Insinöörimatematiikka: Todennäköisyyslaskenta

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2024

Satunnaismuuttujien summat

Otoskeskiarvo, sen varianssi

Jos $X_1, \ldots, X_n$ ovat samoin jakautuneita $((\mu, \sigma^2))$, riippumattomia satunnaismuuttujia ja $\overline{X}_n = \frac{1}{n}(X_1 + \ldots + X_n)$ näiden aritmeettinen keskiarvo (ns. otoskeskiarvo) sekä summa $S_n = X_1 + \ldots + X_n$, on

- $\mathbb{E}(\overline{X}_n) = n \cdot \frac{1}{n}\mathbb{E}(X_1) = \mu$.
- $\mathrm{Var}(\frac{1}{n}(X_1 + \ldots + X_n)) = n \cdot \frac{1}{n^2}\sigma^2 = \frac{\sigma^2}{n}$.

Otoskeskiarvo, sen varianssi

Jos X_1, ..., X_n ovat samoin jakautuneita $((\mu, \sigma^2))$, riippumattomia satunnaismuuttujia ja $\overline{X}_n = \frac{1}{n}(X_1 + \ldots + X_n)$ näiden aritmeettinen keskiarvo (ns. otoskeskiarvo) sekä summa $S_n = X_1 + \ldots + X_n$, on

- $\mathbb{E}(\overline{X}_n) = n \cdot \frac{1}{n}\mathbb{E}(X_1) = \mu$.
- $\mathrm{Var}(\frac{1}{n}(X_1 + \ldots + X_n)) = n \cdot \frac{1}{n^2}\sigma^2 = \frac{\sigma^2}{n}$.
- $\mathbb{E}(S_n) = n \cdot \mathbb{E}(X_1) = n\mu$.
- $\mathrm{Var}(S_n) = n\sigma^2$

Satunnaismuuttujien summat

Keskeinen raja-arvolause

Suurilla n:n arvoilla $\overline{X}_n$ jakautuu likimain normaalijakauman $N(\mu, \frac{\sigma^2}{n})$ mukaisesti.

Satunnaismuuttujien summat

Keskeinen raja-arvolause

Suurilla n:n arvoilla $\overline{X}_n$ jakautuu likimain normaalijakauman $N(\mu, \frac{\sigma^2}{n})$ mukaisesti. Toisin sanoen,

$$\mathbb{P}(\overline{X}_n \leq x) \approx \Phi(\frac{x-\mu}{\sigma/\sqrt{n}})$$

kun n on suuri.

Satunnaismuuttujien summat

Keskeinen raja-arvolause

Suurilla n:n arvoilla $\overline{X}_n$ jakautuu likimain normaalijakauman $N(\mu, \frac{\sigma^2}{n})$ mukaisesti. Toisin sanoen,

$$\mathbb{P}(\overline{X}_n \leq x) \approx \Phi(\frac{x-\mu}{\sigma/\sqrt{n}})$$

kun n on suuri.

Toinen formulointi

$$\mathbb{P}(S_n \leq x) \approx \Phi(\frac{x-n\mu}{\sigma\sqrt{n}})$$

Keskeinen raja-arvolause

Suurilla n:n arvoilla $\overline{X}_n$ jakautuu likimain normaalijakauman $N(\mu, \frac{\sigma^2}{n})$ mukaisesti. Toisin sanoen,

$$\mathbb{P}(\overline{X}_n \leq x) \approx \Phi(\frac{x - \mu}{\sigma/\sqrt{n}})$$

kun n on suuri.

Toinen formulointi

$$\mathbb{P}(S_n \leq x) \approx \Phi(\frac{x - n\mu}{\sigma\sqrt{n}})$$

Huomautus

Jatkuvan jakauman diskretisointi

Esimerkki

Poisson- jakauma

ELISA on a bead

Esimerkki

Binäärinen symmetrinen kanava

$0 \to 1$ ja $1 \to 0$ todennäköisyydellä p.

Esimerkki

Binäärinen symmetrinen kanava

$0 \to 1$ ja $1 \to 0$ todennäköisyydellä p.
Siirrettäessä 2-pituisia sanoja 00, 01, 10, ja 11 virhetodennäköisyys on

$$\binom{2}{1}p(1-p) + \binom{2}{2}p^2 = 2p - p^2$$

Esimerkki

Koodaus

$00 \to 00000$, $01 \to 00111$, $10 \to 11100$ ja $11 \to 11011$ nostaa lähetysaikaa $2,5$-kertaiseksi.

Esimerkki

Koodaus

00 $\to$ 00000, 01 $\to$ 00111, 10 $\to$ 11100 ja 11 $\to$ 11011 nostaa lähetysaikaa $2,5$-kertaiseksi. Merkitään $C = \{00000, 00111, 11100, 11011\}$ ja dekoodausfunktio δ määritellään Hamming-etäisyyden perusteella, siis esim.

$$\delta(10000) = \delta(01000) = \delta(00100) = \delta(00010) = \delta(00001) = 00000.$$

Esimerkki

Koodaus

00 $\to$ 00000, 01 $\to$ 00111, 10 $\to$ 11100 ja 11 $\to$ 11011 nostaa lähetysaikaa $2,5$-kertaiseksi. Merkitään $C = \{00000, 00111, 11100, 11011\}$ ja dekoodausfunktio δ määritellään Hamming-etäisyyden perusteella, siis esim.

$$\delta(10000) = \delta(01000) = \delta(00100) = \delta(00010) = \delta(00001) = 00000.$$

Jos Hamming-etäisyys d_H kahteen eri sanaan on yhtä suuri, määritellään δ mielivaltaisesti. Esim. $\delta(10101) = 11100$ mutta voisi olla myös 00111.

Esimerkki

Huomautus

Todennäköisyys sille, että lähetettäessä sana $\boldsymbol{c}$ saadaankin sana $\boldsymbol{x}$ on

$$\mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = p^{d_H(\boldsymbol{x},\boldsymbol{c})}(1-p)^{5-d_H(\boldsymbol{x},\boldsymbol{c})}$$

Esimerkki

Huomautus

Todennäköisyys sille, että lähetettäessä sana $\boldsymbol{c}$ saadaankin sana $\boldsymbol{x}$ on

$$\mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = p^{d_H(\boldsymbol{x},\boldsymbol{c})}(1-p)^{5-d_H(\boldsymbol{x},\boldsymbol{c})}$$

Esimerkiksi

$$\mathbb{P}(00001 \mid 00000) = (1-p)(1-p)(1-p)(1-p)p = p^1(1-p)^4$$

Esimerkki

Huomautus

Todennäköisyys sille, että lähetettäessä sana $\boldsymbol{c}$ saadaankin sana $\boldsymbol{x}$ on

$$\mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = p^{d_H(\boldsymbol{x},\boldsymbol{c})}(1-p)^{5-d_H(\boldsymbol{x},\boldsymbol{c})}$$

Esimerkiksi

$$\mathbb{P}(00001 \mid 00000) = (1-p)(1-p)(1-p)(1-p)p = p^1(1-p)^4$$

ja

$$\mathbb{P}(01001 \mid 00000) = (1-p)p(1-p)(1-p)p = p^2(1-p)^3.$$

Esimerkki

Määritelmä

Jos $\boldsymbol{c} \in C$, merkitään

$$E_{\boldsymbol{c}} = \{\boldsymbol{x} \in \mathbb{F}_2^5 \mid \delta(\boldsymbol{x}) \neq \boldsymbol{c}\}$$

Esimerkki

Määritelmä

Jos $\boldsymbol{c} \in C$, merkitään

$$E_{\boldsymbol{c}} = \{\boldsymbol{x} \in \mathbb{F}_2^5 \mid \delta(\boldsymbol{x}) \neq \boldsymbol{c}\}$$

ja

$$D_{\boldsymbol{c}} = \{\boldsymbol{x} \in \mathbb{F}_2^5 \mid \delta(\boldsymbol{x}) = \boldsymbol{c}\} = \mathbb{F}_2^5 \setminus E_{\boldsymbol{c}}.$$

Esimerkki

Määritelmä

Jos $\boldsymbol{c} \in C$, merkitään

$$E_{\boldsymbol{c}} = \{\boldsymbol{x} \in \mathbb{F}_2^5 \mid \delta(\boldsymbol{x}) \neq \boldsymbol{c}\}$$

ja

$$D_{\boldsymbol{c}} = \{\boldsymbol{x} \in \mathbb{F}_2^5 \mid \delta(\boldsymbol{x}) = \boldsymbol{c}\} = \mathbb{F}_2^5 \setminus E_{\boldsymbol{c}}.$$

$E_{\boldsymbol{c}}$ on siis niiden sanojen joukko, jotka eivät dekoodaudu koodisanaksi $\boldsymbol{c}$ ja $D_{\boldsymbol{c}}$ sen komplementti.

Esimerkki

Määritelmä

$$\mathbb{P}_{er}(\boldsymbol{c}) = \sum_{\boldsymbol{x} \in E_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c})$$

Esimerkki

Määritelmä

$$\mathbb{P}_{er}(\boldsymbol{c}) = \sum_{\boldsymbol{x} \in E_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = 1 - \sum_{\boldsymbol{x} \in D_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c})$$

kertoo dekoodausvirheen todennäköisyyden kun syötteenä on koodisana $\boldsymbol{c} \in C$.

Esimerkki

Määritelmä

$$\mathbb{P}_{er}(\boldsymbol{c}) = \sum_{\boldsymbol{x} \in E_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = 1 - \sum_{\boldsymbol{x} \in D_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c})$$

kertoo dekoodausvirheen todennäköisyyden kun syötteenä on koodisana $\boldsymbol{c} \in C$.

Keskiarvo

$$\mathbb{P}_{er}(C) = \frac{1}{|C|} \sum_{\boldsymbol{c} \in C} \mathbb{P}_{er}(\boldsymbol{c})$$

Ilmoittaa virhetodennäköisyyden kun käytetään koodia C

Esimerkki

Määritelmä

$$\mathbb{P}_{er}(\boldsymbol{c}) = \sum_{\boldsymbol{x} \in E_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c}) = 1 - \sum_{\boldsymbol{x} \in D_{\boldsymbol{c}}} \mathbb{P}(\boldsymbol{x} \mid \boldsymbol{c})$$

kertoo dekoodausvirheen todennäköisyyden kun syötteenä on koodisana $\boldsymbol{c} \in C$.

Keskiarvo

$$\mathbb{P}_{er}(C) = \frac{1}{|C|} \sum_{\boldsymbol{c} \in C} \mathbb{P}_{er}(\boldsymbol{c})$$

Ilmoittaa virhetodennäköisyyden kun käytetään koodia C, olettaen että koodisanat jakautuvat yhtä todennäköisesti.

Esimerkki

Dekoodautuvat sanat

$$D_{00000} = \{00000, 00001, 00010, 00100, 01000, 01001, 01010, 10000, 10001, 10010\}$$

Esimerkki

Dekoodautuvat sanat

$$\begin{aligned} D_{00000} &= \{00000, 00001, 00010, 00100, 01000, 01001, 01010, \\ &\quad 10000, 10001, 10010\} \\ D_{00111} &= \{00011, 00101, 00110, 00111, 01101, 01110, 01111, \\ &\quad 10101, 10110, 10111\} \end{aligned}$$

Esimerkki

Dekoodautuvat sanat

$$
\begin{aligned}
D_{00000} &= \{00000, 00001, 00010, 00100, 01000, 01001, 01010, \\
&\quad 10000, 10001, 10010\} \\
D_{00111} &= \{00011, 00101, 00110, 00111, 01101, 01110, 01111, \\
&\quad 10101, 10110, 10111\} \\
D_{11100} &= \{01100, 10100, 11000, 11100, 11101, 11110\}
\end{aligned}
$$

Esimerkki

Dekoodautuvat sanat

$$
\begin{aligned}
D_{00000} &= \{00000, 00001, 00010, 00100, 01000, 01001, 01010,\\
&\quad 10000, 10001, 10010\}\\
D_{00111} &= \{00011, 00101, 00110, 00111, 01101, 01110, 01111,\\
&\quad 10101, 10110, 10111\}\\
D_{11100} &= \{01100, 10100, 11000, 11100, 11101, 11110\}\\
D_{11011} &= \{01011, 10011, 11001, 11010, 11011, 11111\}
\end{aligned}
$$

Esimerkki

Dekoodautuvat sanat

$$
\begin{aligned}
D_{00000} &= \{00000, 00001, 00010, 00100, 01000, 01001, 01010,\\
&\quad 10000, 10001, 10010\}\\
D_{00111} &= \{00011, 00101, 00110, 00111, 01101, 01110, 01111,\\
&\quad 10101, 10110, 10111\}\\
D_{11100} &= \{01100, 10100, 11000, 11100, 11101, 11110\}\\
D_{11011} &= \{01011, 10011, 11001, 11010, 11011, 11111\}
\end{aligned}
$$

Virhetodennäköisyydet

$$\mathbb{P}_{er}(00000) = 1 - (1-p)^5 - 5(1-p)^4 p - 4(1-p)^3 p^2$$

Esimerkki

Virhetodennäköisyydet

$$
\begin{aligned}
\mathbb{P}_{er}(00000) &= 1-(1-p)^5-5(1-p)^4p-4(1-p)^3p^2\\
\mathbb{P}_{er}(00111) &= 1-(1-p)^5-5(1-p)^5p-4(1-p)^3p^2\\
\mathbb{P}_{er}(11100) &= 1-(1-p)^5-5(1-p)^4p\\
\mathbb{P}_{er}(00111) &= 1-(1-p)^5-5(1-p)^4p
\end{aligned}
$$

Esimerkki

Virhetodennäköisyydet

$$\begin{aligned}
\mathbb{P}_{er}(00000) &= 1-(1-p)^5-5(1-p)^4p-4(1-p)^3p^2 \\
\mathbb{P}_{er}(00111) &= 1-(1-p)^5-5(1-p)^5p-4(1-p)^3p^2 \\
\mathbb{P}_{er}(11100) &= 1-(1-p)^5-5(1-p)^4p \\
\mathbb{P}_{er}(00111) &= 1-(1-p)^5-5(1-p)^4p
\end{aligned}$$

Keskiarvo

Koodin C virhetodennäköisyys on keskiarvo edellisistä:

$$\mathbb{P}_{er}(C) = 8p^2 - 14p^3 + 9p^4 - 2p^5$$

Koodattu vs. koodaamaton

$$\frac{\mathbb{P}_{er}(C)}{2p - p^2} = \frac{p^2(8 - 14p + 9p^2 - 2p^3)}{2p - 2p^2}$$

Esimerkki

Koodattu vs. koodaamaton

$$\begin{aligned}\frac{\mathbb{P}_{er}(C)}{2p-p^2} &= \frac{p^2(8-14p+9p^2-2p^3)}{2p-2p^2}\\ &= p(4-5p+2p^2)\end{aligned}$$

Esimerkki

Koodattu vs. koodaamaton

$$
\begin{aligned}
\frac{\mathbb{P}_{er}(C)}{2p-p^2} &= \frac{p^2(8-14p+9p^2-2p^3)}{2p-2p^2} \\
&= p(4-5p+2p^2) \\
&\approx 4p
\end{aligned}
$$

Esimerkki

Koodattu vs. koodaamaton

$$\frac{\mathbb{P}_{er}(C)}{2p-p^2} = \frac{p^2(8-14p+9p^2-2p^3)}{2p-2p^2}$$
$$= p(4-5p+2p^2)$$
$$\approx 4p$$

Jos esim. $p = \frac{1}{10^6}$, on $4p = \frac{1}{250000}$

Entropia

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa $x_1, \ldots, x_n$ todennäköisyyksillä $p_1, \ldots, p_n$.

Entropia

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa $x_1, \ldots, x_n$ todennäköisyyksillä $p_1, \ldots, p_n$.
Jakauman $p_1, \ldots, p_n$ *Shannon-entropia* on

$$H(p_1, \ldots, p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio.

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa x_1, ..., x_n todennäköisyyksillä p_1, ..., p_n.
Jakauman p_1, ..., p_n *Shannon-entropia* on

$$H(p_1, \ldots, p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio. Jos $K = \frac{1}{\ln 2}$, sanotaan entropiaa binääriseksi.

Entropia

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa x_1, ..., x_n todennäköisyyksillä p_1, ..., p_n.
Jakauman p_1, ..., p_n *Shannon-entropia* on

$$H(p_1, \ldots, p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio. Jos $K = \frac{1}{\ln 2}$, sanotaan entropiaa binääriseksi. Tällöin $\frac{\ln p_i}{\ln 2} = \log_2 p_i$.

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa x_1, ..., x_n todennäköisyyksillä p_1, ..., p_n.
Jakauman p_1, ..., p_n *Shannon-entropia* on

$$H(p_1, \ldots, p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio. Jos $K = \frac{1}{\ln 2}$, sanotaan entropiaa binääriseksi. Tällöin $\frac{\ln p_i}{\ln 2} = \log_2 p_i$. Määritellään lisäksi $0 \cdot \ln 0 = 0$.

Entropia

Määritelmä

Lähtökohtana on diskreetti satunnaismuuttuja X, joka voi saada n arvoa x_1, ..., x_n todennäköisyyksillä p_1, ..., p_n.
Jakauman p_1, ..., p_n *Shannon-entropia* on

$$H(p_1, \ldots, p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio. Jos $K = \frac{1}{\ln 2}$, sanotaan entropiaa binääriseksi. Tällöin $\frac{\ln p_i}{\ln 2} = \log_2 p_i$. Määritellään lisäksi $0 \cdot \ln 0 = 0$.
Jos diskreetillä satunnaismuuttujalla X on jakauma p_1, ..., p_n, merkitään ylläolevaa entropiaa myös $H(X)$:llä.

Esimerkki

Jos kaikki arvot x_i ilmaantuvat samalla todennäköisyydellä $\frac{1}{n}$, on

$$H(\frac{1}{n}, \ldots, \frac{1}{n}) = -(\frac{1}{n} \log_2 \frac{1}{n} + \ldots + \frac{1}{n} \log_2 \frac{1}{n}) = \log_2 n.$$

Entropia

Esimerkki

Jos kaikki arvot x_i ilmaantuvat samalla todennäköisyydellä $\frac{1}{n}$, on

$$H(\frac{1}{n}, \ldots, \frac{1}{n}) = -(\frac{1}{n}\log_2\frac{1}{n} + \ldots + \frac{1}{n}\log_2\frac{1}{n}) = \log_2 n.$$

Tämä merkitsee sitä, että satunnaismuuttujan X esittämän viestin välittämiseen tarvitaan keskimäärin $\log_2 n$ bittiä.

Esimerkki

Jos kaikki arvot x_i ilmaantuvat samalla todennäköisyydellä $\frac{1}{n}$, on

$$H(\frac{1}{n},\ldots,\frac{1}{n}) = -(\frac{1}{n}\log_2\frac{1}{n} + \ldots + \frac{1}{n}\log_2\frac{1}{n}) = \log_2 n.$$

Tämä merkitsee sitä, että satunnaismuuttujan X esittämän viestin välittämiseen tarvitaan keskimäärin $\log_2 n$ bittiä.

Esimerkki

Jos satunnaismuuttuja X saa arvon x_1 todennäköisyydellä 1 ja muut arvot $x_2,\ldots,x_n$ todennäköisyydellä 0, on

$$H(X) = -(1\cdot\log_2 1 + 0\cdot\log_2 0 + \ldots + 0\cdot\log_2 0) = 0$$

Esimerkki

Satunnaismuuttuja X saa kaksi arvoa x_0 ja x_1, molemmat todennäköisyydellä $\frac{1}{2}$.

Entropia

Esimerkki

Satunnaismuuttuja X saa kaksi arvoa x_0 ja x_1, molemmat todennäköisyydellä $\frac{1}{2}$. Tällöin

$$H(X) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1.$$

Esimerkki

Satunnaismuuttuja X saa kaksi arvoa x_0 ja x_1, molemmat todennäköisyydellä $\frac{1}{2}$. Tällöin

$$H(X) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1.$$

Esimerkki

Satunnaismuuttuja X saa arvon x_0 todennäköisyydellä $\frac{1}{4}$ ja arvon x_1 todennäköisyydellä $\frac{3}{4}$.

Entropia

Esimerkki

Satunnaismuuttuja X saa kaksi arvoa x_0 ja x_1, molemmat todennäköisyydellä $\frac{1}{2}$. Tällöin

$$H(X) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1.$$

Esimerkki

Satunnaismuuttuja X saa arvon x_0 todennäköisyydellä $\frac{1}{4}$ ja arvon x_1 todennäköisyydellä $\frac{3}{4}$. Tällöin

$$H(X) = -(\frac{1}{4}\log_2\frac{1}{4} + \frac{3}{4}\log_2\frac{3}{4}) = 0,811278\ldots$$

Entropia

Lause

Oletetaan että reaaliarvoinen funktio $H(p_1,\ldots,p_n)$ toteuttaa seuraavat ehdot:

- $H(p_1,\ldots,p_n)$ on symmetrinen ja jatkuva
- $H(\frac{1}{n},\ldots,\frac{1}{n})$ on ei-negatiivinen, aidosti kasvava
- Todennäköisyysjakaumille $(p_1,\ldots,p_n)$ ja $(q_1,\ldots,q_m)$ on voimassa

$$\begin{aligned} & H(p_1,\ldots,p_n) + p_n H(q_1,\ldots,q_m) \\ = \; & H(p_1,\ldots,p_{n-1},p_nq_1,\ldots,p_nq_m). \end{aligned}$$

Lause

Oletetaan että reaaliarvoinen funktio $H(p_1,\ldots,p_n)$ toteuttaa seuraavat ehdot:

- $H(p_1,\ldots,p_n)$ on symmetrinen ja jatkuva
- $H(\frac{1}{n},\ldots,\frac{1}{n})$ on ei-negatiivinen, aidosti kasvava
- Todennäköisyysjakaumille $(p_1,\ldots,p_n)$ ja $(q_1,\ldots,q_m)$ on voimassa

$$\begin{aligned} & H(p_1,\ldots,p_n) + p_n H(q_1,\ldots,q_m) \\ = \; & H(p_1,\ldots,p_{n-1},p_n q_1,\ldots,p_n q_m). \end{aligned}$$

Tällöin

$$H(p_1,\ldots,p_n) = -K(p_1 \ln p_1 + \ldots + p_n \ln p_n),$$

missä $K > 0$ on vakio.

Entropia

Yhdistetty entropia

$$H(X, Y) = -\sum p(x, y) \log_2 p(x, y)$$

Entropia

Yhdistetty entropia

$$H(X, Y) = -\sum p(x, y) \log_2 p(x, y)$$

Ehdollinen entropia

$$H(X \mid y_j) = -\sum p(x \mid y_j) \log_2 p(x \mid y_j)$$

Entropia

Yhdistetty entropia

$$H(X, Y) = -\sum p(x, y) \log_2 p(x, y)$$

Ehdollinen entropia

$$H(X \mid y_j) = -\sum p(x \mid y_j) \log_2 p(x \mid y_j)$$

$$H(X \mid Y) = \sum p(y_j) H(X \mid y_j)$$

Entropia

Yhdistetty entropia

$$H(X, Y) = -\sum p(x, y) \log_2 p(x, y)$$

Ehdollinen entropia

$$H(X \mid y_j) = -\sum p(x \mid y_j) \log_2 p(x \mid y_j)$$

$$H(X \mid Y) = \sum p(y_j) H(X \mid y_j)$$

Informaatio

$$I(X \mid Y) = H(X) - H(X \mid Y)$$

Entropia

Määritelmä

Mikäli n-pituinen jono satunnaismuuttujan X arvoista muodostuvia viestejä voidaan koodata $m = \lfloor rn \rfloor$-pituisilla bittijonoilla, sanotaan, että koodaus onnistuu tahdilla (rate) r.

Määritelmä

Mikäli n-pituinen jono satunnaismuuttujan X arvoista muodostuvia viestejä voidaan koodata $m = \lfloor rn \rfloor$-pituisilla bittijonoilla, sanotaan, että koodaus onnistuu tahdilla (rate) r.

Shannonin lause

Jos $r > H(X)$, on mahdollista koodata X:n arvot binääriseen aakkostoon tahdilla r siten että dekoodausvirheen todennäköisyys lähenee nollaa.

Entropia

Määritelmä

Mikäli n-pituinen jono satunnaismuuttujan X arvoista muodostuvia viestejä voidaan koodata $m = \lfloor rn \rfloor$-pituisilla bittijonoilla, sanotaan, että koodaus onnistuu tahdilla (rate) r.

Shannonin lause

Jos $r > H(X)$, on mahdollista koodata X:n arvot binääriseen aakkostoon tahdilla r siten että dekoodausvirheen todennäköisyys lähenee nollaa.
Jos $r < H(X)$, edellämainittu koodaus ei ole mahdollista, vaan dekoodausvirheen todennäköisyys lähenee ykköstä.

Shannonin lause

Määritelmä

Binäärisen symmetrisen kanavan *kapasiteetti* on

$$C(p) = 1 - H_2(p),$$

missä p on kanavan virhetodennäköisyys.

Määritelmä

Binäärisen symmetrisen kanavan *kapasiteetti* on

$$C(p) = 1 - H_2(p),$$

missä p on kanavan virhetodennäköisyys.

Koodin C_n *informaatiosuhde* on

$$R(C_n) = \frac{\log_2 |C_n|}{n}.$$

Shannonin lause

Määritelmä

Binäärisen symmetrisen kanavan *kapasiteetti* on

$$C(p) = 1 - H_2(p),$$

missä p on kanavan virhetodennäköisyys.

Koodin C_n *informaatiosuhde* on

$$R(C_n) = \frac{\log_2 |C_n|}{n}.$$

Shannonin lause 2

Jos $p < \frac{1}{2}$ ja $R < C(p)$ ja $\epsilon > 0$, niin on sellainen rajaluku $N = N(p, R, \epsilon)$, että aina kun $n \geq N$, niin on olemassa n-pituinen binäärikoodi C_n jolle $R(C_n) \geq R$ ja $\mathbb{P}_{er}(C_n) < \epsilon$.