

# Zkouška KG1, Martin Koutecký

**Prezenční** zkouška bude probíhat následovně. Na dalších stranách najdete okruhy - jsou rozděleny do třech skupin (početní, grafové, kombinatorické struktury), v každé skupině je několik podtémat a každé z nich obsahuje seznam a) definic, b) tvrzení/vět. Na zkoušce dostanete z každé skupiny a) definici z jedné podskupiny a b) větu z jiné podskupiny. Tedy např. ze skupiny „Grafové“ můžete dostat definici z toků (např. co je to nasycený tok) a větu z Ramseyovy teorie (třeba nekonečnou vícebarevnou grafovou).

Potom, co témata dostanete, je vaším úkolem **zformulovat** zadané definice/tvrzení. V první fázi od vás **nechci**, abyste je dokazovali. Až budete mít sepsané formulace, přivoláte mě nebo cvičícího, pokud budete mít vše správně, zeptáme se vás, jak byste dokazovali jedno z tvrzení - přibližně strategie/struktura důkazu. Pokud i to bude správně, máte za 1 a jdete domů. Pokud ne, necháme vás důkaz sepsat pořádně. Pokud nastanou problémy už ve formulacích, budeme se dále doptávat a podle množství vašich chybějících znalostí a nutných nápověd se bude zhoršovat vaše známka.

**Distanční** zkouška bude probíhat jinak. Je to z toho důvodu, že ve výše popsaném formátu zkoušky je příliš jednoduché podvádět. Proto na distanční zkoušce budu za všech okolností chtít důkaz nějakého netriviálního tvrzení. Může to být jedno z tvrzení ze seznamu níže, ale může to být i nějaké jednoduché cvičení, které se znalostí definic a vět z přednášky jde relativně snadno dokázat, ale nejde (jednoduše) si jeho řešení předpřipravít.

# Počtení

## Odhady

- Definice
  - Stirlingova formule:  $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$
  - Náhodná procházka
- Věty / důležitá tvrzení
  - $e \left(\frac{n}{e}\right)^n \leq n! \leq en \left(\frac{n}{e}\right)^n$
  - Pro malé  $k$  je OK odhad  $\binom{n}{k} \leq n^k$
  - $\frac{2^n}{n+1} \leq \binom{n}{n/2} \leq 2^n$
  - $\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$
  - Střední hodnota počtu návratů do počátku během náhodné procházky jde k s rostoucím počtem kroků  $n$  k nekonečnu

## Vytvořující funkce

- Definice
  - Mocninná řada
  - Vytvořující funkce posloupnosti
  - Operace s funkcemi a posloupnostmi - jen vyjmenovat; zejména konvoluce
  - Zobecněné binomické číslo  $\binom{n}{r}$  pro  $r$  záporné a neceločíselné
- Věty / důležitá tvrzení
  - Operace s funkcemi a posloupnostmi (ukázat, proč  $\alpha a(x) \approx (\alpha a_0, \alpha a_1, \dots)$  nebo  $x a(x) \approx (0, a_0, a_1, \dots)$  atd.); zejména konvoluce
  - Zobecněná binomická věta (bez důkazu)
  - Odvození uzavřeného vzorce pro Fibonacciho čísla
  - Odvození uzavřeného vzorce pro Catalanova čísla

## Počítání dvěma způsoby

- Definice
  - Množinový systém, řetězec, antiřetězec
  - kostry, ...
- Věty / důležitá tvrzení
  - Spernerova věta
  - Graf bez čtyřcyklu má nanejvýš  $\frac{1}{2}(n^{3/2} + n)$  hran
  - Cayleyho formule:  $\kappa(n) = n^{n-2}$

# Grafové

## Toky

- Definice
  - síť, tok, velikost toku
  - řez, kapacita řezu, elementární řez
  - nasycená/nenasycená cesta, nasycený tok
  - Ford-Fulkersonův algoritmus
  - párování, perfektní párování, vrcholové pokrytí
  - systém různých reprezentantů
- Věty / důležitá tvrzení
  - Max-flow min-cut: pro každou síť je velikost max toku = kapacita min řezu
  - Pro každou  $A \subseteq V, z \in A, s \in V \setminus A$  a libovolný tok platí  $w(f) = f(A, V \setminus A) - f(V \setminus A, A)$
  - $f$  je maximální právě když  $f$  je nasycený
  - F-F doběhne a dá racionální tok pokud jsou kapacity racionální; pokud jsou celočíselné, dá celočíselný tok
  - Celočíselný tok lze rozdělit na celočíselný součet cest a cyklů
  - Königova věta: v bipartitním grafu  $|\max. \text{ párování}| = |\min. \text{ vrcholové pokrytí}|$
  - Hallova věta: SRR / párování pokrývající partitu existuje právě když platí Hallova podmínka
  - Doplnování latinských obdélníků

## Souvislost

- Definice
  - Hranový, vrcholový řez
  - hranová, vrcholová souvislost
  - $G$  je hranově/vrcholově  $k$ -souvislý
  - Ušatá dekompozice 2-souvislých grafů (definice)
- Věty / důležitá tvrzení
  - $k_e(G) - 1 \leq k_e(G - e) \leq k_e(G)$
  - $k_v(G) - 1 \leq k_v(G - e) \leq k_v(G)$
  - Hlavní věta:  $k_v(G) \leq k_e(G)$
  - Ford-Fulkerson:  $G$  je hranově  $k$ -souvislý právě když existuje aspoň  $k$  hranově disjunktních cest mezi každými dvěma vrcholy
  - Menger:  $G$  je vrcholově  $k$ -souvislý právě když existuje aspoň  $k$  vrcholově vnitřně disjunktních cest mezi každými dvěma vrcholy
  - Ušatá dekompozice 2-souvislých grafů (důkaz)

## Ramseyova teorie

- Definice
  - Ramseyovo číslo  $R(k, k)$
  - velikost max kliky  $\omega(n)$ , velikost max nz. mn.  $\alpha(n)$
- Věty / důležitá tvrzení
  - Standardní grafová: pokud má  $G$  alespoň  $\binom{k+l-2}{k-1}$  vrcholů, pak obsahuje buď  $K_k$  nebo  $E_l$ , neboli  $\omega(G) \geq k$  nebo  $\alpha(G) \geq l$

- Dolní odhad:  $\binom{n}{k} 2^{1-\binom{k}{2}} \rightarrow r(k) > n$ , tedy  $r(k) > 2^{k/2}$
- Königovo lemma o nekonečné větvi
- Ramseyova vícebarevná (nekonečná)
- Ramseyova vícebarevná pro p-tice (nekonečná)

## Kombinatorické struktury

### Konečné projektivní roviny

- Definice
  - Konečná projektivní rovina (tři axiomy)
  - Řád KPR
  - Incidenční graf množinového systému
  - Duál konečné projektivní roviny
  - Konstrukce KPR řádu  $n = p^k$  pro nějaké prvočíslo  $p$  (bez důkazu)
  - Latinský čtverec řádu  $n$ , ortogonalita LČ
- Věty / důležitá tvrzení
  - V KPR mají všechny přímky stejný počet bodů
  - Každým bodem prochází  $n+1$  přímek
  - $|X| = n^2 + n + 1 = \#přímek$
  - Duál KPR je opět (ne nutně stejná) KPR
  - Konstrukce KPR řádu  $n = p^k$  pro nějaké prvočíslo  $p$  (s důkazem)
  - Pro daný řád  $n$  může existovat nanejvýš  $n - 1$  NOLČ
  - Existuje  $n - 1$  NOLČ právě tehdy když existuje KPR řádu  $n$

### Samoopravné kódy

- Definice
  - abeceda, zpráva, slovo, kódové slovo, kód
  - velikost kódu, délka kódu, dimenze kódu, minimální vzdálenost kódu,  $(n,k,d)$ -kód
  - totální kód, opakovací kód, paritní kód
  - $A(n,d) = \max \log |C|$
  - Lineární kód, min. vzdálenost lin. kódu, počet prvků, ...
  - Duální kód lineárního kódu
  - Generující a kontrolní matice lineárního kódu
  - Chybový vektor, syndrom, reprezentant
  - perfektní kód
  - Hadamardův kód je duál Hammingova kódu a je dobrý pro obzvlášť nespolehlivé kanály
- Věty / důležitá tvrzení
  - Simpletonův odhad:  $A(n,d) \leq n - d + 1$
  - Parita: pro  $d$  sudé platí  $A(n,d) = A(n-1, d-1)$
  - Kódování a dekódování lineárních kódů
  - Hammingovy kódy - konstrukce (pozorování, že pokud  $P$  je kontrolní matice  $C$ , pak  $\Delta(C) = \max. d$  t.ž. každých  $d-1$  sloupců  $P$  je lineárně nezávislých), Hammingův kód je  $[2^r - 1, 2^r - r - 1, 3]$ -kód, dekódování Hammingova kódu
  - Hammingův odhad na velikost kódu se zadanou  $\Delta(C)$ , důkaz že Ham. kód je perfektní

