

- ③ need meaningful messages
 parameterized message \rightarrow previous construction with $E := (x, h(\text{parameter}))$
- ④ (evil) = $h(\text{innocent}) : A, B \text{ random subsets of } X \quad (|X|=n)$

generate $2^{b/2}$ innocent \rightarrow hash $\rightarrow A$
 \dots
 $2^{b/2}$ evil \rightarrow hash $\rightarrow B$

- ⑤ if h is M.-D. lots of collisions are as hard as 1 collision

in $\sim 2^{b/2}$ steps: $x_1 \neq x'_1 \quad f(v, x_1) = f(v, x'_1) = y_1$ } 2 times x_1, x'_1
 \dots
 $x_2 \neq x'_2 \quad f(y_1, x_2) = f(y_1, x'_2) = y'_2$ } 2² combinations which hash to the same result

in time $2^{b/2} \cdot n$ we produce 2^2 -fold collision

note: Concatenation of 2 hashes $h(x) = h_1(x) || h_2(x)$, how strong?

if one of $h_{1,2}$ is M-D \rightarrow by ⑤ we find $2^{b/2}$ colliding msgs in $b/2 \cdot 2^{b/2}$

\hookrightarrow the other will likely collide for 2 of these \rightarrow collision in time $b/2 \cdot 2^{b/2}$

Real world \rightarrow MD5 (Rivest 1995) 128b result (small) Broken! - can't find collision

SHA-1 (NSA) 160b result - Broken! (2017)

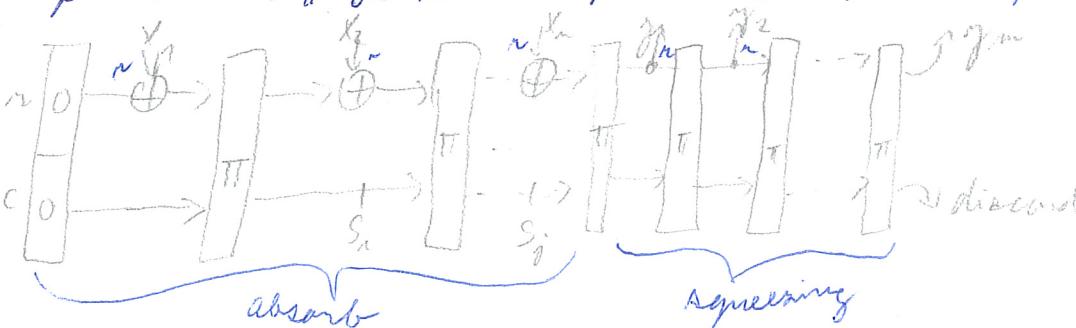
SHA-2 (NSA) 224-512b result not broken yet

Competition by NIST \rightarrow SHA-3 - published in 2015

Sponge construction: Phase 1 - absorbing input

... 2 - squeezing out output

- permutation π on blocks of size $w = n + c$ capacity



Security level against brute-force = ① $2^{N/2}$ by birthday paradox

② internal collisions: in 2^{4t} blocks (attacking output)

we find $i \neq j : s_i = s_j$

first: $\oplus i$

and: $\oplus^{-1}(h_i \oplus h_j)$ } output of π is the same \Rightarrow

we get same output

for t random

security level of sponge $\geq \min(n/2, c/2)$

RC4 (Rivest 1987) permutation based working on bytes

state: 256 bytes

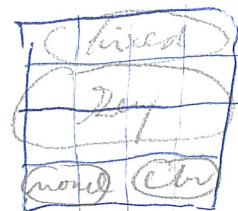


ChaCha 20 (Bernstein 2008) derived from Salsa20
- STREAM see profile

32B key }
168B msg nonce } chacha20 1 block
8B block counter } not bijective of keystream

shake: matrix

32t values



20 rounds

ARX \leftarrow XOR

\uparrow 5 rotation
addition

Hash functions $\{0, 1\}^k \xrightarrow{h} \{0, 1\}^n$

basic properties

1. no collision: $h(x) = h(x')$, $x \neq x'$

2. no second: for given x find x' : $h(x) = h(x')$

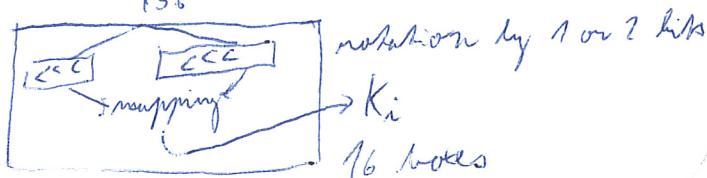
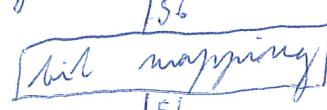
3. no inversion: for given y find x : $h(x) = y$

Use case: signature



DES - Feistel network with 16 rounds
64-bit blocks 56 bit keys

Key scheduler

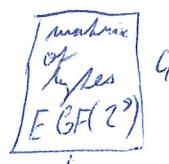


AES advanced encryption standard

- 1997 NIST public competition
- Rijndael \rightarrow became AES in 2001
- 128-bit blocks 128/192/256 bit keys
rounds 10 12 14

Structure: SPN with linear step

internal state
and
round key



Round: 8 Bytes \rightarrow 16 identical S-boxes

P Shift rows - fixed

L Mix columns - linear transform on every column

\oplus Add round key -- XOR with K_i

Round of decryption:

Add round key
Inv Mixcolumns
Inv Shiftrows
Inv Bytesub

↓
Inv mix
Add RK(mixed)

Decryption is very similar to E \leftarrow Inv Bytesub
Inv Shiftrows
Inv Mixcolumns

Implementation technique: see lecture, mostly on real CPU

Critique of AES

- single algebraic structure - advance in lin Alg might break it
- small margin in # rounds
- byte-aligned
- 128-bit key: quantum computer attack
- 128-bit blocks: block collisions in $\approx 2^{64}$ blocks
workaround: change keys after 2^{32} blocks

\rightarrow Grover algorithm
on operations

Other finalists in AES comp

- Serpent 192-bit blocks, 128-256 bit keys / 32 rounds SPN + linear
- Twofish

16 rounds Feistel net
key-dependent S-boxes

Critique of DES

- weak keys: if $K = 0^{56} \Rightarrow \forall i K_i = 0^{56}$
- \rightarrow all rounds are identical

$$E_K = D_K$$

$$- E_K(x) = \overline{E_K(x)} \text{ ?}$$

- too short key: brute force attack
2012 - crack in 28 hours FPGAs-based machine

- too short blocks $\approx 2^{32}$ blocks have collision
- workaround: double DES key size: 112 bits but security level ≤ 57 b (exercice)

3DES $x \xrightarrow{k_1} E \xrightarrow{k_2} D \xrightarrow{k_3} E \xrightarrow{k_4} y$ 168 bit keys sec level ≤ 113

- too much secrets (unexplainable constants)

- attacks on structure ... 2^{47} chosen plaintexts

Generalise one time pad

Group $(G, +, 0)$

$x, y, K \in G$

$K \in \text{ER} G$

$$\mathbb{Z}_n = \{0, \dots, n-1\} \mod n$$

$$E(x, K) = x + K$$

$$D(y, K) = y - K = y + (-K)$$

If a cipher is perfectly secure $\equiv H(X)H(Y) \quad P(E(X, K)=y) \text{ is constant}$

$$P_{\text{OTP}} = \frac{1}{|G|} \quad \text{... it's perfectly secure}$$

usefulness of OTP

- never repeat keys! \rightarrow if same keys $y_1 \oplus y_2 = x_1 \oplus x_2$ - lot of info

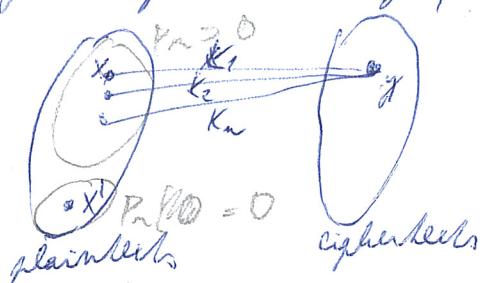
- code book

- replace randomness by pseudorandomness

- attacker toggles $y[i]$ \rightarrow toggles $X[i]$

Theorem: if #keys < #messages, then the cipher is not perfectly secure

proof:



y^i can't be obtained by a key
 \Rightarrow probability is not uniform by

Information theoretic security (Ghamow security)

Secret sharing (splitting)

$\exists S_1 = \text{random}$

$$S_1 \oplus S_2 \rightarrow X \quad (2,2)$$

$$S_2 = X \oplus S_1$$



② $S_1, \dots, S_{k-1} = \text{random}$

$$S_k = S_1 \oplus \dots \oplus S_{k-1} \oplus X$$

$$\bigoplus_i S_i = X$$

Df: (k, l) threshold scheme

split X to shares S_1, \dots, S_k

at any l shares give X
with $< l$ shares no info on X

③ $(k, 2)$ finite field F
looking for $f(x) = ax + b$

$$f(0) = X$$

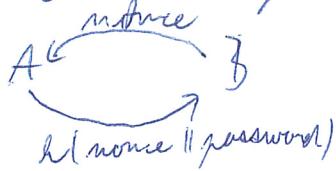
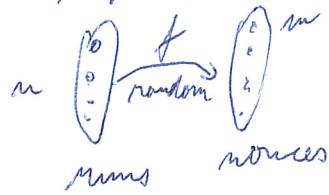
$$f(1) \in F \quad S_1 \dots S_k \quad S_i := f(i)$$

④ (k, l) ... Polynomials
IFF $\begin{cases} \text{irr} \\ \text{injective} \\ \text{of} \\ \text{deg } d \end{cases}$
of $\begin{cases} \text{graphs} \\ \text{of} \\ \text{poly} \\ \text{choices of} \\ y_1 \dots y_d \end{cases}$

- Ⓐ if $x_1 \dots x_l$ are all the roots of p then
 $p(x) = (x-x_1)(x-x_2) \dots (x-x_l) \circ q(x) \in \text{no roots}$
 \Rightarrow nonzero p of deg d has at most d roots
- Ⓑ let p, q polys of deg d with the same graph $\Rightarrow p=q$
Proof: $n := p-q$ deg $d \Rightarrow x_1 \dots x_d$ are roots of $n \Rightarrow n=0 \Rightarrow p=q$
- Ⓒ If $x_1 \dots x_d$ distinct and $y_1 \dots y_d$ $\exists! p$ poly of deg d s.t. $p(x_i) = y_i$
Lagrange theorem

Birthday attacks

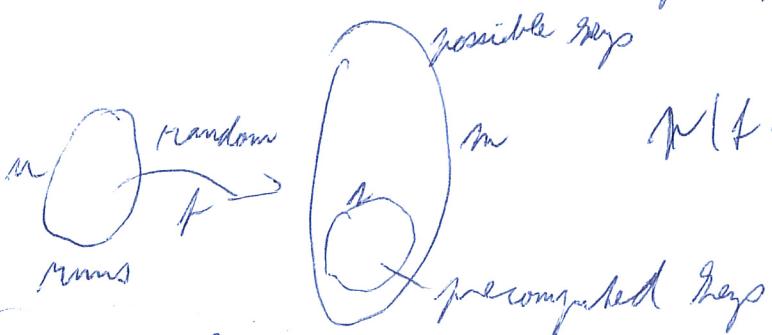
challenge-response scheme

 $2^{b/2} \rightarrow$ likely to repeat nonces23 people 366 days $\rightarrow P(2 \text{ have same bd.}) \geq \frac{1}{2}$ 

$$\begin{aligned}
 P(f \text{ is injective}) &= \frac{\# \text{ injective functions}}{\# \text{ all functions}} = \frac{(m)(m-1)\dots(m-m+1)}{m^m} = \\
 &= \frac{m}{m} \cdot \frac{m-1}{m} \cdot \frac{m-2}{m} \cdot \frac{m-m+1}{m} \quad 1-x \approx e^{-x} \\
 &\approx 1 \cdot \left(1 - \frac{1}{m}\right) \cdot \left(1 - \frac{2}{m}\right) \cdots \approx 1 \cdot e^{-\frac{1}{m}} \cdot e^{-\frac{2}{m}} \cdot e^{-\frac{m-1}{m}} = \\
 &= e^{-\frac{1+2+3+\dots+m-1}{m}} \approx e^{-\frac{m^2}{2m}} \\
 &e^{-\frac{m^2}{2m}} = \frac{1}{2} \\
 -\frac{m^2}{2m} &= \ln \frac{1}{2} \\
 \frac{m^2}{m} &= -2 \ln \frac{1}{2} \approx 1.38 \Rightarrow m^2 \approx m
 \end{aligned}$$

A $\xrightarrow{f} B$
Easy(K, k_{pub})For K_{guess} \rightarrow precompute or tableEasy($K_{\text{guess}}, k_{\text{pub}}$)

Easy
1 key



$$P(f \text{ avoids subset}) = \left(1 - \frac{1}{m}\right)^m \approx e^{-\frac{m}{m}}$$

One-time Pad

message: $x \in \{0,1\}^n$ (remain cipher) - proven to be secure (only one) (perfect security)key: $K \in \{0,1\}^n$ Security level: $\frac{\# \text{key bits}}{2}$ $n := \sqrt{m}$ $m := n^2$ ciphertext: $y = x \oplus K \rightarrow$ independent uniform random bitsdecrypt: $x = y \oplus K$

Asymmetric cipher $D(E(x, K_E), K_D)$

Alice \rightarrow [E] \longrightarrow [D] \rightarrow Bob

(K_E, K_D)
 \uparrow
 Key pair generation

Hash function

$$h : \{0,1\}^* \rightarrow \{0,1\}^b$$

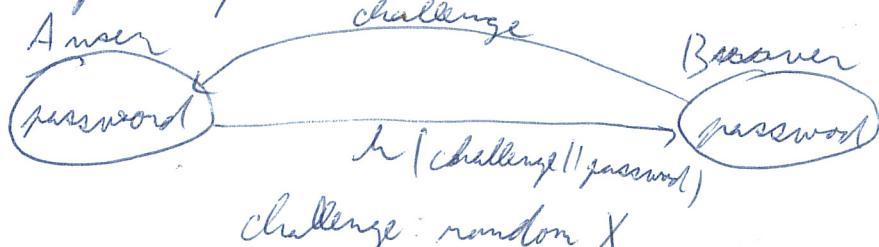
"random"

- ① impossible to invert
 - ② impossible to find collision
- $x \neq x' : h(x) = h(x')$

Applications

- ① signatures : A wants to sign K
 - send x in plaintext
 - $E(h(x); K_{\text{sign}}) \rightarrow D(-; K_{\text{ver}})$

② challenge-response communication



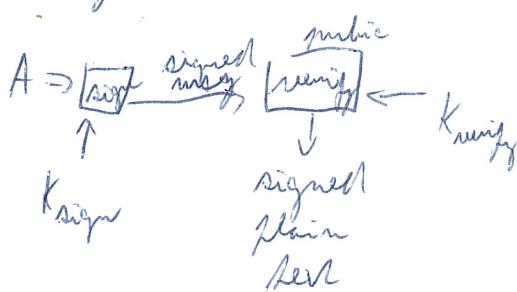
challenge: random X

Random generation - unpredictable, cannot be influenced

multi-party comm. network

- o o o o o
- m pairs of keys
- K_E is public
- K_D are private
- catch: key distribution

Signature scheme



- o o o o o
- m pairs of keys
- K_E is private
- K_D is public

Vigil: Function provided
Toss a coin over
the phone

- Věta: máloobvyčejná vlastnost: orientovaného grafu G je vlastnost, že:
1. G je rozvářený a slabě souvislý
 2. G je konkurenční
 3. G je rozvářený a silně souvislý

Důkaz: $(3) \Rightarrow (1)$ ex

$(2) \Rightarrow (3)$ ex využitost
silna souvislost: $\forall u, v \exists$ orientovaný hranice $u \rightarrow v \Rightarrow$ orientovaná cesta $u \rightarrow v$

$(1) \Rightarrow (2)$ analogicky k předchozí větě

Uprostřed def: G není souvislý graf bez pružnic (acyklický)
def: G je graf jehož komponenty jsou stromy \Rightarrow acyklický graf

def: list je vzdále spojné?

Lemma (o koncovém vrcholu):

Každý strom s aspoň 2 vrcholy má aspoň 2 listy

Důkaz: Uvažme nejdleší cestu $P: n \rightarrow v$

n, v jsou listy

polohy n nebyl list: $\exists l \in \{n\}$ je hrana, která nelze na cestě

$\wedge l \in P \Rightarrow$ část cesty $n \dots l + \{v, l\}$

Nový cyklus

↳

$\wedge l \notin P$

$\wedge \{v, l\}, P$ je delší cesta ↳

Lemma: Nechť v je list grafu G . Pak G je strom $\Leftrightarrow G - v$ je strom

Důkaz: $\Rightarrow G - v$ je souvislý \Leftrightarrow po každou maci $x, y \neq v \exists$ cesta \Rightarrow lesík i v $G - v$, protože list má deg ≥ 1

\Leftarrow G souvislý: $\forall x, y \neq v \exists$ cesta $v - G - v$, ale pak je i v G

cesty $x - v$: nechť $s :=$ soused v

$\forall x \exists s \ni x \ni s \ni v \quad \left\{ \begin{array}{l} \text{hranice } x - v \\ \text{hranice } s - v \end{array} \right.$

G acyklický: v má deg $1 \Rightarrow$ nelze na střed pružnice

Lemma: $A_{ij}^k = \# \text{ sledů délky } k \text{ z } v_i \text{ do } v_j$

Dř: Indukční postupek:

$$1. k=1 \quad \checkmark$$

$$2. k \Rightarrow k+1 \quad A_{ij}^{k+1} = (A \cdot A)_{ij} = \sum_{l=1}^k A_{il}^k A_{lj} \in [v_i, v_j] \in E$$

$v_i =$ počet sledů délky 3

zaznamený sled délky 3

$A_{ii}^3 = \# \text{ sledů délky 3 z } v_i \text{ do } v_i$

$$\# \Delta = \frac{\sum_i A_{ii}^3}{6}$$

$$\sum_{\substack{\text{# sledů délky } l \\ \text{z } v_i \text{ do } v_j}} = \# \text{ sledů délky } l+1 \text{ z } v_i \text{ do } v_j$$

sledů délky $k+1$ z v_i do v_j

Vzdálenost (grafova' métrika) v souvislému grafu G

$$d_G: V^2 \rightarrow N$$

$d_G(u, v) :=$ min. r. délka všech cest mezi u, v

Lemma: $\forall u, v \in G$

$$1. d(u, v) \geq 0$$

$$2. d(u, v) = 0 \Leftrightarrow u = v$$

$$3. d(u, v) = d(v, u)$$

$$4. \text{ směrovost } d(u, v) \leq d(u, w) + d(w, v)$$

Graphové operace:

$G + v, G + e$ přidání'

$G - v, G - e$ smazání' $G - v = G[V(G) \setminus \{v\}]$

G %e dílení hrany $\rightarrow V_1 := V \cup \{x\}$ pro $x \notin V$

$$E_1 := E \setminus \{e_{uv}\} \cup \{(u, x), (v, x)\}$$

$G \cdot e$... rozhraní hrany

$$G \cdot e = G - v - w + x + (e \setminus \{e_{uv}\}) \cup \{x\}$$

pro všechny $e \in E$

$$1. \exists ! e \in \underline{E} \cap \{e_{uv}\} = 1$$

\diamond cesta by mohla délat délkou P_1

Družnice

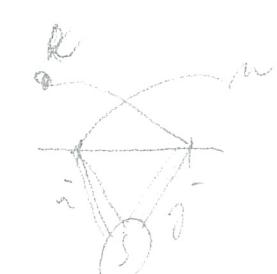
C_1

Věta o střední losotonrosti $D = d_1 \leq \dots \leq d_n$ pro $n \geq 2$ je skóre grafu
 $\Leftrightarrow D' = d'_1 \dots d'_{n-1}$ je skóre grafu & $0 \leq d_n \leq n-1$
 $\quad \{d'_i\} \subseteq \{d_i\}$ pro $i \in \{n-d_n\}$
 $\quad \{d'_i\} \subseteq \{d_i-1\}$ pro $i \geq n-d_n$

DR: \Leftarrow nechť G' je graf se skóre D' a vrcholy v_1, \dots, v_{n-1}
 odpovídající G doplněním vrcholu v_n a hran $\{v_i, v_n\}$ pro $i \in \{n-d_n, \dots, n-1\}$
 $\hookrightarrow G$ má skóre D

\Rightarrow Lemma: $\left\{ \begin{array}{l} \text{Nechť } G \text{ je soubornina všech grafů na vrcholech } \{v_1, \dots, v_n\} \\ \text{se skórem } D, G \neq \emptyset \end{array} \right.$
 Potom $\exists G \in G : \{v_n, v_i\} \in E(G)$ pro některou $i \in \{n-d_n, \dots, n-1\}$
 mohu odstranit v_n a získám G' se skórem D'
 $\text{DR: pro } G \in G \text{ def } j(G) := \max \{j : \{v_j, v_n\} \notin E(G)\}$
 potom $j(G) = n - d_n$ když platí $\forall i < j : \{v_i, v_n\} \in E(G)$

Rozp. $d_n = n-1$
 pro každý $G \in G$
 splňuje lemmu



Najde se $G \in G$ zehož jež je minimální
 spor: Rozp. $j(G) > n - d_n - 1$

$\{v_j, v_n\} \notin E(G)$

$\exists i < j : \{v_i, v_n\} \in E(G)$

$\exists i : \{v_i, v_n\} \notin E(G) \quad \left. \begin{array}{l} \text{pro každé} \\ \{v_j, v_n\} \in E(G) \end{array} \right\} d_i \leq d_j$

Upřesníme graf G na $G_1 : V(G_1) = V(G)$

ale $G_1 \in G$
 $j(G_1) < j(G)$

$$E(G_1) := E(G) \cup \{\{v_n, v_2\}, \{v_j, v_n\}\}$$

$$\backslash \{\{v_n, v_1\}, \{v_j, v_1\}\}$$

Jáhnuťa

$$S_m := \{\pi \mid \pi \text{ permutace na } \{1, \dots, m\}\}$$

i dôsled súčet $\pi(i) = i$

$$\tilde{S}_m := |\{\pi \in S_m \mid \#i : \pi(i) = i\}|$$

$$\Pr[\text{nahodne vybrane } \pi \in \tilde{S}_m] = \frac{\tilde{S}_m}{m!}$$

$$A := \{\pi \in S_m \mid \pi \text{ má pevný bod}\}$$

Definícia

$$A_i := \{\pi \in S_m \mid \pi(i) = i\}$$

$$A = \bigcup_i A_i$$

$$|A_i| = (m-1)!$$

$$|A_i \cap A_j| = (m-2)!$$

následne: $(m-2)!$ 

$$|\bigcup_{i=1}^m A_i| = \sum_{k=1}^m (-1)^{k+1} \sum_{I \in \binom{[m]}{k}} \left| \bigcap_{i \in I} A_i \right|$$

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

$$|A| = \sum_{k=1}^m (-1)^{k+1} \frac{m!}{k!} = m! \left(\frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} - \dots - \frac{(-1)^{m+1}}{m!} \right)$$

$$\tilde{S}_m = m! - |A| = m! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + \frac{(-1)^m}{m!} \right)$$

$$\approx \frac{1}{e}$$

Odkazy

$$\textcircled{1} \quad 2^{m-1} \leq m! \leq m^m$$

$$\textcircled{2} \quad m^{m/2} \leq m! \leq \left(\frac{m+1}{2}\right)^m$$

$$\textcircled{2*} \quad e^{\frac{m}{e}} \leq m! \leq e^m \left(\frac{m}{e}\right)^m$$

Stirlingova formula

$$m! \approx \left(\frac{m}{e}\right)^m \cdot \sqrt{2\pi m}$$

$$\textcircled{3} \quad \left(\frac{m}{e}\right)^m = \left(\frac{m}{e}\right)^m \leq m^m$$

$$\textcircled{4*} \quad \left(\frac{m}{e}\right)^m \leq \left(\frac{e^m}{e}\right)^m$$

$$\textcircled{5} \quad \frac{2^{2m}}{2^{m+1} \min_{\text{prvky}} \leq \text{max}_{\text{prvky}}} \leq 2^{2m}$$

AG vedenie

$$xy > 0$$

$$\sqrt{xy} \leq \frac{x+y}{2}$$

$$(m!)^2 = 1 \cdot 1 \cdot 2 \cdot 2 \cdots m \cdot m$$

$$(1 \cdot 1)(2 \cdot (m-1)) \cdots$$

$$m! = \sqrt{1 \cdot m} \cdot \sqrt{2 \cdot (m-1)} \cdots \sqrt{m \cdot 1}$$

$$i(m-i+1) \geq m$$

$$i=1, i=m \rightarrow \text{prvky}$$

$$m \cdot m \geq 2$$

$$m \cdot m \geq m$$

$$m! \geq (\sqrt{m})^m = (m^{\frac{1}{2}})^m = m^{m/2}$$

$$\sqrt{i(m-i+1)} \leq \frac{n+m-i+1}{2} = \frac{m+1}{2}$$

$$m! \leq \left(\frac{m+1}{2}\right)^m$$

nespořádaných k-tic z m-prvkové možnosti N
nepr. k-tic = n^k
nepr. k-tic bez opakování = $n^{\underline{k}}$ → odlišné pořadí způsobují jen pořadí = $\underline{k}!$

$$\text{Def: Kombinacní číslo } \binom{n}{k} := \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{1\cdot 2\dots k}$$

Df: Pro možnosti X a $k \geq 0$: $\binom{|X|}{k} := \{A \subseteq X \mid |A|=k\}$

$$\text{Věta } \forall X \quad \forall k \geq 0 \quad |\binom{|X|}{k}| = \binom{|X|}{k}$$

k-prvky
podmožin

Vlastnosti komb. čísel

$$\binom{n}{0} = 1 = \binom{n}{n} = 1 \quad \binom{m}{1} = m = \binom{m}{m-1} \quad \binom{m}{k} = \binom{m}{m-k}$$

$$\text{5. } \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$6. \sum_{k=0}^m \binom{m}{k} = 2^m$$

$$\text{Důs: } |X| = n \quad \begin{array}{c} \text{obsah} \\ \binom{|X|}{k} \end{array} \quad \begin{array}{c} X \setminus \{a\} \\ k-1 \end{array}$$

$a \in X$ $\xrightarrow{\text{nechá}} \quad \begin{array}{c} \text{obsah} \\ \binom{|X|}{k} \end{array}$

spojitkový výsledek podmožin

Věta: (Binomická) pro $n \geq 0 \quad \forall x, y \in \mathbb{R}$

$$(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i$$

$$\text{Důs: } \overbrace{(x+y)(x+y)\dots(x+y)}^n$$

$$\binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1$$

$\xrightarrow{\text{počet xy výprav}} \quad \xrightarrow{\text{počet xy výprav}}$

Diskuter

$$x=1 \quad y=-1$$

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} \dots (-1)^n \binom{n}{n}$$

$$\hookrightarrow |Y| = |Z|$$

Def: Pro $(X; \leq)$ ČUM

• $x \in X$ je nejmenší $\equiv \forall y \in X \quad x \leq y$

minimum $\equiv \exists y \in X \quad y \leq x$

analogicky

největší, maximum

Lemma: Kždá konečná neprázdná ČUM má minimální prvek

Důk: $x_1 \in X$ zvolíme libovolný / pořad x_1 není minimální $\exists x_2 \in X$

$x_2 \dots - - - - - x_3 < x_2$

$x_p \leq x_i = x_j$
pro $i < j$

pomoc antisymetrie
nikdy nerovnat

Def: Pro $(X; \leq)$ ČUM

• $A \subseteq X$ je řetězec $\equiv \forall a, b \in A$ jsou porovnateльné

• $A \subseteq X$ je antireťezec/posloupnost možna \equiv
 $\exists a, b$ možné a porovnateľné

• $w(X, \leq) := \max \text{ s délkou řetězce}$ (kždá napořádatelná)

• $\alpha(X, \leq) := \max \text{ s délkou antireťezce}$ (kždá napořádatelná)

Věta o dvojkém a řínokém: $\forall (X, \leq) \text{ ČUM} : \alpha(X, \leq) \cdot w(X, \leq) \geq |X|$

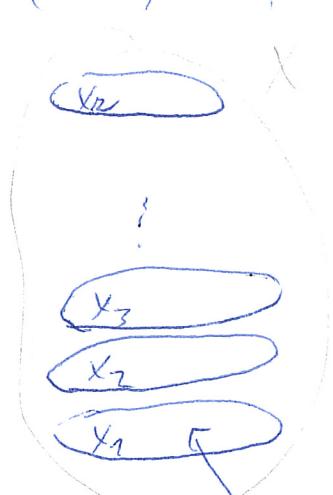
Důk: $X_1 := \{x \in X \mid x \text{ je minimální}\}$

Předpokládejme $X_1 = \emptyset$

$Z_i := X \setminus \bigcup_{j=1}^i X_j \xrightarrow{\text{Dopř } Z_i = \emptyset} \text{ když}$

$X_{i+1} := \{x \in Z_i \mid x \text{ je minimální}\}$

$X_1 X_2 X_3 \dots X_D$



① Kždá x_i je antireťezec $|X_i| \leq \omega$ $\leq \omega$

② $\{X_1 \dots X_D\}$ krouží posloupnost $X^{d-w} \leq |X_1| + \dots + |X_D| = |X|$

min
pomoc
antisymetrie
-vratný
v A diagramu

③ $\exists n_1 \in X_1 \dots n_D \in X_D : \{n_1 \dots n_D\}$ je řetězec $\omega \leq \omega$

n_1 zvolíme libovolnou z X_1

$n_D \notin X_{D-1} \Rightarrow \exists n_{D-1} \in X_{D-1} : n_{D-1} < n_D \dots$ pokle do n_1

QED

DM

P02 S04

\mathcal{G} : množinový systém $\mathcal{G} \subseteq 2^X$ je rozklad množiny $X =$

① $\forall A \in \mathcal{G}: A \neq \emptyset$

② $\forall A, B \in \mathcal{G}: A \neq B \Rightarrow A \cap B \neq \emptyset$

③ $\bigcup_{A \in \mathcal{G}} A = X$

$x R y \Leftrightarrow \exists A \in \mathcal{G}:$
 $\{x, y\} \subseteq A$

Operace s relacemi

Inverzce R^{-1} je relace nosí y a x

$$R^{-1} := \{(y, x) \mid (x, y) \in R\}$$

Úpláštnění relaci

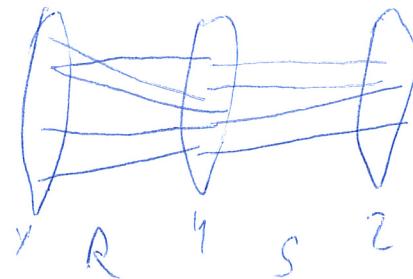
R měří $X_1 Y$; S měří Y_2

T měří $X_1 Y_2$

$$x T z = \exists y \in Y : x R y \wedge y S z$$

Diagonála

$$\Delta_X := \{(x, x) \in X\}$$



$$T = R \circ S$$

Funkce (zobrazení)

$$f: X \rightarrow Y$$

Df: Funkce f mimožný X do množiny Y je relace A měří X a Y

$$\forall x \in X \exists! y \in Y : x A y$$

značení: $f(x) \dots y : x A y$

$$f(S) := \{f(x) \mid x \in S\}$$

řešení: ① $\sin: \mathbb{R} \rightarrow [-1; 1]$

$$x \mapsto \sin x$$

$$x \mapsto a \sin \varphi x$$



"nesoučinná" matice může být využita
rel. $\in \mathcal{I}(y)$

② $\text{sgn}: \mathbb{R} \rightarrow \{-1, 0, 1\}$

③ $|A|: \mathbb{Z}^N \rightarrow \mathbb{N} \cup \{\infty\}$ kardinalita

Úpláštnění funkcií

④ $f(x) = x$ identická Δ_X

$$f: X \rightarrow Y \text{ a } g: Y \rightarrow Z$$

⑤ $f(a, b) \in Y \quad A \times B \rightarrow Y$

$$\begin{smallmatrix} A & \otimes & B \end{smallmatrix}$$

$$\text{pak } f \circ g: X \rightarrow Z$$

Matematika

- definice
- poset \rightarrow věta
- \downarrow
dúlka
- axiomy

Dúlka sponem

největší $\rightarrow \varphi$ Věta: Použití sel \Rightarrow největšího sponuDef: sponem p_1, \dots, p_n je to největší pravého

$$f(p) := \prod_{i=1}^n p_i$$

($f(p) + 1$) mod $p_i = 1 \Rightarrow f(p)$ nemá dělitelky
zády na pravostranu
($f(p) + 1$) je větší než všechna pravácky
 $\Rightarrow f(p) + 1$ je maximální pravého

Množina
symetrické diference $A \Delta B$

$$(A \setminus B) \cup (B \setminus A)$$

potence: $2^A := \{B \mid B \subseteq A\}$ $P(A)$

$$\{x \in N \mid x \text{ mod } 7 = 1\}$$

systém podmnožin

$x \in X$
divočí množiny

 $x \notin X$

kohodlá množiny

Věta: Neexistuje maxima všech množin

Def sponem

$K := \{x \in M \mid x \in X\}$ maxima všech kohodlých množin

Je K kohodlá? $\Leftrightarrow \forall x \in K \exists y \in K$ takže $x \in y \wedge y \in x$



Inverz 2: Pro matici $A \in T^{m \times n}$ a neg matici $Q \in T^{n \times m}$

$$\textcircled{1} R(QA) = R(A)$$

$$\textcircled{2} A_{*k} = \sum_{j \neq k} d_{ij} A_{*j} \text{ zvo negatice } \stackrel{\text{def}}{=} \text{adj } ET \Leftrightarrow (QA)_{*k} = \sum_{j \neq k} d_{ij} (QA)_{*j}$$

Dz(1) $R(QA) \subseteq R(A)$ z Inverz 1; ažížeme tva 1 ještě plní na QA využitího Q^{-1} abo
 $R(A) = R(Q^{-1}QA) \subseteq R(QA)$

\(\Rightarrow\) Zleva máme z tva 1

$$\Leftarrow \text{zprávě tva 1 na } QA \text{ využitího } Q^{-1} \text{ zleva } (Q^{-1}QA)_{*k} = \sum_{j \neq k} d_{ij} (Q^{-1}QA)_{*j} \quad \square$$

Věta 1: Pro matici $A \in T^{m \times n}$ a jíž REF bude A^R a jinak na

pořadích $(1, p_1) \dots (n, p_m)$, kde $n = \text{rank}(A)$ platí:

1. nejdolejší řádky A^R ($A_{11}^R \dots A_{1n}^R$) jsou bázi $R(A)$

2. sloupce $A_{*p_1} \dots A_{*p_n}$ jsou bázi $S(A)$

3. $\dim S(A) = \dim R(A) = n$

Dz: Vizuje se že Q n.s. $QA = \text{REF}(A) = A^R$ (Q je reg $\in T^{m \times m}$)

\(\textcircled{1}\) podle Inverz 2 $R(A) = R(QA) = R(A^R)$; nejdolejší řádky A^R jsou lin. nezávislé a jsou bázi $R(A) \Rightarrow$ tedy i $R(A)$

\(\textcircled{2}\) Sloupce $A_{*p_1}^R \dots A_{*p_n}^R$ jsou lin. nezávislé a generují $S(A)$

$$A_{*j}^R = \sum_{i=1}^n a_{ij}^R e_i = \sum_{i=1}^n d_{ij} e_i = \sum_{i=1}^n a_{ij}^R A_{*p_i}^R \Rightarrow$$

Důkaz sloupce dle tva 2 a opatřeno CK \Rightarrow

\Rightarrow generuje $S(A) \Rightarrow$ jsou lin. nezávislé k těm ~~jsou~~ bázi $S(A^R) \Rightarrow$

\Rightarrow 2 Inverz 2 jsou bázi $S(A)$

\(\textcircled{3}\) $\dim R(A) = n$ podle 1 \Rightarrow je tím bázi velikosti n
 $\dim S(A) = n$ podle 2 \Rightarrow je tím bázi velikosti n

\square

Důkaz: pro rozdelené matici $A \in T^{m \times n}$ platí $\text{rank}(A) = \text{rank}(A^T)$

$$\text{rank}(A) = \dim R(A) = \dim S(A) = \dim S(A^T) = \dim R(A^T) = \text{rank}(A^T)$$

Věta k SLR: Gaussova $Ax = b$ je řešitelná $\Leftrightarrow b$ je CK sloupcem matice A - - -
 $b \in S(A)$, což nastane $\Leftrightarrow S(A) = S(A|b)$

Cílem této věty: Gaussova $(A|b)$ má řešení $\Leftrightarrow \text{rank}(A|b) = \text{rank}(A)$

Jmz: pro vš VP V plati: \Rightarrow jsou-li $x_1 \dots x_m \in V$ lin. nesav., pak $m \leq \dim V$. Potom $m = \dim V$, pak je $x_1 \dots x_m$ báze V

2. Jeantli $y_1 \dots y_n$ generátory V, pak $n \geq \dim V$. Potom $n = \dim V$ pak $y_1 \dots y_n$ je báze V

Ds: $d = \dim V$, $x_1 \dots x_d$ je báze V

1. $x_1 \dots x_m$ jsou lin. nezávislé a $x_1 \dots x_d$ jsou generátory $\Rightarrow m \leq d$; jiní $m = d$

2. $x_1 \dots x_m$ doplnit $\xrightarrow{d-m=0}$ do věty na systém generátorek V $\Rightarrow x_1 \dots x_m$ báze V

2. $x_1 \dots x_d$ jsou nezávislé a $y_1 \dots y_n$ jsou generátory $\xrightarrow{\text{Světa}}$ $d \leq n$; potom $n = d$ pak $y_1 \dots y_n$ lin. nezávislé a báze

Věta: Každý lin. nes. systém $\xrightarrow{VP^V}$ lze doplnit na bázi V.

Ds: máme $x_1 \dots x_m \in V$ nezávislé a bázi $x_1 \dots x_d$, $d = \dim V$

poklelý věty můžeme $x_1 \dots x_m$ přidat $x_{d+1} \dots x_{d+m}$, kdežto může d generátorem $V \Rightarrow$ nové bázi poklelý věty 2.

Dimenze podprostoru: Věta: Jeli $W \subseteq V \Rightarrow \dim W \leq \dim V$ a je $\dim W = \dim V \Rightarrow W = V$

Ds: Definujeme $M = \emptyset$, $\text{span}(M) = W$ jsou lokální. Jinak $\exists v \in W$ jiný než n. Přidáme v do M a upřejme M je lin. nes. $\Rightarrow |M| \leq \dim V$, po konečné mnoha krocích $W = \text{span}(M)$ a M bude bázi W většinou $\dim W = |M| \leq \dim V$, pokud $\dim W = \dim V$ ~~pak~~ $\Rightarrow M$ je bázi V poklelý věty

Upravený podprostor V a V VP_W := { $w + v : w \in W, v \in V\}$

Jmz: Pro podprostory V a V VP_W W plati $U + V = \text{span}\{U \cup V\}$

Ds: \subseteq : klasická a užávrenost na součty proskon $\exists U \cup V \xrightarrow{U \cup V \subseteq U + V}$

\supseteq : Užávrem $U + V \supseteq U \cup V$ a $U + V \subseteq W$, pro věty $\forall x \in U \cup V$

$U + V \subseteq W$ ovětme užávrenost na součty a množby

Mějme $x_1, x_2 \in U + V$ a skladbu $\Rightarrow x_1 = u_1 + v_1, x_2 = u_2 + v_2$ $u_1, u_2 \in U$ a $v_1, v_2 \in V$

Součty: $x_1 + x_2 = u_1 + v_1 + u_2 + v_2 = (u_1 + u_2) + (v_1 + v_2) \in U + V$

Množby: $\{x_1 = u_1 + v_1, x_2 = u_2 + v_2\} \subseteq U + V$

Dimenze upozornit: Věta: Pro podprostory U, V VP_W W plati: $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$

Ds: 2 užávrenosti podprostoru na prvního $\Rightarrow U \cap V \subseteq W$ a mě bázi $x_1 \dots x_d$ \Rightarrow a věty o rovněžnosti na

bázi rozšíření na $x_1 \dots x_d$ a $x_1 \dots x_m$ podprostoru U a $x_1 \dots x_d$ $y_1 \dots y_n$ podprostoru V

Užávrem: $x_1 \dots x_d$ $y_1 \dots y_n$ $x_1 \dots x_m$ je báze $U + V$ (užávrem, že jsou to generátory a je lin. nesav.)

Generičnost: máme $x \in U + V$ pak $x = u + v$ pro $u \in U$ $v \in V$

$$\text{nejednáme } n = \sum_{i=1}^d \alpha_i x_i + \sum_{j=1}^m \beta_j y_j \quad \text{a } v = \sum_{i=1}^d \gamma_i x_i + \sum_{j=1}^n \delta_j y_j$$

$$\text{pak } x = u + v = \sum_{i=1}^d (\alpha_i + \gamma_i) x_i + \sum_{j=1}^m \beta_j y_j + \sum_{j=1}^n \delta_j y_j$$

je lin. komb. $x_1 \dots x_d, x_1 \dots x_m, y_1 \dots y_n$

lineární nezávislost: chceme udělat, že všechny koeficienty $\alpha_i, \beta_j, \gamma_i, \delta_j = 0$ $\Rightarrow 0 = \sum_i \alpha_i x_i + \sum_j \beta_j y_j$

onečinné $x = \sum_i \alpha_i x_i + \sum_j \beta_j y_j = \sum_i \alpha_i x_i \Rightarrow x \in U \cap V$ leží mezi $\alpha_i = \sum_{i=1}^d \alpha_i x_i = \sum_{i=1}^d \beta_i x_i + \sum_{j=1}^m \beta_j y_j = 0$

$x_1 \dots x_d, y_1 \dots y_n$ jsou lineárně nezávislé $\Rightarrow \alpha_1 = \dots = \alpha_d = \beta_1 = \dots = \beta_m = 0$ po dosazení $\sum_i \alpha_i x_i + \sum_j \beta_j y_j = 0$

$x_1 \dots x_d, x_1 \dots x_m = 0 \Rightarrow \alpha_1 = \dots = \alpha_d = \beta_1 = \dots = \beta_m = 0$

Potom $U \cap V = \emptyset$ pak $U + V$ nazveme direktním součtem podprostorů a nazávme $U \oplus V$

Každý $w \in W$ může zapsat jako jedinou způsobem $w = u + v$ $u \in U$ $v \in V$

$$w: Q^2 = \text{span}\{e_1\} \oplus \text{span}\{e_2\}$$

Důsledek: $\dots v_1 \dots v_n$ jsou lin. závislé $\Leftrightarrow \text{span}\{v_1 \dots v_n\} = \{v_1 \dots v_{n-1}, v_{k+1} \dots v_n\}$

meboť $v_k \dots v_n$ jsou LGS již nesou množinu nadbýčku pro generování

Důsledek: B : minimální - prioritní jsou generátorky

$$\Sigma: \text{librový } w = \beta_0 v_0 + \sum_{i \neq 0} \beta_i v_i \Rightarrow w = \beta_0 \left(\sum_{i \neq 0} v_i \right) + \sum_{i \neq 0} \beta_i v_i \Rightarrow w = \sum_{i \neq 0} (\beta_0 l_i + \beta_i) v_i$$

$$\Leftrightarrow \text{a někdy } v_k \in \{v_1 \dots v_{k-1}, v_{k+1} \dots, v_n\} = \{v_1 \dots v_n\}$$

$$\text{span}\{v_1, v_2, \dots, v_{k-1}, v_k\}$$

Def: Nechť V je VP, kdežto je základní lin. nezávislý systém generátorů pro prostor V .

... systém generátorů V minimální co do inklinace

Nejdříve máme

Kanonická báze v P^n $\{e_1 \dots e_n\}$, kde e_i má 1 na pozici i , jinde 0
 P^n má bázi $1, x, x^2 \dots x^n$

Této: Nechť $B = \{v_1 \dots v_n\}$ je bázi VP V , pak $k_i \in V \exists k_1 \dots k_n \in T$

podrovnění: $w = \sum_{i=1}^n a_i v_i$

Dk: Dostatečné: 2 definice báze $\{k_1 \dots k_n\}$ t.j. $\sum_{i=1}^n k_i = w$

Stavomyslost: Sporem $k_1 \dots k_n, B_1 \dots B_n$ pro nejazec k_i se $k_i \neq B_i \Rightarrow$

$$\Rightarrow w - w = 0 \Rightarrow \sum_{i=1}^n v_i - \sum_{i=1}^n B_i v_i = 0 \Rightarrow \sum_{i=1}^n (k_i - B_i) v_i = 0, \text{ zvlášť pro } k_i - B_i \neq 0 \text{ spolu s lin. nezávislostí}$$

Koefficienty $k_1 \dots k_n$ nazývame souřadnicemi $[w]_B$

s lin. nezávislostí

$$\text{Vlastnost: } [u+v]_B = [u]_B + [v]_B \quad \text{a} \quad [lu]_B = l[u]_B$$

Věta o dílečné bázi: Každý VP má bázi

Dk pro konečně generované VP:

Nechť $v_1 \dots v_n$ je systém generátorů VP

pokud jsou $v_1 \dots v_n$ lin. závislé \Rightarrow koňčí bázi

Jinak podle důsledku vykazujeme v_k takový: $\text{span}\{v_1 \dots v_n\} = \text{span}\{v_1 \dots v_{k-1}, v_{k+1} \dots v_n\}$

což je nerovna bázi

měsídy míté srozumě protiže $v_1 \dots v_n$ je konečný

□

Malá Fermatova věta

Pro každou prvočíslo p a nemurové $a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod p$

$$\mathbb{Z}_p = 1 \text{ v klasickém } \mathbb{Z}_p$$

$$\begin{aligned} \text{Důkaz: } a \text{ prvočíselnosti } \{0, 1, 2, \dots, p-1\} &= \{0a, 1a, \dots, (p-1)a\} \\ \text{pravočíslo } 0a = 0 &\quad \{1, \dots, p-1\} = \{1a, \dots, (p-1)a\} \\ 1 \cdot 2 \cdot \dots \cdot (p-1) &= (1a) \cdot (2a) \cdots (p-1)a \\ &\text{uprostřed } 1 \cdots p-1 \\ 1 &= a \cdot a \cdots a = a^{p-1} \end{aligned}$$

Zamořené řady

- solvenciální - dekorace 1. řady ; zdrojemi - oprava 1. řady

- Hammingov řada (7, 4, 3) - generující matice , detektivní matice

Vektorové prostor

- reprezentace \mathbb{R}^n

Def: Bud T kolo s neul pravky $0, 1$ pro sečk. a násob.

Vektorový prostor nad T je množina V s operacemi sečkání vektorů
+ : $V^2 \rightarrow V$ a násobení vektoru skalárem $\circ : T \times V \rightarrow V$: $\forall a, b \in T, v \in V$:

1. $(V, +)$ je Abelova grupa

2. $(\lambda \beta)v = \lambda(\beta v)$ asociaativita

3. $1v = v$

4. $(\lambda + \beta)v = \lambda v + \beta v$ distributivita

5. $\lambda(v + w) = \lambda v + \lambda w$ - " -

Prí: \mathbb{R}^m ; prostor matic $T^{m \times n}$, P -polynomy proměnné X , \mathbb{P}^n stupně $\leq n$
f všechny reálné funkce, C spojité funkce, $C_{a,b}$ v intervalu

Jednotné - základní vlastnosti

1. $0v = 0$

Def: analogie k kolům

2. $\lambda 0 = 0$

3. $\lambda v = 0 \Rightarrow \lambda = 0 \vee v = 0$

4. $-v = (-1)v$

Vektorový podprostor

$U \subseteq V$ je podprostорem pokud když VP nad T se stejnými

operacemi. an. $U \subseteq V$.

Char.: U musí mít o v když množinu na obě operace

1. $0 \in U$

2. $\forall u, v \in U : u + v \in U$

3. $\forall \lambda \in T, u \in U : \lambda u \in U$

prí: kolo $V \subseteq V$, $\{0\} \subseteq V$

Def: \Rightarrow pokud $U \subseteq V$, kde když má vlastnosti

splňuje

prí: kolo $P \subseteq \mathbb{C}[X]$

je kolo množina když má vlastnosti

symetrické množ. rádiu $r \in \mathbb{R}^{>0}$

když má vlastnosti na množinu

$Q \subseteq \mathbb{Q} \subseteq \mathbb{Q}^m$ nad \mathbb{Q} a $\mathbb{Q}^m \subseteq \mathbb{R}^m$ nad \mathbb{R}

je kolo množina když má vlastnosti

an 2. $(-1)v = -v$

Symetrická grupa (S_n, \circ)
 ↗ vlastnosti
 možnost permutací

Rozšiřovací grupa je isomorfna nějaké podgruppe symetrické grupy S_{48} -mubikova rovnice

Tělesa

- robenem i sítěmi oboru

Def.: Těleso je možina T spolu se dvěma binárnimi komutativními operacemi $+ a \circ$

1. $(T, +)$ je abelova grupa (neutralní prvek 0 , inverzni $a - a^{-1}$)

2. $(T \setminus \{0\}; \circ)$ je abelova grupa (1 a^{-1})

3. $\forall a, b, c \in T : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita)

Rozděl těleso má aspoň 2 prvky, $0 \neq 1$

inversní operace $-a / a^{-1}$ $a - b = a + (-b)$
 $a / b = a \cdot (a^{-1})$

podtěleso

příklady: Q, R, C

$\{0, 1\}$ sčítání násobení mod 2

((Quaternion)) - nekomutativní těleso

Základní vlastnosti těles

$$1. 0a = 0$$

$$2. ab = 0 \Rightarrow a = 0 \vee b = 0$$

$$3. -a = (-1)a$$

Vlastnosti grup (G, \circ)

1. $a \circ c = b \circ c \Rightarrow a = b$ pravem'

2. neutrální prvek je užíván jednoznačně

3. $\forall a \in G$ má právě 1 inverzní prvek4. novice $a \circ x = b$ má právě 1 řešení $\forall a, b \in G$

5. $(a^{-1})^{-1} = a$

6. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Dle 1. $a \circ c = b \circ c \Rightarrow a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1}) \Rightarrow a \circ e = b \circ e \Rightarrow a = b$

recht. návazecy

2. $\ell_1 = \ell_1 \circ \ell_2 = \ell_2 \Rightarrow \ell_1 = \ell_2$

3. recht. inverzní prvek $a_1, a_2 \neq a \Rightarrow a_1 \circ a = a_2 \circ a \Rightarrow a_1 = a_2$

4. $a \circ x = b$ vynakládání sleva $a^{-1} \Rightarrow x = a^{-1} \circ b$ - to je jednoznačné

5. krit. a na obě strany

6. krit. $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$

Podgrupa

def podgrupa (G, \circ) je $\#(H, \circ)$ k.t. $H \subseteq G$ a $\forall a, b \in H$ $a \circ b = a \circ b$ pravem' $(H, \circ) \subseteq (G, \circ)$ prv: primitivní podgrupy $(\{e\}, \circ)$; $(\{e\}, \circ)$

Permutation

* bijekce --- prosté a mnoho

* permutace na X je bijekce $\pi: X \rightarrow X$ * S_n = množina všech permutací

Zápis: Salut! -- nahoru vzory, dolu obrany

graf



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

rozložení na cykly $(1, 2)(3)(4, 5)$

.. obrázek je následný

identita: id

$$(1, 2)(4, 5)$$

transpozice: jediný cyklus délky 2, pravosměr i, j

$$(i, j)$$

Inversion makes a SCR

Q regulärer $\Rightarrow Ax = b$ je äquivalent zu $(QA)x = (Qb)$

Dl: Žádné různe měřitelné prokore spěch mizíme jít násobeném

Q^{-1} slava =

dividir por A regular:

Neha: sonshava movie & inversion matrix

$$A \in \mathbb{R}^{n \times n} \text{ regularne} \Rightarrow \overset{\text{rever!}}{A^{-1}} x = b \quad \text{je dano} \quad x = A^{-1} b$$

Geometrie

$A \in \mathbb{R}^{n \times n}$ regulär! , so dass es $x \mapsto Ax$

$$\forall y \in R^n \exists x \in R^m Ax = y$$

- roba zem' je bijele
- inverzni mat. predstavljaju $y \mapsto A^{-1}y$

$Ax = b$ nesem znamená hledat vektor b při zadání $x \mapsto Ax$

pozorní složení zobrazenem $a \mapsto (BA)^{-1} a$

$$R \mapsto (A^{-1}S^{-1})R$$

Matice elementárních úprav

- množství zleva "elementární úpravou"

$$\text{pravidelné a nepravidelné} \\ E_{ij} = \begin{pmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots \end{pmatrix}$$

Věta: $A \in \mathbb{R}^{m \times m}$, $\exists Q \in \mathbb{R}^{m \times m}$ (regulařní): $RREF(A) = QA$

Důkaz: $RREF$ je konečné mnoho elementárních kroků

$$RREF(A) = E_k \dots E_2 E_1 A = QA \quad \text{dok } Q = \underbrace{E_k \dots E_1}_{\text{regulařní}} \quad \Rightarrow Q \text{ regulařní}$$

Jednačka: $\forall A \in \mathbb{R}^{n \times n}$ lze vyjádřit jako součin konečné mnoha el. matic
Důkaz: A doraženým úpravami do $I_n \Rightarrow I_n$ mohou úpravit na A , protože bezdále el. úprava má invenci

Inverzní matice

$$\text{Def: } B^{-1} = I_n = B^{-1}B$$

Věta: \Leftrightarrow existuje inverzní matice

$$\text{Podle } A \in \mathbb{R}^{n \times n} \quad A \text{ je regulařní} \Rightarrow \exists A^{-1} \text{ všechna jednoznačně} \\ \exists A^{-1} \quad \Rightarrow A \text{ je regulařní}$$

Důkaz: existence

$$A \text{ je regulařní} \Rightarrow Ax = e_j \text{ má řešení } x_j \quad \forall j$$

uvažujeme $A^{-1} = (x_1 | x_2 | \dots | x_n)$ je hledaná inverze

$$1. AA^{-1} = I \quad \text{po slovách } \dots \forall j \quad (AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = I_{*j}$$

2. ^{prokazat}

$$AA^{-1}(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$$

$$\text{tedy } \forall j \text{ platí } A(A^{-1}A - I)_{*j} = 0 \quad \text{a regulařit } A(A^{-1}A - I)_{*j} = 0 \Rightarrow A^{-1}A = I$$

Důkaz: jednoznačnost

$$\text{neplatí } AB = BA = I$$

$$B = B(I) = B(AB^{-1}) = (BA)B^{-1} = IA^{-1} = A^{-1}$$

Důkaz: 2. implikace

neplatí pro A existuje inverzní matice, když x řešení $Ax = 0$, pak

$$x = (Ax = (AA^{-1})x = A(Ax)) = A^{-1}0 = 0 \quad \text{tedy } A \text{ je regulařní}$$

Ausz: $A \in \mathbb{R}^{m \times n}$ nur plausibel

$$1. Ae_j = A_{*j}$$

$$2. \cancel{A^T = A_{ij}^*} \quad l_i^T A = A_{i*}$$

Ausz.

$A \in \mathbb{R}^{m \times m}$ $B \in \mathbb{R}^{n \times p}$

$$1. (AB)_{*j} = A B_{*j}$$

$$2. (AB)_{i*} = A_{i*} B$$

dR 1:

$$(AB)_{*j} = (AB)e_j = A(Be_j) = AB_{*j} \quad \square$$

Grundmaße a verloren

Ausz: $A \in \mathbb{R}^{m \times m}$ $x \in \mathbb{R}^m$ $y \in \mathbb{R}^m$

$$1. Ax = \sum_{j=1}^m x_j A_{*j}$$

$$2. y^T A = \sum_{i=1}^m y_i A_{i*}$$

$$1. \left(\alpha A_{*1} A_{*2} \cdots A_{*m} \right) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ A_{*1} \\ A_{*2} \\ \vdots \\ A_{*m} \end{pmatrix} x_1 + \begin{pmatrix} 0 \\ A_{*1} \\ A_{*2} \\ \vdots \\ A_{*m} \end{pmatrix} x_2 + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} x_m$$

Operace s maticemi

Def: rovnost: 2 matice se rovnají $A=B$ pokud mají stejný rozměr $m \times n$ a $A_{ij}=B_{ij}$ pro všechna případná i, j

Def: součet $A, B \in \mathbb{R}^{m \times n}$ $A+B$ je matice $m \times n$ s průzky $(A+B)_{ij} = A_{ij} + B_{ij}$ pro případná i, j

Def: násobek $\lambda \in \mathbb{R}$ λA má průzky $(\lambda A)_{ij} = \lambda A_{ij}$

\rightarrow odčítání $A + (-1)B$

mluví matice 0 nebo $0_{m \times n}$

Vlastnosti součtu a násobku matic (pozemí) dle 1
operace, že mají stejný typ

$$1. A+B = B+A \quad \text{komutativita}$$

$$2. -(A+B)+C = A+(B+C) \quad \text{associtativita}$$

$$3. \lambda(A+B) = \lambda A + \lambda B \quad \text{distributivita}$$

$$4. (\lambda+\beta)A = \lambda A + \beta A \quad - \quad -$$

$$5. \lambda 0 = A$$

$$6. A+(-1)A = 0$$

$$7. \lambda(\beta A) = (\lambda\beta)A$$

$$8. 1A = A$$

$$(A+B)_{ij} = A_{ij} + B_{ij}$$

$$(B+A)_{ij} = B_{ij} + A_{ij}$$

$$A_{ij} + B_{ij} = B_{ij} + A_{ij}$$

$$(A+B)_{ij} = (B+A)_{ij} \quad \square$$

Produkt matic \nearrow 1. má stejný počet sloupců jako 2. řádky

def: $A \in \mathbb{R}^{m \times p}, B \in \mathbb{R}^{p \times n}$ AB je matice typu $m \times n$ s průzky

$$(AB)_{ij} = \sum_{k=1}^p A_{ik} B_{kj}$$

Vlastnosti

$$1. \text{ obecně } AB \neq BA$$

$$2. (A B)C = A(BC) \quad \text{associtativita}$$

$$3. A(B+C) = AB + AC \quad \text{distributivitaleva}$$

$$4. (A+B)C = A(C+B) \quad - \quad - \quad \text{sprava}$$

$$5. \lambda(A+B) = (\lambda A) + (\lambda B) = A(\lambda B)$$

dle: associtativita

$$A \in \mathbb{R}^{m \times p}, B \in \mathbb{R}^{p \times n}, C \in \mathbb{R}^{n \times m}$$

$$\begin{aligned} & \text{obě } (AB)C \text{ a } A(BC) \text{ jsou } m \times n \\ & ((AB)C)_{ij} = \sum_{k=1}^p (ABC)_{ik} C_{kj} = \sum_{k=1}^p \left(\sum_{l=1}^p A_{il} B_{lj} \right) C_{kj} \end{aligned}$$

$$\begin{aligned} & \text{sprava } (A(BC))_{ij} = \sum_{k=1}^p A_{ik} (BC)_{kj} = \sum_{k=1}^p A_{ik} \sum_{l=1}^n B_{kl} C_{lj} \\ & \text{výsledky jsou shodné až na pořadí sčítaní} \end{aligned}$$

sloupec dole je pivot jsem basice'

plodnost matice

pocet nemlujicich radku v REF rank(A)

dobre definovani prokaze posice pivota jsem jednoznamen

Algoritmus REF

1. $i = 1 \ j = 1$

2. if $a_{11} = 0 \ \forall k \geq i \wedge \forall l \geq j$ then donee

3. $j^* = \min \{l | l \geq j, a_{ll} \neq 0 \text{ pro nizkade } k \geq i\}$

4. mci $a_{ij} \neq 0, k \geq i \text{ a ryeme } A_{ik} \neq A_{jk}$ // ryeme ne na
nizkade kde je na
mimo policko

5. $\forall k > i \text{ polož } A_{kj} := A_{kj} - \frac{a_{ij}}{a_{ii}} A_{ik}$ // ryeme policko

6. $i++ \ j++ \ goto 2.$

punk. v INF se zprasky vybral radek s nejvetsim abs(asj) viz Karacan
na
zadani
je
matice

Gaussova eliminace

mame $(A | b) \ A \in \mathbb{R}^{m \times n} \ b \in \mathbb{R}^m$

prevedene na REF $(A' | b')$, $r = \text{rank}(A | b)$

(A) nemam reseni

posledni sloupec jo basicky (\Leftrightarrow) v poslednim sloupcu jo pivot
 $\text{rank}(A) < \text{rank}(A | b)$

(B) ma reseni 1 reseni

$\text{rank}(A) = \text{rank}(A | b)$

(B1) jedinec reseni $n = r = \sum_{j=r+1}^n a_{ij} x_j$
spredna substitucia $x_{ri} = \frac{b'_{ri} - \sum_{j=r+1}^n a'_{rij} x_j}{a'_{rr}}$

(B2) neskoncne mnoho reseni $n < r$
nebasické promenne - parametry





Transmission parameters

latency - delay

jitter - variance of delay

data loss - needs resending or loss of information (can cause channel congestion)

bandwidth ("speed")

Order - we want to dedicate bandwidth x urgent messages

- QoS say

- best efforts strategy

History

isolated systems \rightarrow terminal systems \rightarrow WAN (consequently client-server)
proprietary lines + LAN

LAN

- geographically limited
- sharing resources (printers, Internet) of nearby computers
- mostly private and centralised

WAN

- public, managed by multiple organisations
- ~~data transfers~~

VPN

- private link connects to LAN through WAN
- encrypted

Internet history

60s - packet switching

69 - Arpanet

77 - network connected to ARPANET backbone

83 - TCP/IP dominates

80s TCP/IP into BSD UNIX

Request for Comments (RFC)

- Internet "standardization", information, best practices
- many rules are too restrictive \rightarrow users and servers violate
- recommendation receiver: liberal sender: conservative



zadává paměť i na svůj R - protokol

adresu bajku

pamatový adresový prostor \rightarrow adresy $0 - (2^n - 1)$

kapacitační rozsahy 8b

1B ... 10b

$MB = 1024 \cdot B$

≈ 1024 bajky

čísla v řádku jsou výrobci periférních čipů

1MiB mezičípele, kterou můžete nejdřív vidět

paměť v registered - latch (4-6 transakcí)

SRAM (RANDOM access memory)
(nejrychlejší)

{ slavnostní zápis - nejdříve si paměť
random ... nejpravděpodobnější! } \rightarrow operace slavnostní nebo mezi
čipem a zápisem 10-100GB/s

čipem je sepsan
volatile

access time < 1ms

Pamatová 1B - 1KB - 1MB

DRAM 1GB - 10 GB

1bit \approx 1 kondenzátor, 1 transistor

dynamická paměť \rightarrow nás rapsodem
- refresh

rychlosť 1 - 10 GB/s
access time ~ 10 ns

slovo (word)

- jednotková přenosu mezi 8b slovo

n-bikové slovo \Rightarrow n-bikové paměti

doubleword (dword), opword

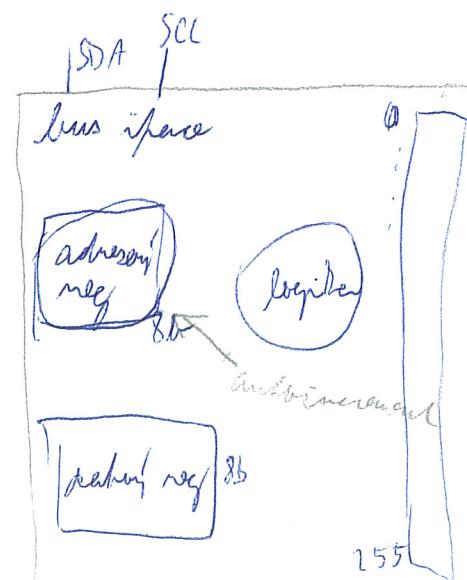
standardní definice: 16-b

burst přenos ... aktivace

čipem: nápis do adresy než 2 transakce

čipem s další než 2

v DRAM čipem myslíši než sepsan

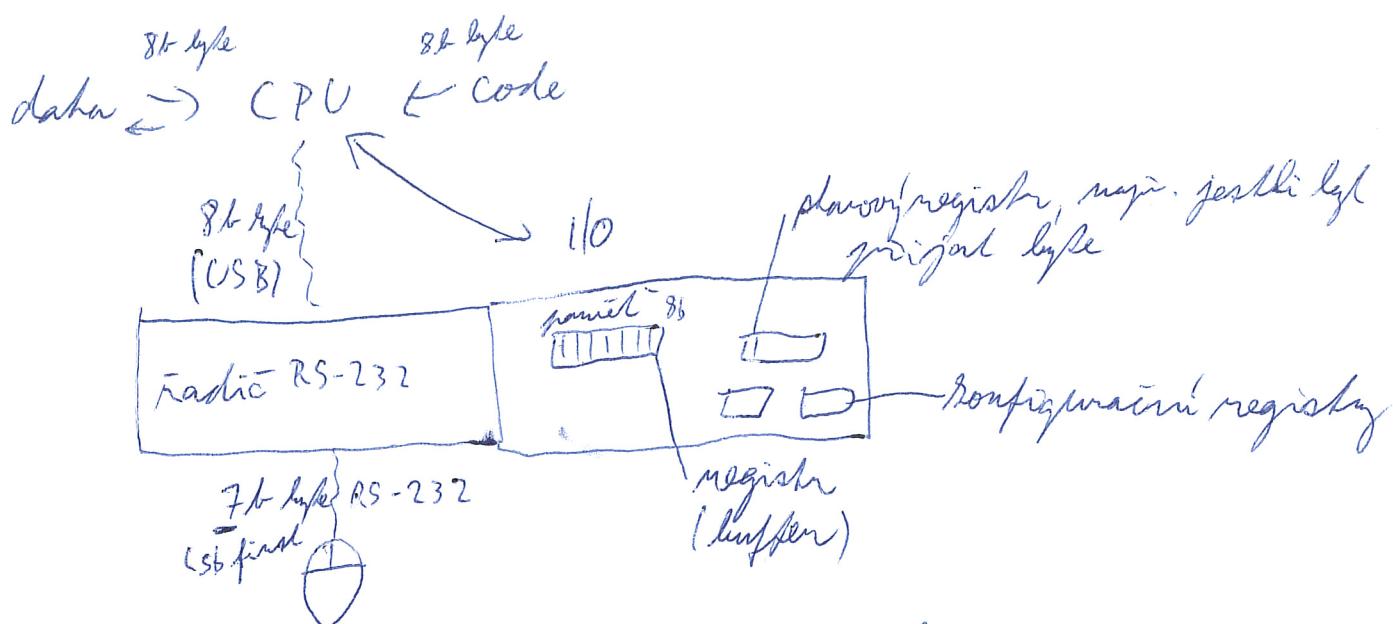




~~Radic~~ PP

P02 S02

Radic RS-232



Python: pip instal pyserial

```
import serial
```

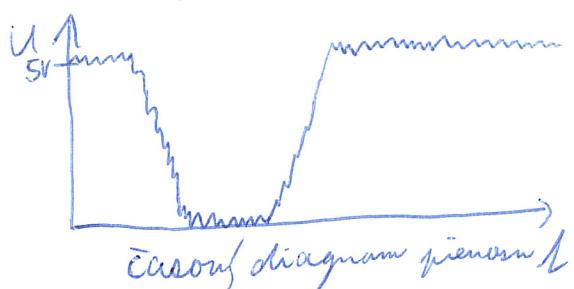
```
    . . . timeout = 0.5 . . .
```

```
serialPort = open() načítá konfiguraci do radice
```

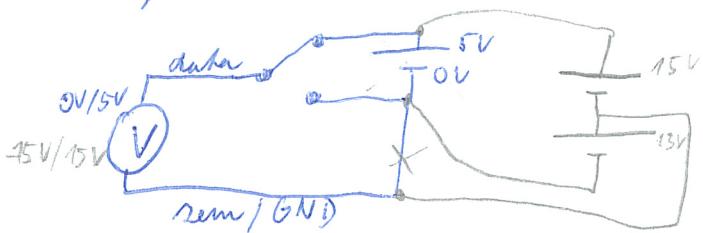
Binary file

Sériový prenos

1011

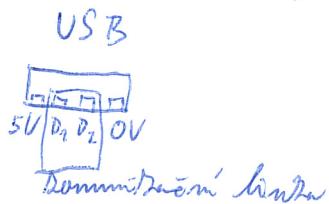
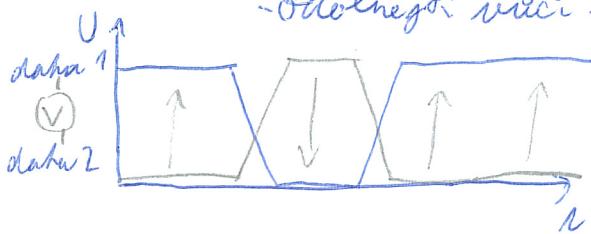


typického vývaha



2 vodice - diferenciální prenos

- odděleným vodičem - oba vodice stejně polarizované



interpretace čísel

mocniny 2

1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	...	65536	$\sim 10^6$
2^4								2^8		2^{10}		2^{12}		2^{16}		2^{20}

 $\sim 16\ 000\ 000$ $\sim 4200\ 000\ 000$ 2^{24} 2^{32} poradí bitů $\frac{1011}{MSb\ LSb}$ $LSb \times MSb$ první bikorden

1011

délka linky \rightarrow prenosová rychlosť (transfer rate) b/s band (symbol/s)
synchronizace?