Motto: "Matematika je schovaná všude,
ovšem ne každý ji vidí"

Cílem přednášky je ukázat několik abstraktních matematických výsledků, které se používají při řešení praktických problémů. Některé matematické věty ovšem našly uplatnění až mnoho desítek či stovek let po svém vzniku.

Samoopravný kód (diskrétní matematika)

Slouží k detekci a opravování chyb vzniklých při přenosu dat.

Představme si situaci, že potřebujeme poslat data po telekomunikační lince, která není příliš spolehlivá, takže při přenosu může vlivem šumu dojít k řadě chyb. Pro nás je důležité zajistit, aby příjemce obdržel data bez chyb, a proto jsme ochotní poslat i více informací, pokud to pomůže případné chyby eliminovat. Protože je přenos drahý, chceme, aby celkový objem dat byl co možná nejmenší.

Data, která odesíláme ... posloupnost n bitů.

Pravděpodobnost chyby v přenosu jednoho bitu ... p (chyby jsou navzájem nezávislé).

1. přístup:

Data pošleme bez jakékoliv úpravy. Pravděpodobnost, že budou přijata bez chyby, tj. u všech bitů nedojde k chybě, je $(1-p)^n$. Pokud bude $n = 100$ a $p = 0,01$ (1%) vychází pravděpodobnost bezchybného příjmu 37%.

```
          Testovani posilani zprav bez uprav
 ------------------------------------------------------
  Zprava o 100 bitech je opakovane 100 krat poslana,
  s pravdepodobnosti 0.010000 nastane chyba pri prenosu 1 bitu.

  Prumerny pocet chyb pri prenosu jedne zpravy je 1.020000
  Z 100 prenosu bylo 33 bezchybnych,
  tj. 33.0 procent prenosu bylo bezchybnych.

 ------------------------------------------------------
  Teoreticky plati, ze pri posilani zpravy o n bitech,
  s pravdepodobnosti chyby pri prenosu 1 bitu p je
  pravdepodobnost bezchybneho prenosu cele zpravy:

    (1-p)^n = (1-0.010000)^100 = 0.366032
```

2. přístup:

Každý bit pošleme vícekrát (lichý počet), např. $3x$, a při příjmu zvolíme většinovou hodnotu.

Bit 0 odešleme jako 000 Bit 1 odešleme jako 111

Při příjmu dekódujeme trojice podle pravidel

000, 001, 010, 100 $\rightarrow$ 0 111, 110, 101, 011 $\rightarrow$ 1

Spočteme pravděpodobnost správného dekódování. Jednotlivý bit se dekóduje právě tehdy, když při přenosu příslušné trojice nastává nejvýše jedna chyba:

$$\underbrace{(1-p)^3}_{\text{bezchybný přenos}} + 3 \cdot \underbrace{p(1-p)^2}_{\text{přenos i-té složky s chybou}} = (1-p)^2(1+2p)$$

Pravděpodobnost správného dekódování n bitů získáme umocněním předchozího vztahu na n. Pro $n = 100$ a $p = 0,01$ vychází pravděpodobnost bezchybného příjmu 97%.

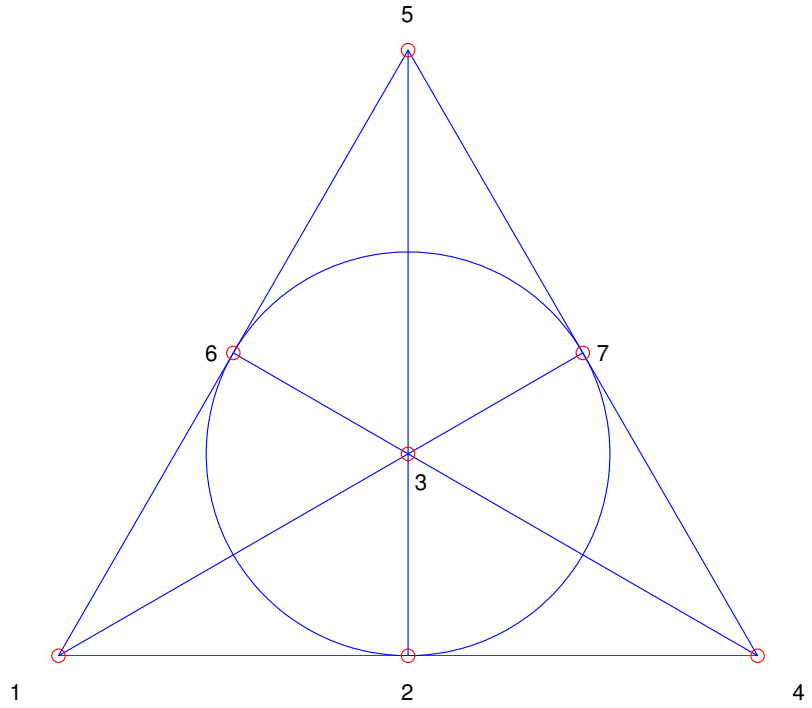
```
          Testovani posilani duplicitnich zprav
-------------------------------------------------------
 Puvodni zprava ma 100 bitu.
 Kazdy bit zpravy je poslan 3 krat za sebou.
 Pravdepodobnost chyby pri prenosu jednoho bitu je 0.01.
 Pri testovani cely proces opakujeme 100 krat.

 Prumerny pocet chyb pri prenosu jedne zpravy je 0.040000
 Z 100 prenosu bylo 96 bezchybnych,
 tj. 96.0 procent prenosu bylo bezchybnych.
 -------------------------------------------------------
 Teoreticky plati, ze pri posilani zpravy o n bitech,
 s pravdepodobnosti chyby pri prenosu 1 bitu p, pricemz
 kazdy bit posilame o krat, je pravdepodobnost bezchybneho
 prenosu opakovane poslaneho bitu dano souctem:

  (1-p)^o  ...  v o-tici zadna chyba
    = (1-0.010000)^3 = 0.970299

  (o nad 1) p^1 (1-p)^(o-1)  ...   v o-tici 1 chyb
    = (3 nad 1) 0.010000^1 (1-0.010000)^(3-1) = 0.029403

 v souctu pro jeden bit:  0.999702

 Pravdepodobnost bezchybneho prenosu cele zpravy:
  0.999702^n = 0.999702^100 = 0.970635
```

3. přístup: **Hammingův kód**

Uvažujeme tzv. hypergraf Fanovy roviny:

7 vrcholů (bodů) a 7 hran

Každá hrana obsahuje 3 body a každé dvě hrany se protínají právě v jednom bodě.



Body: 1, 2, 3, 4, 5, 6, 7.

Hrany: $\{1,2,4\}$, $\{1,3,7\}$, $\{1,5,6\}$, $\{2,3,5\}$, $\{2,6,7\}$, $\{3,4,6\}$, $\{4,5,7\}$.

Každé hraně přiřadíme tzv. charakteristický vektor, tj. vektor o sedmi složkách tak, že je-li $i-$tý bod bodem hrany bude na $i-$té pozici charakteristického vektoru 1 jinak 0.

$$\{1,2,4\} \to [1101000]$$
$$\{1,3,7\} \to [1010001]$$
$$\{1,5,6\} \to [1000110]$$
$$\{2,3,5\} \to [0110100]$$
$$\{2,6,7\} \to [0100011]$$
$$\{3,4,6\} \to [0011010]$$
$$\{4,5,7\} \to [0001101]$$

Těchto 7 charakteristických vektorů doplníme jejich 7 doplňky:

$$[0010111], [0101110], [0111001], [1001011], [1011100], [1100101], [1110010]$$

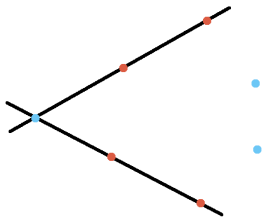
a dále vektory [1111111], [0000000].

Dostaneme 16 vektorů, tzv. kódová slova. Platí zajímavá vlastnost:

Věta: Každá 2 různá kódová slova se liší alespoň ve 3 souřadnicích.

Poznámka:

A Vezmu-li si libovolné 2 hrany v původním hypergrafu, mají vždy společný právě jeden bod, a tudíž zbylé 2 body na každé hraně jsou navzájem různé, tj. zbývají dva body, které nejsou ani v jedné ze zadaných hran. ⇒ Pro libovolné 2 různé hrany původního hypergrafu platí, že se jejich charakteristické vektory shodují právě ve 3 souřadnicích a zbylé 4 mají odlišné.



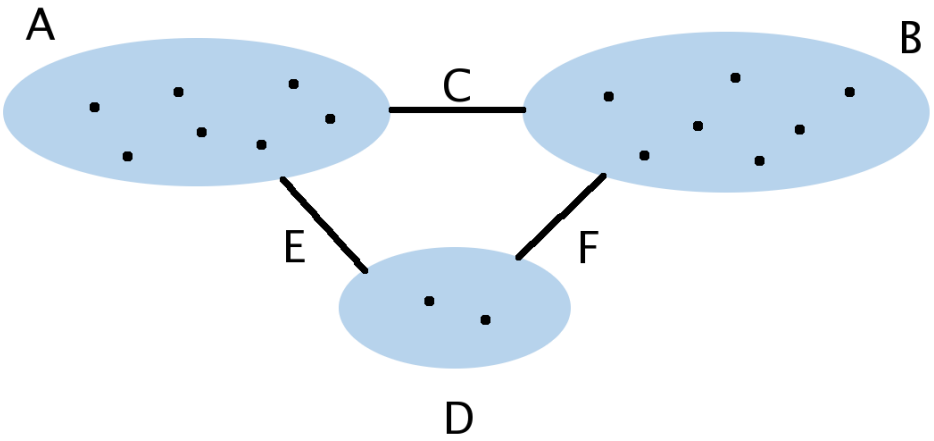
B Pokud budeme uvažovat skupinu 7 doplňkových vektorů, bude pro ně platit stejná vlastnost jako pro skupinu původních vektorů.

C Pokud vezmeme libovolný vektor z původních 7 a přidáme libovolný vektor z doplňkových, potom můžeme určit vzor doplňkového vektoru a pro něj a pro vybraný vektor z původních opět musí platit, že mají shodné 3 souřadnice a zbylé 4 mají odlišné, nebo jde o stejný vektor. Pokud se opět vrátíme k doplňkovému vektoru, potom bude platit, že na začátku zvolené vektory se budou shodovat na 4 pozicích a lišit se budou na 3 pozicích nebo se liší na všech pozicích.

D Pokud uvážíme 2 poslední doplněné vektory [1111111] a [0000000], ty se liší na všech pozicích.

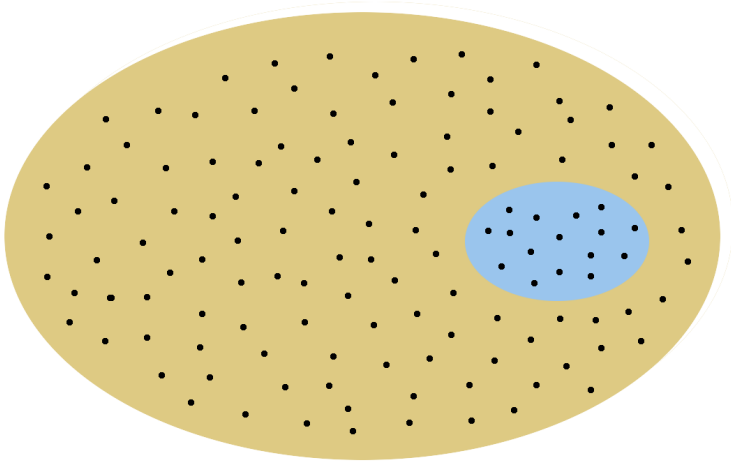
E Pokud budu srovnávat lib. vektor z původních 7 vektorů s vektorem [1111111], budou se lišit ve 4 pozicích, protože každá hrana měla právě tři body (tj. vektor měl vždy 3 jedničky); analogicky pokud budu srovnávat lib. vektor z původních 7 s vektorem [0000000], budou se lišit ve třech pozicích.

F Pro srovnání skupiny doplňkových vektorů s [1111111] a [0000000] platí analogicky jako v E.



Ukázali jsme, že lib. dvojice vektorů ze všech 16 vektorů splňuje to, že se liší minimálně ve 3 souřadnicích.

Podívejme se na problém z druhé strany: Uvažujeme lib. vektor o 7 složkách, kde na každé pozici může být 0 nebo 1. Těchto vektorů je $2^7 = 128$ a mezi nimi i těch 16 našich.



Předchozí věta se dá upřesnit takto:

Věta: Ve skupině našich 16 vektorů se lib. 2 z nich liší buď na 3, 4 nebo 7 pozicích.
(Dokážeme, projdeme-li body A, B, ..., F.)

Důsledek: Pokud ke každému z našich 16 vektorů přiřadíme 7 vektorů tak, že se tyto budou lišit právě v jedné ze 7 pozic, dostaneme celkem $8 \cdot 16 = 128$ vektorů, to jsou ovšem všechny možnosti, které máme, protože ke každým 2 různým vektorům ze 16 původních jsou přiřazeny různé "modifikované vektory".

A, B ... vektory ze "16"

A ... modifikujeme na $\widetilde{A}$ (v 1 pozici)

B ... modifikujeme na $\widetilde{B}$ (v 1 pozici)

A a B se liší minimálně ve třech pozicích $\Rightarrow$ $\widetilde{A}$ a $\widetilde{B}$ se liší minimálně v 1 pozici.

Dostaneme silné tvrzení:

Pro každý vektor délky 7 (obsahující 0 nebo 1) existuje právě jeden vektor z naší "16" tak, že se buď shodují nebo se liší právě na jedné pozici.

$\Rightarrow$ Pokud se při přenosu poruší nejvýše jeden bit, lze ho opravit.

Využití: Vrátíme se k problému přenést $n-$tici bitů. Tu rozdělíme na bloky o čtyřech bitech. Potom každý blok je dvojkovým zápisem jednoho čísla od 0 do 15 (16 možností). Místo, abychom posílali tyto bloky, budeme posílat naše kódové vektory ze "16", které jednoznačně přiřadíme číslům 0 a 15.

Příklad:

Chceme poslat posloupnost 0100 1101 1111 0011 0101.

Získáme bloky 0100 1101 1111 0011 0101.

Místo abychom posílali tyto bloky, pošleme příslušné kódové vektory, tj.

$$0100011 \mid 1101000 \mid 1111111 \mid 0011010 \mid 0101110\ .$$

Všimněme si, že pro každou čtveřici číslic existuje právě jeden vektor z naší "16", který takto začíná.

```
       Zprava vyuzivajici Hamminguv kod
-------------------------------------------------

 Zadej zpravu v binarnim tvaru  = 01001101111100110101

 Zpravu rozdelime na bloky po 4 bitech:
  0100   |1101   |1111   |0011   |0101   |

 Bloky doplnime na kodova slova:
  0100011|1101000|1111111|0011010|0101110|
```

Přenášená posloupnost je delší než n bitů, konkrétně $n+\frac{3}{4}n = \frac{7}{4}n$ bitů. Pravděpodobnost, že při přenosu jednoho bloku (kódového vektoru) nastane nejvýše jedna chyba je:

$$(1-p)^7 + 7 \cdot p \cdot (1-p)^6 = (1-p)^6(1+6p).$$

Kódových slov je $\frac{n}{4}$, a proto celková pravděpodobnost, že se data správně dekódují je

$$\left((1-p)^6(1+6p)\right)^{\frac{n}{4}} = (1-p)^{\frac{3n}{2}} \cdot (1+6p)^{\frac{n}{4}}.$$

Pro náš případ $n = 100$ a $p = 0,01$ vyjde $\approx 95\%$.

To je skoro stejně vysoká pravděpodobnost jako, když jsme informaci posílali 3x za sebou. Objem přenášených dat ale není $3n$, ale pouze $\frac{7}{4}n$, tj. stačí přenášet $\approx 58\%$ dat.

```
        Testovani posilani kodovanych zprav
-------------------------------------------------------
 Puvodni zprava ma 100 bitu.
 Pravdepodobnost chyby pri prenosu jednoho bitu je 0.010000.
 Pri testovani cely proces opakujeme 100 krat.

 Prumerny pocet chybnych bloku pri prenosu jedne zpravy je 0.040000
 Z 100 prenosu bylo 96 bezchybnych,
 tj. 96.0 procent prenosu bylo bezchybnych.

-------------------------------------------------------
 Teoreticky plati, ze pri posilani zpravy o n bitech,
 s pravdepodobnosti chyby pri prenosu 1 bitu p, pricemz
 posilame n + 3/4 n bitu (doplnili jsme kodova slova),
 je pravdepodobnost bezchybneho prenosu jednoho bloku
 (mohla nastat nejvyse jedna chyba):

  (1-p)^7 + 7p(1-p)^6  = (1+6p)(1-p)^6  =
    = (1+6*0.010000)(1-0.010000)^6  = 0.997969

 Kodovych slov je posilano n/4, proto
 pravdepodobnost bezchybneho prenosu cele zpravy je

  ( (1+6p)(1-p)^6 )^(n/4)  = 0.950442
```

Poznámky: Kontrolní mechanismy se používají v řadě případů, například při přidělování **rodného čísla** (v jiných státech se používají různé alternativy identifikačního čísla).
https://cs.wikipedia.org/wiki/Rodné_číslo

850916/1573

Dalším příkladem je konstrukce **ISBN**, tj. identifikačního čísla pro knihy,
https://cs.wikipedia.org/wiki/International_Standard_Book_Number

podobné zabezpečení má v sobě i **čárový kód**, který je dnes vlastně na každém výrobku,
https://cs.wikipedia.org/wiki/Čárový_kód

ISBN 978-0-7334-2609-4

9780733426094

dále **QR kód**, atd. atd.
https://cs.wikipedia.org/wiki/QR_kód
https://ipadvetride.cz/tag/qr-kod
https://www.qrgenerator.cz/

Teorie grafů

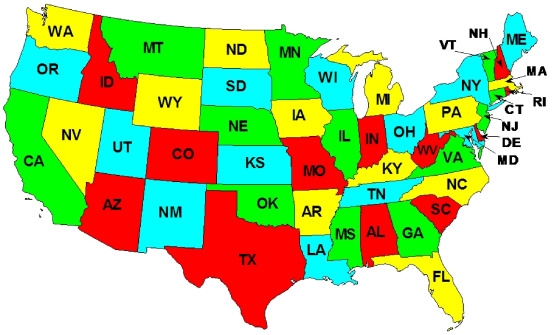
Obyčejný graf je dvojice (V, E), kde V je množina vrcholů (uzlů) a E je množina hran a každé 2 vrcholy spojuje nejvýše 1 hrana.

Graf je rovinný, jestliže existuje takové jeho nakreslení, že se žádné 2 hrany nekříží. Je-li navíc "souvislý" (pro každé 2 vrcholy existuje spojení), pak platí tzv. **Eulerův vztah**:

$$v + u = e + 2,$$

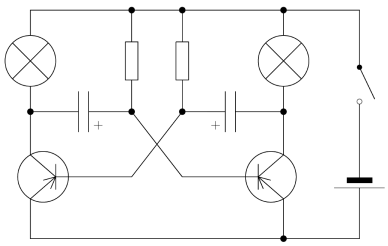
v ... počet vrcholů, e ... počet hran, u ... počet stěn.

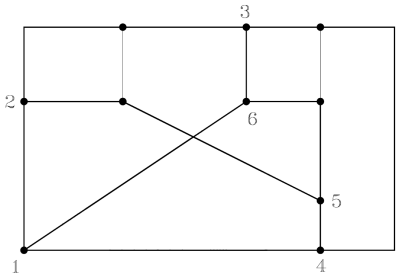
- V roce 1976 byl vyřešen **problém 4 barev**, tj. dokázalo se, že každou mapu lze obarvit nejvýše 4 barvami tak, že žádné dva sousední státy nemají stejnou barvu.



- Návrh integrovaných obvodů a desek s plošnými spoji.

  Př.: Schéma obvodu pro dvoužárovkový blikač a odpovídající graf.

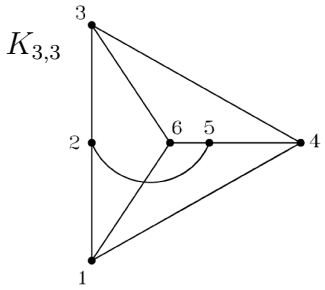


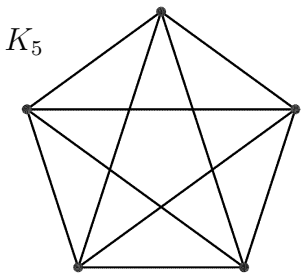


Otázka: Existuje takové nakreslení grafu, že se žádné 2 vodiče nekříží?

Řešení vychází z následující věty.

Věta: Obyčejný graf je rovinný právě tehdy, když neobsahuje část izomorfní s dělením grafu $K_{3,3}$ nebo K_5. (1930 Kuratowsky, složitý důkaz)





Snadno ověříme, že pokud budeme uvažovat pouze očíslované uzly a vynecháme tenké hrany, dostaneme přesně graf $K_{3,3}$.

$\Rightarrow$ Graf není rovinný.