

Principy počítaců

P01S01

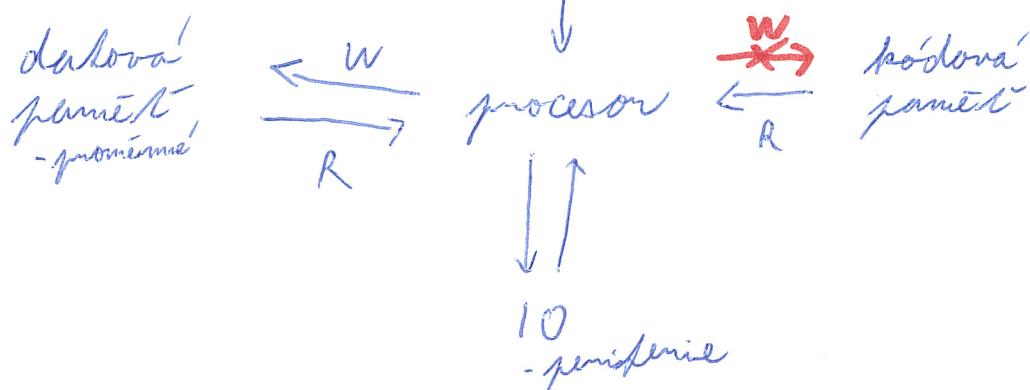
na předmětu pouze abstrakce

v algoritmu je důležitá hromadnost

plánovací architektura

programovatelný součástka
nemá pevně danou funkci

externí magie



Charles Babbage

Analytical engine 1837

Turing complete

podobná architektura na pánu

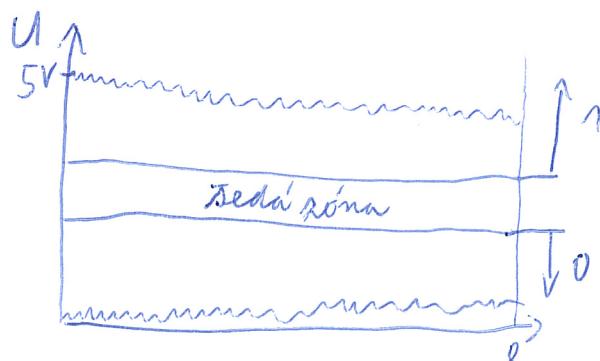
Ada Lovelace

mammal s te

vise převodem libovolných dat na čísla

Reprezentace čísel

Fyzika je kvantová → vodiče mají odpor
odpor se mění s teplotou
elektromagnetického záření odolu
analogový přenos - hodnota napětí reprezentuje číslo
digitální přenos $0V = 0 / 1 = 5V$ bit





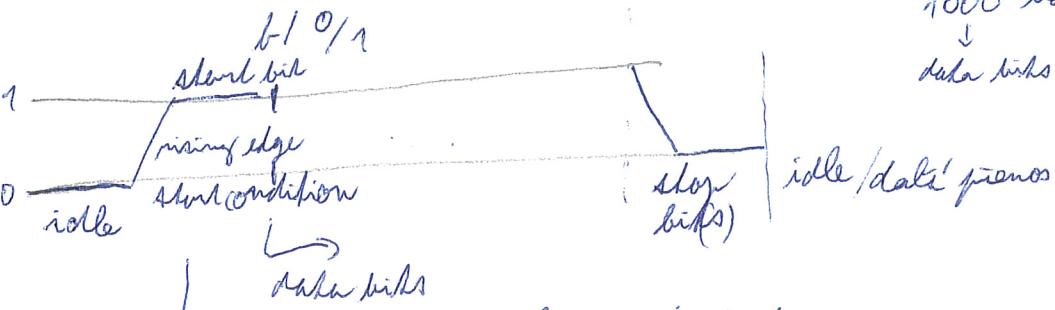
první dleba bitu **RS-232**

- problém se synchronizací

1 1 1 1

3-slav logika $\frac{0}{1}$

- idle at floating start/Hi-Z



1000 baud ... 1 písmo
↓
data bits (bps)
idle/dataline periods

20% overhead

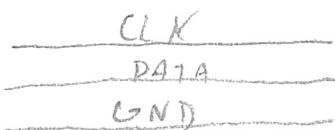
rozšemka

prvajíci si synchronizuje hodiny

- pořád se může stát desynchronizace v pořadí ... max N bit

ii
8→bajl B

Linka s clock signálem **I²C**



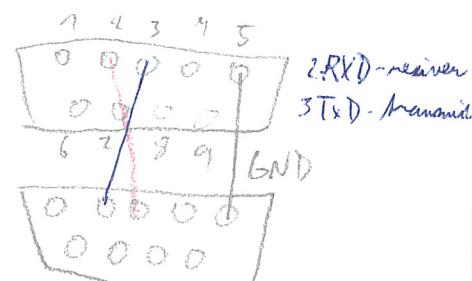
DATA

CLK



- méně praktické, lepší je o pol periody posunout a čist, tedy na CLK rising edge falling

volnou aboje
DDR písmo



out of band signály
- když se dělá něco mimořádného

Simplex x duplex písmos

→ half duplex - po 1 lince

→ full duplex - nesavislé linky **RS232**

Kommunikacní protokol

- definovaný paket

read - běžící funkce

respektive soušava

$0x23$ $\$23$ 23_h 23_{16}

get()

format(a, "04X")

naší cípy (dorovnat nulami)

bitové operace

a oper b \rightarrow c
 n-bit n-bit n-bit

operace se provádí rezonančně po bitech

OR | - jiná interpretace (bitmask) NOT ~

set 1010 hodnota
 1100 prázdnas

AND & prázdnas : když 1 každý sádrový
 reset

XOR ^ selective flip

Příkazé posuny

SHL / posun doleva / <<

a << x → b
co je to
očekávám
posun směrem k MSB

$\begin{array}{r} 1101 \\ \times 010 \\ \hline 11010 \end{array}$ SHL 1

posun směrem k MSB

SHR / posun doprava

z LSb a >> x → b

$\begin{array}{r} 1101 \\ \times 001 \\ \hline 001 \end{array}$ SHR 2

rotate left / ROL

$\begin{array}{r} 1101 \\ \times 0110 \\ \hline 1101 \end{array}$ ROL 3

rotate right / ROR

problem dvojité mít

selection (deplň)
+ → jde o unsigned
- → NOT(abs(a))

unsigned integers
n bitů 0 - $2^n - 1$

signed integers
1 sign bit n-1 value
rozšíření operač.

dvojí rozšíření

+ → unsigned

- → NOT(abs(A)) + 1

rozšíření mít signed compare

rozšíření

nint8 - rozšíření n-bit typ považovat mod 2^m

zero extension - dešifra smysl pro unsigned

signed extension

$\begin{array}{r} 0101 \\ \times 1000 \\ \hline 0101 \end{array}$

rozšíření smysl MSB

RS-232
full duplex
seriální

datový přenos - operační přenos -

master - chee data
slave - předávané data

write ↑ read

směrov se mění role

CPU je vždy master

→ připravuje načítat předávané data z masteru

point to point

multidrop linka (bus) ((abérnice)) → CPU

- identifikaci slaven: adresa: min 7 max 127

- adresy jsou rozloženy na 7bit

- half duplex - každý slaven má receiver a transmitter

- full duplexer - linka ve slaven 1, poté nejake následující slaven 0 (and so on)

I²C (Inter Integrated Circuit)

- SDA - serial data

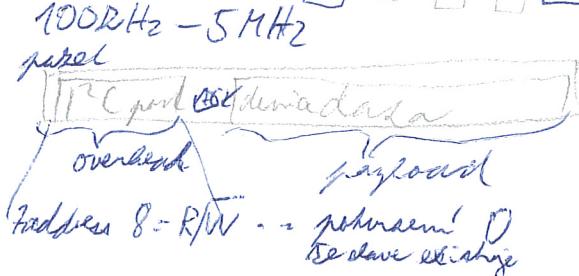
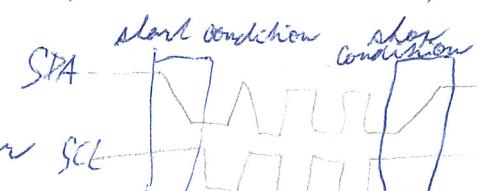
- SCL - serial clock - poslouží pro synchronizaci generuje master

- multimaster x (USB - single master)

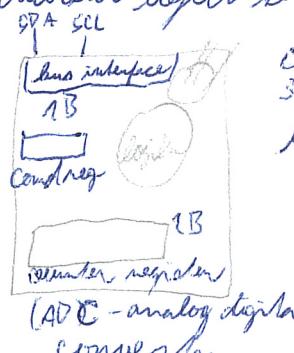
- 9 bit - byte 8b + ACK (NAK)

- MSb first, ACK v obrácené hodnotě ACK

- Clock stretching - slave obdrží CLK na 0



Ambient light sensor (ALS)



číslování adresy
START/STOP příkaz

hardwareově zadávaná adresa

write only register (cmd)

read only register (ADC)

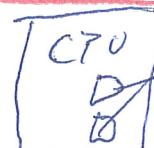
RW register

LSB first

instrukce - v byte

instrukční sada

posloupnost instrukcí - machine code



registry

PC - Program counter

IP - Instruction pointer

- adresa instrukce

- velikost adresového prostoru



opcode argumenty (adresy paměti)

magická architektura přepisuje z data do code memory

překladač + interpret

endianství (endianness)

LSB-first - little endian LE → deino sýnobem
procesor

MSB-first - big endian BE → dnes většinou LE

Von Neumannova architektura



rozdíly mezi magickou inicializací
RAM

historie

UNIVAC → ALTAIR 8000
1951 Intel 8080

1976 → APPLE 1 → APPLE 2

Apple II čip MOS 6502

→ ATARI 2600 → ATARI 800

1977

řídit slova v CPU

16 bit adresní prostor (64KB)

IBM PC - Intel 8088
1981 - 16 bit slovo
- 20 bit adresní prostor (1MB)

→ PC 64b
současnost 64b
Intel i3/i5/i7
magická instrukční sada
kterouž PC je návle

instrukce: v rozdílu k CPU jiné! assembler

NOP - posune IP na další instrukci NOP

Jump - - - na danou adresu JMP

immediate load do regA

LDA

load z adresy

regX

LDX

Store

STA

Copy

STX

TAX

v CPU
speciální reg
obecné registry
- load pomocné
- STORE

Communication

- Identification - introduction needed
- Method - you need to use common methods
 - Language
- Speed
- Process
- Types - human
 - telecom - centralised, only interface in telephone
 - computers - embedded logic, network only manages transmission
 - converged network (VoIP, mobile internet)

Mail



Same actions in email

circuit switching

- if broken data is lost
- faster, less reliable

packet switching

- each packet finds its own way
- slower, fault-tolerant

Security

- new requirement - now it's simple to have malicious software
- authentication, antivirus, encryption

Scalability

- layers - core - ~~backbone~~ connection to ISP
 - routers, switches (can be in separate room)

(LAN)

- distribution - cables and switches
 - vertical layer
- access layer - terminated as close as possible to users
 - access for end devices

Tier 1 - direct access to Internet backbone

(WAN) Tier 2 - without access to backbone whose customers are ISPs

Tier 3 - ISPs who connect end customers

Algoritmus

- burovadny, konecny, vysledek lze nista mechanicky
- poslonyost konecneho počtu elementarnich kroků vedouci k řešení daneho typu úlohy

Programovaci jazyky

- prirozeny jazyk se nehodi

Prekladac vs. Internet

Python

- 1991
- open-source

R̍íšem' běhu programu

- skoř x shodzovanej programovani

al - Chování

- abstraktní řízení
- načítání algebra

↓

algoritmus

- vlastnosti
- konečnost
- hromadnost
- rezultativnost
- jednoznačnost
- determinismus

Formální modely

- Turingov stroj
 - Busy beaver
 - Počet znakov potřebných na napsání určitého počtu?
- | | |
|---|---|
| 1 | 1 |
| 2 | 4 |

3 6

4 13

5 ?

- RAM počítač
- Rekursivní funkce
- Lambda kalkul

invarianty algor.

Ověření správnosti

- paralelní výpočetnost
- konečnost

formální efektivity

- čas \rightarrow funkce velikosti vstupu
- prostor
- analýza - náborův průjezd
- primární
- pravděpodobnostní

úlohy: rozložit a nejdříve řešit, l. následně řešit

Asymptotická notace

O - asymptotická horní mezin

Ω - dolní mezin

Θ - funkce $f \in \Omega(g(n)) \wedge f \in O(g(n))$

například $s = f(n) = O(g(n))$

$$f(n) = f(n/2) + O(n)$$

měření délky vstupu

$a_1 \dots a_n$

n = počet pravé posloupnosti

graf

n = počet vrcholů

matice

n = počet řádek

n = ráz matice

přirozené číslo $\lfloor \log n \rfloor + 1$

Algoritmy Rekurzivní SLL

Test pravého selnosti

- brusle poře

- velké do Tn

Generování pravého sel

Erashošenovo síko - jivo rozdělí číslo výloučivě jeho násobky

vylepšení - posuvník od p^2

Matice

obdélníkové schéma $m \times n$ množina všech reálných matic $\mathbb{R}^{m \times n}$

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Lomený vektor

- matice typu $m \times 1$

* notace

 A_{i*} i-th řádek A_{*j} j-th sloupec

Řešení soustav lineárních rovnic

řešením je vektor vyhovující všem rovniciám

matice soustavy rozšířena

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad (A|b) = \left(\begin{array}{c|c} a_{11} & \dots & a_{1n} \\ \hline a_{m1} & \dots & a_{mn} \end{array} \right) | b_1 \quad | b_m$$

geometricky

 $2 \times 2 \rightarrow$ průnik 2 přímek $3 \times 3 \rightarrow$ průnik 3 rovinpro libovolné n rovnice popisuje nadrovník

Elementární maticové úpravy

uzávorem i lebo maticou reálnym číslom $\lambda \neq 0$

protože maticu

pričem' nasoben maticu λ jiném

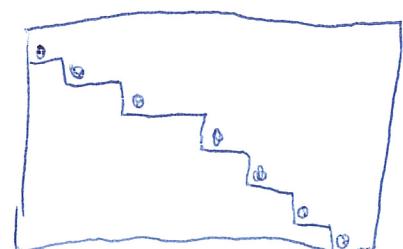
Odkupovování lva matic (REF)

Fm: řádky $1 \dots n$ jsou neměnné

m+1 ... m jsou měnné

$$p_i = \min \{ j : a_{ij} \neq 0 \}$$

$$p_1 < p_2 < p_3 \dots < p_n$$



Frobeniova věta: soustava $(A|b)$ má alespoň jedno řešení

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

přesněji
Lze dle řešit
jednotlivé

RREF

pivohy můžeme nastavit na 1

můžeme srovnávat hodnoty nad pivohem

$$\text{def: } a_{1p_1} = a_{2p_1} = \dots = a_{np_1} = 1$$

$$\forall i \in \{2, \dots, n\} \quad a_{1p_i} = a_{2p_i} = \dots = a_{np_i} = 0$$

RREF je jednoznačný

Gauss - Jordanova eliminace

převodové soustavy $(A|b)$ na RREF $(A'|b')$

základní
 \Leftrightarrow soustava nemá řešení

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

(B) alespoň 1 řešení

(B1) jediné řešení $n = n$
 \uparrow \uparrow # pivohy # proměnných

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & b_1 \\ 0 & 1 & 0 & 0 & b_2 \\ 0 & 0 & 1 & 0 & b_3 \\ 0 & 0 & 0 & 1 & b_4 \\ 0 & 0 & 0 & 0 & b_5 \end{array} \right) \quad \begin{array}{l} x_1 = b_1 \\ x_2 = b_2 \\ x_3 = b_3 \\ x_4 = b_4 \\ x_5 = b_5 \end{array}$$

zákonem mimo řešení!

(B2) několiké mnoho řešení $n < n$

$$x_{pr} + \sum_{\substack{j \in N \\ j > p_r}} a_{rj} x_j = b'_r \quad r = 1, \dots, n$$

nebozícké proměnné

zákonem!

Gaussova eliminace je \Leftrightarrow o $\frac{1}{3}$ rychlejší!

\Leftrightarrow - J. lze být třeba pro invenci matic

Jednotková matice řádu n
 Obverseová, na diagonále 1 $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix}$

Jednotkový vektor e_i : i-ty sloupec jednotkové matice $e_i = I_{xi}$
 Tzv: pro $A \in \mathbb{R}^{m \times n}$ platí $I_m A = A I_n = A$

Def: Transpozice matice

$$A \in \mathbb{R}^{m \times n} \quad A^T \in \mathbb{R}^{n \times m} \quad (A^T)_{ij} := A_{ji}$$

překlopení olehlavou diagonálou

tv. vlastnosti

1. $(A^T)^T = A$
2. $(A+B)^T = A^T + B^T$
3. $(\lambda A^T)^T = \lambda A^T$
4. $(AB)^T = B^T A^T$

dok: omezení stejného typu
 $A \in \mathbb{R}^{m \times n} \Rightarrow A^T \in \mathbb{R}^{n \times m} \Rightarrow (A^T)^T \in \mathbb{R}^{m \times n}$
 porovnání pravé strany
 $((A^T)^T)_{ij} = (A^T)_{ji} = A_{ij} \quad \square$

Def: Symetrická matice

$$A \in \mathbb{R}^{m \times n} \text{ je symetrická} \Leftrightarrow A = A^T \quad \text{napiš } I_m, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$$

Název: sym matice jsou vztahové na sonciel

nejspíru nazývané na sonciel

úvod: matice vzdálenosti, rovnicové matice, Hessián

Yončim vektorů

$$x^T y = \sum_{i=1}^n x_i y_i \quad \text{skalární součin}$$

$$x^T y^T = \begin{pmatrix} x_1 y_1 & \dots & x_1 y_n \\ \vdots & \ddots & \vdots \\ x_n y_1 & \dots & x_n y_n \end{pmatrix} = \begin{pmatrix} -x_1 y^T & - \\ \vdots & \vdots \\ -x_n y^T & - \end{pmatrix} = \begin{pmatrix} 1 & & 1 \\ x_1 y_1 & \dots & x_n y_n \\ 1 & & 1 \end{pmatrix} \begin{array}{l} \text{onejší} \\ \text{druhý} \\ \text{třetí} \end{array}$$

Avš. Matice $A \in \mathbb{R}^{m \times n}$ má hodnoty?

$$x_i^T x_j = 0 \quad x_i^T x_j^T = 1 \quad (\because x_i^T x_j^T = 1)$$

$\overset{\Leftrightarrow}{A = x^T y}$ jde nejdříve nejdříve
 vektor $x^T y$

LA1

PO3 SO1

Matice a lineární zobrazení

$A \in \mathbb{R}^{m \times n}$ \rightarrow zobrazení $x \in \mathbb{R}^n$ do \mathbb{R}^m definované $x \mapsto Ax$

jméno: $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ identity

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \cos \varphi - x_2 \sin \varphi \\ x_1 \sin \varphi + x_2 \cos \varphi \end{pmatrix}$ otáčení o φ

$\dots \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \dots \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$ projekce

\rightarrow řešit soustavu lin. rovnic $Ax = b$ znane vektory mají všechny vektory x , které se zobražují na vektor b .

\rightarrow složené zobrazení BA ... násobení matic

Regulařní matice

$A \in \mathbb{R}^{m \times n}$, A je regulařní, pokud $Ax = 0$ má jediné řešení $x = 0$
jinak je singulařní

Tzv: $A \in \mathbb{R}^{m \times n}$ může být jistou ekvivalentní

1. A je regulařní

2. $RREF(A) = I_m$

3. $\text{rank}(A) = m$

4. $\forall b \in \mathbb{R}^m$ má soustava $Ax = b$ jediné řešení

Tzv: $A, B \in \mathbb{R}^{m \times n}$ jsou ~~AB~~ regulařní $\Rightarrow AB$ je regulařní

Dk: Pokud x řešení soustavy $ABx = 0$, pak je $Bx = 0$, protože x je nulový vektor
 $y = Bx \dots Ay = 0$

$y = 0$ je regulařní matice A $x = 0$ je regulařní matice B

Tzv: Pokud je alespoň 1 z $A, B \in \mathbb{R}^{m \times n}$ singulařní, AB je také singulařní

Dk: 2 případů 1. B je singulařní $\dots Bx = 0$ pro nějaké $x \neq 0$
 $(AB)x = A(Bx) = A0 = 0$ tedy AB je singulařní (x nenulový řešením soustavy $ABx = 0$)
2. B je regulařní $\Rightarrow A$ je singulařní $\exists y \neq 0 : Ay = 0 \Rightarrow$
 $\exists x \neq 0 : Bx = y \Rightarrow (AB)x = A(Bx) = Ay = 0$ tedy AB je singulařní

Vlastnosti regulárních matic

Tzv. A je neg $\Rightarrow A^T$ je neg

$$\text{D}\ddot{\text{o}}: AA^{-1} = A^{-1}A = I_n$$

dáledej:

$$(A^T)^{-1} = (A^{-1})^T \text{ nebo } A^{-T}$$

$$(AA^{-1})^T = (A^{-1}A)^T = I_n^T$$

$$(A^{-1})^T A^T = A^T (A^{-1})^T = I_n \Rightarrow \text{matica } A^T \text{ má inversi} \Rightarrow \text{je regulární}$$

Věta jednou rovnost shodn

$A, B \in \mathbb{R}^{n \times n}$ $BA = I_n \Rightarrow$ obě maticy jsou regulární a vzájemné
inversní ... $B = A^{-1}$ $A = B^{-1}$

D\ddot{o}: Regulárna platí a vždy \& e. inversní matici když existují A^{-1}, B^{-1}

$$B = B I_n = B(AA^{-1}) = (BA)A^{-1} = I_n A^{-1} = A^{-1}$$

sak A symetricky \square

Výpočet inversní maticy

Věta² $A \in \mathbb{R}^{n \times n}$

$$A(I_n) = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 1 & 0 \\ 3 & 5 & 7 & 0 & 0 & 1 \end{array} \right) \xrightarrow{\text{RREF}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -0,5 & -6 & 3,5 \\ 0 & 1 & 0 & 1,5 & 1 & -0,5 \\ 0 & 0 & 1 & 3 & 1 & -1 \end{array} \right) = (I_n | A^{-1})$$

$$- \text{RREF}(A|I_n) = (I_n | B) \Rightarrow B = A^{-1}$$

- jinak je A singulární

D\ddot{o}: Zde RREF(A|I_n) = (I_n | B) \Rightarrow \exists Q\text{-regulární}: (I_n | B) = Q(A|I_n)

$$I_n = QA \quad a \quad B = QI_n$$

$$Q = A^{-1} \quad B = Q = A^{-1}$$

Přijměte nějakou kde RREF nedá (n
A je singulární) \square

Vlastnosti inversní maticy

$$1. (A^{-1})^{-1} = A$$

$$2. (A^{-1})^T = (A^T)^{-1}$$

$$3. (\alpha A)^{-1} = \frac{1}{\alpha} A^{-1} \text{ pro } \alpha \neq 0 \quad \text{D\ddot{o}: platí } (\lambda A)(\frac{1}{\lambda} A^{-1}) = \frac{\lambda}{\lambda} A A^{-1} = I_n$$

$$4. (AB)^{-1} = B^{-1}A^{-1} \quad \text{D\ddot{o}: } (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = A I_n A^{-1} = A A^{-1} = I_n$$

vzoreček pro $(A+B)^{-1}$ nem!

Grupy

Def: Grupa je dvojice (G, \circ) , kde G je množina a $\circ: G^2 \rightarrow G$ je binární operace na množině

správající

1. $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c$ asociativita

2. $\exists e \in G \forall a \in G : e \circ a = a \circ e = a$ neutrální prvek

3. $\forall a \in G \exists b \in G : a \circ b = b \circ a = e$ inverzní prvek

Abelova grupa

4. $\forall a, b \in G : a \circ b = b \circ a$ komutativita

Zdoby je \circ sčítání, neutrální prvek je 0 , inverzní - a
 \circ násobením a^{-1}

- příklad:

1. $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ $(\mathbb{C}, +)$

2. $(\mathbb{Q} \setminus \{0\}, \cdot)$ $(\mathbb{R} \setminus \{0\}, \cdot)$

3. grupa matic

4. Kongruenční grupa: $(\mathbb{Z}_m, +)$ kde $\mathbb{Z}_m \in \{0, \dots, m-1\}$, sčítání
 se provádí mod m

5. grupa polynomů $(\{f(x) : f \text{ je polynom}\}, +)$

ne mohou být Abelová

1. množina nesouhodobná s operací sčítání

2. množina nesouhodobná regulárních matic řádu n s násobením

Neogrupo

$(\mathbb{N}, +)$ (\mathbb{Z}, \cdot)

Operace s permutacemi

1. inverzí permutace p^{-1}

$$p^{-1}(i) = j \text{ znamená } p(j) = i$$

2. sčítání $p, q \in S_m$

nem' komutativní!

$$(p \circ q)(i) = p(q(i))$$

$$p \circ \text{id} = p = \text{id} \circ p$$

$$p \circ p^{-1} = \text{id} = p^{-1} \circ p$$

Znaménko permutace

$p \in S_m$ se sčítá s λ cykly

$$\text{sgn}(p) = (-1)^{\lambda}$$

$$\text{sgn}(\text{id}) = 1 \quad \text{sgn}((i, j)) = -1$$

Věta o znaménku složení permutace s transpozicí

$$p \in S_m, \lambda = (i, j) \in S_m \quad \text{sgn}(p) = - \underset{j}{\text{sgn}}(t \circ p) = - \text{sgn}(p \circ t)$$

Df: 1. i, j jsou ve stejném cyklu

nebo cyklus se rozloží na 2 $\Rightarrow \lambda = 1$

2. i, j jsou ve stejném cyklu

2 cykly se spojí v 1 $\Rightarrow \lambda = -1$

přesměněny
jsou
do i a j

Věta: Dvojice permutací lze rozložit na složení transpozic.

Df: Rozložení na transpozice rozložíme všechny cykly

$$\text{rozložení cyklu } (w_1 \dots w_n) = (w_1, w_2) \circ (w_2, w_3) \circ \dots \circ (w_{n-1}, w_n) \circ$$

důsledek:

$$\text{sgn}(p) = (-1)^n, \text{ kde } n = \#(i, j) \text{ v rozkladu } p$$

důsledek 2

$$\forall p, q \in S_m \text{ platí } \text{sgn}(p \circ q) = \text{sgn}(p) \cdot \text{sgn}(q)$$

důsledek 3

$$\forall p \in S_m \text{ platí } \text{sgn}(p) = \text{sgn}(p^{-1})$$

Konečná tělesa

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

$$-\mathbb{Z}_2, \mathbb{Z}_3 \quad \mathbb{Z}_4 \text{ ne protože nelze } \mathbb{Z}^{-1}$$

Lemma

pro prvočíslo n a $a \in \mathbb{Z}_n$ jíž nesoběžné mod n
 platí $\{0, 1, \dots, n-1\} = \{0a, 1a, \dots, (n-1)a\}$ (řádky jsou se nesoběžné)

Důkaz: sponem $ka \equiv la \pmod{n}$ pro $k, l \in \mathbb{Z}_n$
 nebo $(k-l)a \equiv 0$, protože n je prvočíslo n delí $k-l$
 protože $n > a$, $k-l$ nebo $a \neq 0$ nebo $k-l = 0$ \square

Věta

\mathbb{Z}_n kroví těleso $\Leftrightarrow n$ je prvočíslo

Důkaz: \Rightarrow sponem $n = pq$ pro $1 < p, q < n$
 žež \mathbb{Z}_n těleso $pq \equiv 0 \pmod{n} \Rightarrow p=0 \vee q=0 \pmod{n} \quad \square$

\Leftarrow ověříme axiomy tělesa, existence inverse a^{-1} plyne z lemma (na důkazu, kritické)

(takže násobky a musí být 1) \square

- předchozí výsledky (Gaußova eliminace) platí nad libovolným tělesem
 $\mathbb{F}^{m \times n}$ matice nad tělesem \mathbb{T}

Věta o velikosti konečných těles

Konečná tělesa existují o velikostech pravé p^n kde p je prvočíslo a $n \geq 1$

$GF(p^n)$ - polynomický řetězec $n-1$ s koeficienty $\in \mathbb{Z}_p$
 sčítáním jaro jaro reálné polynomy
 nesoběžný - \square mod irreducibilním polynomem
 sčítání n

- Galois field - každé konečné těleso je izomorfum

Charakteristika tělesa

def: nejmenší n takové, že $\underbrace{1+1+\dots+1}_n = 0$
 nejdříve nebo 0

$p \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$ mají danou $\mathbb{Z}_p - n$

Jihoa: charakteristika rozděleného tělesa je 0 nebo prvočíslo

Důkaz: $1 \cdot 0 \neq 0 \cdot 1 \Rightarrow$ dan nemůže být 1

sponem: $n = p \cdot q$ $0 = \underbrace{1+1+\dots+1}_{n=pq} = \underbrace{\underbrace{(1+1+\dots+1)}_{p} \underbrace{(1+1+\dots+1)}_{q}}$
 následe ab=0 $\Rightarrow a=0 \vee b=0$, nebo $q=0 \quad \square$

Lineární obal

Výs: Nechť V je VP nad \mathbb{T} . Pak \cap libovolného systému $(V_i)_{i \in I}$, VPP je také VPP V .

Důk: Prodele abstraktní definici $\cup \in \Delta_{\text{rel}}$, V_i a určení množiny \cup s vlastními vlastnostmi a následně dle.

$\forall i : V_i \neq \emptyset \Rightarrow V_i \supseteq \emptyset$

$\Rightarrow \forall u, v \in \bigcup_{i \in I} V_i \Rightarrow u, v \in V_i \quad \forall i \in I \Rightarrow u + v \in V_i \quad \forall i \in I \Rightarrow u + v \in \bigcup_{i \in I} V_i$

$\Rightarrow \text{následkem zdaleka analogicky}$

□

Def: Pro VP V nad \mathbb{T} a $W \subseteq V$ je lineární obal množiny W $\cap_{i \in I} W$

Značíme $\text{span}(W)$

primitivní výsledek podpořený tím, že $W \subseteq W \subseteq W \subseteq V$

Def Generátor: Nechť $U = \text{span}(W)$ pro nějaké $W \subseteq V$. Pak W generuje prostor U , pravý množina W je generátorem prostoru U .

$- U$ je konečně generovaný potom je W konečná

Def: Bud V VP nad \mathbb{T} a $v_1, \dots, v_n \in V$, pak lineární kombinace v_1, \dots, v_n je výraz $\sum_{i=1}^n \lambda_i v_i$, kde $\lambda_i \in \mathbb{T}$

Věta: Nechť V je VP nad \mathbb{T} a $v_1, \dots, v_n \in V$. Pak $\text{span}(v_1, \dots, v_n) = \left\{ \sum_{i=1}^n \lambda_i v_i : \lambda_i \in \mathbb{T} \right\}$

Důk: Inkluze \supseteq : Lin. obal je PP V obsahující $v_1, \dots, v_n \Rightarrow$ je množina souběžná s nás. sl. \Rightarrow obsahuje všechny lin. komb. $\sum_{i=1}^n \lambda_i v_i$

Inkluze \subseteq : Uzavřeme, že M je PP V obsahující v_1, \dots, v_n ; M je jediný z PP souběžnou souběžnou množinou $\text{span}(v_1, \dots, v_n)$

$\Rightarrow \emptyset \in M \Leftrightarrow$ ano souběžná $\lambda_1 = 0, \forall i$

$\Rightarrow v_1, \dots, v_n \in M \Leftrightarrow$ ano souběžná $\lambda_i = 1 \quad \forall i$

\Rightarrow Nechť $n \in \mathbb{N}$ a $\lambda_1, \dots, \lambda_n \in \mathbb{T}$ a $\lambda_i = 0 \quad \forall i > n$ a $\lambda_1, \dots, \lambda_n \in M$ \Rightarrow $\sum_{i=1}^n \lambda_i v_i \in M$ \Rightarrow $\sum_{i=1}^n \lambda_i v_i = \sum_{i=1}^n \lambda_i v_i + \sum_{i=n+1}^n 0 \cdot v_i = \sum_{i=1}^n (\lambda_i + 0) v_i = \sum_{i=1}^n \lambda_i v_i \in \text{span}(v_1, \dots, v_n)$

□

Def: Nechť V je VP nad \mathbb{T} a $v_1, \dots, v_n \in V$, pak v_1, \dots, v_n jsou lineárně nezávislé, pokud $\sum_{i=1}^n \lambda_i v_i = 0$ máloze pouze pro $\lambda_i = 0 \quad \forall i$

V opačném případě jsou lineárně závislé

- pro nezávislou množinu N : N je lineárně nezávislá pokud dálejší podmínky N

Je lineárně nezávislá: slouží i vzdály neg. matice jsou lineárně nezávislé

Věta: Nechť V je VP nad \mathbb{T} a $v_1, \dots, v_n \in V$ jsou lin. závislé $\Leftrightarrow \exists \lambda_1, \dots, \lambda_n \in \mathbb{T}$ a

$\lambda_1, \dots, \lambda_n \neq 0$ a $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$

Důk: \Rightarrow $\sum_{i=1}^n \lambda_i v_i = 0$, nezáleží $\lambda_i \neq 0 \Rightarrow \lambda_1 v_1 + \dots + \lambda_n v_n = 0 \Rightarrow \lambda_1 v_1 = - \sum_{i=2}^n \lambda_i v_i = - \sum_{i=2}^n \lambda_i \cdot v_1$

$$\Leftrightarrow \lambda_1 v_1 = \sum_{i=2}^n \lambda_i v_i \quad \# \Rightarrow \underbrace{\lambda_1 v_1}_{\text{lin. kombinace}} - \underbrace{\sum_{i=2}^n \lambda_i v_i}_{\text{lin. kombinace}} = 0$$

v_1 je lin. kombinace

a $\lambda_1 \neq 0 \neq 1$

□

Lemma o rozdílu

Nechť $y_1 \dots y_n$ je systém generátorů VP V a $x \in V$ má vyjádření
 $x = \sum_{i=1}^n d_i y_i$, pak pro libovolné $\lambda \in \mathbb{K} \neq 0$ je $y_1 \dots y_{n-1}, \lambda y_n \dots y_n$
 systémem generátorů V .

$$\text{Díl: } x = \sum_{i=1}^n d_i y_i \Rightarrow x - \sum_{i \neq n} d_i y_i = d_n y_n \Rightarrow y_n = \frac{1}{d_n} \left(x - \sum_{i \neq n} d_i y_i \right)$$

$$\text{je libovolný vektor } \alpha = \sum_{i=1}^m \beta_i y_i \Rightarrow \beta_n y_n + \sum_{i \neq n} \beta_i y_i \Rightarrow \frac{\beta_n}{d_n} \left(x - \sum_{i \neq n} d_i y_i \right) + \sum_{i \neq n} \beta_i y_i$$

Herrmannova věta o rozdílu

Nechť $x_1 \dots x_m$ je lineárně nezávislý systém ve V , nechť $y_1 \dots y_n$ jsou
 generátory V .

Ta $m \leq n$

Za každý rozdílný mísání indexů $i_1 \dots i_{m-m}$ k. t. $x_{i_1}, \dots, x_{i_{m-m}}, y_{i_1}, \dots, y_{i_{m-m}}$ jsou generátory V

Díl: indukční podle m

$m=0$... triviale!

$m-1 \Rightarrow m$

podle IP jsou $x_1 \dots x_{m-1}$ lin. nezávislé a $m-1 \leq m$ a každý rozdílný mísání indexů $i_1 \dots i_{m-m+1}$ k. t. $x_{i_1}, \dots, x_{i_{m-m+1}}, y_{i_1}, \dots, y_{i_{m-m+1}}$ generátory V .

Díl: $m-1 = m$ k. t. $x_1 \dots x_{m-1}$ generátory $V \Rightarrow x_m \in \text{Span}\{x_1 \dots x_{m-1}\}$ je lineárně
 k. t. $m-1 < m \Rightarrow m \leq m$, k. t. 1. číslo deklarace

x_m lze vyjádřit jako $x_m = \sum_{i=1}^{m-1} \alpha_i x_i + \sum_{j=1}^{m-m+1} \beta_j y_{i_j}$ $\exists \beta_j \neq 0$ aby nebyl spor s lin. nezá.

podle lemma o rozdílu mísíme x_m na $y_{i_1}, \dots, y_{i_{m-m+1}}$ a $x_1 \dots x_{m-1}, y_{i_1}, \dots, y_{i_{m-m+1}}$ pak

Dosledel: Každý bázis zadané generovaného prostoru V generuje V

Díl: 2 k. t. $x_1 \dots x_m ; y_1 \dots y_n$ jsou stejně velké

$x_1 \dots x_m$ je nezávislý systém \Rightarrow podle IP $n \leq m$

$y_1 \dots y_n$ je ... $\Rightarrow \dots \leq m \Rightarrow m = m$

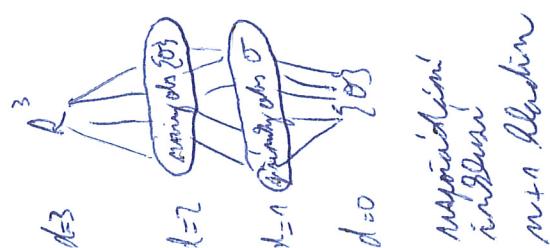
Def: Dimenze zadané generovaného prostoru je velikost nejdé jde báze.

Díl: je nem. KG $\Rightarrow \infty$

$\dim \mathbb{K}^{m \times n} = mn$

je nime je báze
stejných a je stejně
velká

grafické
poloprostor
grafický diagram
poloprostor V



Matice v prostoru
pro matice $T^{m \times n}$ svedeme jinostory:

- sloupcový p. $S(A) = \text{span}\{A_{*1}, A_{*2}, \dots, A_{*m}\}$
- řádkový p. $R(A) = \text{span}\{A_{*1}, A_{*2}, \dots, A_{*n}\} = S(A^T)$
- jádro $\text{ker}(A) = \{x \in T^n : Ax = 0\}$

je definice je $S(A) \subset T^m$ a $R(A) \subset T^n$

ukážeme, že $\text{ker}(A) \subset T^n$:

- $0 \in \text{ker}(A)$, protože $A0 = 0$
- rovněž na součty: pro $x, y \in \text{ker}(A)$ platí $Ax = Ay = 0 \Rightarrow A(x+y) = Ax + Ay = 0 + 0 = 0$
- (1) málož: pro $x \in \text{ker}(A)$ platí $Ax = 0 \Rightarrow \forall \lambda \in \mathbb{C} \quad A(\lambda x) = \lambda(Ax) = \lambda 0 = 0$

Ukážení: pro $A \in T^{m \times n}$ platí

$$S(A) = \{Ax : x \in T^n\} \quad R(A) = \{A^T y : y \in T^m\}$$

množina všech výsledků díl A

D: 1. $Ax = \sum_{j=1}^m x_j A_{*j}$ - to je lin. komb sloupců A, což jsou dílečky

2. $A^T y = \sum_{i=1}^m y_i A_{*i}$ - to je lin. kombinace řádků A \square

Ukážení: Pro $V \subset T^m$ $\exists A \in T^{m \times n}$ a $B, C \in T^{m \times m}$ A.s.

1. $V = S(A)$
2. $V = R(B)$
3. $V = \text{ker}(C)$

D: 1. generujeme všechny v₁ ... v_m buď sloupec x a matici B

Pom: Buď f obrazem $T^n \rightarrow T^m$ $f(x) = Ax$

platí $\text{ker}(A)$ je a definice kořenovým $x : f(x) = 0$

$S(A)$ pak buď množina všech obrazů f z neboře $f(T^n)$

Ukážení: Pro matice $A \in T^{m \times n}$ a $Q \in T^{n \times m}$ platí

① $R(QA) \subset R(A)$ ② platí $A_{*k} = \sum_{j \neq k} l_{ij} A_{*j}$ po nejdéle a nějaké $l_{ij} \neq 0 \Rightarrow (QA)_{*k} = \sum_{j \neq k} l_{ij} (QA)_{*j}$

D: ① všechny $R(QA) \subset T^m$, protože $R(QA) \subset R(A)$; $\forall x \in R(QA) \exists y \in T^N$ t. i. $x = (QA)^T y = A^T Q^T y = A^T (Q^T y) \in R(A)$

② $(QA)_{*k} = QA_{*k} = Q \left(\sum_{j \neq k} l_{ij} A_{*j} \right) = \sum_{j \neq k} l_{ij} QA_{*j} = \sum_{j \neq k} l_{ij} (QA)_{*j}$ \square

pro sloupec 1 nemá smysl, 2 funguje taky

náhled -- obrazován sloupců

Věta 2: $\forall A \in T^{m \times n}$ platí $\dim \text{Ker}(A) + \text{rank}(A) = n$

DK: Pro $n = \dim \text{Ker}(A)$ máme bázi v_1, \dots, v_n jádra $\text{Ker}(A)$

Počle věty o rozšíření na bázi máme $v_1, \dots, v_n, \dots, v_m$ bázi prostoru T^n
členeme dočíslat, že $A v_{n+1}, \dots, A v_m$ je bázi $S(A)$, protože podle věty? je
 $\text{rank}(A) = \dim(S(A)) = n - n$

Geometricky: $\forall y \in S(A) \exists x \in T^n : y = Ax$; krové x může

Rapsal: $x = \sum_{i=1}^n l_i v_i$

dosažime

$$y = A \left(\sum_{i=1}^n l_i v_i \right) = \sum_{i=1}^n l_i A v_i = \sum_{i=n+1}^n l_i (A v_i)$$

které jsou nezávislá lib. množina
novou v_{n+1}, \dots, v_m , které je to
systém generátor ~~systém~~

z def. Ker je $\sum l_i v_i = 0$

Lin. nezávislost:

$$\text{členeme } \sum_{i=1}^n l_i (A v_i) = 0 \Rightarrow A \left(\sum_{i=n+1}^n l_i v_i \right) = 0 \in \text{Ker}(A)$$

které jež je
vzájemně závislé
závislá v_{n+1}, \dots, v_m

$$\Rightarrow \sum_{i=n+1}^n l_i v_i = \sum_{i=1}^n \beta_i v_i \Rightarrow \sum_{i=1}^n (-\beta_i) v_i + \sum_{i=n+1}^n l_i v_i = 0 \quad \dots \text{to je výslednem}
v bázi $v_1, \dots, v_n, \dots, v_m$ (také
je lin. nezávislá) $\Rightarrow$$$

$$\Rightarrow \beta_i = 0 = l_i \quad \square$$

Geometrie V2: máme $f: T^n \rightarrow T^m$ dané $f(x) = Ax$... je tojí sobresyje
 n -dimensionální prostor T^n na m -dimensionální ~~prostor~~ $S(A)$, kde $n = \text{rank}(A)$
 $n - m \geq 0$ je dim $\text{Ker } A$, kdežto tím větu jádro, jeho množinou obraz
funkce nazýváme "degenerace" obrazem, máme i popis protize všem
máme právě ty všechny, které se objevují na počátku

Aplikace: Interpolace body

Dekreca obecně

Lagrangeova interpolacní polynom

6 lidí v autobuse

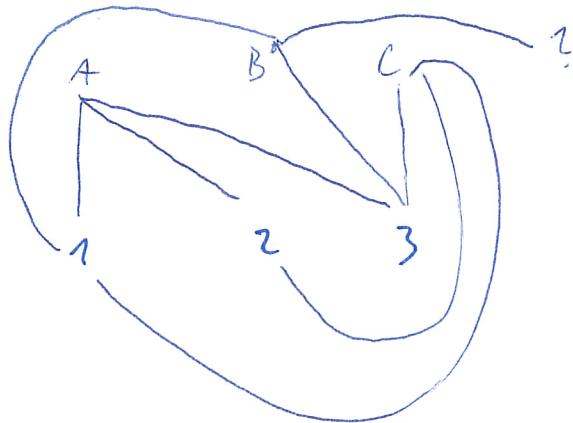
výhry $\exists \vdash \circ$ nebo $\exists \circ \circ$

DB:

0

\rightarrow Ramseyovy výhry

Rozvadění sousedů



Košlem' novinového grafu

Schodiště

$S_n := \#$ způsobů, jak vystoupit schodiště výšky n
1-schody a 2-schody



$$S_0 = 1$$

$$S_1 = 1$$

$$S_2 = 2$$

$$S_3 = 3$$

$$S_4 = 5$$

$$S_n = S_{n-1} + S_{n-2} \Rightarrow \text{fibonacciho čísla}$$

$$F_n = \frac{1}{\sqrt{5}} \left(\varphi^n - \left(\frac{-1}{\varphi}\right)^n \right)$$

uspořádané dvojice (x, y) $\{(x, y), (y, x)\}$

Rankízsky' součin $A \times B := \{(a, b) | a \in A, b \in B\}$

n. r. k.nice (x_1, \dots, x_n) $(x, y, z) \sim (x, (y, z)) \sim ((x, y), z)$

Doplňková množina $A^n = \underbrace{A \times \dots \times A}_{n}$ Rankízsky' součin je asociační!

Relace

$x \rightarrow$ relace \rightarrow ano/ne
 $y \rightarrow$ relace

Def: A je binární relace mezi soubadnicemi $X \times Y \equiv A \subseteq X \times Y$

Def: A je relace na množině X mezi $X \times X$ ($A \subseteq X^2$)

Př. $A = \{1, 2, 3, 4, 5\}$

① $x = y \quad \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$

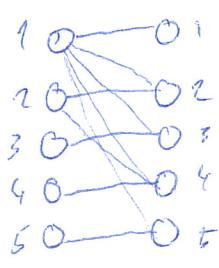
		1	2	3	4	5
1	1	m	m	m	m	m
	2		m			
3			m			
4				m		
5					m	

② $x + y \leq 5$

		1	2	3	4	5
1	1	m	m	m	m	m
	2		m	m	m	m
3			m	m	m	m
4				m	m	m
5					m	m

④ \varnothing prázdná relace

2. způsob



$(x, y) \in R$

struktu
 $x R y$



⑤ $\{1, 2, 3, 4, 5\}^2$ universální relace

Vlastnosti funkcií

Df: Funkcia $f: X \rightarrow Y$ je

- prostá (injektívna) $\Leftrightarrow \forall x_1, x_2 \in X : x_1 \neq x_2 \wedge f(x_1) = f(x_2)$

- na Y (surjektívna) $\Leftrightarrow \forall y \in Y \exists x \in X : f(x) = y$

- nazývame jednoznačná (bijektie) (1-1) $\Leftrightarrow \forall y \in Y \exists! x \in X : f(x) = y$
 $\Rightarrow f^{-1}$ je funkcia z Y do X

Df: Relacia R na X je

- reflexívna $\Leftrightarrow \forall x \in X : x R x$
 $(\forall x \in R)$

- symetrická $\Leftrightarrow \forall x, y \in X : x R y \Rightarrow y R x \quad R = R^T$

- antisymetrická $\forall x, y \in X : x R y \wedge y R x \Rightarrow x = y$

- transitívna $\Leftrightarrow \forall x, y, z \in X : x R y \wedge y R z \Rightarrow x R z \quad \text{nás} (=) (>) (<)$

Ekvivalence

Df: Relacia R na X je ekvivalence $\Leftrightarrow R$ je reflexívna, symetrická a transitívna

Ekvivalentné skupiny

praktické $x \in X$

$x R y \Leftrightarrow x \in R[y] \Leftrightarrow y \in R[x]$

$R[x] = \{y \in X \mid x R y\}$

Vetorek ① $\forall x \in X \quad R[x] \neq \emptyset$ reflexívita $x R x \Rightarrow x \in R[x]$

② $\forall x, y \in X$ bud $R[x] = R[y]$, nebo $R[x] \cap R[y] = \emptyset$

③ $\{R[x] \mid x \in X\}$ má viacero ekvivalentných jednoznačných pre ②

dôk ②: Akoby $R[x] \cap R[y] \neq \emptyset$ nar. $R[x] = R[y]$ (dovede dôkazovanie)

$\exists a \in R[x] \cap R[y]$ chceme $R[x] \subseteq R[y]$ lebo $\forall a \in R[x] : a \in R[y]$

$a R x \wedge x R a \Rightarrow a R a$

$y R a \wedge a R y \Rightarrow y R y$



Def: Relace R je na množině X je uspořádání $\Leftrightarrow R$ je reflexivní, transitivní
a antisymetrická

Def: ^{částečné} Uspořádaná směsina (X, R)
 $\subseteq, \leq, \leqslant$

Příklady:

① (N, \leq) lineární

③ Δ_X

$(R, \{0\})$ není uspořádání

② (Q, \leq) lineární

④ (N^+, \setminus) dělitelnost

-/-/- není antisym.

⑤ (Z^+, \leq) množina

některé prvky nejsou srovnatelné

Def: $x, y \in X$ jsou porovnateльné $\Leftrightarrow x R y \vee y R x$

uspořádání R je lineární $\Leftrightarrow \forall x, y \in X$ porovnateľné

⑥ lexicografické uspořádání

def: $(X, \leq) \subseteq U \Rightarrow (X, \leq'): x \leq y \Leftrightarrow x \leq y$

(A, \leq) lin. uspořádaná směsina (abeceda)

ostatní porovnání
ostatní "uspořádání"

A^2 def \leq_{lex}

$(x_1, y_1) \leq (x_2, y_2) \Leftrightarrow x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \leq y_2)$

(A^*, \leq_{lex})

(A^*, \leq_{lex}) $\xrightarrow{\text{zde se liší}},$ rozložit p

1 slovo slovo ... S

↑ Doseňaná posloupnost pravík z A

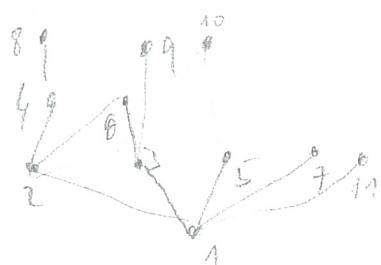
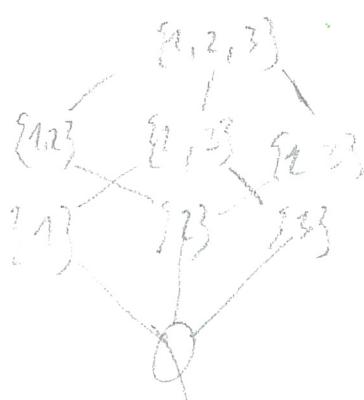
Hasseův diagram pro poslěné ČVM

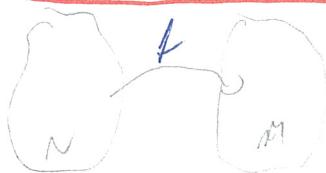
Def x je bezprostředním předchůdcem y v uspořádání $\leq \Leftrightarrow$

$x < y \wedge (\forall z : x < z \wedge z < y)$

pro dělitelnost

$(Z^{\{1,2,3\}}, \leq)$





$$\# f: N \rightarrow M = m^n$$

$$|N| = m \quad |M| = m^n$$

$$m, n > 0$$

Dle indukce podle n

$$1. n=1 \quad \# f: m = m^1$$

$$2. n \rightarrow n+1$$

$(n+1)$ -prostota N , m prostota M
zvolime pevné $x \in N$

f je jednoznačně určena: $f(x)$ musí být

$$\# f = m \cdot m = m^{n+1} \quad \boxed{f: N \setminus \{x\} \rightarrow M \text{ ind. funk.}}$$

Věta: Je-li N n -prostota a M m -prostota
 $\# \{2^N\} = 2^m$

Dk: $A \subseteq N$

$$\downarrow$$

$$c_A: N \rightarrow \{0, 1\} \quad c_A(x) \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}$$

charakteristická funkce

$$\# \text{podmnožin } A = \# \text{char funkcií} = 2^m \quad \square$$

Věta: Necht $X \neq \emptyset$ konečná

$$Y := \{S \subseteq X \mid \forall |S| \text{ je sudé}\}$$

$$Z := \{L \subseteq X \mid |L| \text{ je liché}\}$$

Pokud

$$|Y| = |Z| = 2^{m-n}$$

Dk: Platí důkaz $|Y|=|Z|$

Definujeme bijekci $f: Y \rightarrow Z$
zvolime si $a \in X$

$$f(S) := S \Delta \{a\}$$

$$1. f(S) \in Z$$

2. k tomu plynne, že je

$$2. f \text{ má inverse } -f^{-1}=f$$

\square

Věta: Necht N je n -prostota
 M je m -prostota

Dk: jde o pravou větu, nemůže opakovat

pokud $\# N \rightarrow M$ prostých =

$$= m \cdot \underbrace{(m-1) \cdot \dots \cdot (m-m+1)}_{m \text{ členů}} \quad m^{\underline{m}}$$

Kelovské funkce

$$\circ X \rightarrow \{0, 1\} \dots 2^X$$

$$\circ \{1, 2\} \rightarrow X \dots (x_1, x_2) \in X^2$$

$$\circ \{1, 2, \dots, n\} \rightarrow X \dots \text{uspořádání } k\text{-lice } X^n$$

$$\circ N \rightarrow X \dots \text{netonečné posloupnosti funkcií } X$$

$$\circ \text{permutace na } X: f: X \rightarrow X \text{ bijekce}$$

$$n = |X| \quad f: \{1, \dots, n\} \xrightarrow{\text{bijekce}} X \text{ lineární uspořádání na } X$$

$$\# \text{perm na } X = \# \text{ prostých funkcí z } \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

$$= n \cdot (n-1) \cdot \dots \cdot 1 = n! \quad (0! = 1)$$

$$|T|=15 \quad |K|=5 \quad |E|=11$$

$$|T \cap K|=3 \quad |K \cap E|=5 \quad |T \cap E|=2 \quad |T \cap K \cap E|=1$$

$$|T \cup K| = |T| + |K| - |T \cap K| = 17$$

$$|T \cup K \cup E| = |T| + |K| + |E| - |T \cap K| - |K \cap E| + |T \cap K \cap E|$$

Nášlež: Princip inkluze a exkluze pro součetné množiny A_1, \dots, A_n

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^m (-1)^{k+1} \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=k}} \left| \bigcap_{i \in I} A_i \right|$$

alternativně

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\substack{I \subseteq \{1, \dots, n\} \\ \emptyset \neq I \subseteq \{1, \dots, n\}}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|$$

Dle: pro každý prvek $x \in \bigcup_{i=1}^n A_i$ spočítatme příspěvy z L a P shaně
nechť \times patří do první jmenoviny z A_1, \dots, A_n výzv. 1 výzv.

Principy L-kic:

- ① $k > j \rightarrow$ příspěje 0
- ② $k \leq j \dots (-1)^{k+1} (\text{z})$

$$n = \binom{0}{1} - \binom{0}{2} + \binom{0}{3} - \dots - (-1)^{k+1} \binom{0}{k} \rightarrow \text{leinnov věta} \quad 0 = (1-1)^n = \binom{n}{0} - \binom{n}{1} + \dots$$

$n = 1$ QED

$$DZ = \prod_{i=1}^n (1+x_i) = \sum_{\substack{I \subseteq \{1, \dots, n\}}} \prod_{i \in I} x_i$$

$$x_i := c_{A_i}$$

$$\prod_i (1-c_{A_i}) = \left(\sum_{\substack{I \subseteq \{1, \dots, n\}}} (-1)^{|I|} \prod_{i \in I} c_{A_i} \right) + 1$$

$\underbrace{\phantom{\prod_i (1-c_{A_i})}}_{1-c_{\bigcup_i A_i}}$ $\underbrace{\phantom{\prod_i (1-c_{A_i})}}_{c_{\bigcap_i A_i}}$

$$1 + c_{\bigcup_i A_i} = \left(\sum_{\substack{I \subseteq \{1, \dots, n\}}} (-1)^{|I|+1} \cdot c_{\bigcap_{i \in I} A_i} \right) + 1$$

$$\left| \bigcup_i A_i \right| = \sum_I (-1)^{|I|+1} \underbrace{\left\{ c_{\bigcap_{i \in I} A_i}(a) \right\}}_{\left| \bigcap_{i \in I} A_i \right|}$$

$$0 = \binom{0}{0} - n$$

$$0 = 1 - n$$

Nechť $A = \bigcup_i A_i$

Pro $B \subseteq A$: $c_B: A \rightarrow \{0, 1\}$

$$c_{x \cup y} = c_x + c_y - c_{x \cap y}$$

pro $a \in A$ $c_B(a) = \begin{cases} 0 & \text{1 pokud} \\ 1 & \end{cases}$

$$c_x = 1 - c_{\bar{x}} \quad \overline{x \cup y} = \bar{x} \cap \bar{y} \quad a \in B$$

$$1 - c_{x \cup y} = (1 - c_x)(1 - c_y)$$

$$\sum_{a \in A} c_x(a) = |X|$$

Def: Graf je uspořádána dvojice (V, E) , kde:

- V je konečná neprázdná množina vrcholků
- $E \subseteq \binom{V}{2}$ je množina hran

Rozšíření

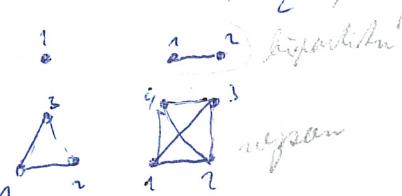
- orientovaný
- smyčky
- multigrafy
- neorient.

základy

nízky graf K_n

$$V(K_n) := \{1, \dots, n\}$$

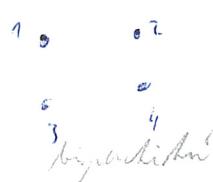
$$E(K_n) := \binom{V(K_n)}{2}$$



prásdy graf E_m

$$V(E_m) := \{1, \dots, m\}$$

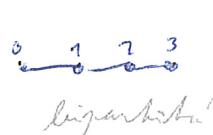
$$E(E_m) := \emptyset$$



cesta P_m

$$V(P_m) := \{0, \dots, m\}$$

$$E(P_m) := \{\{i, i+1\} \mid 0 \leq i < m\}$$



dvorce C_n

$$V(C_n) := \{0, \dots, n-1\}$$

$$E(C_n) := \{\{i, (i+1) \bmod n\} \mid$$

$$\text{ende } 0 \leq i < n\}$$



nízky bipartitní graf $K_{m,n}$

$$V(K_{m,n}) := \{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}$$

$$E(K_{m,n}) := \{(a_i, b_j) \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

Def: Graf G je bipartitní \Leftrightarrow

je rozklad množiny $V(G)$ na X, Y

$$\text{a.s. } E(G) \subseteq \{(x, y) \mid x \in X, y \in Y\}$$

alternativně

$$\forall e \in E(G) : |\deg_X(e)| = 1 \quad \& \quad |\deg_Y(e)| = 1$$

Def: Grafy G a H jsou izomorfní $\Leftrightarrow \exists f: V(G) \rightarrow V(H)$ bijekce

$$\text{a.s. } \forall u, v \in V(G) : \{(u, v)\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(H)$$

\cong je ekvivalence

Def: Graf G je k -regulární ($k \in \mathbb{N}$)

$$\Leftrightarrow \forall u \in V(G) : \deg_G(u) = k$$

Def: Skoře graf G je posloupnost stupňů všech vrcholků

$$\sum_{v \in V} \deg_G(v) = 2|E|$$

Def: Graf G je regulární

družstev

je sude číslo
vrcholů lichého stupně je sudý

zpravidla sudostí
zpravidla sudostí

množství izomorfismů = $\frac{2^{\binom{n}{2}}}{n!}$

$$\# \text{grafů } (V, E) = |2^{\binom{n}{2}}| = 2^{\binom{n}{2}}$$

? když máme $n!$ grafů

Def: Graf je podgrafem grafu $G = (V, E) \iff V' \subseteq V \wedge E' \subseteq E$

Def: $G'(V', E')$ je indukovaným grafem grafu $G(V, E) = V' \subseteq V \wedge E' = E \cap \binom{V'}{2}$

Def: Cesta v grafu $G = (V, E)$ je

1. $G' \subseteq G : G' \cong P_m$ pro nějaké $m \rightarrow$ koncové vrcholy cesty

2. $(v_0, e_1, v_1, \dots, e_n, v_n)$, kde v_0, \dots, v_n jsou různé vrcholy
 e_1, \dots, e_n jsou hrany

$$V_i \cap E_i = \{v_{i+1}, v_i\}$$

Def: Družnice v grafu

1. $G' \subseteq G : G' \cong C_n$ pro nějaké n

2. $(v_0, e_1, v_1, \dots, v_{n-1}, e_n, v_0)$, v_0, \dots, v_{n-1} jsou různé vrcholy
 e_1, \dots, e_{n-1} hrany

def: sled (walk)

$(v_0, e_1, \dots, e_n, v_n)$ tedy $= [v_0, v_1, v_2]$

def: kolo nezavírá se hrany
cesta sám vrcholy

Def: Graf G je souvislý \iff

$\forall v, w \in V(G) \exists$ cesta v G s druhými vrcholy u, v, w

Def: Dosežitelnost v G je relace na $V(G)$ t. j. $w \sim v \iff \exists$ cesta v G s druhými vrcholy w, v

Lemma: relace \sim je ekvivalence

Def: Komponenty souvislosti jsou podgrafy indukované vztahem ekvivalence \sim

Ps lemma: Rel: $w \sim w \vee (\text{minimální cesta})$

sym: $w \sim w \iff w \sim w \vee$

trans: $w \sim w \wedge w \sim w \Rightarrow w \sim w$

Lemma druhé: \exists cesta mezi $w, v \iff \exists$ sled mezi w, v

: \exists pravidlo: Použití cesta je sled

\Leftarrow Když se v S mohou rozptylovat vrcholy je to cesta

potom $v_k = v_l \quad \forall l \in$

potom $v_k = v_l \quad \forall l \in$

Dopř. symetrie, když
jde o sled

$v_0, e_1, \dots, e_n, v_n, e_{n+1}, \dots, e_l, v_l, \dots, e_m, v_m$

opravujeme dokud S není cesta

□

Matice sousednosti

$A_{ij} := |\{v_i, v_j\} \in E|$ $\Leftrightarrow A$ je symetrická, součty řádků/sloupců jsou stejně vrcholy

$A_{ij}^2 = \sum_{k=1}^n A_{ik} \cdot A_{kj} = \sum_{k=1}^n |\{v_i, v_k\} \in E| \cdot |\{v_k, v_j\} \in E|$

sledová délka ≥ 2 s vrcholy v_i, v_j

Eulerovský tah def: obsahuje všechny vrcholy a hranou grafu (uzavřený): cyklický

Def: graf je eulerovský (\Leftrightarrow) $\forall v \in V$ užití $\deg(v)$ je sudé
všechny stupně sudé \Rightarrow souvislý

Teku: Graf G je eulerovský $\Leftrightarrow G$ je souvislý $\wedge \forall v \in V: \deg_G(v)$ je sudý

Df: \Rightarrow sudost s kohže hranu musí vstoupit i vystoupit

souvislost: $\forall u, v \in V(G) \exists$ tah mezi $u, v \Rightarrow$ eukl. \Rightarrow souvislý

\Leftarrow uvažme $T :=$ nejedelník tah

1. T je uzavřený: opět: Rely by nebyl uzavřený

• měl by v je jeden z konců tahů

• tah obsahuje dva různé hranu incidentní s v

• v má sudý stupeň \Rightarrow hranu se incidentní s $T \Rightarrow T$ by prošel $v \Rightarrow$



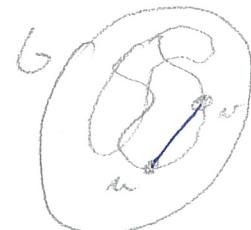
2. T je uzavřený

• pokud $\{u, v\} \in E(G)$, $u, v \in T$ pak $\{u, v\} \in T$

• Rely by to pro nějaké u, v v nějaké pravde

• T rozpojíme při některém průchodu u

• na nové průderné $\{u, v\}, v \Rightarrow$ delší tah \Rightarrow



$\wedge T$ obsahuje všechny vrcholy

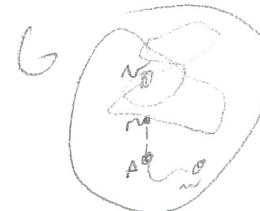
• Rely by $\exists u \in E(G) \cap v \notin T$:

• Nového $v \in T$ libovolné

• souvislost $\Rightarrow \exists$ cesta mezi u, v

• $\exists u, s \in C: u \in T, s \notin T \quad \{u, s\} \in E(G)$

• T rozpojíme a prodloužíme $v \in T, s \Rightarrow$ delší tah \Rightarrow



cíci
uzavřený auk tah
souvislost
mává možnost
libky shaptí

Pro multigraf s nerozdílnými hranami funkce funguje
součet - počítáme do deg obecně

orientované grafy - sedly, česky, řečnicí jsou orientované

$E \subseteq V^2 \times \{(x, x) | x \in V\}$ - matice sousednosti nemusí být symetrická

• souvislost \wedge dráž počítadlo \rightarrow slabá def: podgrafem graf je souvislý
dosáhnutelnost vedené \rightarrow silná def: $\forall u, v \in V(G) \exists$ orientované cesty z u, v

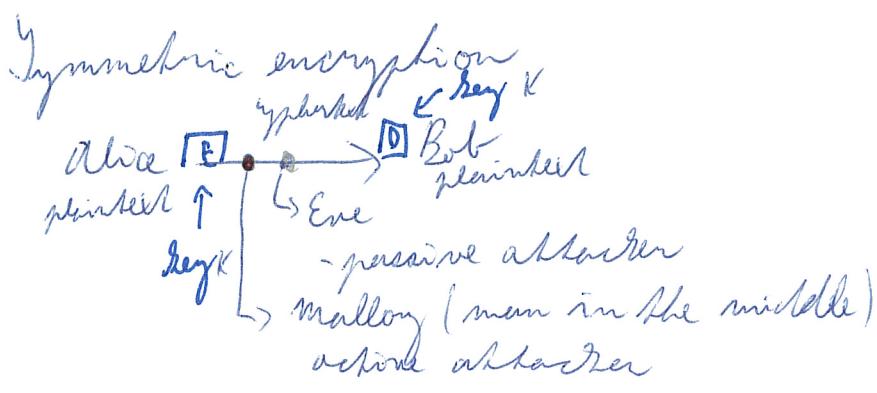
def: podgrafem graf je klo grafu $G = (V, E)$: $G^\circ = (V, E^\circ)$ kde $\{u, v\} \in E^\circ \Leftrightarrow (u, v) \in E(G) \vee (v, u) \in E(G)$

def: $\deg^{\text{in}}(v) = \#\{u : (u, v) \in E(G)\}$ $\deg^{\text{out}}(v) = \#\{u : (v, u) \in E(G)\}$

def: Graf je regulérní $\Leftrightarrow \forall v \in V \deg^{\text{in}}(v) = \deg^{\text{out}}(v)$

Goal: cryptography → crypt. primitives
 ↓
 protocols
 implementation

understand existing protocols
 design of protocols



$$E: \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^m$$

plaintext key ciphertext

$$E(x, k) = y$$

$$D: \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^m$$

$$D(y, k) = x$$

$$\forall k \forall x \quad D(E(x, k), k) = x$$

for fixed x : $\xrightarrow{Ek} \xleftarrow{Dk}$

E_k as a permutation on $\{0,1\}^m$
 we want "random"

Henseloffs principle
 "Secret should be the π
 not the algorithm"

Reason:

- (1) good ciphers are hard to find
- (2) well known ciphers are well analysed

- (3) keys are easier changed when compromised

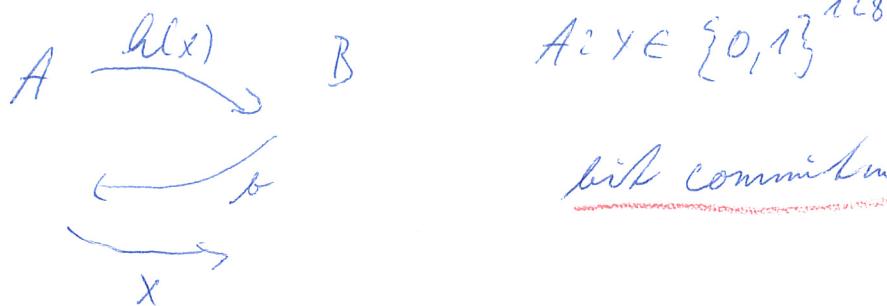
Ceser cipher

messages: $\{0, \dots, 25\} \subset \mathbb{Z}_{26}$
 Keys \mathbb{Z}_{26}

$$E(x, k) = x + k \quad D(y, k) = y - k$$

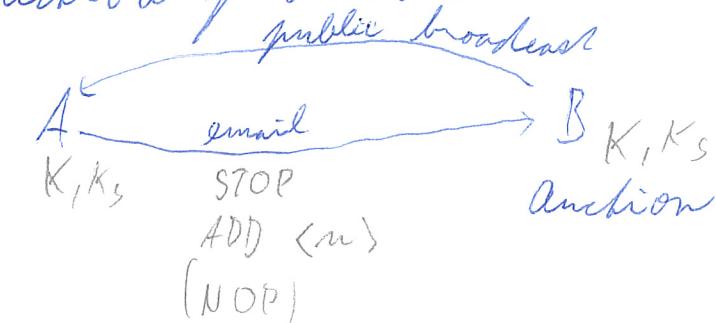
weak because keys are limited

Tossing a coin over the phone call



bit commitment protocol

Auction protocol



Secrecy?

- against whom
- for how long

message authentication code (MAC)

signature ← $h(K_3 \parallel \text{encrypted grant} \parallel \text{session ID})$

fixed size
 sequential #
 nonce
 command
 padding

E_K

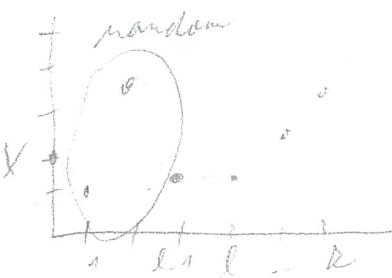
Kinds of attacks

- known ciphertext → recover plaintext
- known plaintext → recover key
- chosen plaintext
- distinguishing attack

How to measure strength of primitives

b: security level (bits) ... attacker requires $\geq 2^b$ operations to break the protocol

continuation (4)



Polynomials of degree $\leq l$
unique poly p shares: $S_n := p(i)$

symmetric ciphers
block cipher → stream
fixed sized blocks

$$E: \{0,1\}^b \times \{0,1\}^n \rightarrow \{0,1\}^b$$

$$E_K: \{0,1\}^b \rightarrow \{0,1\}^b \text{ bijection/permuation on set of block values}$$

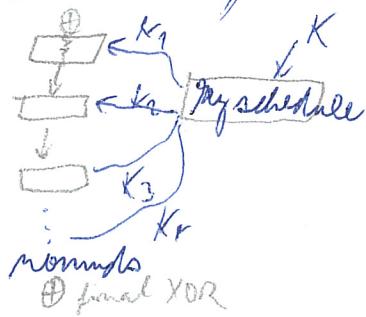
Security of block cipher

distinguisher oracle E_K with random key K
or random permutation

Genie \leftrightarrow a distinguisher with $\Pr[\text{success}] \geq \frac{2}{3}$ and $\frac{\text{run time}}{2}$ security level

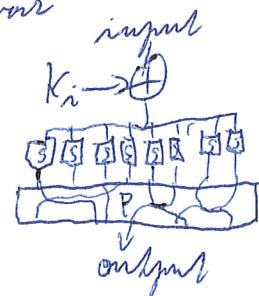
In real constructions: almost always even permutations

Blended cipher

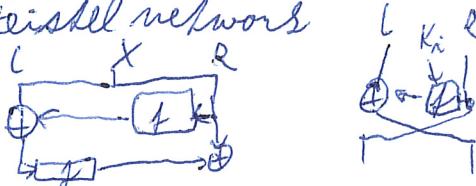


Substitution permutation network

- Round: - S-boxes confusion
- P-box diffusion
- mixing round key
↳ round is invertible
→ again SPA
- reverse schedule of keys
→ permute round keys
inverse for P, inverse Ss

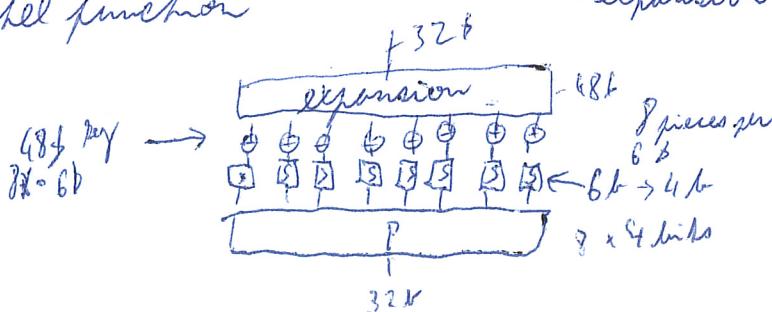


Feistel network



f needn't be injective
inverse of FN is FN

Feistel function



DES (data encryption standard)

- 1970s IBM & US government NSA
- 64 bit blocks, 56 bit keys
- S-boxes were replaced by NSA

- Feistel network
- all S-boxes are different
- expansion: each block takes 1b from each side

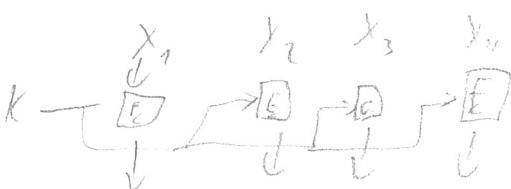
Use of block ciphers:

block ciphers modes of operation

Padding - fill the rest of the last block



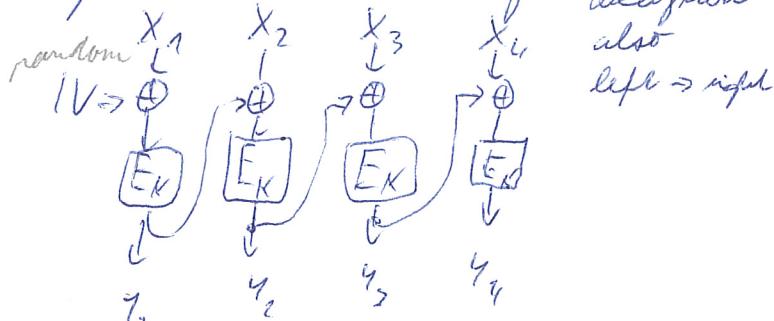
ECB: Electronic Code Book



AVOID

- no initial value (IV)
- reveals $X_i = X_j \Leftrightarrow Y_i = Y_j$
- flip bit in $Y_i \Rightarrow$ destroy X_i
swap ciphertext \Leftrightarrow swap plaintext

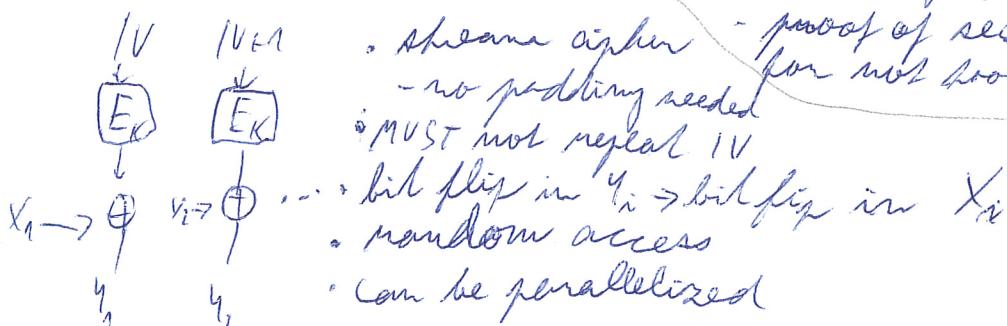
CBC: Cipher block chaining



Decryption
also
left \rightarrow right

- requires random IV
- Bit flip in Y_i , destroys X_i
flip in X_{i+1}
- $Y_i \Leftrightarrow Y_j$: flips in predictable way
- proof of security (chosen plaintext attack)
for not too long messages

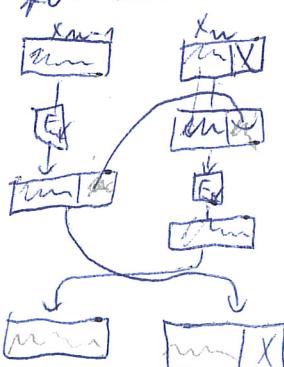
CTR: Counter



OFB: Output feedback



Cipher block stealing - trick for avoiding padding
for ECB - see lecture



$$\text{CBC } Y_i = E_K(X_i \oplus Y_{i-1})$$

$$Y_i = Y_j$$

Only happens after $2^{b/2}$ blocks

$$X_i \oplus Y_{i-1} = X_j \oplus Y_{j-1}$$

$$X_i \oplus X_j = Y_{i-1} \oplus Y_{j-1}$$

known
to attacker
leads to bits of data

on CBC

padding oracle attack
side channel attack
attacker can distinguish
between wrong padding and
wrong signature.

Garbage

$$\text{ECB: } Y_i = Y_j \Leftrightarrow X_i \Leftrightarrow X_j$$

$$\text{CTR } Y_i = X_i \oplus E_K(IV + i - 1)$$

$$C_1 \dots C_m \quad C_i = E_K(IV + i - 1)$$

\Leftrightarrow all C_i 's are different

$$Y_i \oplus Y_j = (X_i \oplus C_i) \oplus (X_j \oplus C_j) =$$

$$= (X_i \oplus X_j) \oplus (C_i \oplus C_j)$$

$\overbrace{\quad}^{r \neq 0}$

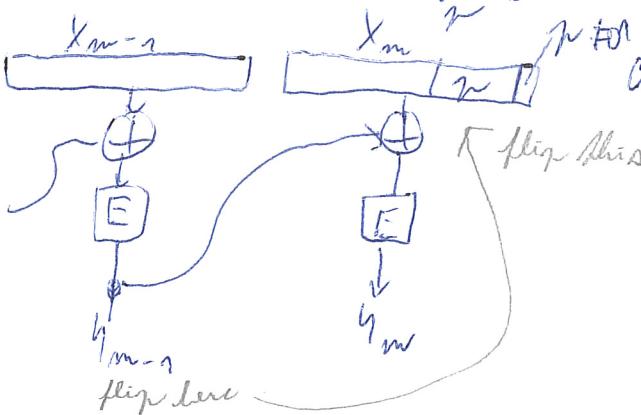
$$Y_i \oplus Y_j \neq X_i \oplus X_j$$

rules? and
of 2^b

$$\text{bias: } b - \log(2^b - 1) \approx C \cdot 2^{-b}$$

bits leaked $\leq \binom{m}{2} \cdot C \cdot 2^{-b}$... constant for
pairs $\leq m \approx 2^{b/2}$

Padding scheme: data \xrightarrow{P} n types of value p



Sometimes in TLS

Stream ciphers

$$X_i \xrightarrow{\oplus} Y_i$$

$G \in K$
register

STREAM project

- goal: find new stream ciphers
2004 -- finals 2008

profile 1: SW \rightarrow 4 ciphers

profile 2: HW \rightarrow 3 ciphers

TRIVIUM
288 bits of state
- key - 80b
- IV - 80b
- constants --
1152 idle steps
see level 80

Assume $P = 01$,

exactly one solution
with correct padding
 $P \oplus F = 01$
↳ recovered $f \oplus P$

P types under control
by increasing padding
size by $p+1$

original $\oplus F = P+1$

↳ recover last
block easily

Complexity to recover B
types

Then you can
get last block
and recover
every except final

(if you can change IV)

LFSR - Linear feedback shift register



↳ trivial in hardware

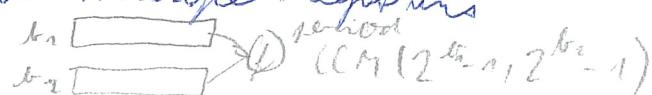
↳ trivial to crack in KPA - Known plaintext
attack

Attempts to save

- Non-linear feedback (\oplus)

- Non-linear output

- Combine multiple registers



control clock of register out of reg 2



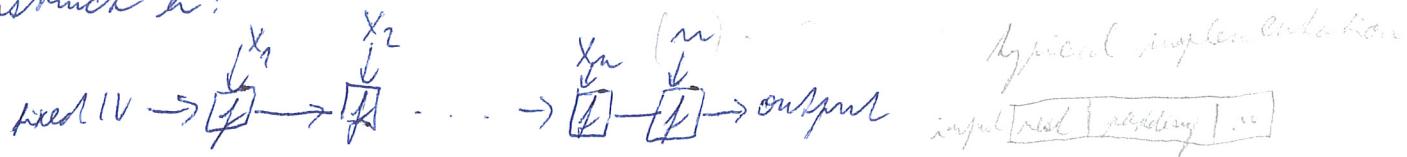
Ex A5/1 (GSM)
privately developed \Rightarrow weak

Hash functions: want collision resistance

Merkle-Damgaard construction

Given a compression function $f: \{0,1\}^b \times \{0,1\}^b \rightarrow \{0,1\}^b$

construct h :



Theorem: If f is collision resistant, then h is collision resistant

Proof: If we have $h(x_1, \dots, x_m) = h(x'_1, \dots, x'_n)$ different

for contradiction either $m \neq n$... collision in f $f(-, m) = f(-, n)$

or $m = n$... we go backwards and we have no final different blocks with collision

□

Length extension property

~~we can break signature
secret sign: h(secret || com)
com: $\perp \perp$ evil commands~~

~~prefix p $\perp \perp$~~

for random it is possible: given $h(p)$, compute $h(p||q)$

$$\text{prefix } p \xrightarrow{\perp \perp} \text{random } q \xrightarrow{\perp \perp} h(p||q)$$

How to obtain compression function f ?

S Davies-Meyer construction from block cipher

$$f(u, v) := E_u(v) \oplus v$$

Theorem: With an ideal block cipher, f is collision-resistant

f is collision-resistant

For attack evaluating E/D of times

$$\Pr[\text{collision point}] \leq q^2 / 2^b$$

Proof: WLOG we ask no redundant questions

$$u \text{ can ask } E_u(v) \rightarrow f(u, v) = E_u(v) \oplus v$$

$$D_u(w) \rightarrow f(u, D_u(w)) = w \oplus D_u(w)$$

If we find collision in step i ($i \in [q]$) we found pair in $i-1$ previous

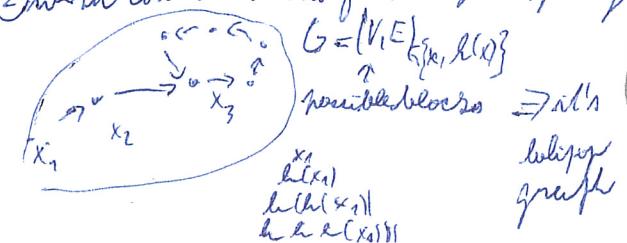
for every pair: $\Pr[\text{collision}] = \frac{1}{2^b} \leq \frac{1}{2^{b-i-1}} \leq \frac{1}{2^{b-1}}$

$$\Pr[\text{collision}] \leq \frac{1}{2^{b-1}} \cdot \# \text{pairs} \stackrel{(P)}{=} \frac{q^2}{2^{b-1}} = \frac{q^2}{2^b}$$

Finding collision

(1) brute force ... by birthday paradox ... matching $2^{b/2}$ steps (with lost of memory)

(2) with constant memory: imagine of a graph



duration: 1 step
home: 2 steps
wait until they meet - that's the collision with previous step

→ after 1 steps they are on the cycle and can't escape \Rightarrow they meet (only at that point?)