Teorie Informace

Miroslav Skrbek

LS 2011/2012

Verze 0.1

Literatura

- Mareš M.: Základy teorie informace. Zdroje informace a jejich měření. Jihočeská univerzita v Českých Budějovicích, 2011
- Hankerson, D., Harris, G., A., Johnson, P., D.: Introduction to Information Theory and Data Compression. Chapman & Hall/CRC. Second Edition. 2003. ISBN 1-58488-313-8.
- Hans-Jochen Bartsh: Matematické vzorce. Studentské vydání. ACADEMIA, Praha 2006.

Čísla

- Přirozená čísla (N)
  - Příklad: 1, 2, 3, … !! nepatří sem 0 ani záporná čísla
- Nezáporná celá čísla (N_0)
  - Příklad: 0, 1, 2, …
- Celá čísla (Z nebo I)
  - Přirozená čísla, nula (0) a záporná čísla
- Racionální čísla (Q)
  - Možno popsat zlomkem x/y, kde x϶I, y϶I nebo konečným počtem desetinných míst, případně nekonečným počtem desetinných míst periodicky se opakujících.
- Iracionální čísla
  - nelze popsat zlomkem celých čísel, nekonečný počet desetinných míst, které se periodicky neopakují
- Reálná čísla (R)
  - sjednocení množin racionálních a iracionálních čísel
- Komplexní čísla (C)
  - a+ib, 1+i4; i je imaginární jednotka (odmocnina z -1)

Výrokový počet

Výrok je každé tvrzení, které může být pravdivé nebo nepravdivé

Pravdivý výrok označujeme **T** (true)

Nepravdivý výrok označujeme **F** (false)

Logické spojky

Konjunkce

$\wedge$

Disjunkce

$\vee$

Negace

$\neg$

Implikace

$\Rightarrow$

Ekvivalence

$\Leftrightarrow$

Konjunkce

A	B	$A \wedge B$
F	F	F
F	T	F
T	F	F
T	T	T

Značení v aplikacích: a, and, &&, ., nic

Disjunkce

A	B	$A \vee B$
F	F	F
F	T	T
T	F	T
T	T	T

Jiné označení: : nebo, or, ||, |, +

Implikace

A	B	$A \Rightarrow B$
F	F	T
F	T	T
T	F	F
T	T	T

Jiné označení: plyne

Ekvivalence

A	B	$A \Leftrightarrow B$
F	F	T
F	T	F
T	F	F
T	T	T

Jiné označení: tehdy a jen tehdy, ==

Negace

A	$\neg A$
F	T
T	F

Jiné označení: negace, not, !, ', #

Tautologie

Výrok, který je pravdivý pro jakékoliv ohodnocení vstupních výroků

Příklady

$$A \vee (\neg A)$$

$$\neg(A \wedge (\neg A))$$

$$((A \Rightarrow B) \wedge A) \Rightarrow B)$$

$$((A \Rightarrow B) \wedge (\neg B)) \Rightarrow (\neg A)$$

$$((A \Rightarrow B) \wedge (B \Rightarrow A)) \Leftrightarrow (A \Leftrightarrow B)$$

Kvantifikátory

Existuje alespoň jedno x z M, pro které platí výrok V

$$\exists_{x \in M} (V(x) = T)$$

Pro všechna x z M platí výrok V

$$\forall_{x \in M} (V(x) = T)$$

Pokud chceme existenční kvantifikátor omezit pouze na existenci jediného prvku množiny splňujícím podmínku, píšeme

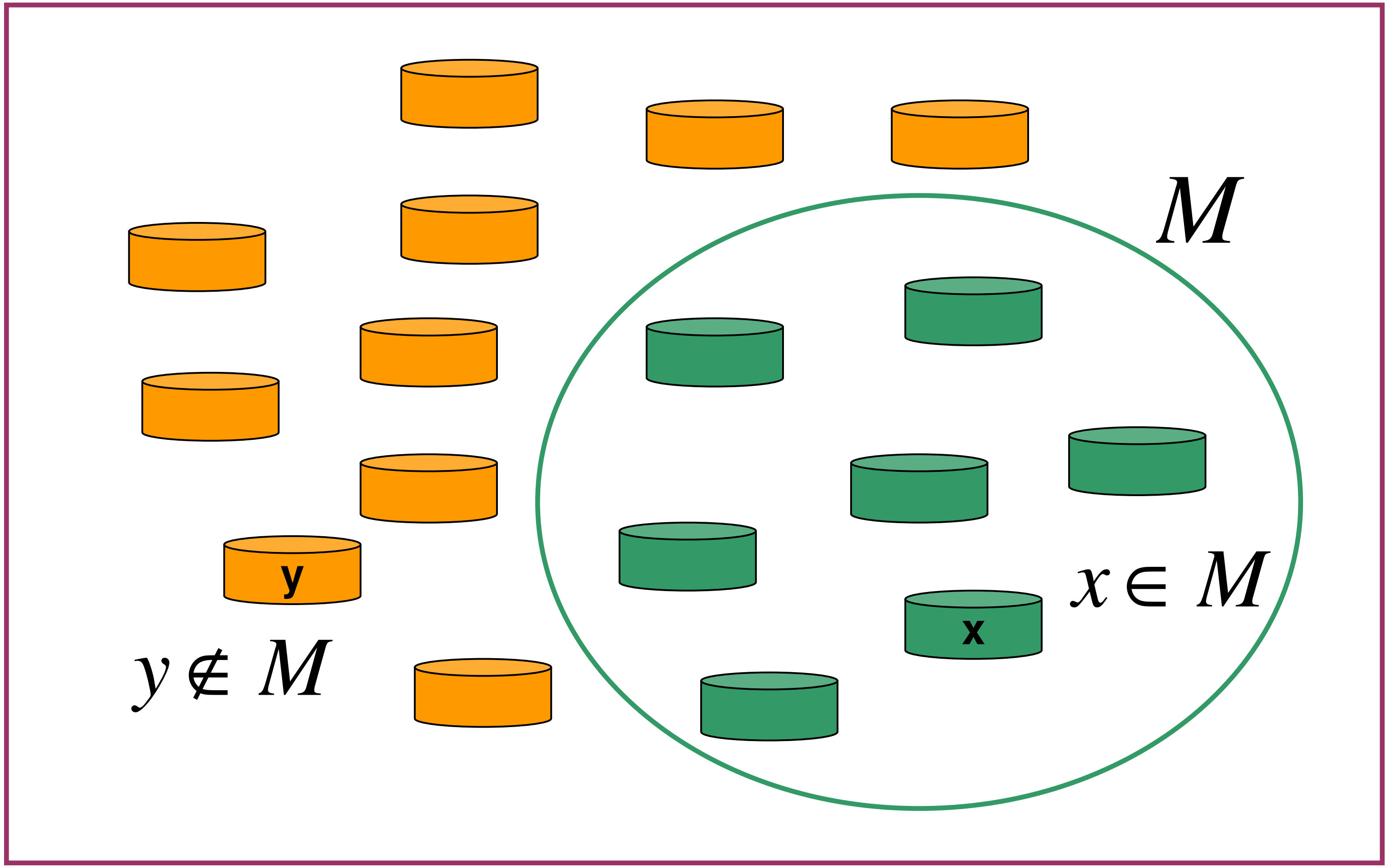
$$\exists!_{x \in M} (V(x) = T)$$

Teorie množin

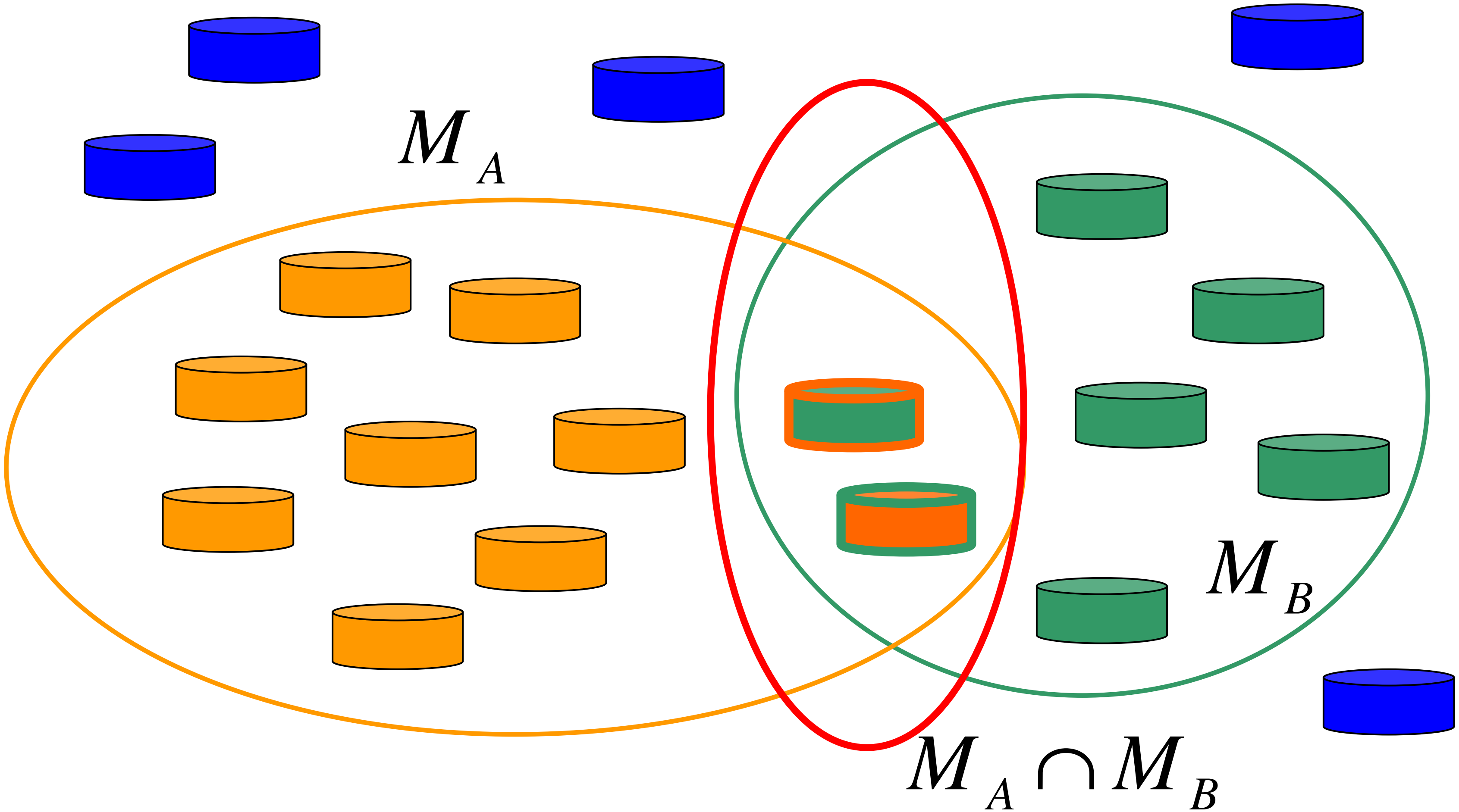
- Množina je třída prvků vybraných z nějakého univerza U
- Prvek do množiny patří nebo nepatří
- Množinové operace
  - Sjednocení
  - Průnik
  - Doplněk
  - Rozdíl
- Prázdná množina (∅)
  - Neobsahuje žádný prvek

Množina

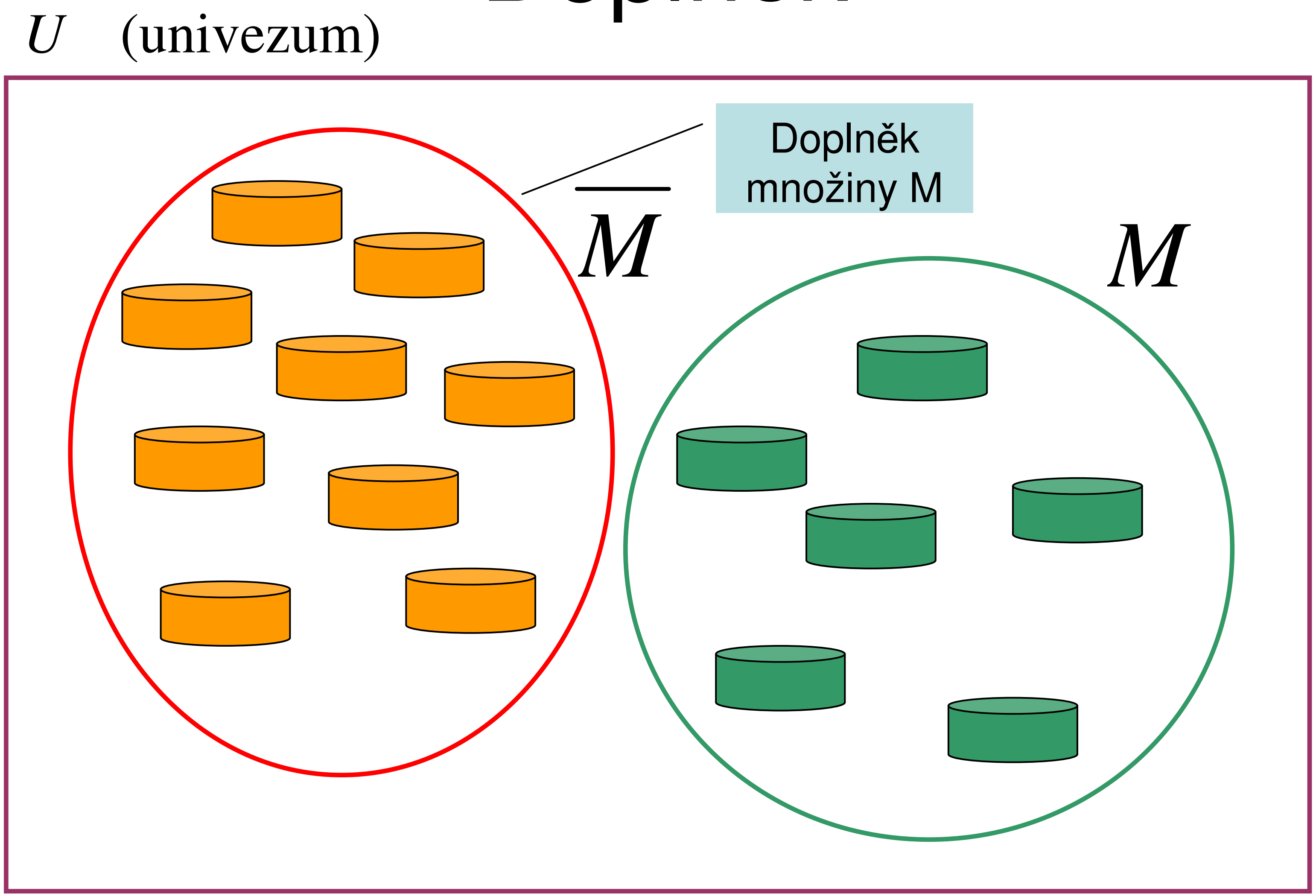
U (univezum)



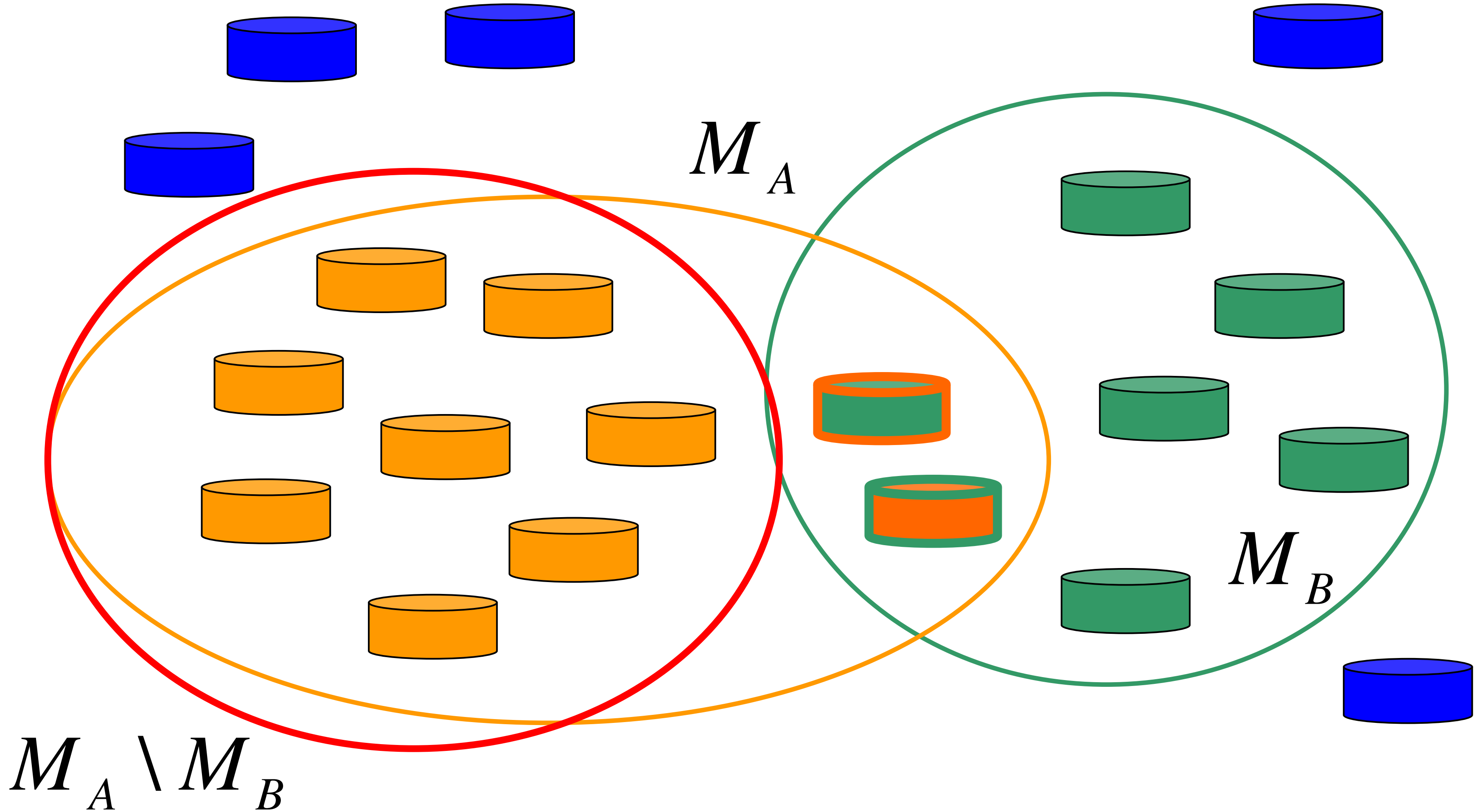
Průnik



Doplněk

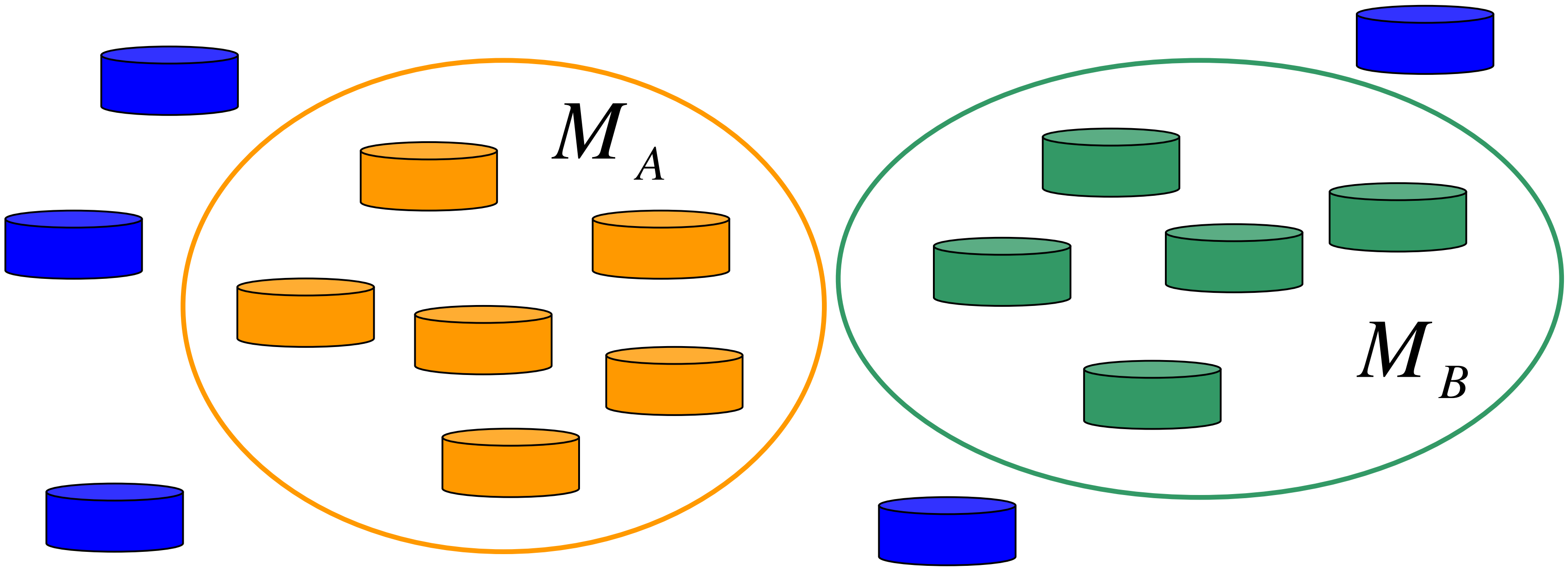


Rozdíl



Disjunktní množiny

$$M_A \cap M_B = \phi$$



Kardinalita (mohutnost) množiny

Kardinalita (mohutnost) množiny - počet prvků v množině

$$|\phi| = 0$$

$$|M_A \cup M_B| = |M_A| + |M_B| - |M_A \cap M_B|$$

$$|\overline{M_A}| = |U| - |M_A|$$

$$|M_A \setminus M_B| = |M_A| - |M_A \cap M_B|$$

Konečná množina: $|M| < \infty$

Nekonečná množina: $|M| = \infty$

Spočetná množina: $\exists P : M \rightarrow N$

Existuje zobrazení, které mapuje množinu M do množiny přirozených čísel

De Morganova věta

Jsou-li A,B množiny, pak platí

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Zobrazení

Zobrazení z množiny L do množiny M je předpis, který přiřazuje prvky množiny M (obrazy) prvkům množiny L (vzory).

Zobrazení je specifickým typem binární relace, tedy podmnožina kartézkého součinu L×M.

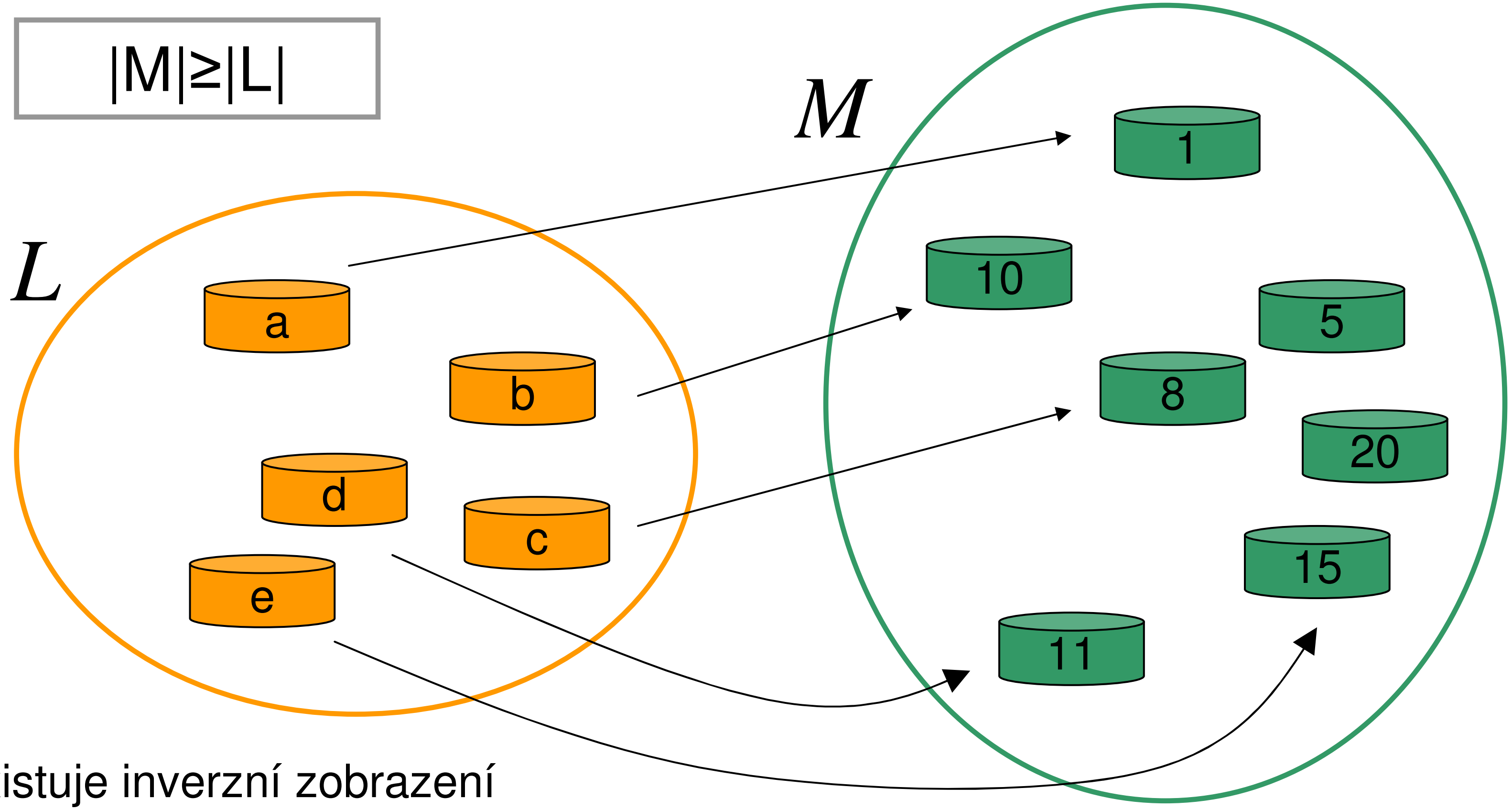
$$Z : L \to M$$

Zobrazení Z je projekcí množiny L do množiny M

Typy zobrazení:

- Injektivní (prosté)
- Surjektivní
- Bijektivní

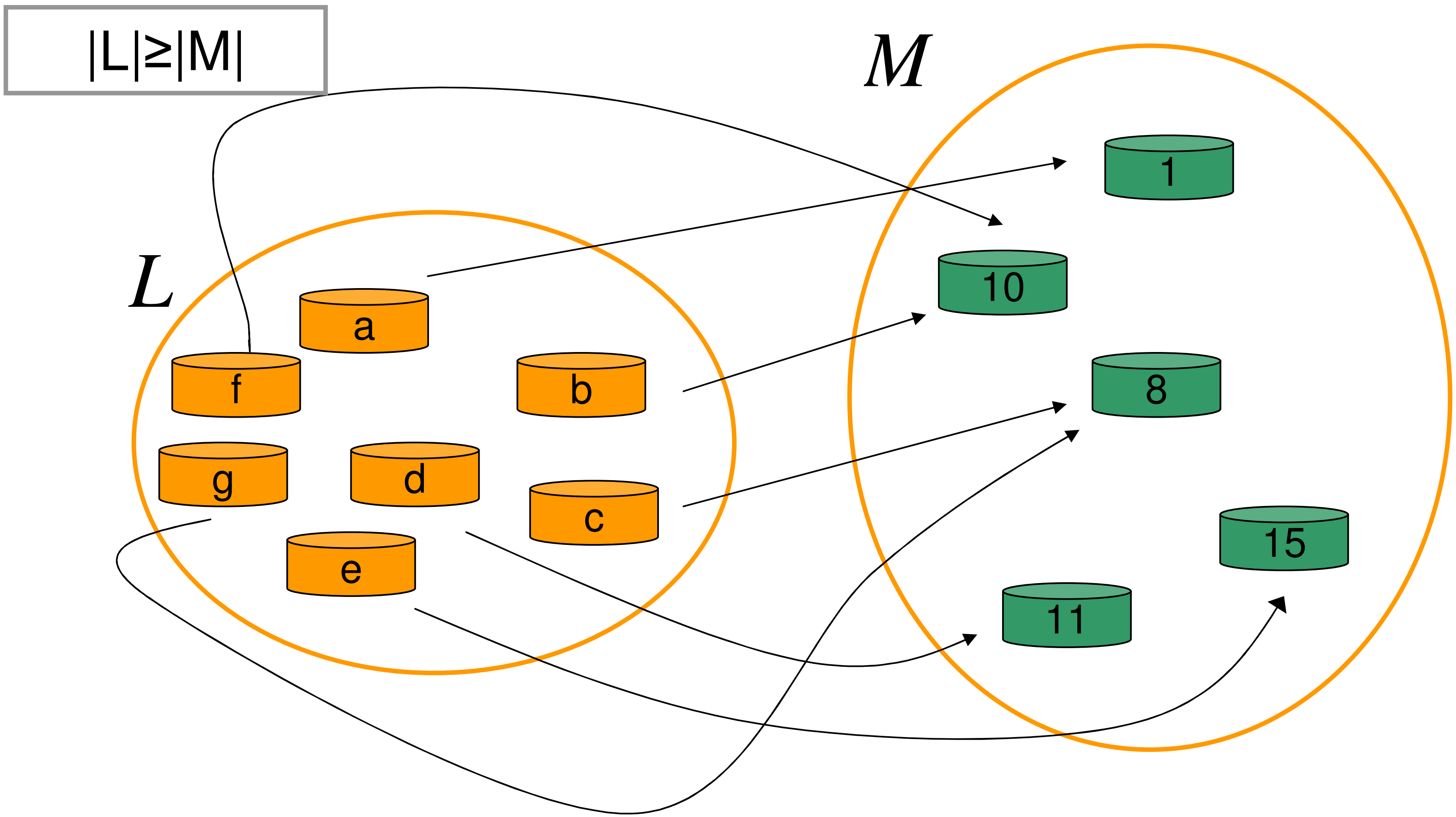
Zobrazení injektivní (prosté)



Existuje inverzní zobrazení

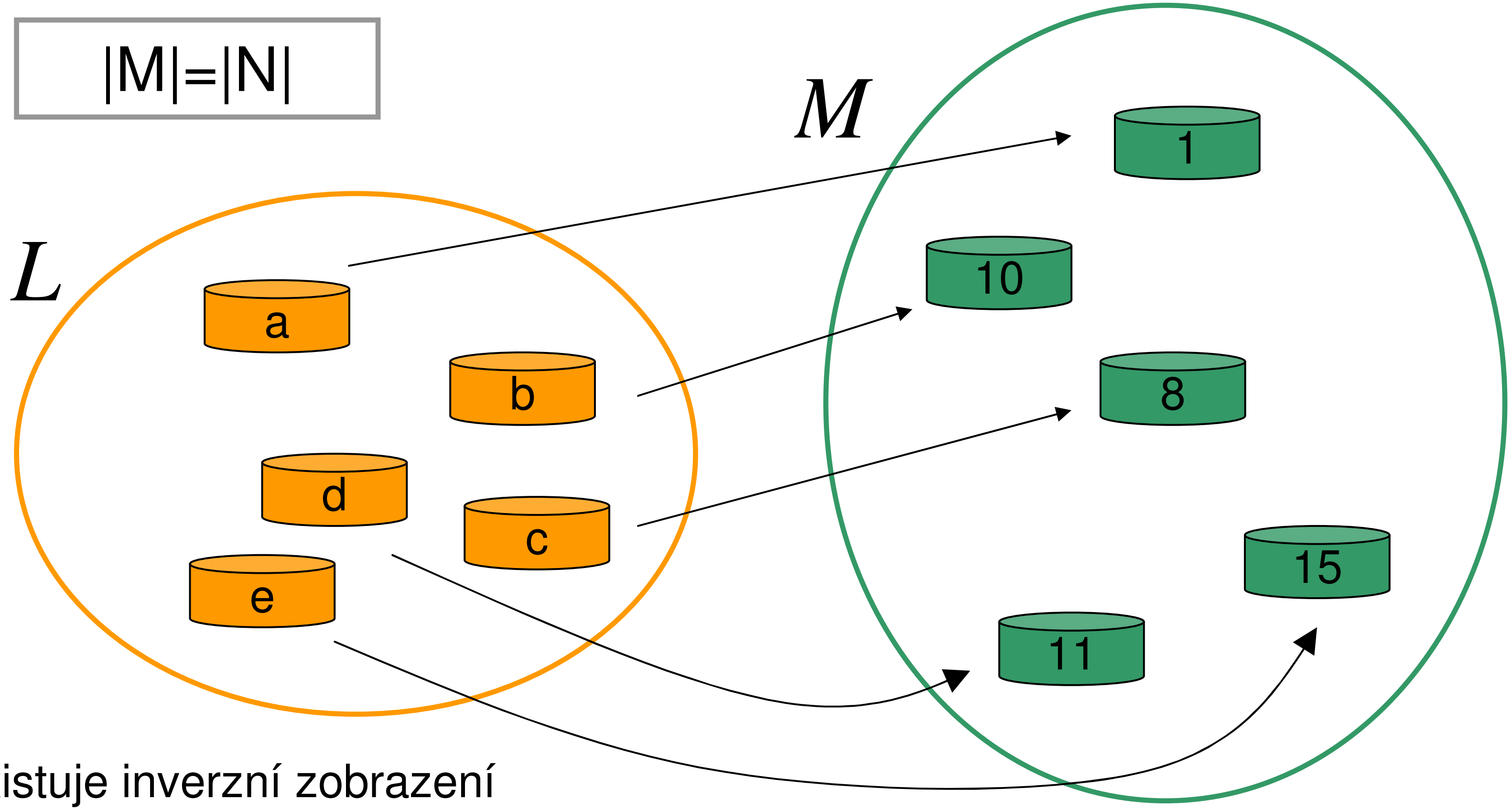
Jeden obraz z M, může mít nejvýše jeden vzor v L.
Různé obrazy musí mít tedy různé vzory.

Zobrazení surjektivní



Zobrazení na množinu, kdy každý obraz z M musí mít alespoň jeden vzor z M. Každý obraz může mít více vzorů.

Zobrazení bijektivní



Existuje inverzní zobrazení

Bijektivní zobrazení je injektivní a zároveň surjektivní. Jde tedy o zobrazení na množinu, které je injektivní. L a M musí mít stejný počet prvků.

Kombinatorika I

Kombinační číslo:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Pascalův trojúhelník

(vyhledejte si v literatuře)

Binomická věta:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Jak souvisí následující vztah s binomickou větou ?

$$(a+b)^2 = a^2 + 2ab + b^2$$

Čemu se rovná

$$(a+b)^3$$

Kombinatorika II

Permutace (bez opakování) z n-prvkové množiny

$$P_e(n) = n!$$

Kombinace k-té třídy z n-prvků bez opakování

$$C_k(n) = \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

$$\boxed{\begin{array}{l}\text{V k-tici nezáleží na pořadí prvků} \\ \text{Například } (1,2,3) = (3,2,1)\end{array}}$$

Kombinace k-té třídy z n-prvků s opakováním

$$C_k^{'}(n) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{(n-1)!\,k!}$$

Kombinatorika III

Variace k-té třídy z n-prvků bez opakování

$$V_k(n) = \binom{n}{k} k! = \frac{n!}{(n-k)!}$$

Záleží na pořadí v n-tici.
Například

$$(1,2,3) \neq (3,2,1)$$

Variace n-té třídy z n prvků bez opakování je permutace z n prvků proto

$$V_n(n) = P_e(n) = n!$$

Variace k-té třídy z n-prvků s opakováním

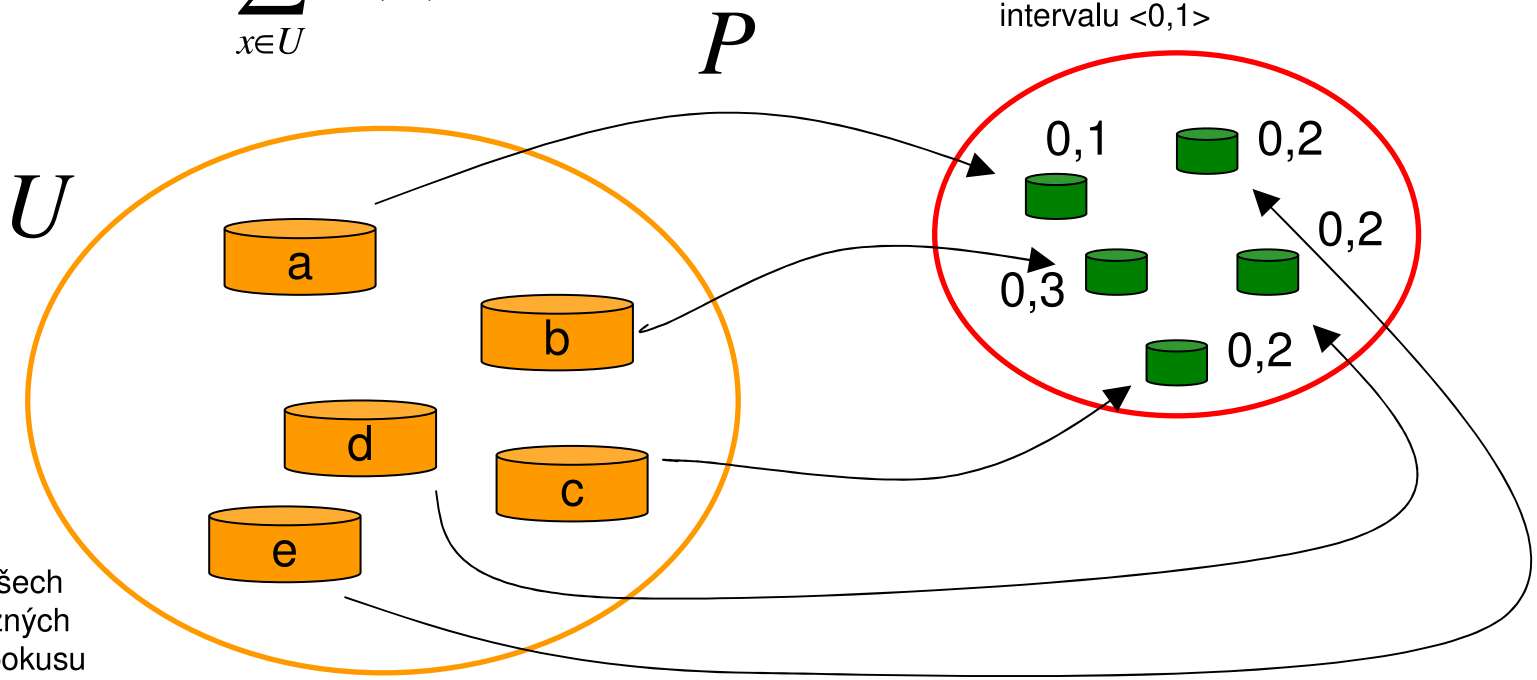
$$V_k^{'}(n) = n^k$$

Záleží na pořadí v n-tici

Konečný pravděpodobnostní prostor

Definice *Konečný pravděpodobnostní prostor je dvojice (U, P), kde U je neprázdná konečná množina a P: U→<0,1> je funkce splňující podmínku* $\sum_{x \in U} P(x) = 1$

Množina všech reálných čísel na intervalu <0,1>

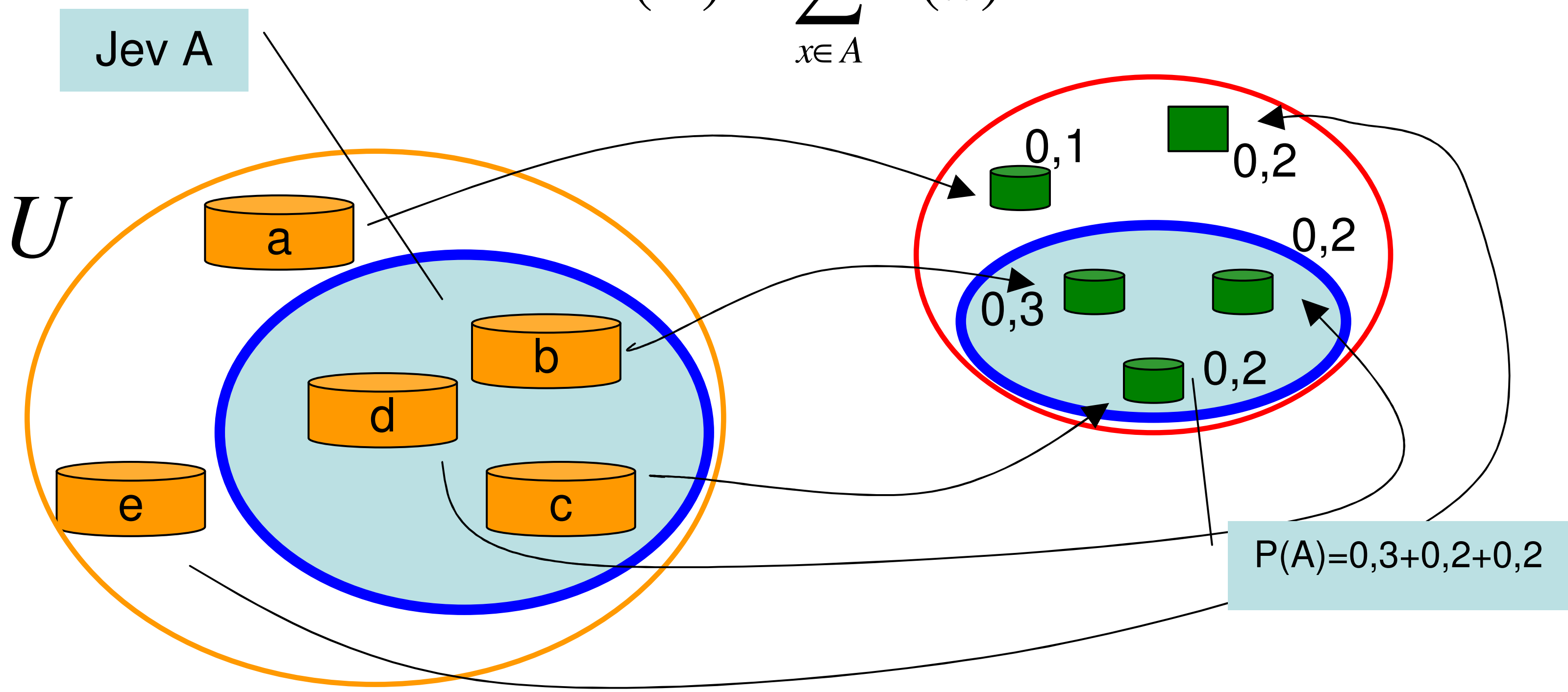


Množina všech
všech možných
výsledků pokusu

Náhodný jev I

Definice Nechť *(U, P) je pravděpodobnostní prostor. Náhodný jev A v prostoru (U,P) je podmnožinou U. Jestliže A je podmnožina U, pak pravděpodobnost jevu A je*

$$P(A) = \sum_{x \in A} P(x)$$



Náhodný jev II

1. Pravděpodobnost jevu A obsahujícího jediný prvek ***s*** se rovná pravděpodobnosti prvku **s**.

$$s \in U \Rightarrow P(\{s\}) = P(s)$$

2. Jev **nemožný** má pravděpodobnost rovnu nule

$$P(\phi) = 0$$

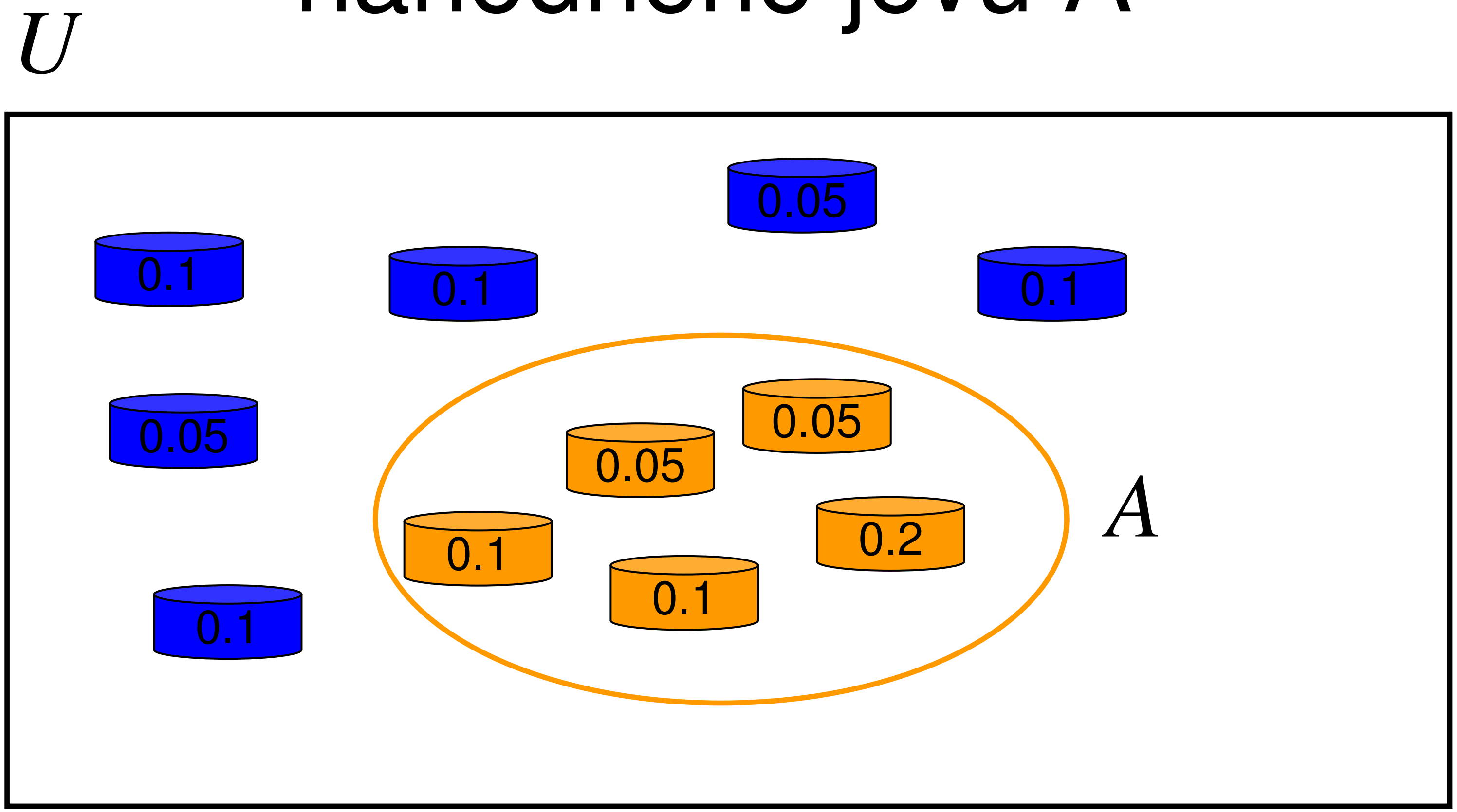
3. Jev **jistý** má pravděpodobnost rovnou jedné

$$P(U) = 1$$

4. Jsou-li všechny prvky v množině U stejně pravděpodobné, pak pravděpodobnost jevu A je podíl mohutnosti množiny A a mohutnosti množiny U.

$$\forall x \in U : P(x) = konst. \Rightarrow \forall A \subseteq U : P(A) = |A| / |U|$$

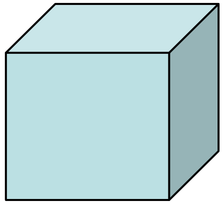
Pravděpodobnost náhodného jevu A



$$P(x \in U) = P(U) = 1; \qquad P(x \in A) = P(A) = 0.5$$

$$P(x \notin A) = P(\overline{A}) = 1 - P(A) = 0.5$$

Hrací kostka I



$$U = \{1,2,3,4,5,6\}$$

$$P(1) = P(2) = P(3) = P(4) = P(5) = P(6) = 1/6$$

Jev A: padne liché číslo

$$A = \{1,3,5\} \qquad P(A) = \frac{|A|}{|U|} = 3/6 = 1/2$$

Jev B: padne číslo menší rovno 2

$$B = \{1,2\} \qquad P(B) = \frac{|B|}{|U|} = 2/6 = 1/3$$

Jev C: padne číslo menší rovno 4

$$C = \{1,2,3,4\} \qquad P(C) = \frac{|C|}{|U|} = 4/6 = 2/3$$

Jev D: padne nějaké číslo

(jev jistý, určitě něco padne)

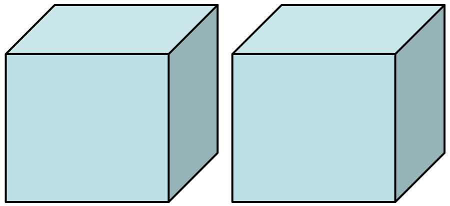
$$P(D) = \frac{|U|}{|U|} = 6/6 = 1$$

Jev E: nepadne žádné číslo

(jev nemožný, určitě něco padne)

$$P(E) = \frac{|\phi|}{|U|} = 0/6 = 0$$

Dvě hrací kostky
(dva hody jednou kostkou)



$$U = \{(1,1),(1,2),\ldots,(2,1),(2,2),\ldots,(6,6)\}$$

$$|U| = n^k = 6^2 = 36$$

Variace s opakováním

$$P((x,y)) = \frac{1}{|U|} = \frac{1}{36}$$

Jev A: padne součet 5

$$P(A) = P((1,4)) + P((4,1)) + P((2,3)) + P((3,2)) = 4/36 = 1/9$$

Jev B: padne součet menší roven 4

$$P(B) = P((1,1)) + P((1,2)) + P((1,3)) + P((2,1)) + P((2,2)) +$$

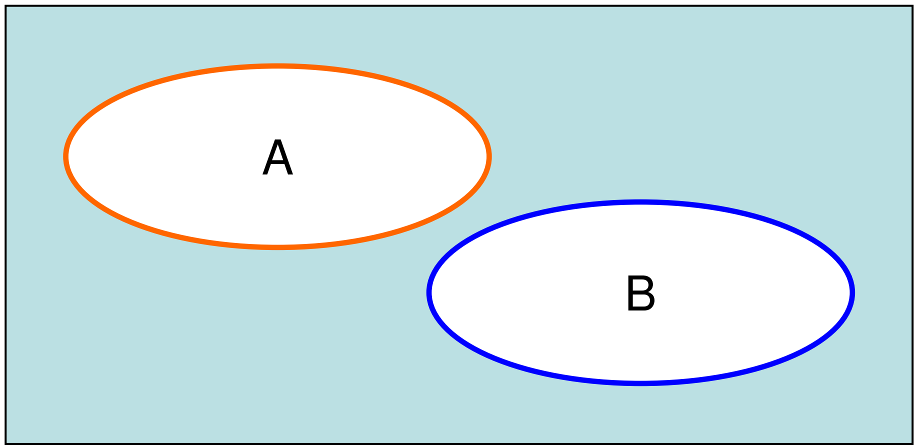
$$+ P((3,1)) = 6/36 = 1/6$$

Neslučitelné jevy

Definice Nechť (U,P) je konečný pravděpodobnostní prostor a A,B jsou dva jevy v tomto prostoru. Jevy A,B jsou neslučitelné tehdy a jen tehdy pokud platí

$$P(A \cap B) = 0$$

V tomto případě jevy (podmnožiny U) jsou disjunktní



Bernouliho pokus

Definice Bernouliho pokus je náhodný pokus, který má pouze dva možné výsledky (ano/ne, správně/chybně, …). V sérii mají jednotlivé realizace Bernouliho pokusu stejnou pravděpodobnost.

Pravděpodobnost k úspěšných výsledků v n nezávislých realizacích náhodného Bernouliho pokusu je

$$P(k,n) = \binom{n}{k} p^k (1-p)^{n-k}$$

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Kde p je pravděpodobnost úspěšného výsledku jednoho Bernouliho pokusu.

Výše uvedený vzorec např. umožňuje spočítat, jaká je pravděpodobnost, že padne 5 hlav, když si 10x hodím korunou.

Užitečné vztahy

Nechť (U,P) je konečný pravděpodobnostní prostor a A, B, C, D jsou náhodné jevy v tomto prostoru. Pak platí

1/ $$A \subseteq B \Rightarrow P(A) \leq P(B)$$

2/ Jestliže A a B jsou neslučitelné jevy a $C \subseteq A$ a $D \subseteq B$, pak C a D jsou také neslučitelné jevy.

3/ Jestliže jevy A_1, A_2, … A_n jsou vzájemně (po dvojicích) neslučitelné, pak platí

$$P(\bigcup_{i=1}^{N} A_i) = \sum_{i=1}^{N} P(A_i)$$

4/ $$A \subseteq B \subseteq U \Rightarrow P(B \setminus A) = P(B) - P(A)$$

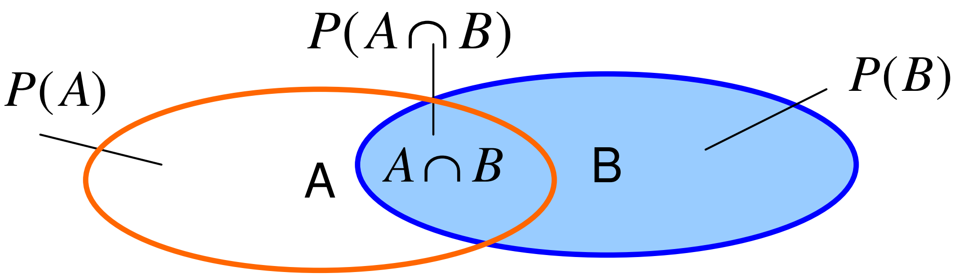
5/ $$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Podmíněná pravděpodobnost

Definice Nechť (U,P) je konečný pravděpodobnostní prostor, A a B jsou podmnožiny U a P(B)≠0. Pravděpodobnost jevu A za podmínky, že nastal jev B je

$$P(A|B)=\frac{P(A\cap B)}{P(B)}$$

$P(A\cap B)$ Je pravděpodobnost, že nastal zároveň jev A i jev B



Nezávislost jevů

Definice Nechť (U,P) je konečný pravděpodobnostní prostor a A, B jsou podmnožiny U. Jevy A a B jsou nezávislé tehdy a jen tehdy

$$P(A \cap B) = P(A)P(B)$$

Důsledky:

$$P(A \mid B) = P(A)$$

$$P(B \mid A) = P(B)$$

Náhodná veličina

Definice Nechť (U,P) je konečný pravděpodobnostní prostor.
Náhodná veličina X na tomto pravděpodobnostním prostoru je funkce z množiny U do množiny reálných čísel R.

Jestliže $X : U \to R$
je náhodná veličina na (U,P), pak očekávaná nebo také střední hodnota náhodné veličiny X je

$$E(X) = \sum_{u \in U} X(u) P(u)$$

Příklad

Vysílač vysílá kódovanou zprávu složenou z písmen z abecedy Σ={a,b,c,d,e}. Každé písmeno vysílá s jinou pravděpodobností a jinou hodnotou vyzářeného výkonu. Hodnoty jsou dány v tabulce. Určete střední hodnotu vyzářeného výkonu při nepřetržitém vysílání.

Písmeno	Pravděpodobnost	Výkon [mW]
a	0,1	1
b	0,5	2
c	0,1	3
d	0,2	4
e	0,1	5

$$U = \Sigma = \{a, b, c, d, e\}$$

$$P : U \to R$$ (označeno červeně)

$$(U, P)$$

$$X : U \to R$$ (označeno zeleně)

$$E(X) = 1 * 0{,}1 + 2 * 0{,}5 + 0{,}1 * 3 + 4 * 0{,}2 + 5 * 0{,}1 = 2{,}7\,\mathrm{mW}$$

Úplný systém jevů

Definice Nechť (U,P) je konečný pravděpodobnostní prostor. Úplný systém jevů je množina N po dvojicích neslučitelných jevů A_i, pro které platí

$$P\left(\bigcup_{i=1}^{N} A_i\right) = 1$$

- všechny jevy A_i jsou vzájemně disjunktní (neslučitelné)
- sjednocením jevů A_i dostaneme jev jistý (tj. pokrývají celou množinu U)

Příklad: U = {1,2,3,4,5,6,7,8,9,10}

Q_1={{1},{2,4,8},{3,9},{5,6,7}{10}}

Q_2={{1,3,5,7,9}, {2,4,6,8,10}}

Q1 a Q2 jsou dva =uplné systémy jevů

Příklad

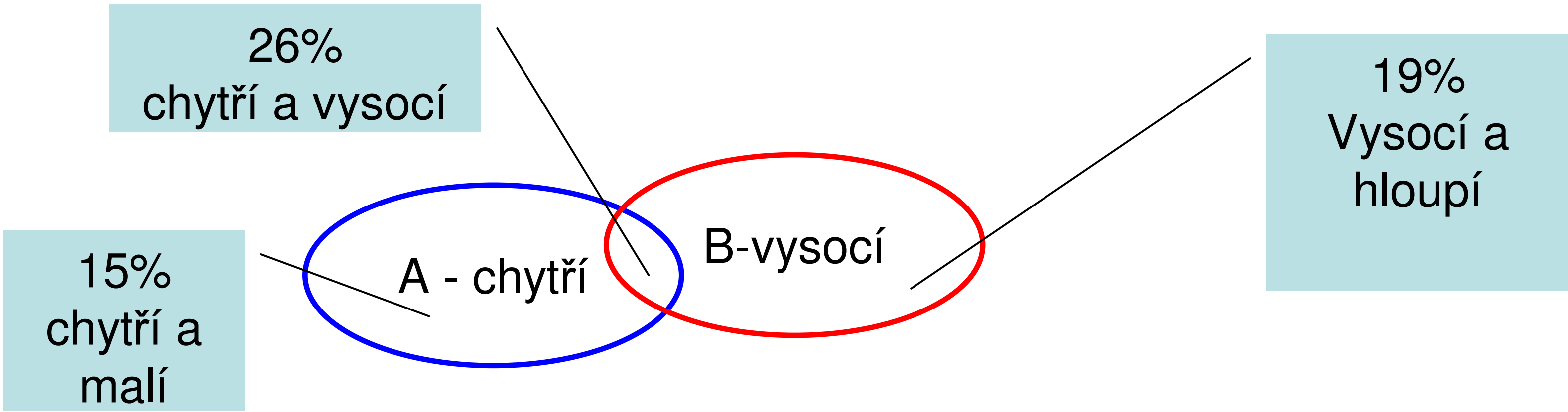
V populaci je 26% lidí chytrých a vysokých. 40% lidí je hloupých a malých a 45% vysokých.

Poznámka: smyšlená data

Určete

1. Kolik procent lidí je chytrých ?
2. Jaká je pravděpodobnost, že potkám chytrého nebo vysokého člověka ?
3. Jaká je pravděpodobnost, že člověk bude chytrý, když vidím, že je vysoký ?
4. Jsou oba jevy neslučitelné ?
5. Jsou jevy nezávislé ? Pokud ne, jak by musely vypadat pravděpodobnosti ?

Příklad



$$P(A \cup B) = 1 - P(\neg A \cap \neg B) = 1 - 0.4 = 0.6\,(60\%)$$

$$P(A) = P(A \cup B) - P(B) + P(A \cup B) = 0.6 - 0.45 + 0.26 = 0.41$$

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{0.26}{0.45} = 0{,}58$$

$$P(A \cap B) = 0.26 \neq P(A)P(B) = 0.45 * 0.41 = 0.18 \text{ jsou tedy závislé}$$

$$\text{pro } P(A \cap B) = 0.26 \wedge \mathrm{P(B)} = 0.45 \wedge \mathrm{P(A)} = 0.26/0.45 = 0{,}58$$

by byly nezávislé

Bayesova věta

$$\boxed{P(A|B) = \frac{P(A)P(B|A)}{P(B)}}$$

Vztah vyplývá z

$$P(A)P(B/A) = P(A \cap B) = P(B)P(A|B)$$

Informace - definice

Nechť (U,P) je konečný pravděpodobnostní prostor. Jestliže A je nějaký jev v tomto prostoru, pak množství informace obsažené v tomto jevu je

$$I(A) = \log(1/P(A)) = -\log(P(A))$$

Na základu logaritmu v principu nezáleží. Základ logaritmu pouze určuje jednotku množství informace. Pro základ logaritmu 2 je množství informace měřeno v bitech, tj.

$$I(A) = \log_2(1/P(A)) = -\log_2(P(A))$$

Informace - příklad

Zpráva je složena z 256 písmen kódovaných čísly v rozsahu 0-255. Všechna písmena ve zprávě jsou stejně pravděpodobná. Spočtěte množství informace, které nese jedno písmeno zprávy. Množství informace uveďte v bitech.

Příklad zprávy: 1,5,5,2,4,3,4,1,3, …

U={0,1,2,3,…, 255}

$$P(x) = \frac{1}{|U|} = \frac{1}{256}, \text{kde } x \in U$$

Srovnejte výsledek s počtem bitů nutných pro zakódování jednoho písmene.

$$I(x) = \log_2(1/P(x)) = \log_2\left(\frac{1}{\frac{1}{256}}\right) = \log_2(256) = 8 \text{ bitů}$$

Podmíněná informace

Nechť (U,P) je konečný pravděpodobnostní prostor. Jestliže A a B jsou jevy v tomto prostoru a P(B)>0, pak podmíněná informace, která je podmíněná jevem B, je dána

$$I(A \mid B) = -\log(P(A \mid B)) = -\log(\frac{P(A \cap B)}{P(B)})$$

$$\boxed{\text{Pro } P(A \cap B) = 0 \text{ je } I(A \mid B) = \infty}$$

Obdobně lze psát

$$I(B \mid A) = -\log(P(B \mid A)) = -\log(\frac{P(A \cap B)}{P(A)})$$

Sdružená informace

Nechť (U,P) je konečný pravděpodobnostní prostor. Jestliže A a B jsou jevy v tomto prostoru, pak sdružená informace je dána

$$I(A,B) = -\log(P(A \cap B))$$

Pro dva nezávislé jevy, pro které platí $P(A \cap B) = P(A)P(B)$

je sdružená informace dána

$$I(A,B) = -\log(P(A)P(B)) = I(A) + I(B)$$

Sdružená informace je informace, kterou nese výsledek experimentu, ve které nastanou oba jevy A a B současně

Vzájemná informace

Nechť (U,P) je konečný pravděpodobnostní prostor. Jestliže A a B jsou jevy v tomto prostoru a P(A)>0 a P(B)>0, pak vzájemná informace je dána

$$I_m(A,B) = \log\left(\frac{P(A \cap B)}{P(A)P(B)}\right)$$

Pro dva nezávislé jevy A, B, kdy $P(A \cap B) = P(A)P(B)$,
je $I_m(A,B) = 0$

Vzájemná informace je informace, která spojuje jevy A a B

Entropie informace

Definice Nechť (U,P) je konečný pravděpodobnostní prostor a A_1, A_2, … A_N jsou podmnožiny U. Jestliže A1, A2, … A_N jsou náhodné jevy na U, pak průměrné množství informace připadající na jeden jev A_i je

$$H(A_1, A_2, ..., A_N) = \sum_{i=1}^{n} P(A_i) I(A_i) =$$

$$= -\sum_{i=1}^{n} P(A_i) \log P(A_i)$$

Vzájemná informace na úplných jevových systémech

Definice Nechť α, β jsou dva úplné systémy jevů v konečném pravděpodobnostním prostoru (U,P). Vzájemná informace mezi těmito systémy jevů je definována vztahem

$$I(\alpha,\beta) = \sum_{i\in I}\sum_{j\in J} P(A_i \cap B_j) I(A_i, B_j) =$$

$$= \sum_{i\in I}\sum_{j\in J} P(A_i \cap B_j) \log \frac{P(A_i \cap B_j)}{P(A_i)P(B_j)}$$

$$\text{kde } A_i \in \alpha, B_i \in \beta$$

Diskrétní bezpaměťový kanál

Pravděpodonostní model přenosového kanálu

Vstupní abeceda

$$A = \{0,1\}$$

$$A = \{0,1\}$$

$$A = \{00,01,10,11\}$$

Výstupní abeceda

$$B = \{0,1\}$$

$$B = \{0,1,*\}$$

$$B = \{0,1,00,01,10,11,0*,1*,*0,*1\}$$

Přenosové pravděpodobnosti

Binární symetrický kanál

$$A = \{0{,}1\} \qquad B = \{0{,}1\}$$

A je vstupní a B je výstupní abeceda

Matice přenosových pravděpodobností

$$Q = \begin{bmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{bmatrix} = \begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix}$$

Pravděpodobnost k chyb v přenesených datech o délce n je $P(k,n) = \binom{n}{k} p^{n-k}(1-p)^k$

a průměrný počet chyb $n(1-p)$

Přenosové pravděpodobnosti

Obecný kanál

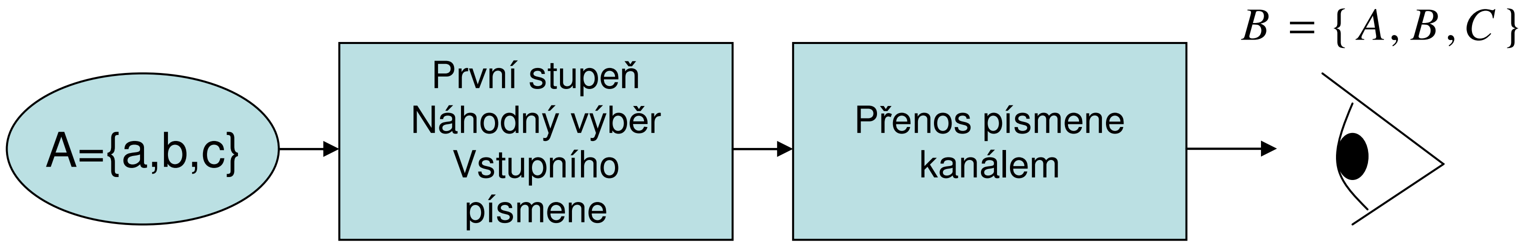
$$A = \{a, b, c\} \qquad B = \{A, B, C\}$$

A je vstupní a B je výstupní abeceda

Matice přenosových pravděpodobností

$$Q = \begin{bmatrix} q_{aA} & q_{aB} & q_{aC} \\ q_{bA} & q_{bB} & q_{bC} \\ q_{cA} & q_{cB} & q_{cC} \end{bmatrix} = \begin{bmatrix} 0.8 & 0.1 & 0.1 \\ 0.2 & 0.7 & 0.1 \\ 0.05 & 0.05 & 0.9 \end{bmatrix}$$

Vstupní písmena s různými četnostmi výskytu



a_i	$P(a_i)=p_i$
a	0.1
b	0.3
c	0.6

$$Q = \begin{bmatrix} q_{aA} & q_{aB} & q_{aC} \\ q_{bA} & q_{bB} & q_{bC} \\ q_{cA} & q_{cB} & q_{cC} \end{bmatrix} = \begin{bmatrix} 0.8 & 0.1 & 0.1 \\ 0.2 & 0.7 & 0.1 \\ 0.05 & 0.05 & 0.9 \end{bmatrix}$$

$$P(b_j \mid a_i) = q_{ij}$$

$$P(b_j, a_i) = P(a_i \cap b_j) = p_i q_{ij}$$

$$P(b_j) = \sum_{i=1}^{n} p_i q_{ij}$$

b_j	$P(b_j)=\Sigma p_i\, q_{ij}$
A	0.17
B	0.25
C	0.58

Kapacita kanálu

Věta Nechť A={a_1,a_2,…,a_n} je vstupní abeceda a B={b_1,b_2,…,b_k} je výstupní abeceda a q_{ij}, kde i={1,2,..n} a j={1,2,…,k}, je přenosová matice. Pravděpodobnosti p_1, p_2, …, p_n jsou optimální vstupní pravděpodobnosti tehdy a jen tehdy, když pro nějaké C splňují

$$\sum_{i=1}^{n} p_i = 1 \wedge \sum_{j=1}^{k} q_{ij} \log \frac{q_{sj}}{\sum_{t=1}^{n} p_t q_{tj}} = C, \forall s \in \{1,2,\ldots,n\}$$

C je kapacita kanálu

Kapacita binárního symetrického kanálu

$$Q = \begin{bmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{bmatrix} = \begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix}$$

Vstupní pravděpodobnosti p_0 a p_1

Pro p=1/2, lze odvodit, že I(A,B)=0, že kanál nepřenese žádnou informaci.

Pro p≠1/2 a p0=p1=1/2 lze odvodit, že

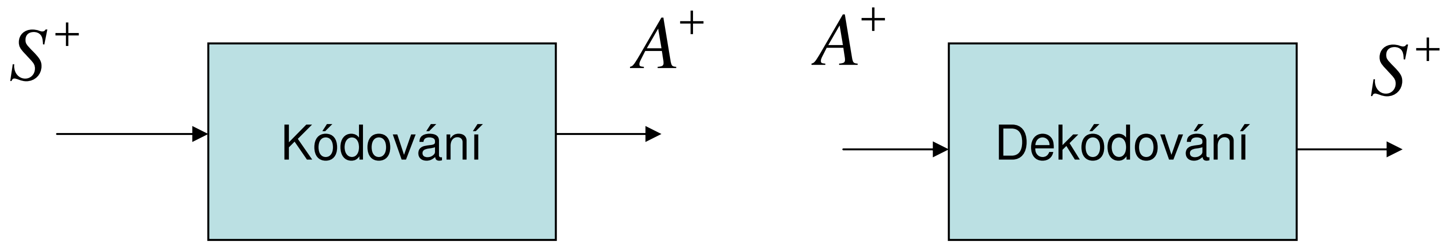
$$C = p \log 2p + (1-p) \log 2(1-p)$$

Kódování

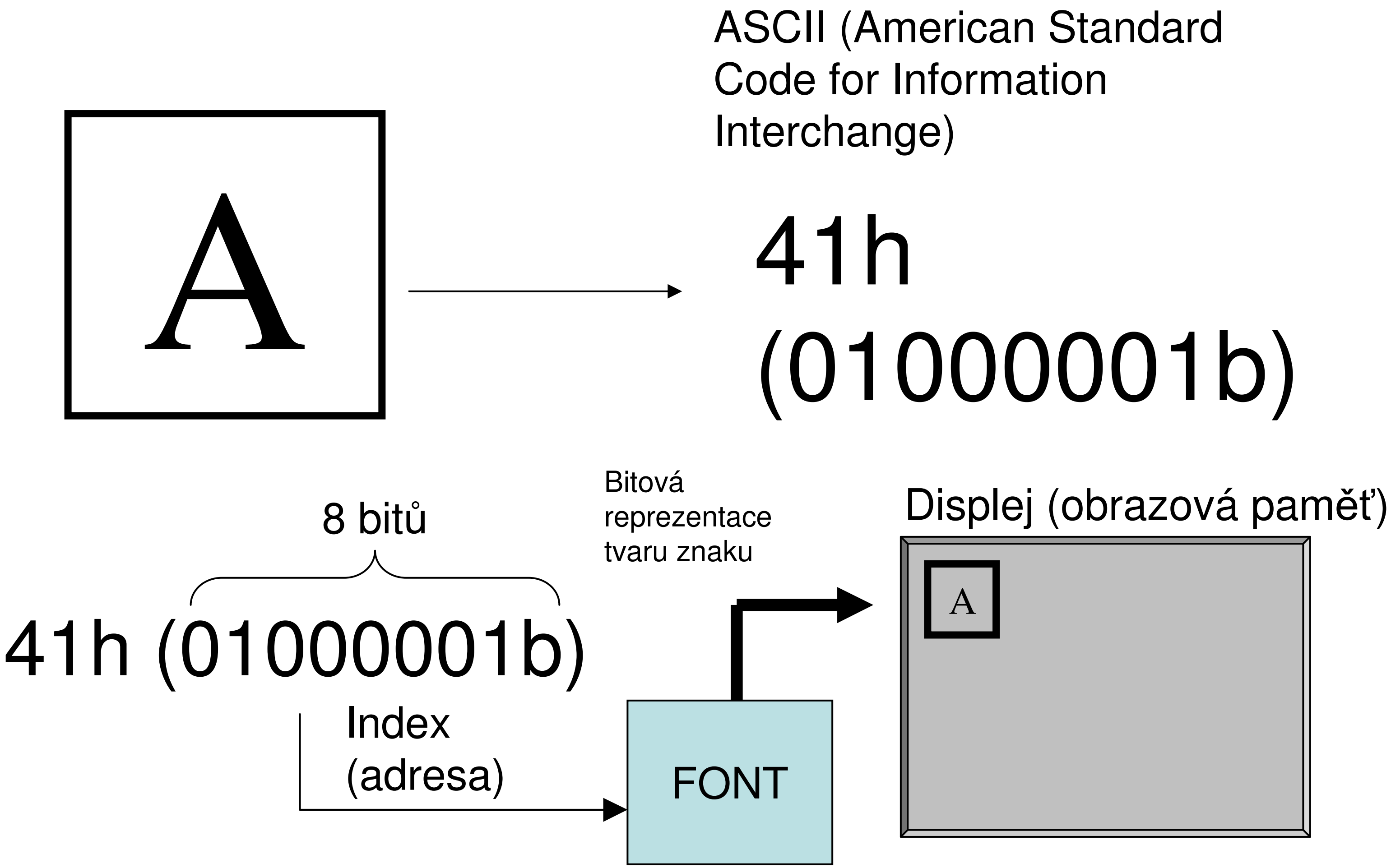
Nahrazení jedné abecedy jinou abecedou (kódovou abecedou)

Definice Kódovací funkce je zobrazení $\phi : S^+ \rightarrow A^+$

- Jednoznačné (zobrazení musí být injektivní)
- Nejednoznačné



Kódování znaků



ASCII tabulka

Bits				b_7 b_6 b_5	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b_4 ↓	b_3 ↓	b_2 ↓	b_1 ↓	Column → / Row ↓	0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	@	P	`	p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	#	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
1	0	0	0	8	BS	CAN	(	8	H	X	h	x
1	0	0	1	9	HT	EM	)	9	I	Y	i	y
1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
1	0	1	1	11	VT	ESC	+	;	K	[	k	{
1	1	0	0	12	FF	FC	,	<	L	\	l	|
1	1	0	1	13	CR	GS	-	=	M	]	m	}
1	1	1	0	14	SO	RS	.	>	N	^	n	~
1	1	1	1	15	SI	US	/	?	O	_	o	DEL

Zdroj: http://en.wikipedia.org/wiki/File:ASCII_Code_Chart-Quick_ref_card.png

Koduje znaky do 7 bitů (0-127). Nezohledňuje diakritiku.

Jiná kódování

- ISO8859-1 (8bitů, západoevropské jazyky)
- ISO8859-2 (8bitů, středoevropské jazyky)
- CP1250 (8bitů, windows)
- UNICODE
  - UTF7
  - UTF8 (úsporný)
  - UTF16 (16 bitů, nejpoužívanější)
  - UTF32 (32 bitů)

Zápis čísel - historie

Zářezy na holi - II (2), IIII (4), ~~IIII~~ (5), ~~IIII~~ III (8)

Římské číslice - I(1), V(5), X(10), L(50), C(100), D(500), M(1000)

Příklady: II (2), IV (4), IX (9), CCLXI (256), MMXII (2012),

Problematické počítání, pomůcka abakus (počítadlo)

Poziční soustavy - 123_{10} (sto dvacet tři), 1110_2 (14)

Arabské číslice

Problém nuly, dlouho neřešen, bez nuly náchylné na chybné čtení čísla

Poziční soustavy I

Číslo v poziční soustavě z-adické soustavě

$$A_z = (a_n a_{n-1} \ldots a_1 a_0 , a_{-1} + \ldots a_{-m})_z ; a_i , n, m \in N$$

Binární čáka (nebo tečka)

Příklady: $(11345)_{10}$, $(1100.011)_2$, $(ABCD.1234)_{16}$

$$A_z = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z^1 + a_0 + a_{-1} z^{-1} + \ldots a_m z^m =$$

$$= \sum_{i=0}^{n} a_i z^i + \sum_{i=1}^{m} a_{-i} z^{-i} = \sum_{i=-m}^{n} a_i z^i$$

a_i je z-adická číslice
z je základ soustavy
n je nevyšší řád s nenulovou číslicí-m
je nejnižší řád s nenulovou číslicí

Dvojková (binární) soustava

$z = 2$

Mocnina	Hodnota
2^{-2}	0,25
2^{-1}	0,5
2^{0}	1
2^{1}	2
2^{2}	4
2^{3}	8
2^{4}	16
2^{5}	32
2^{6}	64
2^{7}	128
2^{8}	256

Mocnina	Hodnota
2^{9}	512
2^{10}	1024 (1Ki)
2^{11}	2048
2^{12}	4096
2^{13}	8192
2^{14}	16384
2^{15}	32768
2^{16}	65536 (64Ki)
2^{20}	1024^{2} (1 Mi)
2^{30}	1024^{3} (1 Gi)
2^{40}	1024^{4} (1 Ti)

$A = 1001101_2$

$$A = 1.2^6 + 0.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0 = 64 + 8 + 4 + 1 = 77$$

Ki (kibi)
Mi (mebi)
Gi (gibi)

Příklady

Převeďte

$101110111_2 \rightarrow ??_{10}$

$111101101_2 \rightarrow ??_{10}$

$101_2 \rightarrow ??_{10}$

$58_{10} \rightarrow ??_2$

$101_{10} \rightarrow ??_2$

Algoritmus převodu desítková→dvojková
čísla celá kladná

z (základ cílové číselné soustavy)

```
156 : 2 = 78        zbytek → 0 nejnižší řád (LSB)
 78 : 2 = 39        zbytek → 0
 39 : 2 = 19        zbytek → 1
 19 : 2 = 9         zbytek → 1
  9 : 2 = 4         zbytek → 1
  4 : 2 = 2         zbytek → 0
  2 : 2 = 1         zbytek → 0
  1 : 2 = 0         zbytek → 1 nejvyšší řád (MSB)
```

$$156_{10} \rightarrow 10011100_2$$

Poznámka: ***Algoritmus je platný i pro převod do jiných číselných soustav***

Algoritmus převodu desítková→dvojková

zlomková část v intervalu <0,1)

```
0,375 * 2 = 0,75  celá část → 0 nejvyšší řád (2⁻¹)
0,75  * 2 = 1,5   celá část → 1

0,5   * 2 = 1     celá část → 1 nejnižší řád (2⁻³)
```

$$0{,}375_{10} \rightarrow 0{,}011_2$$

Poznámka: ***Algoritmus je platný i pro převod do jiných číselných soustav***

Sčítání čísel ve dvojkové soustavě

Součet

a/b	0	1
0	0	1
1	1	10

Přenos do vyššího řádu

$$
\begin{array}{r}
10011101_2 \\
10110001_2 \\
\hline
101001110_2
\end{array}
$$

Přenos do vyššího řádu

Násobení čísel ve dvojkové soustavě

Součin

a/b	0	1
0	0	0
1	0	1

Používáme stejný algoritmus, který nás naučili na základní škole pro desítkovou soustavu

$$
\begin{array}{r}
1001_2 \\
110_2 \\
\hline
0000 \\
1001 \\
1001 \\
\hline
110110_2
\end{array}
$$

Dělení čísel ve dvojkové soustavě

$$
\begin{array}{l}
10101_2 : 110_2 = 011_2 \\
1010 \\
\underline{-110} \\
1001 \\
\underline{-110} \\
011
\end{array}
$$

Používáme stejný algoritmus, který nás naučili na základní škole pro desítkovou soustavu.

Všimněte si, že je snazší uhodnout, kolikrát se dělitel vejde do dělence (buď se vejde, nebo ne). V desítkové soustavě musíme ještě uhodnout, kolikrát (např. osmkrát).

Algoritmus převodu dvojková → desítková
čísla celá kladná

Princip je shodný s převodem z desítkové do dvojkové soustavy, ale operace je nutno provádět ve dvojkové soustavě.

```
10011011101 : 1010 = 1111100   zbytek → 101  (5)
    1111100 : 1010 = 1100      zbytek → 100  (4)
       1100 : 1010 = 1         zbytek →  10  (2)
          1 : 1010 = 0         zbytek →   1  (1)
```

Algoritmus převodu desítková→dvojková
zlomková část v intervalu <0,1)

Princip je shodný s převodem z desítkové do dvojkové soustavy, ale operace je nutno provádět ve dvojkové soustavě.

```
0,0011010011 * 1010 =   10,0000111110 celá část → 10   (2)
0,0000111110 * 1010 =    0,1001101100 celá část →  0   (0)
0,1001101100 * 1010 =  110,0000111000 celá část → 110  (6)
0,0000111000 * 1010 =    0,1000110000 celá část →    0 (0)
0,1000110000 * 1010 =  101,0111100000 celá část → 101  (5)
0,0111100000 * 1010 =  100,1011000000 celá část → 100  (4)
0,1011000000 * 1010 =  110,1110000000 celá část → 110  (6)
0,1110000000 * 1010 = 1000,1100000000 celá část → 110  (8)
0,1100000000 * 1010 =  111,1000000000 celá část → 111  (7)
0,1000000000 * 1010 =  101,0000000000 celá část → 101  (5)
```

$$0{,}0011010011_2 \rightarrow 0{,}2060546875_{10}$$

Šestnáctková soustava

$$z = 16$$

Tuto tabulku budete znát zpaměti

Dekadicky	Binárně	Hexadecimálně
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7

Dekadicky	Binárně	Hexadecimálně
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

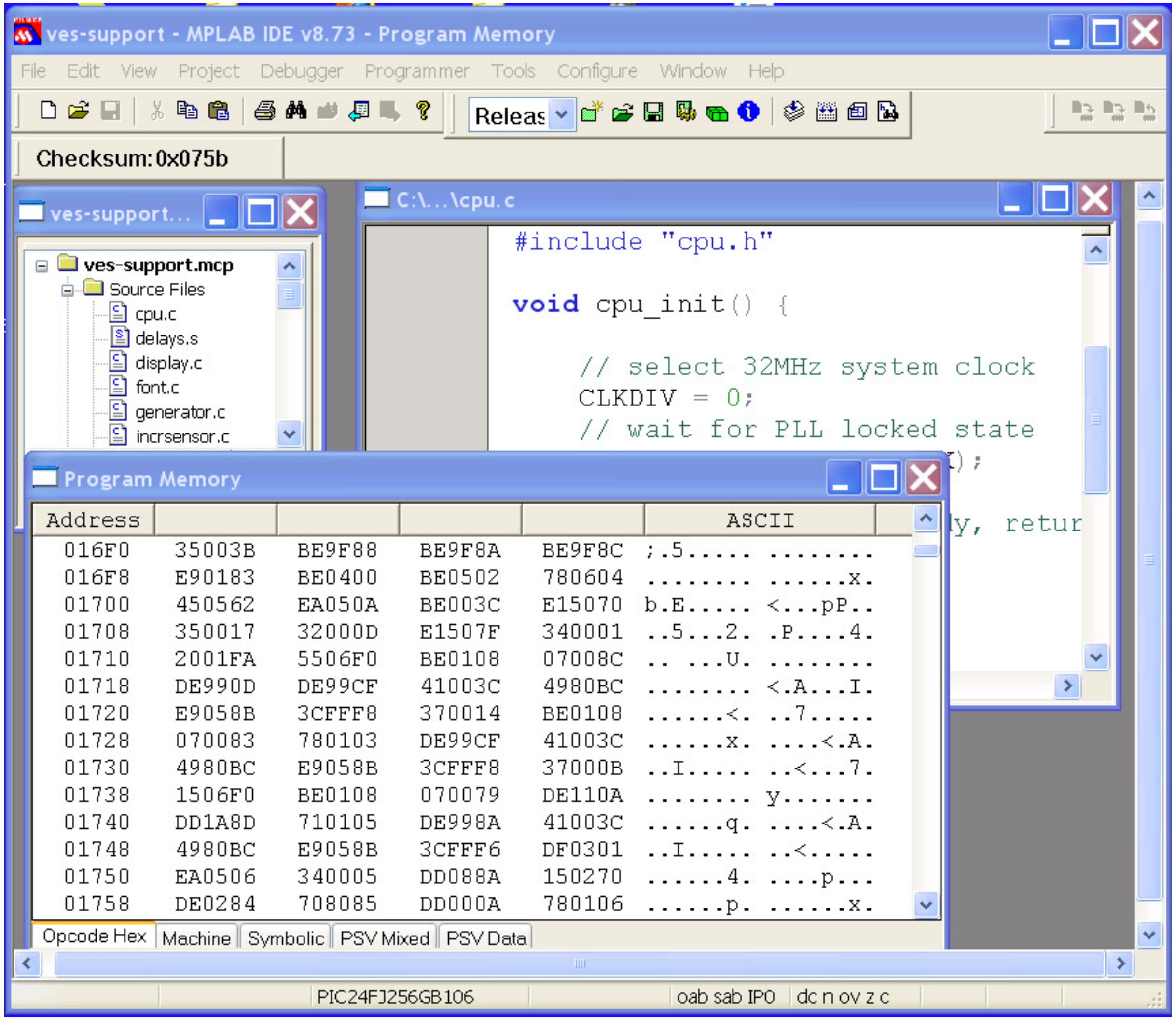
Příklady

$$11_{16} = 1.16^1 + 1.16^0 = 17_{10}$$

$$FF_{16} = 15.16^1 + 15.16^0 = 255_{10}$$

$$A5_{16} = 10.16^1 + 5.16^0 = 165_{10}$$

Výpis paměti v šestnáctkové soustavě – současný vývojový nástroj mikrokontroléry



Příbuzné soustavy

Příbuzné číselné soustavy jsou takové soustavy, kde základ jedné soustavy je mocninou základu druhé soustavy.

Příklady

z=10, z=100, z=1000, …

z=3, z=9, z=27, …

z=2, z=4, z=8, z=16, …

Převod je snadný, ukážeme si to mezi dvojkovou a šestnáctkovou soustavou:

```
1011|0001|0010|1010|0010|₂
  B |  1 |  2 |  A |   2|₁₆
```

Číslo ve dvojkové soustavě rozdělíme na skupiny po čtyřech číslicích a čtveřice převedeme na hexadecimální číslice. Pro opačný převod pouze zapíšeme hexadecimální číslice binárně. U čtyřkové soustavy vytváříme dvojice a u osmičkové trojice.

Příklady

Převeďte

$1010001001010100101010_2 \rightarrow ??_{16}$

$1010101001111101101010_2 \rightarrow ??_8$

$1010101001000101101010_2 \rightarrow ??_4$

$A1B2C3D4E5F6_{16} \rightarrow ??_2$

$347345767337_8 \rightarrow ??_2$

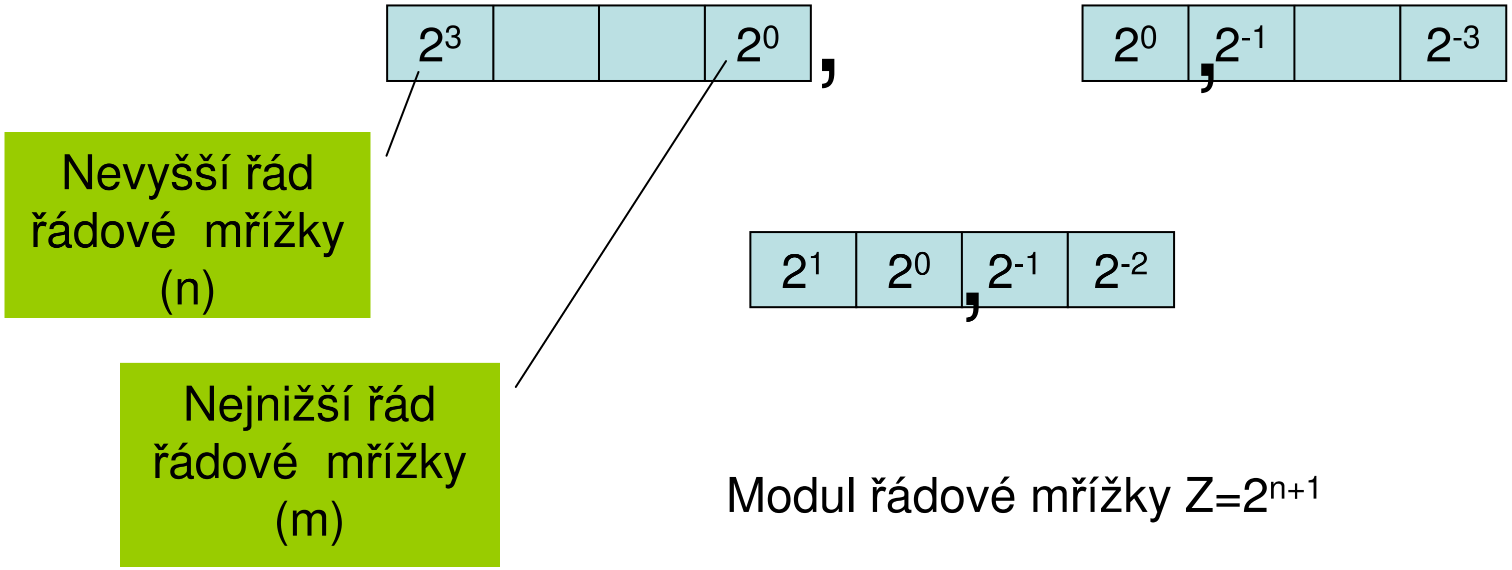
$13222302110_4 \rightarrow ??_2$

Racionální čísla v různých soustavách

- Racionální čísla mohou mít v dané soustavě nekonečný rozvoj (skupiny číslic se ve zlomkové části periodicky opakují). Například 1/3=0.3333…
- Má-li číslo v dané soustavě nekonečný rozvoj, pak v jiné může mít rozvoj konečný. 1/3 ve trojkové soustavě je $0{,}1_3$.

Řádová mřížka

Z důvodu omezení při zobrazení čísel (např. na rozsah 1 bytu) se v počítači zavádí pojem řádová mřížka, která popisuje formát zobrazených čísel.



Modul řádové mřížky $Z=2^{n+1}$

Zobrazení (kódování) záporných čísel

V paměti počítače lze uložit pouze kladná celá čísla. Např. v paměti (nebo registru) o velikosti 1 byte (8 bitů) lze uložit jedno číslo z intervalu <0,255>.

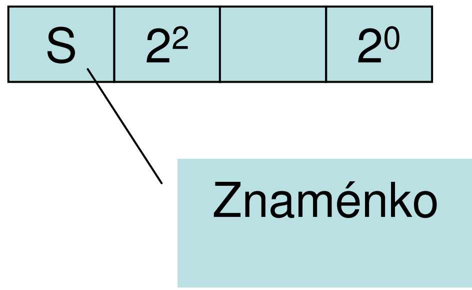
Záporná čísla se musí tedy mapovat (kódovat, zobrazovat) na kladná celá čísla vhodným typem zobrazení.

Používaná zobrazení (kódy)

- Doplňkový kód (veškeré celočíselné typy)
- Přímý kód (mantisa čísel s pohyblivou řádovou čárkou)
- Aditivní kód (exponent čísel s pohyblivou řádovou čárkou)

Doplňkový kód

$$D(x) = \begin{cases} x & 0 \leq x \leq Z/2-1 \\ Z-x & Z/2-1 \leq x < 0 \end{cases}$$



Kde Z je modul řádové mřížky 2^{n+1}.

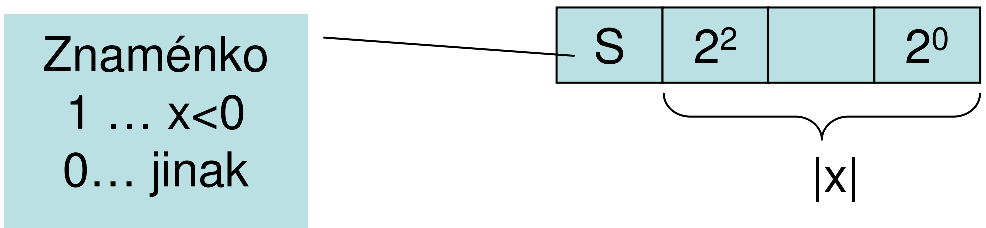
Příklad 1 byte (8 bitů) $Z=2^8=256$

x	**D(x)**	**x**	**D(x)**
0	**0**	**-1**	**255**
1	**1**	**-2**	**254**
…		**…**	
127	**127**	**-127**	**129**
		-128	**128**

Přímý kód

$$P(x) = \begin{cases} x & 0 \le x \le 2^n - 1 \\ 2^n - x & -2^n + 1 \le x < 0 \end{cases}$$

n je nejvyšší řád řádové mřížky



V přímém kódu existují dvě nuly (kladná a záporná). Rozsah pro osmibitové číslo se znaménkem je tedy <-127,127>

Aditivní kód

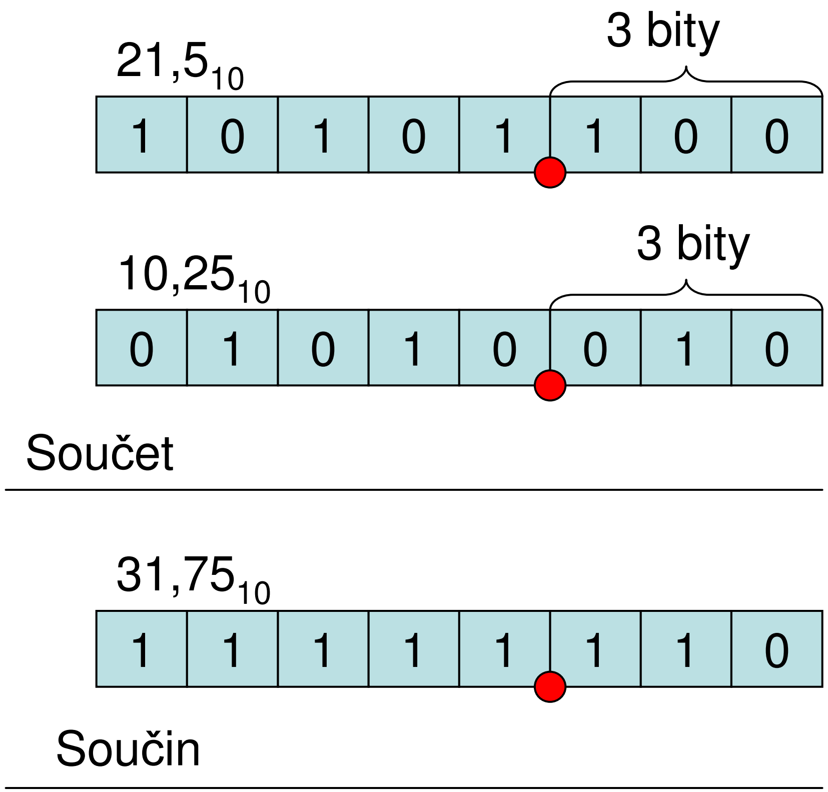
$$A(x) = x + K$$

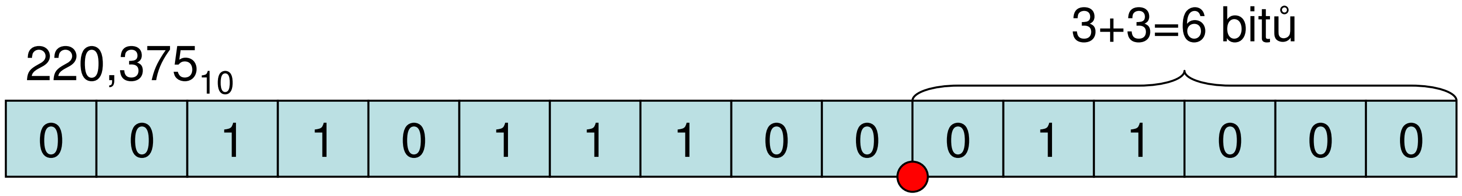
Typicky K = Z/2 (polovina modulu řádové mřížky)

Pro Z=16 je typicky K=8

x	A(x)	x	A(x)
0	8	-1	7
1	9	-2	6
…		…	
7	15	-8	0

Čísla v pevné řádové čárce





Součet při výpočtu nevyžaduje žádných změn oproti součtu celých čísel.

U součinu je nutné po vynásobení obou čísel jako celých čísel provést výsledný posun řádové čárky vpravo o počet míst rovnající se **součtu bitů** ve zlomkové části operandů.

Připomeňme se ještě, že součin operandů délky n a m bitů dává výsledek délky m+n bitů.

Čísla v plovoucí řádové čárce

Exponent

$$A = m.z^{e}$$

Základ číselné soustavy

Mantisa

Známe z desítkové soustavy

$$A = 3{,}25.10^{3}$$

Počítačově zapsáno
A=3.25E3

Ve dvojkové soustavě

$$B = 1{,}11_{2}.2^{3} = 14_{10}$$

Reprezentace čísel dle normy IEEE754

Binary32 (float) jednoduchá přesnost (single precision)

znaménko exponent mantisa

A

0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0

mantisa

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Exponent – aditivní kód K=127

Mantisa v rozsahu (-2,2), jednička (1, …) v normalizovaném tvaru vždy přítomna, nevyjadřuje se, proto se jí říká skrytá jednička.

$$A = 1{,}75.2^{1} = 3{,}5$$

Binary64 (double) dvojitá přesnost – 11 bitů exponent - aditivní kód K=1023, 52 bitů mantisa, 1 bit znaménko

Grayův kód

Je kódem, kde mezi dvěma po sobě jdoucími kódovými slovy dochází pouze ke změně v jednom bitu.

Číslo	Binární	Grayův
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111
6	110	101
7	111	100

Grayúv kód se používá například v optických snímačích polohy nebo pro implementaci asynchronních konečných automatů.

Nadbytečnost (redundance) kódu pro slova stejné délky

$$K(A^m, B^n) = \frac{|B^n| - |A^m|}{|B^n|}$$

Kde A^m je množina slov délky m generovaných zdrojem a B^n je množina kódových slov, kterými po dobu přenosu slova A^m nahrazujeme.

$|B^n| = |A^m|$, tj mohutnosti obou množin jsou stejné, pak je nadbytečnost nulová.

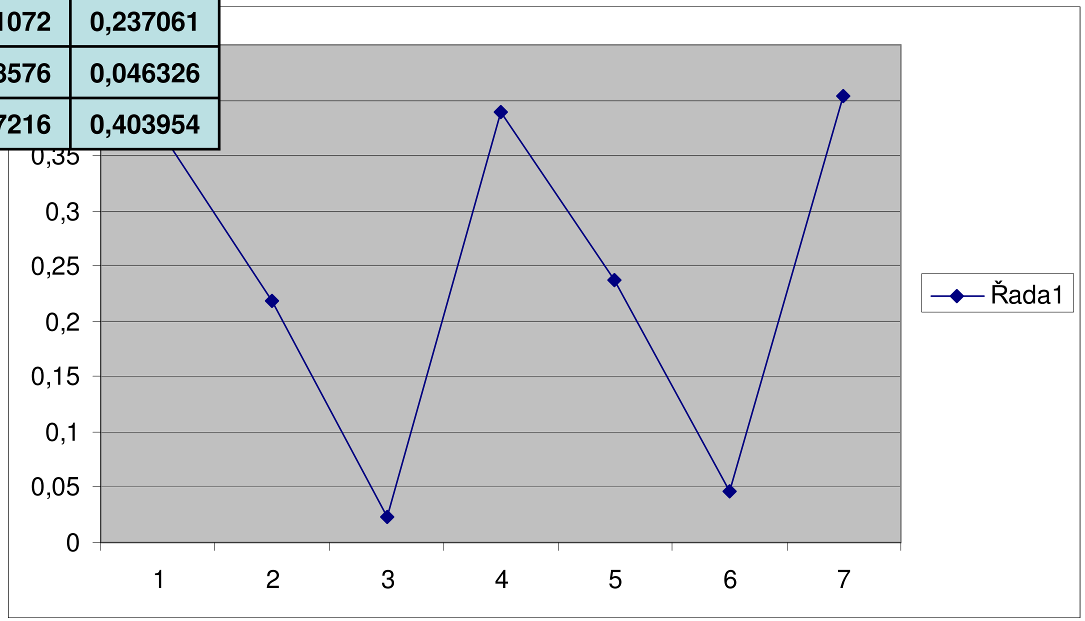
$|B^n| > |A^m|$ počet kódových slov je větší, pak je nadbytečnost větší než nula.

$|B^n| >> |A^m|$ počet kódových slov je mnohem větší, pak se nadbytečnost blíží jedné. Tento případ nemá praktický smysl.

| Bn | < |Am| počet kódových slov je menší, nemá smysl, kódování je nejednoznačné, dochází ke ztrátě informace.

Příklad kódování slov dané délky v binárním kódu

m	n	$\|A^m\|$	$\|B^n\|$	K
1	4	10	16	0,375
2	7	100	128	0,21875
3	10	1000	1024	0,023438
4	14	10000	16384	0,389648
5	17	100000	131072	0,237061
6	20	1000000	1048576	0,046326
7	24	10000000	16777216	0,403954



$|A|=10$

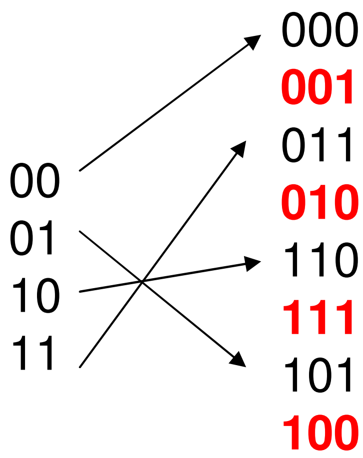
$|B|=2$

Jedná se vlastně o kódování čísel v desítkové soustavě čísly ve dvojkové soustavě

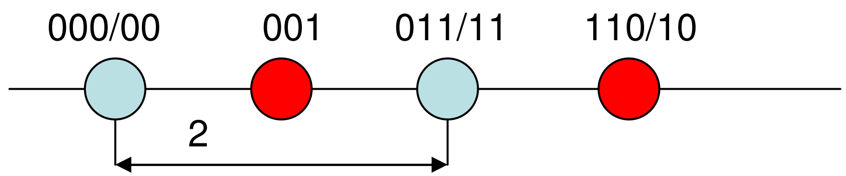
Redundance

- Nenulová redundance znamená v jistém smyslu plýtvání (přenos trvá delší dobu, čas jsou peníze => vyšší cena za přenos)
- Vyšší náklady na přenos rádi oželíme, když redundance
  - Zajistí přenos hodinové frekvence datového signálu a my učetříme za další vodič (sériové přenosy dat)
  - Zajistí vyšší spolehlivost přenosu (bezpečnostní kódy, detekce a opravy chyb)

Bezpečnostní kódy, opravy a detekce chyb



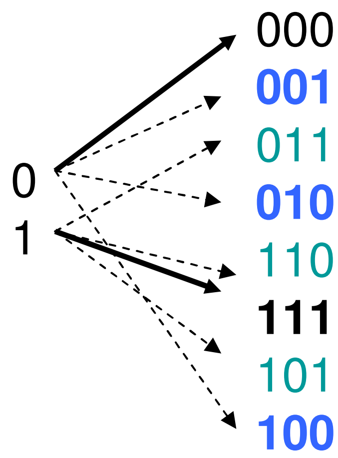
Sudá parita, kódová vzálenost 2, detekce jedné chyby



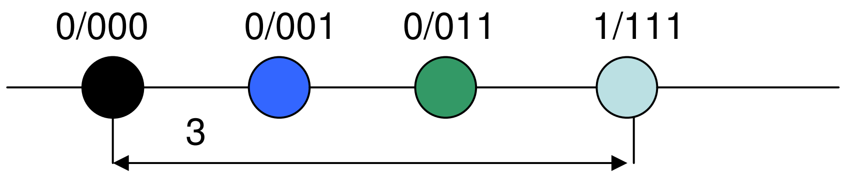
Bezpečnostní kódy, opravy a detekce chyb

Kódová vzdálenost 3

Princip: hodnotu 3x zopakujeme



Kódová vzdálenost 3, jednu chybu opravíme



Hufmannovo kódování

Pravděpodobnosti seřadíme vzestupně

P(x)={0.65,0.2, 0.1,0.05}

```
A    B    C    D
0.65,0.2,0.1,0.05
```

1. Sečteme poslední dvě — 0.65, 0.2, **0.15**

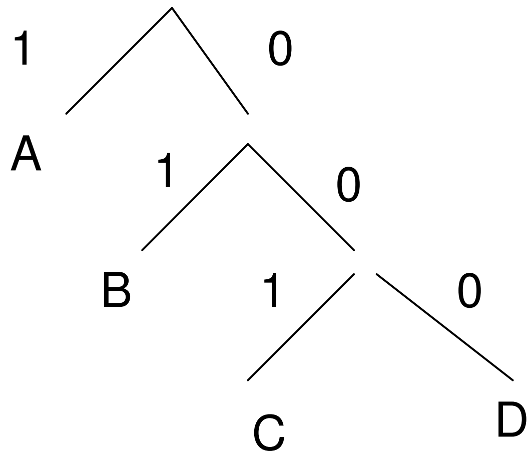
2. Sečteme poslední dvě — 0.65, **0.35**

C,D

B

B,C,D

Vytvoříme binární strom



Po každém
kroku řadíme
dle velikosti !

Příklad

S využitím Huffmanova kódování zakódujte řetězec a výsledek porovnejte s zakódováním v ASCII kódu

40 bytů

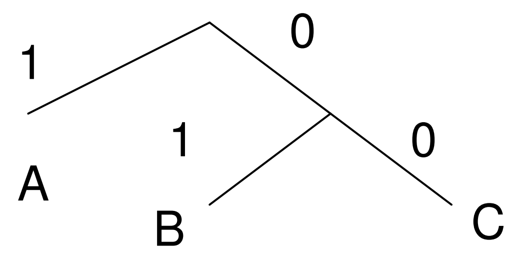
ABAAAAAABABAAAAAAACAAAAABABAAAAAAABAAABAAA
414241414141414142414241414141414141434141414141424142414
1414141414241414142414141h

Řešení

n=40

Znak	Četnost	p(x)
A	32	32/40=0,8
B	7	7/40=0,175
C	1	1/40=0,025

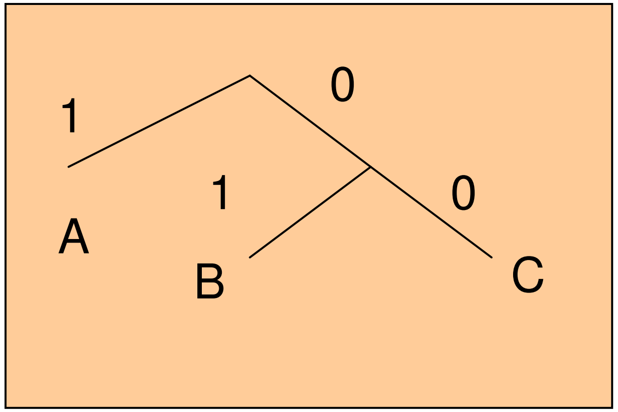
A	B	C
0,8	0,175	0,025
0,8	0,2	



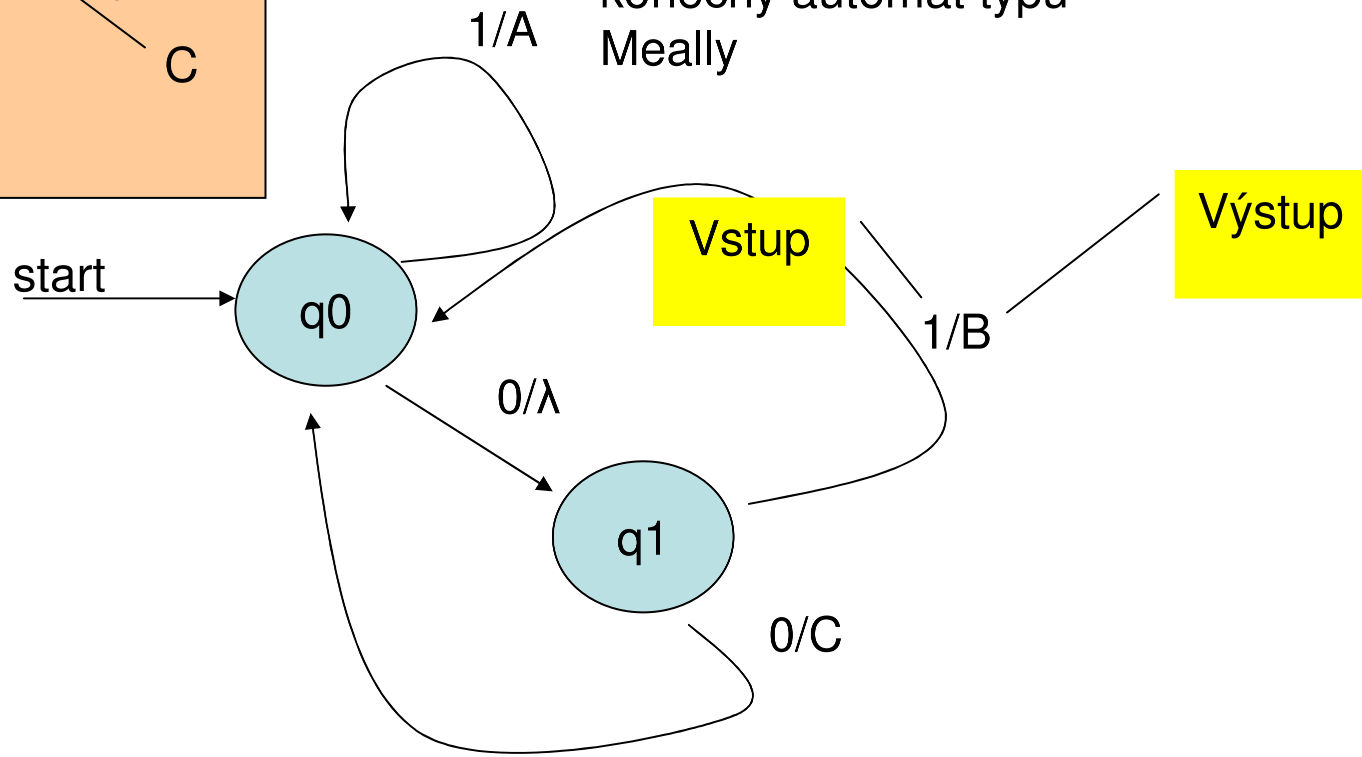
6 bytů

1011111110110111111100111110110111111101111101111
BFB7F3EDFDEFh

Dekodér



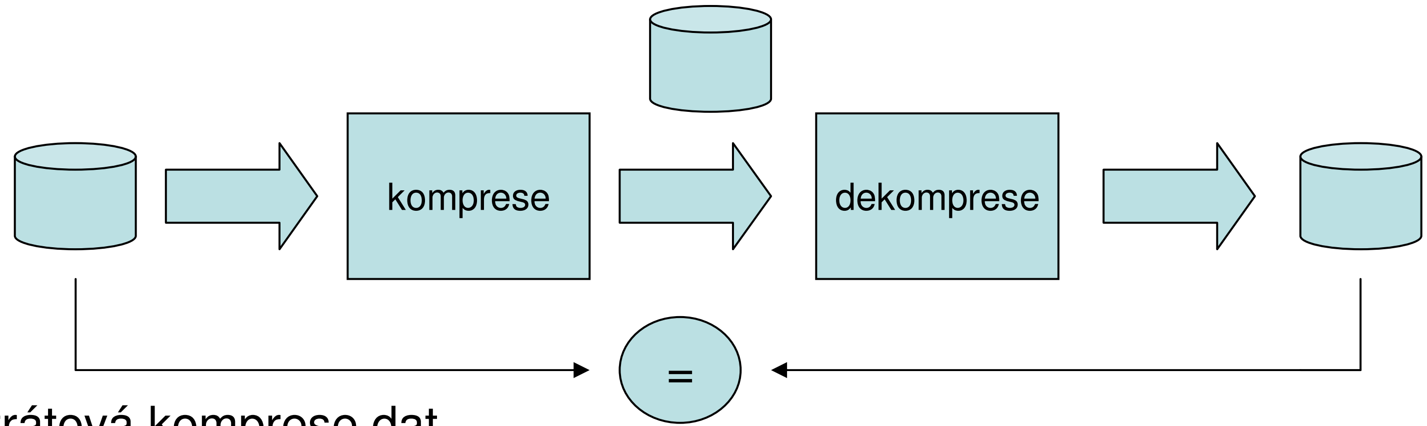
Deterministický konečný automat typu Meally



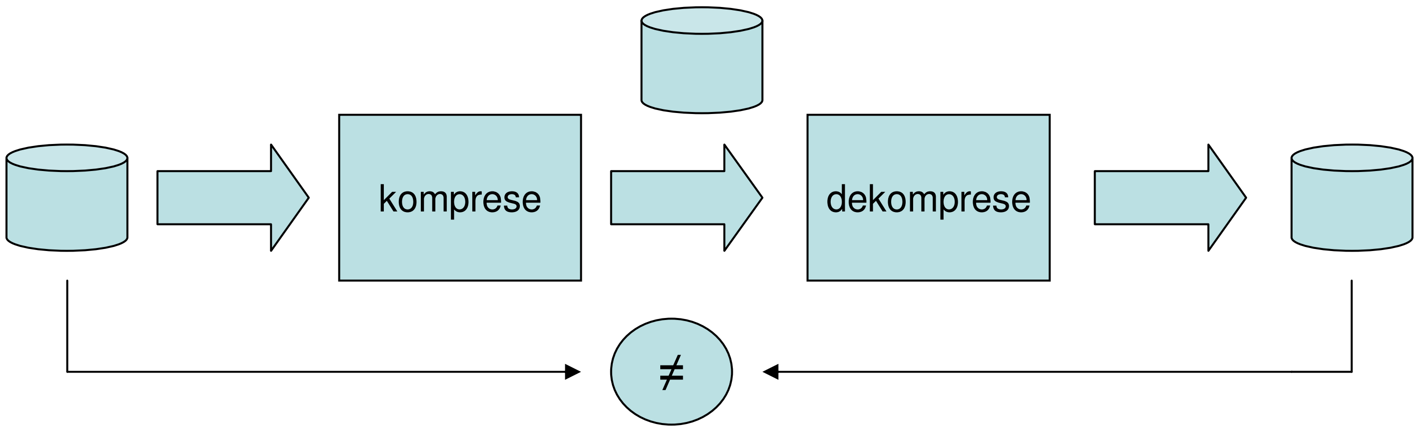
Pozn: λ značí prázdný řetěz

Komprese dat

Bezeztrátová komprese dat



Ztrátová komprese dat



Bezeztrátová komprese

- Komprese dat (souborů)
- Příklady ZIP, RAR, GZIP, BZIP
- Používané metody
  - Shannon-Fanovo kódování
  - Huffmanovo kódování
  - Aritmetické kódování
  - Run length encoding (RLE)

Run Length Encoding

AAAABCBBBBBBBBBAAAAAAACCCCCCBBCCA

4A1B1C9B7A6C2B2C1A

Znak

Počet opakujících se znaků

Pro znaky střídající se po jednom nevýhodné, dva byty (délka, znak) na jeden znak

Pro střídající se dvojice znaků neúčinné (nulová komprese)

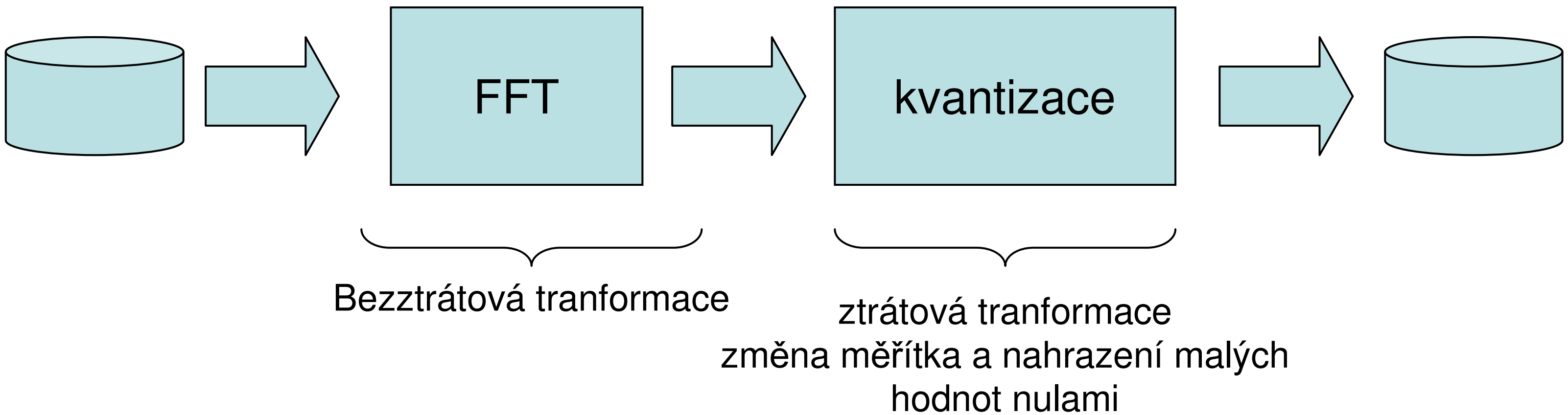
Pro větší skupiny znaků účinné

Používá se jako pomocný algoritmus pro kompresi obrázků, zejména účinné pro kreslené obrázky (velké plochy stejné barvy)

Ztrátová komprese

- Komprese obrázků (využívá např. JPEG)
- Při kompresi se část informace ztratí (například koeficienty Fourierovy transformace nebo DCT menší než daná hodnota se považují za nulové)
- Informace obsažená v původních je větší než datech, která prošla kompresí a dekompresí.
- Hodí se například pro kompresi fotek, ale nevhodné pro obrázky kreslené s velkými jednobarevnými plochami.

Princip ztrátové komprese



Fourierova transformace (v JPEG diskrétní kosínová transformace) převádí signál z časové oblasti do frekvenční, tj $y=f(t) \to Y=F(\omega)$. Tato transformace koncetruje podstatnou informaci do několika prvních koeficientů (výrazně se liší od nuly), ostatní koeficienty jsou malé a mohou se zanedbat.

Podmíněná informace

Informace nesená znakem abecedy $I_p(x) = -\log(p(x))$

Podmíněná pravděpodobnost znaku y za předpokladu, že předchází znak x

$$I_p(y \mid x) = -\log(p(y \mid x))$$

Podmíněná pravděpodobnost znaku y za předpokladu, že předchází posloupnost znaků x1,x2, …

$$I_p(y \mid x_1, x_2, x_3, x_4, \ldots, x_n) = -\log(p(y \mid x_1, x_2, x_3, x_4, \ldots, x_n))$$

Sdružená informace

Sdružená informace dvou znaků statisticky nezávislých

$$I_p(y,x) = -\log(p(y,x)) = -\log(p(x).p(y)) = I_p(x) + I_p(y)$$

Sdružená informace nesená znaky (předpoklad nezávislosti)

$$I_p(x_1,x_2,x_3,x_4,\ldots,x_n) = I_p(x_1) + I_p(x_2) + I_p(x_3) + \ldots + I_p(x_n)$$

Sdružená informace nesená dvěma znaky (statisticky závislé)

Viz. Bayesova věta

$$I_p(y,x) = -\log(p(y,x)) = -\log(p(x).p(y\,|\,x)) = I_p(x) + I_p(y\,|\,x)$$

$$I_p(x_1,x_2,\ldots,x_n) = I_p(x_1) + I_p(x_2\,|\,x_1) + I_p(x_3\,|\,x_1,x_2) + \ldots$$
$$+ I_p(x_n\,|\,x_1,x_2,\ldots,x_{n-1})$$

Posloupnost signálů a mluvnice

Spojování do konečných posloupností je aditivní operace.

$$I_p(x, y) = I_p(y, x)$$
$$I_p(x, y, z) = I_p((x, y), z) = I_p(x, (y, z))$$

Dále platí (vyplývá z Bayesovy věty)

$$I_p(x \mid y) + I_p(y) = I_p(y \mid x) + I_p(x)$$

Pokud se podmíněné pravděpodobnosti výrazně liší od nepodmíněných, pak mluvíme o zdroji s mluvnicí. Výskyt znaku silně závisí na tom, co mu předcházelo.

Podmíněné entropie I

$$H_0(A,p)=\sum_{x\in A} p(x) I_p(x)$$

$$A=\{q,r,s\}$$

$$H_0 = 0{,}1 . 3{,}32 + 0{,}2 * 2{,}32 + 0{,}7 * 0{,}51 = 1{,}15$$

y	p(y)	$I_p(y)$
q	0,1	3,32
r	0,2	2,32
s	0,7	0,51

Podmíněné entropie II

$$H_1(A,p) = \sum_{y \in A} \sum_{c \in A} p(y \mid c) I_p(y \mid c)$$

$$H_1 = 0{,}3 * 1{,}74 + \ldots + 0{,}1 * 3{,}32 = 4{,}15$$

$p(y\|c)$* $I_p(y\|c)$	c			
y		q	r	s
	q	0,3*1,74	0,6*0,74	0,1*3,32
	r	0,2*2,32	0,5*1	0,3*1,74
	s	0,4*1,33	0,5*1	0,1*3,32

Podmíněné entropie III

$$H_2(A,p) = \sum_{y\in A}\sum_{c\in A}\sum_{b\in A} p(y\mid c,b) I_p(y\mid c,b)$$

$$H_2 = \ldots$$

p(y|c,b)		b			
y=q			q	r	s
	c	q	0.01	0.1	0.15
		r	0.3	0.05	0.14
		s	0.05	0.1	0.1

p(y|c,b)		b			
y=s			q	r	s
	c	q	0.13	0.2	0.1
		r	0.2	0.06	0.02
		s	0.1	0.11	0.08

p(y|c,b)		b			
y=r			q	r	s
	c	q	0.05	0.3	0.15
		r	0.1	0.01	0.05
		s	0.14	0.15	0.05

Spočtěte podmíněné informace a výslednou H_2

Sdružené entropie

$$H^{[1]}(A,p) = H(A,p) = \sum_{x\in A} p(x) I_p(x)$$

$$H^{[2]}(A,p) = \sum_{y\in A} \sum_{c\in A} p(y,c) I_p(y,c)$$

$$H^{[n]}(A,p) = \sum_{y\in A} p(y,c,b,\ldots,a) I_p(y,c,b,\ldots,a)$$

Vlastnosti

$$H^{[2]}(A,p) = H(A,p) + H(A,p)$$

$$H^{[r]}(A,p) = H^{[m]}(A,p) + H^{[n]}(A,p)$$

$$I_{1/N}(x) = H^*(A,p) \geq H_0(A,p) = H(A,p)$$

$$0 \leq H_1(A,p) \leq H_0(A,p) = H(A,p)$$

Pro nezávislé znaky

$$H_1(A,p) = H_0(A,p) = H(A,p)$$