}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$ . Virheenkorjaus perustuu vektoreihin  $H\mathbf{e}^T$ .

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Lineaariset koodit

Jos  $\mathbf{c} \in C$  ja  $\mathbf{x} = \mathbf{c} + \mathbf{e}$  on "virheellinen", on kuitenkin  $H\mathbf{x}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$ . Virheenkorjaus perustuu vektoreihin  $H\mathbf{e}^T$ . näitä kutsutaan *syndromeiksi*.

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Lineaariset koodit

Jos  $\mathbf{c} \in C$  ja  $\mathbf{x} = \mathbf{c} + \mathbf{e}$  on "virheellinen", on kuitenkin  $H\mathbf{x}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$ . Virheenkorjaus perustuu vektoreihin  $H\mathbf{e}^T$ . näitä kutsutaan *syndromeiksi*.  
Ns. Syndromipankki muodostetaan tallentamalla muistiin Hamming-painon suhteen kaikkein kevyimmät syndromin tuottavat vektorit  $\mathbf{x} \in \mathbb{F}_2^n$ .

## Syndromit

- Jos  $\mathbf{x} \in \mathbb{F}_2^n$  toteuttaa  $H\mathbf{x}^T = \mathbf{0}$ , on  $\mathbf{x} \in C$  koodisana, eikä virhettä tulkita tapahtuneen.
- $H\mathbf{x}^T \neq \mathbf{0}$ , tulkitaan virhe tapahtuneeksi.

## Lineaariset koodit

Jos  $\mathbf{c} \in C$  ja  $\mathbf{x} = \mathbf{c} + \mathbf{e}$  on "virheellinen", on kuitenkin  $H\mathbf{x}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$ . Virheenkorjaus perustuu vektoreihin  $H\mathbf{e}^T$ . näitä kutsutaan *syndromeiksi*.  
Ns. Syndromipankki muodostetaan tallentamalla muistiin Hamming-painon suhteen kaikkein kevyimmät syndromin tuottavat vektorit  $\mathbf{x} \in \mathbb{F}_2^n$ . Dekoodaus perustuu näihin, *johtajiksi* kutsuttuihin vektoreihin.

## Dekoodaus

- Vastaanotettaessa (mahdollisesti) virheellinen vektori  $\mathbf{x} \in \mathbb{F}_2^n$ , lasketaan  $\mathbf{e} = H\mathbf{x}^T$  ja valitaan syndromipankista vektori  $\mathbf{s}$  joka toteuttaa ehdon  $H\mathbf{s}^T = \mathbf{e}$ .

## Dekoodaus

- Vastaanotettaessa (mahdollisesti) virheellinen vektori  $\mathbf{x} \in \mathbb{F}_2^n$ , lasketaan  $\mathbf{e} = H\mathbf{x}^T$  ja valitaan syndromipankista vektori  $\mathbf{s}$  joka toteuttaa ehdon  $H\mathbf{s}^T = \mathbf{e}$ .
- Dekoodataan vektori  $\mathbf{x}$  vektoriksi  $\mathbf{x} - \mathbf{s}$ .

## Esimerkki: Hammingin [7, 4]-koodi

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

on [7, 4]-koodin tarkistusmatriisi (Huomio että  $H$ :n sarakkeet ovat lukujen 1–7 binääriesitykset).

## Esimerkki: Hammingin [7, 4]-koodi

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

on [7, 4]-koodin tarkistusmatriisi (Huomio että  $H$ :n sarakkeet ovat lukujen 1–7 binääriesitykset). Generoijamatriisi voidaan muodostaa ehdon  $G^T H = O$  perusteella, mutta dekooodaus edellyttää syndromipankin luomista. Voidaan valita

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

## Syndromit

$$H(0000000)^T = (000)^T$$

$$H(0000001)^T = (001)^T$$

$$H(0000010)^T = (010)^T$$

...

$$H(1000000)^T = (110)^T$$

## Esimerkki: Hammingin koodi

$$(1, 0, 1, 1) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1, 0, 1, 1, 0, 1, 0).$$

## Esimerkki: Hammingin koodi

$$(1, 0, 1, 1) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1, 0, 1, 1, 0, 1, 0).$$

## Virhe lähetyksessä

$$(1, 0, 1, 1, 0, 1, 0) \mapsto (1, 0, 1, 1, 0, 0, 0)$$

## Esimerkki

$$H(1, 0, 1, 1, 0, 0, 0)^T = (0, 1, 0),$$

## Esimerkki

$$H(1, 0, 1, 1, 0, 0, 0)^T = (0, 1, 0),$$

jota vastaava syndromipankin alkio on  $(0, 0, 0, 0, 0, 1, 0)$ .

## Esimerkki

$$H(1, 0, 1, 1, 0, 0, 0)^T = (0, 1, 0),$$

jota vastaava syndromipankin alkio on  $(0, 0, 0, 0, 0, 1, 0)$ .

Dekoodattu vektori on siis  $(1, 0, 1, 1, 0, 1, 0)$ .

## Hammingin koodi

- $[7, 4, 3]$ -koodi
- Hintana  $7/4 = 1.75$ -kertainen lähetysaika
- 1 virhe korjattavissa / 7- pituinen lohko

## Hammingin koodit

Jokaista  $r \geq 1$  kohti on olemassa  $[2^r - 1, 2^r - r - 1, 3]$ -koodi, jonka tarkistusmatriisi muodostetaan kaikista  $r$ -bittisten lukujen  $\neq 0$  binääriesityksistä.

## Hammingin koodit

Jokaista  $r \geq 1$  kohti on olemassa  $[2^r - 1, 2^r - r - 1, 3]$ -koodi, jonka tarkistusmatriisi muodostetaan kaikista  $r$ -bittisten lukujen  $\neq 0$  binääriesityksistä.

## Huomautus

Hammingin koodit korjaavat lähtökohtaisesti vain yhden virheen, mutta osoittavat, että informaatio suhde voidaan saada korkeaksi: Hintana  $(2^r - 1)/(2^r - r - 1)$ -pituisen lähetysaika

## Ongelmia

- Useampien kuin yhden virheen korjaus.

## Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaationsuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevät.

## Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaationsuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevät.
- Informaationsuhteen parantaminen teoreettisesti.

## Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaationsuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevät.
- Informaationsuhteen parantaminen teoreettisesti.
- Maksimaalisen informaationsuhteen etsiminen.

## Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaationsuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevät.
- Informaationsuhteen parantaminen teoreettisesti.
- Maksimaalisen informaationsuhteen etsiminen.
- Generoija- tai tarkistusmatriisin esittäminen kompaktisti.

## Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaationsuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevät.
- Informaationsuhteen parantaminen teoreettisesti.
- Maksimaalisen informaationsuhteen etsiminen.
- Generoija- tai tarkistusmatriisin esittäminen kompaktisti.

## Ratkaisuja

- BCH-koodit

## Ratkaisuja

- BCH-koodit
- Reed-Solomon -koodit

## Ratkaisuja

- BCH-koodit
- Reed-Solomon -koodit
- Reed-Muller -koodit

## Ratkaisuja

- BCH-koodit
- Reed-Solomon -koodit
- Reed-Muller -koodit
- Hadamardin koodit