Verjetnostni račun:

Dogodki: $A, B, N, G, ...$

Verjetnosti: $P(N)=0$, $P(G)=1$, $P(A)=\frac{n_A}{n}$

Vsota: $P(A+B)=P(A)+P(B)-P(AB)$

Nezdružljiva dogodka: $P(A+B)=P(A)+P(B)$

Zmnožek: $P(AB)=P(A)P(B|A)=P(B)P(A|B)$

Neodvisna dogodka: $P(AB)=P(A)P(B)$

Popolna verjetnost: $P(A)=\sum_{i=1}^{N}P(H_i)P(A|H_i)$

Bayes: $P(H_i|A)=\frac{P(H_i)P(A|H_i)}{\sum_{k=1}^{N}P(H_k)P(A|H_k)}$

Diskretne naključne spremenljivke:

Zaloga vrednosti: $X=\{x_1,\cdots,x_n\}$

Standardna normalna (Gaussova) porazdelitev: $\varphi(z)=\frac{e^{-\frac{z^2}{2}}}{\sqrt{2\pi}}$

Enakomerna porazdelitev: $p_i=1/n$

Geometrijska porazdelitev: $p_i=p(1-p)^{i-1}, p=P(A)$

Binomska porazdelitev: $p_i=\binom{n}{i}p^i(1-p)^{n-i}$, $\binom{n}{i}=\frac{n!}{(n-i)!i!}$, $p=P(A)$

Poissonova porazdelitev: $p_i=\frac{\lambda^i\ e^{-\lambda}}{i!}$

Entropija diskretnih naključnih spremenljivk:

Spremenljivki: $X=\{x_1,\cdots,x_m\}$, $Y=\{y_1,\cdots,y_n\}$

Verjetnosti: $p_i=P(X=x_i)$, $p'_j=P(Y=y_j)$

Verjetnosti: $p_{ij}=P(X=x_i,Y=y_j)$, $p_{i|j}=P(X=x_i|Y=y_j)$, $p'_{j|i}=P(Y=y_j|X=x_j)$

Zveze: $p'_j=\sum_{i=1}^{m}p_ip'_{j|i}=\sum_{i=1}^{m}p_{ij}$, $p_i=\sum_{j=1}^{n}p'_jp_{i|j}=\sum_{j=1}^{n}p_{ij}$, $p_{i|j}=\frac{p_ip'_{j|i}}{p'_j}=\frac{p_{ij}}{p'_j}$, $p'_{j|i}=\frac{p'_jp_{i|j}}{p_i}=\frac{p_{ij}}{p_i}$

Lastna entropija: $H(X)=-\sum_{i=1}^{m}p_ilog_dp_i$

Vezana entropija: $H(X,Y)=-\sum_{i=1}^{m}\sum_{j=1}^{n}p_{ij}log_dp_{ij}$

Entropija razbitja: $H(p_1,...,p_m,r_1,...,r_n)=H(p,r)+pH\left(\frac{p_1}{p},...,\frac{p_m}{p}\right)+rH\left(\frac{r_1}{r},...,\frac{r_n}{r}\right)$

Pogojna entropija: $H(X|Y)=\sum_{j=1}^{n}p'_jH(X|Y=y_j)=-\sum_{j=1}^{n}p'_j\sum_{i=1}^{m}p_{i|j}log_dp_{i|j}$

Pogojna entropija: $H(Y|X)=\sum_{i=1}^{m}p_iH(Y|X=x_i)=-\sum_{i=1}^{m}p_i\sum_{j=1}^{n}p'_{j|i}log_dp'_{j|i}$

Zveze: $H(X|Y)\leq H(X)$, $H(X,Y)=H(X)+H(Y|X)=H(Y)+H(X|Y)$, $H(X,Y)\leq H(X)+H(Y)$

Vzajemna informacija diskretnih naključnih spremenljivk:

$I(X,Y)=H(X)-H(X|Y)=H(Y)-H(Y|X)=H(X)+H(Y)-H(X,Y)$

Diskretni viri informacije:

Vir z abecedo: $A=\{x_1,\cdots,x_a\}$ oddaja nize dolžine n znakov $(x_1,\cdots,x_n)$.

Entropija stacionarnega vira: $H_n=H(X_1,\cdots,X_n)$, $H=\lim_{n\to\infty}H_n$, kjer je vsaka $\mathcal{Z}(X_i)=\{x_1,\cdots,x_a\}$

$\cdots\quad H_n=-\frac{1}{n}K\sum P(x_1,\cdots,x_n)log_dp(x_1,\cdots,x_n)$

Odvečnost stacionarnega vira: $R=1-\frac{H}{log_da}$

Entropija stac. vira brez spomina: $H=-\sum_{i=1}^{a}p_ilog_dp_i$, $p_i=P(A=x_i)$

Stac. Markovov vir s spominom: $\mathbf{P}_Q=[q_{ij}]=[P(X_t=x_j|X_{t-1}=x_i)]$, $i,j=1,\cdots,a$

Stac. porazdelitev Markovovega vira: $\mathbf{p}=(p_1,\cdots,p_a)$, $\mathbf{p}=\mathbf{p}\mathbf{P}_Q$

Entropija stac. Markovovega vira: $H=-\sum_{i=1}^{a}p_i\sum_{j=1}^{a}q_{ij}log_dq_{ij}$

Komunikacijski kanali:

Kapaciteta zveznega kanala: $C=Flog_d(1+S/N)$, F je mejna frekvenca in S/N je razmerje moči

Diskretni kanal: $U=\{x_1,\cdots,x_u\}$, $V=\{y_1,\cdots,y_v\}$, $\mathbf{P}_k=[a_{ij}]=[P(V=y_j|U=x_i)]$

Diskretni kanal brez spomina: $[a_{ij}]=[P(Y=y_j|X=x_i)]$, $P_X=\{p_1,\cdots,p_u\}$, $p_i=P(X=x_i)$

Kapaciteta diskretnega kanala brez spomina: $C=\max_{P_X}\{I(X,Y)\}$ $C'=C/\tau=C\cdot\nu$

Kapaciteta simetričnega diskretnega kanala: $C=log_dv+\sum_{i=1}^{v}r_ilog_dr_i$, r_i so elementi vrstice $\mathbf{P}_k$

Kodiranje vira:

Kod vira: $A=\{x_1,\cdots,x_a\}$, $B=\{z_1,\cdots,z_b\}$, $f:A\to E$, $p_i=P(A=x_i)$

Enakomerni kod: $E=B^m$,

Mera gospodarnosti koda: $\bar{n}=\sum_{i=1}^{a}p_in_i$, Uspešnost koda: $\eta=H/\bar{n}$,

Kraftova McMillanova neenačba: $\sum_{i=1}^{a}b^{-ni}\leq 1$

$H=-\sum_{i=1}^{a}p_ilog_dp_i$; Aritmetični kod: $R_0=[s,z)$; $R_{n+1}=[s',z')$; $s'=s+(z-s)s_i$; $z'=s+(z-s)z_i$;

Shannonov izrek o gospodarnosti kodiranja: $\frac{H}{log_db}\leq\bar{n}<\frac{H_1}{log_db}+1$ in $\frac{H_1}{log_db}\leq\frac{\bar{n}_r}{r}<\frac{H_1}{log_db}+\frac{1}{r}$

Tajno kodiranje:

Vigener šifriranje/dešifriranje: $c_i\equiv(m_i+k_i)\bmod\sigma$, $m_i\equiv(c_i-k_i)\bmod\sigma$; XOR šifra: $c_i=m_i\underline{\vee}k_i$, $m_i=c_i\underline{\vee}k_i$

RSA ključa: $n=qq'$, $\varphi(n)=(q-1)(q'-1)$, $e\cdot d\equiv 1\bmod\varphi(n)$ ali $e\cdot d=k\varphi(n)+1$ $NSD(d,\varphi(n))=1$

RSA [šifriranje/dešifriranje: $c_i=m_i^e\bmod n$, $m_i=c_i^d\bmod n$

Kodiranje in dekodiranje za prenos po kanalu z motnjami:

Kod kanala: $\mathbf{z}_i=(z_1,\cdots,z_k)\to\mathbf{x}_i=(x_1,\cdots,x_n)$, kjer je $i=1,\cdots,M$ in $M\leq b^k$

Dvojiški kod kanala: $\mathbf{z}_i\in B^k$, $\mathbf{x}_i\in U^n$, $B=U=\{0,1\}$, $b=2$, $M\leq 2^k$

Hitrost koda: $R=\frac{k}{n}$

Dekodiranje: $\mathbf{y}_i=(y_1,\cdots,y_n)\to\hat{\mathbf{x}}$,

Idealni opazovalec: $P(\hat{\mathbf{x}}|\mathbf{y})=\max_{1\leq i\leq M}\{P(\mathbf{x}_i|\mathbf{y})\}$

Idealna funkcija odločanja: $P(\mathbf{y}|\hat{\mathbf{x}})=\max_{1\leq i\leq M}\{P(\mathbf{y}|\mathbf{x}_i)\}$

Hammingova razdalja: $d_H(\mathbf{x},\mathbf{y})=\sum_{i=1}^{n}|x_i-y_i|$

Idealna funkcija odločanja: $d_H(\hat{\mathbf{x}},\mathbf{y})=min_{\mathbf{x}}\{d_H(\mathbf{x},\mathbf{y})\}$

Optimalna dolžina kodnih zamenjav pri: $d_H(\mathbf{x}_i,\mathbf{x}_j)\geq 2e+1$, $i\neq j$

Hammingov pogoj spodnje meje: $M\sum_{i=0}^{e}\binom{n}{i}\leq 2^n$

Gilbertov pogoj zgornje meje: $M\sum_{i=0}^{2e}\binom{n}{i}\geq 2^n$

Linearni bločni kod: $\mathbf{H}\cdot\mathbf{x}^T=\mathbf{0}^T$, $rang(\mathbf{H})=m$, $m<n$, $k=n-m$, $\mathbf{H}\cdot\mathbf{y}^T=\mathbf{s}^T=\mathbf{H}\cdot\mathbf{e}^T$

Sistematični kod: $\mathbf{H}=[\mathbf{I}_m|\mathbf{B}_{mk}]$, $\mathbf{G}=[\mathbf{B}_{mk}^T|\mathbf{I}_k]$, $\mathbf{x}_i=\mathbf{z}_i\cdot\mathbf{G}$

Hammingov kod: $n=2^m-1$, $m\geq 2$, $M=2^k=2^{n-m}$, $d_{Hmin}=3$, $e=1$