MATEMATIKA

Naše pedagogická realita

FRANTIŠEK KUŘINA

Přírodovědecká fakulta Univerzity Hradec Králové

V tomto příspěvku přinášíme rozbor řešení čtyř úloh z matematiky základní a střední školy. Úlohy řešilo 46 studentů prvního ročníku bakalářského studia učitelství matematiky naší školy a šetření probíhalo jako součást projektu *Matematická gramotnost a řešení úloh*. Vypracování úloh bylo anonymní, každý student však o sobě vyplnil dotazník, jehož otázky postupně uvedeme. Na zpracování projektu se podíleli tito studenti: *Aneta Jahelková*, *Zdena Trefilíková*, *Jan Krejcar* a *Lenka Horní*. Matematickou gramotností budeme v tomto textu rozumět v souladu s publikací [1]

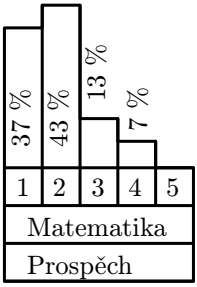
- schopnost porozumět matematickému textu (slovnímu, symbolickému nebo obrázkovému,
- schopnost vybavovat si potřebné matematické pojmy, postupy a teorie,
- dovednost řešit úlohy jak z matematiky, tak i z jejích aplikací, které jsou (obvykle bezprostředním) užitím probraného učiva.

K řešení úloh problémového charakteru je třeba větší míra tvořivosti, která představuje vyšší úroveň matematické kultury. Tato úroveň nemůže být požadována od celé populace. Základní matematickou gramotnost by ovšem měl dosáhnout každý absolvent příslušného typu školy.

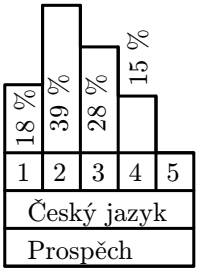
Domníváme se, že úkoly, jejichž rozbor uvádíme, jsou vhodným materiálem k testování matematické gramotnosti. Skutečnost, že někteří absolventi střední školy této úrovně nedosahují (jak prokážeme naším šetřením), je alarmující.

Charakteristika skupiny

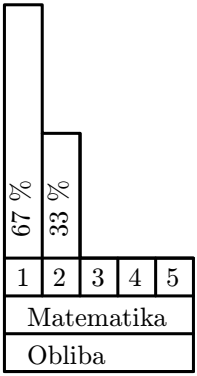
Ze 46 studentů bylo 26, tj. 63 % z gymnázií, ostatní studovali na těchto školách: střední průmyslová škola (4 studenti), obchodní akademie (4), střední pedagogická škola (2), střední škola informatiky (2), hotelová škola (2) a po jednom studentu přišlo ze střední školy podnikání, zahradnické školy a ekonomického lycea. Středoškolský prospěch studentů naší skupiny v matematice (průměr 1,89) a v českém jazyku (průměr 2,41) je popsán grafy na obr. 1 a 2. Oblíbenost matematiky a českého jazyka ve stupnici velmi rád (1), rád(a) (2), nevadí mi (3), nerad(a) (4), velmi nerad(a) (5) je znázorněn na obr. 3 a 4. Každý sloupec grafu vyjadřuje příslušný počet procent.



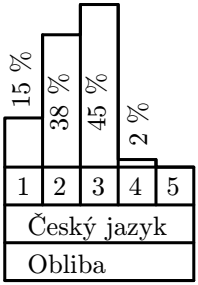
Obr. 1



Obr. 2



Obr. 3



Obr. 4

V dotazníku odpovídali studenti na čtyři otázky.

a) *Jaký je váš oblíbený předmět?*

Pořadí oblíbenosti předmětů (v závorce je počet studentů, kteří příslušný předmět uvedli, přičemž někteří uvedli oblíbených předmětů více):

1. Matematika (26)
2. Tělesná výchova (13)
3. Dějepis (6)
4. Výtvarná výchova (4)
5. Angličtina (3)
6. Biologie (3)
7. Zeměpis (2)
8. Informační technologie (2)
9. Fyzika (2)
10. Hudební výchova (2)
11. Základy společenských věd (2)

Po jednom hlasu dostaly: dějiny umění, sadovnická tvorba, logika, chemie, ruský jazyk, deskriptivní geometrie, dílny, francouzský jazyk, německý jazyk a latina. Jeden student si neoblíbil ani jeden předmět, přesto se chce stát učitelem.

b) *Jaký máte životní cíl?*

Celkem 19 studentů považuje za svůj životní cíl dostudovat, pro 11 studentů je cílem stát se učitelem, 8 má za cíl založit rodinu, 8 mít práci.

Z dalších cílů uveďme: být prospěšný společnosti, nezklamat rodiče, vychovat děti, něco dokázat, spokojeně prožít život, být finančně zajištěn, získat titul RNDr., mít dobré zdraví, být slušný a upřímný, bydlet v domě, živit se jako trenér, být dobrou kytaristkou, být lepší rodič než byli moji rodiče, pracovat kreativně a s elánem. Vyskytuje se i cíl koupit si psa nebo protloukat se životem na jednostopém vozidle. Tři studenti neuvedli žádný životní cíl.

c) *Jaký je váš oblíbený autor (spisovatel, hudebník, malíř, umělec, ...)?*

Sedm studentů nemá žádného oblíbeného autora. Nejoblíbenější autoři jsou: K. Čapek (u 4 studentů), J. Steinbeck (2), Rowlingová (2), A. Camus (2), M. Weewegh (2, započítáme-li i Viewegha), Miler (autor krtečka) (2), L. Amstrong (2), Remarque (2). Po jednom hlasu získali např. J. Škvorecký, J. Verne, S. Dali, J. Čapek, O. Pavel, A. Einstein, B. Hrabal, K. Poláček a další.

d) *Máte nějaký životní vzor? Jaký?*

Celkem 23 studentů neuvedlo vzor žádný. Matku má za svůj vzor 5 studentů, otce 4 studenti, učitele 3 studenti, Boha 2 studenti. Jedenkrát se vyskytovali např. T. G. Masaryk, W. Churchil, L. Špaček, K. Kryl, R. Federer, dědeček.

Rozbor řešení úloh

Úloha 1. *Z obnosu byla nejdříve utracena jeho polovina a pak třetina zbytku. Zůstalo 50 Kč. Kolik činí původní obnos? Postup řešení zapište.*

80 % studentů došlo ke správnému výsledku (150 Kč). 20 % studentů našlo nesprávný výsledek nebo neuvedli výsledek žádný. To je na takto jednoduchou úlohu dosti malý úspěch.

Správná řešení můžeme rozdělit do pěti typů.

a) Řešení rovnicí, např. v podání studenta (4):

původní obnos ... x

$x - \frac{1}{2}x - \frac{1}{3} \cdot \frac{1}{2}x = 50$

...

$x = 150$.

b) Řešení pomocí obrázku nebo schématu.

V kruhu nebo obdélníku vyznačili tito řešitelé třetinu celku, která představuje 50 Kč. Odtud určili výsledek.

c) Student (19) řešil úlohu zpaměti s výsledným zápisem:

$2 \cdot (50 + \frac{1}{2} \cdot 50) = 150$.

d) Úsudkem zapsaným slovně nebo symbolicky řešili úlohu 2 studenti.

e) Jeden student uhodl výsledek a provedl zkoušku.

Algebraicky pomocí rovnice řešilo úlohu 13 % studentů.

Nesprávná řešení úlohy spočívala např. v neporozumění textu, v neúspěšném pokusu o převedení textu do jazyka algebry, v numerických chybách (např. $\frac{1}{2} + \frac{1}{3} = \frac{1}{6}$, $75 \cdot 2 = 120$) nebo v neúspěšném pokusu řešit úlohu trojčlenkou.

Patří-li k matematické gramotnosti i správné užívání matematického jazyka, o čemž jsme přesvědčeni, pak nemůžeme být spokojeni, neboť v řadě řešení, která vedou ke správným výsledkům, se vyskytují zápisy typu: $50 : 2 = 25 \cdot 3 = 75 = \frac{1}{2}$, $\frac{2}{3} = 50$, $\frac{1}{5} = 75$, $1 = 150$.

Úloha 2. *Načrtněte v soustavě souřadnic přímku $p = PB$ a napište její rovnici* ($P[0;0]$, $B[4;2]$).

Výsledky můžeme shrnout do tabulky:

	Správná rovnice	Nesprávná rovnice
Správný obrázek	20 %	41 %
Nesprávný obrázek	9 %	30 %

Do kategorie nesprávný (obrázek nebo rovnice) zahrnujeme i případy, kdy příslušný výsledek zcela chybí.

Skutečnost, že 71 % studentů nedokázalo najít rovnici přímky PB je dokladem nezvládnutí jazyka analytické geometrie. Ačkoliv lze směrnicový tvar rovnice přímky bezprostředně vidět z obrázku, vyskytoval se tento přístup přibližně v jedné třetině pokusů o řešení. Ve stejném rozsahu vycházeli studenti z obecného nebo parametrického vyjádření přímky. Studenti se opírali spíše o postupy, které jim ze školy utkvěly v paměti, než o rozbor konkrétní geometrické situace.

Úloha 3. *Vypočítejte obsah pravidelného dvanáctiúhelníku vepsaného do kružnice poloměru r.*

Jediný student došel k výsledku $S = 3r^2$, šest studentů uvedlo výsledek ve tvaru, který lze na konečný tvar snadno upravit, např.

$S = 12\,r^2 \sin 15^\circ \cos 15^\circ$,

$S = 12\,r^2 \cdot \frac{1}{2} \sin 30^\circ$,

$S = 12\,r \cdot \sin 15^\circ \cdot \sqrt{r^2 - r^2 \sin^2 15^\circ}$,

$S = 12 \cdot \frac{1}{2} \cdot 2r \cdot \cos 75^\circ \cdot \sin 75^\circ \cdot r$.

Správný výsledek tak dosáhlo 15 % řešitelů.

50 % studentů úlohu vůbec neřešilo, nebo jen naznačilo, jak by se snad mohlo postupovat.

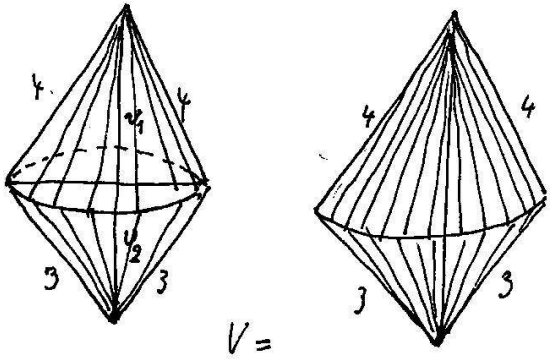
35 % řešitelů došlo ke zcela nesprávným výsledkům. Chyby, kterých se dopouštěli, prokazují naprostou matematickou negramotnost. Uveďme některé: Obsah trojúhelníku o stranách a, b je roven $S = \frac{1}{2}ab$ nebo $S = \frac{1}{2}(a + v_a)$. Obvod pravidelného dvanáctiúhelníku je roven délce kružnice, obsah je zaměněn za obvod, sinus je poměr dvou sousedních stran trojúhelníku, ...

Úloha 4. *Načrtněte a popište těleso, které vznikne otáčením pravoúhlého trojúhelníku s odvěsnami* 3 cm *a* 4 cm *kolem přepony. Vypočítejte objem tohoto tělesa.*

Všimněme si nejdříve úkolu nakreslit těleso.

Správnou představu o tělese si učinilo 30 % řešitelů, polovina z nich nakreslila dosti výstižný obrázek. Za všechny zde reprodukujeme obr. 5 studenta (4). Zbývající řešitelé z této skupiny těleso slovně popisovali, někteří ovšem s použitím nesprávné terminologie (dva jehlany spojené podstavou tvaru kružnice, dva válce otočené k sobě podstavami, dvojkužel se

základnami u sebe). Řada obrázků bylo zcela nesprávná. U dvou studentů nevyvolává termín otáčení představu prostoru. Jeden z nich, absolvent (23) průmyslové školy strojnické (!), odpovídá, že rotací trojúhelníku vznikne deltoid, studentka (40) píše: „Nelze udělat objem trojúhelníku.“



Obr. 5

Celkem 63 % řešitelů si neudělalo žádnou nebo zcela špatnou představu o tělese popsaném v textu úlohy. To svědčí o velmi nízké gramotnosti těchto studentů, neboť geometrická představivost je podle našeho názoru její složkou.

Objem tělesa vypočítali (až na drobné nedostatky) čtyři gymnazisté (9 % řešitelů), úlohu neřešilo nebo řešilo zcela nesprávně 85 % studentů, někteří počítali objem kužele např. podle „vzorců“ $V = \frac{4}{3}\pi r^3 v$, $V = \frac{a^2 v}{2}$.

Protože geometrická úloha (5) z našeho šetření byla relativně obtížná, připojíme zde k posouzení geometrické gramotnosti studentů rozbor zcela elementární geometrické úlohy z jiného průzkumu.

Úloha 5. *Sestrojte všechny kružnice, které procházejí daným bodem B a dotýkají se v daném bodě T dané přímky p. Konstrukci popište a zdůvodněte.* (Bod B na přímce p neleží.)

Tuto úlohu řešila skupina 33 absolventů různých středních škol. Pouze dva studenti úlohu vyřešili: jedna absolventka gymnázia a jeden absolvent průmyslové školy.

Šest studentů se ani nepokusilo nakreslit dané prvky. Pět studentů pochopilo úlohu tak, že daný bod B je středem hledané kružnice a nakreslili

kružnici se středem B poloměrem $|BT|$. Osm studentů považovalo úsečku BT za průměr hledané kružnice. Zbývajících 12 studentů kreslilo nejrůznější zmatené náčrtky, které nevedly k řešení.

Řešitelé této úlohy prokázali totální geometrickou negramotnost, neboť mnozí ani nedokázali slovní text přetransformovat do jazyka geometrického obrázku. Není jim jasná role rozboru konstrukční úlohy, nedokáží si ani položit vhodnou otázku, která by mohla být počátkem nalezení řešení.

Nedostatky, které se zde prokazatelně vyskytly, se týkají učiva základní školy, přesto však se učivo znovu probírá na školách středních. Konstrukční úlohy jsou podle mého názoru dobře zpracovány v učebnici [3], naše úloha 6 je zde podrobně vyřešena v kapitole 2.5 *Konstrukce kružnic*.

Kdybychom měli hodnotit výuku geometrie podle výsledků řešení našich úloh, museli bychom konstatovat, že studenti znají z geometrie velmi málo. Nejen že nedokáží vyřešit základní konstrukční úlohy. Neznají ani geometrickou terminologii (rotací trojúhelníku vznikne jehlan ...), ani základní vzorce pro obsahy geometrických útvarů ($S = \frac{1}{2}(a+b+c)$ (obsah trojúhelníku), $V = \frac{1}{3}v \cdot 2\pi r$ (objem kužele) ...).

Závěry

Šetření, o němž podáváme zprávu v tomto textu, si samozřejmě nemůže dělat nároky na kvalifikovanou výpověď o úrovni absolventů našich středních škol v roce 2010 a 2011. Může však poskytnout obrázek o tom, jaká je matematická kultura 46 maturantů z naší skupiny.

Znovu si při této příležitosti klademe otázku, jak se u těchto absolventů středních škol podařilo naplnit cíle, které si matematické vzdělávání u nás klade. Vždyť již absolvent základní školy má mít mimo jiné tyto *klíčové kompetence* (citováno volně podle *Rámcového vzdělávacího programu pro základní školy*):

- samostatně a kriticky myslet,
- formulovat a vyjadřovat své myšlenky a názory v logickém sledu,
- používat správně základní pojmy z různých vzdělávacích oblastí, chápat jejich smysl a význam a aplikovat je,
- operovat s obecně užívanými termíny, znaky a symboly
- ...

Okřídlená slova *Gustava Adolfa Lindnera* z počátku dvacátého století „*Chceme vychovat obry a vychováváme trpaslíky*“ platí i dnes. Nemůžeme

se tomu divit, jestliže naše společnost přijala tezi „že úroveň vzdělanosti se zvýší tím, že se zvýší procento lidí s maturitou (a s vysokoškolským vzděláním)“ (citováno podle [2, s. 196]).

Všimneme-li si znovu obr. 3, vidíme, že naše úlohy řešili, a to s tak ubohými výsledky studenti, kteří uvádějí, že mají matematiku velmi rádi (67 %) nebo rádi (33 %). Snad chtěli tímto přiznáním nějak ospravedlnit svou volbu studia. Tito studenti byli ovšem na střední škole hodnoceni v matematice výborně (v 37 %) nebo chvalitebně (v 43 %)! Výsledky v mateřském jazyce se zdají být adekvátnější jejich výkonům.

Základem účinného matematického vzdělávání by měla být taková koncepce vyučování, při níž učitel zná a respektuje možnosti svých žáků. Někteří vyučující přednášejí pro nejlepší studenty v posluchárně, s nimiž jsou v kontaktu (sledují, jak studenti reagují, kladou dotazy, ...), ostatní zapisují přednášku a ani se nemohou dobře soustředit na porozumění učivu. Přednáška absolvovaná bez porozumění je zárodkem formálního přístupu ke vzdělávání. Student při přípravě na zkoušku nemá již někdy čas učivo hluboce promýšlet. Učí se zpaměti definice, věty, ba i důkazy — bez hlubšího přemýšlení. A někdy může u zkoušky i projít.

Je přirozeně obtížné přizpůsobit výuku nestejné a mnohdy nízké úrovni nejen znalostí, ale i abstraktního myšlení studentů. Prvním předpokladem realistického přístupu k vyučování je, aby každý student měl k dispozici učebnici. Pak se vyučující může hlouběji soustředit na příklady, které výklad nejen ilustrují, ale i motivují. Může uvádět i dostatek příkladů aplikačních.

Sonda, o níž podáváme zprávu v tomto textu, ukazuje na neutěšený stav části našeho školství. Studenti jsou produktem našich základních a středních škol. V jistém smyslu za úroveň svých vědomostí nemohou. Jestliže se však rozhodli, že chtějí být učiteli matematiky, musí své nedostatky buď překonat, nebo studium ukončit. Jiná cesta není.

Literatura

[1] *Hošpesová, A.*: Matematická gramotnost a vyučování matematice. Jihočeská univerzita, České Budějovice, 2011.

[2] *Kobíková, Z., Fuchs, E.*: Rozhovor o státní maturitě. Učitel matematiky, ročník 2012 (2012), č. 4, s. 195–200.

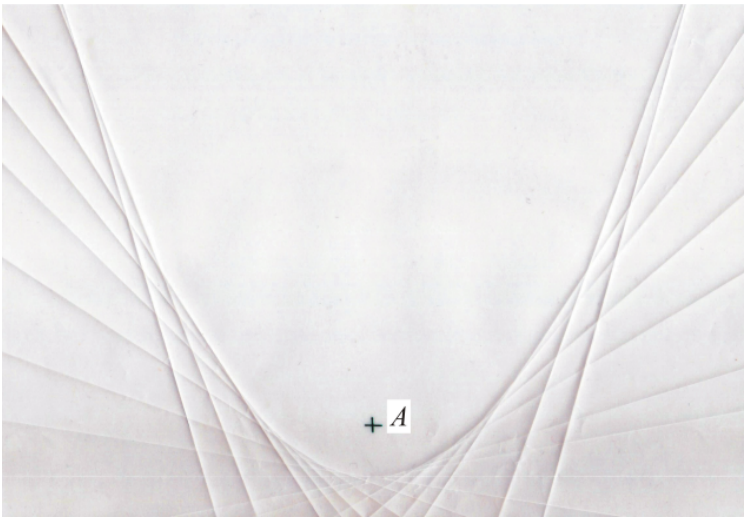
[3] *Pomykalová, E.*: Matematika pro gymnázia. Planimetrie. Prométheus, Praha, 1999.

Od řešení Heronovy úlohy k modelům kuželoseček

PAVEL LEISCHNER – LIBUŠE SAMKOVÁ

Pedagogická fakulta JU, České Budějovice

Víte, že pouhým překládáním listu papíru se dají vymodelovat kuželosečky? Vezměte si list papíru, při jeho dolním okraji uprostřed vyznačte bod A a přehněte list tak, aby jeho dolní okraj procházel bodem A. Pak list narovnejte do původní polohy. Když postup několikrát zopakujete a vytvoříte různé přehyby, zjistíte, že obalují parabolu (obr. 1).



Obr. 1: Modelování paraboly překládáním papíru

Články [1], [2] zmiňují podobné postupy i pro vymodelování elipsy a hyperboly. Náš příspěvek je rovněž věnován této problematice. Navíc si ukážeme úzkou souvislost takového modelování s Heronovou úlohou.

Heronova úloha

Heron Alexandrijský (10–75 n.l.) zkoumal ve spisu *Catoptrica* zákonitosti šíření světla. Předpokládal, že světlo se šíří vždy tak, aby jeho trajektorie měla minimální délku. Tento princip nejkratší dráhy použil k vyřešení problému, v jakém místě na zrcadle se musí světelný paprsek odrazit, má-li se odrazem dostat z bodu A do bodu B. Matematická varianta problému se nazývá Heronova úloha: *V rovině je dána přímka p a body A, B, které na ní neleží. Sestrojte bod $C \in p$ tak, aby pro všechny body $X \in p$, $X \neq C$ platilo $|AX| + |XB| > |AC| + |CB|$.*

Stejnou situaci popisuje také následující slovní úloha: *Jezdec na planině má namířeno z bodu A do bodu B. Cestou musí napojit koně u řeky, kterou představuje přímka p. Najděte místo, kde má jezdec koně napojit, aby jeho cesta byla co nejkratší.*

V případě, že každý z bodů leží v jiné polorovině určené přímkou p, je řešení triviální: jezdec pojede přímo z bodu A do bodu B a bude doufat, že se mu podaří řeku přebrodit. Tedy, bod C je průsečíkem přímky AB a přímky p.

Zbývá nám případ, kdy oba body leží ve stejné otevřené polorovině určené přímkou p. Při hledání bodu C využijeme osovou souměrnost podle přímky p: obraz bodu A v osové souměrnosti podle osy p si označíme A' a zvolíme bod C jako průsečík úsečky $A'B$ a přímky p. Vyznačme si na přímce p bod X různý od bodu C (obr. 2). Pak z osové souměrnosti plyne rovnost

$$|AX| + |XB| = |A'X| + |XB|,$$

z trojúhelníkové nerovnosti v trojúhelníku $BA'X$ dostáváme

$$|A'X| + |XB| > |A'B|$$

a z faktu $C \in A'B$ s pomocí osové souměrnosti zjistíme, že

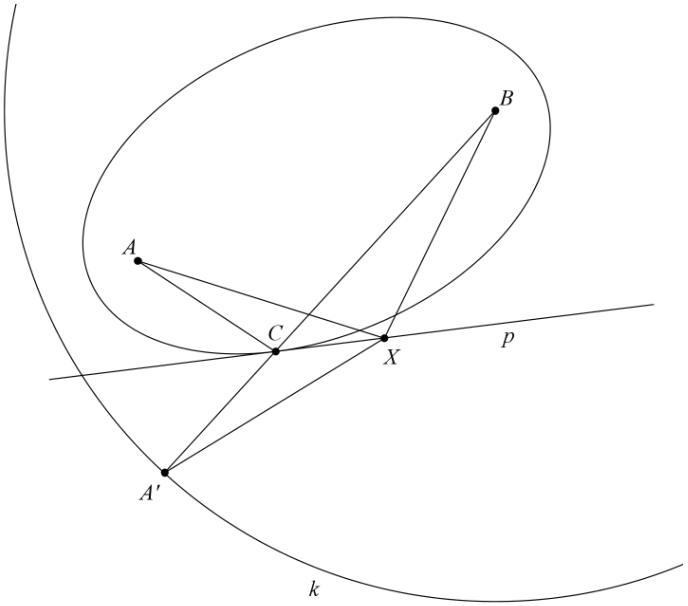
$$|A'B| = |A'C| + |CB| = |AC| + |CB|.$$

Dokázali jsme, že pro libovolný bod $X \in p$ různý od bodu C je

$$|AX| + |XB| > |AC| + |CB|,$$

tedy cesta přes bod C je nejkratší.

Konstrukcí bodu C jsme dokázali jeho existenci i jednoznačnost. Z řešení případu, kdy oba body leží ve stejné otevřené polorovině, navíc plyne, že přímka p se dotýká v bodě C elipsy $\{X;\ |AX| + |XB| = s\}$, kde $s = |AC| + |CB| > |AB|$.



Obr. 2: Rozbor situace pro elipsu

Záměna závislosti

V Heronově úloze bylo dáno A, B, p a hledali jsme bod $C \in p$ a číslo s tak, aby

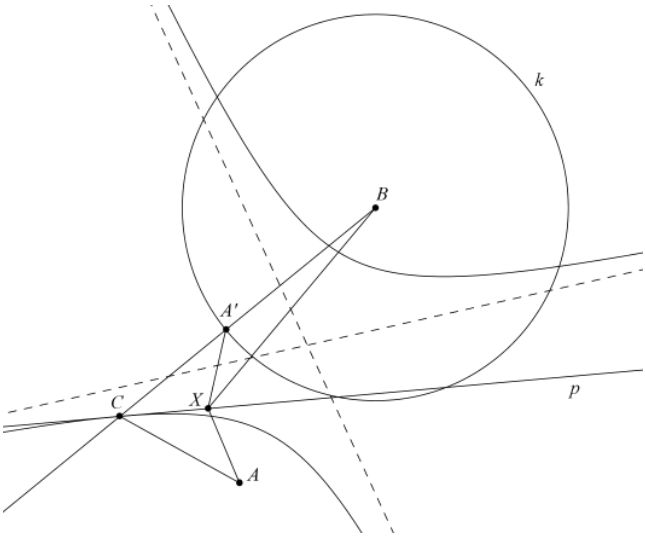
$$s = |AC| + |CB| < |AX| + |XB| \quad \text{pro všechna } X \in p,\ X \neq C. \qquad (1)$$

Pozměňme ji nyní tak, že budou dány body A a B s číslem $s > |AB|$ a budeme hledat přímku p s bodem $C \in p$ splňující vztah (1).

Z podmínky $|A'B| = s$ plyne, že bod A' leží na kružnici k se středem B a poloměrem s. Ke každému bodu $A' \in k$ pak lze sestrojit přímku p jako osu úsečky AA' a bod C jako průsečík úsečky $A'B$ s přímkou p. Jak plyne ze vztahu (1), je přímka p tečnou elipsy, která má ohniska A, B a hlavní osu délky s. Bod C je bodem dotyku. Všechny takové přímky p tedy obalují elipsu $\{X;\ |AX| + |XB| = s\}$, která je množinou všech možných bodů C.

Zabývejme se dále situací, kdy $0 < s < |AB|$. Trojúhelník ABC z obr. 2 za této podmínky neexistuje, protože neplatí trojúhelníková nerovnost. Pro

téměř každý bod $A' \in k(B; s)$ však můžeme sestrojit bod C jako průsečík přímky $A'B$ s osou úsečky AA' (obr. 3).



Obr. 3: Rozbor situace pro hyperbolu

Z trojúhelníkové nerovnosti $|A'B| > \big||A'X| - |XB|\big|$ a z osové souměrnosti zjistíme, že:

$$s = \big||AC| - |CB|\big| > \big||AX| - |XB|\big| \quad \text{pro všechna } X \in p,\ X \neq C. \quad (2)$$

Všechny přímky p nyní obalují hyperbolu $\{X;\ \big||AX| - |XB|\big| = s\}$, která je množinou všech možných bodů C.

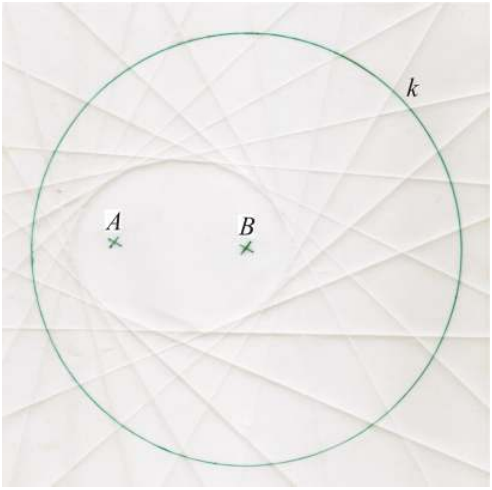
Poznamenejme, že bod C nelze sestrojit, když $A' \in \{T_1, T_2\}$, kde T_1, T_2 jsou body dotyku tečen z bodu A ke kružnici k. Přímky p_1 a p_2, které jsou osami úseček AT_1 a AT_2, jsou totiž asymptotami dané hyperboly.

Doporučujeme čtenáři, aby si promyslel speciální situace:

a) Pro $A = B$ a $s > 0$ je množinou všech bodů C kružnice s poloměrem $s/2$.
b) Pro $A \neq B$ a $s = 0$ je množinou všech bodů C osa úsečky AB.
c) Pro $A \neq B$, $B \to \infty$ a $s > |AB|$ znázorníme kružnici k v blízkosti bodu A jako přímku a množinou všech bodů C je parabola jako limitní případ elipsy. Podobně pro $A \neq B$, $s \to \infty$ a $|AB| > s$ vznikne parabola jako limitní případ hyperboly.

Modelování kuželoseček skládáním papíru

Přehnutí papíru, které umístí bod A' na bod A vytváří přehyb, model osy úsečky AA'. Jestliže si tedy na pauzovací papír narýsujeme kružnici k se středem B a poloměrem s a bod A v její vnitřní oblasti, modelujeme takovým překládáním papíru pro různé body $A' \in k$ přímky, které obalují elipsu $\{X;\ |AX| + |XB| = s\}$ (obr. 4).



Obr. 4: Modelování elipsy překládáním papíru

Přímky obalující hyperbolu $\{X;\ \big||AX| - |XB|\big| = s\}$ vytvoříme analogicky, pokud bod A umístíme do vnější oblasti kružnice k (obr. 5).

Výroba modelu paraboly byla popsána v úvodu. Postup můžeme obměnit tak, že dolní okraj listu papíru nahradíme přímkou q, která neprochází bodem A.

Závěr

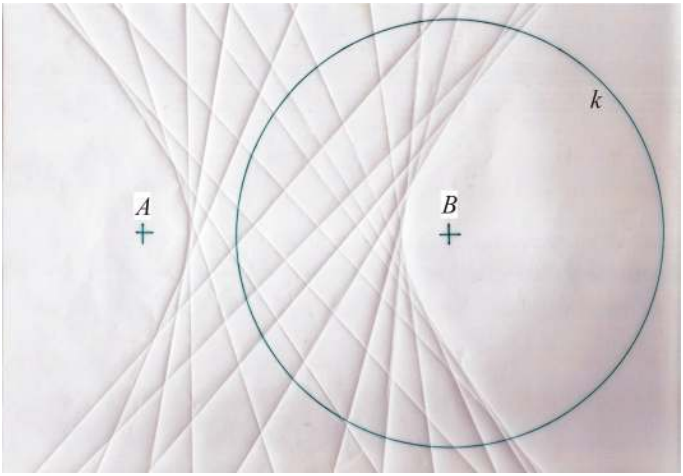
Modelování kuželoseček skládáním papíru může být vítaným zpestřením práce v zájmové matematice. Kromě rozvoje dovedností poskytuje i netradiční pohled na poznatky o vlastnostech tečen kuželoseček. Ty se v učebnicích matematiky a deskriptivní geometrie probírají obvykle suchou formou „věta - důkaz“, kdežto zde jsou přirozenými důsledky úvah spojených se zajímavou činností. Konkrétně máme na mysli větu, že tečna

elipsy, resp. hyperboly půlí úhel průvodičů, a poznatky o tzv. řídící kružnici kuželosečky, kterou v našich úvahách představuje kružnice k.

Rádi bychom také zdůraznili užitečnost úvahy o změně fixace parametrů, které v úloze vystupovaly — fixace parametru s, původně závislého na umístění objektů A, B a p, umožnila přechod od Heronovy úlohy k tečnám kuželoseček. Fixace parametrů patří k základním matematickým metodám.

Popsané činnosti je možné vizualizovat prostřednictvím dynamické geometrie. Tomuto tématu se budeme podrobně věnovat v některém z příštích čísel časopisu.

Nakonec bychom rádi upozornili na webové stránky zaměřené na metody řešení geometrických úloh `www.pf.jcu.cz/stru/katedry/m/mrg.html`, na nichž čtenář najde uvedenou problematiku zpracovanou s využitím Cabri geometrie a kromě ní i řadu dalších zajímavých informací.



Obr. 5: Modelování hyperboly překládáním papíru

Literatura

[1] *Smith, S. G.*: Paper Folding and Conic Sections. Mathematics Teacher, roč. 96 (2003), str. 202–207.

[2] *Leischner, P.*: Vizualizace některých vlastností kuželoseček v Cabri. Sborník příspěvků 3. konference Užití počítačů ve výuce matematiky, 8.–10. listopadu 2007, Jihočeská univerzita v Českých Budějovicích, České Budějovice, 2007, s. 163–168.

Využitie metódy Monte Carlo pri vyučovaní pravdepodobnosti

JANA PÓCSOVÁ

Fakulta BERG, Technická univerzita v Košiciach

Pre výučbu pravdepodobnosti je stále charakteristické riešiť úlohy prostredníctvom klasickej definície pravdepodobnosti s využitím kombinatorických výpočtov. Tento prístup je pre mnohých žiakov náročný. Nazdávame sa, že nesprávne predstavy žiakov vyplývajú z nedostatku skúseností. Domnievame sa, že tieto skúsenosti je možné získať práve simuláciou a vlastným experimentovaním.

Preto v tomto článku navrhujeme spôsob využitia simulácie a experimentovania pri vyučovaní pravdepodobnosti prostredníctvom štatistickej metódy známej ako metóda Monte Carlo.

Podstatou tejto metódy pri simulácii hodnôt náhodných premenných je využitie náhodných čísel. S rozvojom tejto metódy sú späté mená *S. M. Ulama* a *J. von Neumanna* ([1]).

Ako je uvedené v literatúre [5], usudzovanie spojené so stochastickou simuláciou, formulovanie vierohodných úsudkov vyplývajúcich zo štatistických údajov, zbieranie a spracovanie štatistických dát sú dôležitými prvkami stochastického vzdelávania. Preto v článku navrhujeme, ako metódu Monte Carlo sprístupniť žiakom. Teoretické pozadie problémov a ilustrácie simulácií sú uvedené len pre čitateľa, ktorý chce hlbšie preniknúť do riešených problémov. Neodporúčame ho demonštrovať na bežnej hodine matematiky pre žiakov strednej školy, keďže k jeho pochopeniu je nutné poznať základy pravdepodobnosti a matematickej štatistiky preberanej v základných vysokoškolských kurzoch. Riešenie navrhnutého problému (bez jeho matematického zdôvodnenia) odporúčame pre žiakov strednej školy po oboznámení sa s pojmom aritmetický priemer.

V článku rešpektujeme základné fázy metódy Monte Carlo, tak ako boli navrhnuté v [7, s. 506–524]. Sú nimi:

- konštrukcia simulačnej schémy (pojem vysvetlíme neskôr),
- určenie spôsobu realizácie simulačnej schémy pomocou generátorov náhodných hodnôt,

- identifikovanie parametra (charakteristiky), ktorého hodnotu chceme odhadnúť,
- zbieranie a spracovanie štatistických údajov vhodnými nástrojmi,
- určenie hodnoty parametra (charakteristiky) na základe získaných údajov,
- fáza interpretácie.

Keďže v článku pracujeme s nasledujúcimi pojmami, pripomenieme ich definície.

Pod *náhodným pokusom* rozumieme jav, experiment, o ktorého priebehu a výsledku rozhoduje náhoda, pričom množina výsledkov pokusu je konečná alebo spočítateľná a pre každý výsledok možno kvantitatívne ohodnotiť pravdepodobnosť, s akou sa pokus týmto výsledkom skončí [3, s. 14]. (Náhodný pokus označujeme podľa [2] gréckym písmenom δ.)

Stochastický model náhodného pokusu δ je dvojica (Ω, p), kde Ω je množina všetkých výsledkov náhodného pokusu δ a p je funkcia, ktorá každému výsledku priradí pravdepodobnosť, s akou náhodný pokus δ môže skončiť týmto výsledkom ([3, s. 36, 44, 62]).

Simulačná schéma náhodného pokusu δ je náhodný pokus δ_s vykonávaný prostredníctvom losovacích nástrojov s matematickými vlastnosťami (prostredníctvom kociek, úrn, ruliet, mincí), ktorý má s náhodným pokusom δ izomorfný stochastický model ([3, s. 98], [2, s. 255]).

Odhad strednej hodnoty náhodnej premennej metódou Monte Carlo

V rámci rôznych reklamných kampaní sa spoločnosti pokúšajú zvýšiť svoj predaj tým, že do jednotlivých balení pridávajú atraktívne ceny. Často je získanie tejto odmeny podmienené vyzbieraním série lósov, ktoré sú do týchto balení pridané.

Našou snahou je pretransformovať tento problém do žiackeho prostredia.

Reálny problém – Motivácia

V každom balení cereálií je iba jedna zo série šiestich postavičiek z rozprávky Madagaskar. Po vyzbieraní a predložení celej série postavičiek výrobca garantuje jedno balenie zdarma. Koľko balení cereálií môžeme očakávať, že je potrebné kúpiť, kým získame právo na výhru? (Porov. [2, s. 342], [7, s. 506].)

V takto formulovanom probléme sú zamlčané niektoré dôležité fakty.

- 6 postavičiek je rozdelených do balení rovnomerne.
- Jeden človek zbiera samostatne postavičky. Predpokladáme, že nie je možne po čase zamieňať už nazbierané postavičky, v prípade, že sa v zbierke opakujú.
- Predpokladáme tiež, že obchod, z ktorého nakupujeme, má neobmedzené množstvo balení pričom v každom z nich je jedna postavička. A aj po kúpe balenia z danou postavičkou sa pravdepodobnosť kúpy balenia s rovnakou postavičkou neznižuje.

V probléme sa stretávame s dvoma náhodnými pokusmi:

- kúpa balenia s náhodnou postavičkou (δ),
- opakovanie kúpy balení tak dlho, až získame celú sériu postavičiek. (Tento pokus ma náhodný počet opakovaní. Ďalej v texte ho označujeme δ_r).

Riešenie problému prostredníctvom metódy Monte Carlo, v prvej fáze, vyžaduje uvedomenie, že postavičky sú v baleniach rozdelené rovnomerne. Preto kúpe jedného zo šiestich balení zodpovedá hod kockou. Každej postavičke zodpovedá jedno číslo na kocke. Preto pokus δ_r možno simulovať opakovaním hodu kockou tak dlho, až na nej padne každé z čísel aspoň raz. Tento analogický pokus k pokusu δ_r budeme označovať δ_s.

V druhej fáze metódy Monte Carlo je potrebné popísať spôsob simulácie náhodného pokusu δ_s pomocou generátoru náhodných čísel. Uprednostníme skutočnú realizáciu pokusu δ_s s hracou kockou.

Kvôli hlbšiemu preniknutiu do problému navrhujeme sformulovať analogickú matematickú úlohu, pričom jej samotná formulácia by mohla byť výsledkom diskusie a analýzy problému so žiakmi:

Koľko krát môžeme očakávať, že je potrebné hodiť kockou, aby padli všetky čísla od jedna po šesť?

Cereálie kupujeme tak dlho, až získame celú sériu, resp. hádžeme kockou dovtedy, až získame celú sériu čísel. Tento čas čakania na sériu je náhodnou premennou T, ktorá nadobúda hodnoty od šesť počnúc. Stredná (očakávaná) hodnota $E(T)$ náhodnej premennej T je jej charakteristikou, ktorú je potrebné určiť v tretej fáze metódy Monte Carlo.

Na základe štatistických údajov získaných opakovaním náhodného pokusu δ_s bude možné určiť aritmetický priemer počtu opakovaní pokusu δ_s.

Podľa zákona veľkých čísel je aritmetický priemer dobrým odhadom strednej hodnoty náhodnej premennej ([2, s. 484]). (Vychádzajúc z našich skúseností s realizáciou vyučovacej hodiny podľa tohto návrhu, je použitie aritmetického priemeru prirodzeným objavom žiakov. Ale pri samotnej realizácii sme tejto fáze ponechali väčší časový priestor a presunuli sme ju až za štvrtú fázu.)

V štvrtej fáze navrhujeme použiť Tab. 1 na spracovanie získaných údajov. Jednotlivé riadky (od 1 do 10) znamenajú opakovanie pokusu δ_s. V druhom až siedmom stĺpci sú znázornené výsledky po hode kockou. Posledný stĺpec zachytáva celkový počet opakovaní pokusu δ_s.

Ako príklad uvádzame takú postupnosť čísel, ktorá padla pri jednom čakaní na kompletnú sériu $(1, 6, 4, 5, 4, 6, 2, 1, 3)$. Túto situáciu sme znázornili v prvom riadku Tab. 1.

	⚀	⚁	⚂	⚃	⚄	⚅	Počet opakovaní pokusu δ_s
1.	II	I	I	II	I	II	9
…							
10.							

Tab. 1. Záznam 10 pokusov δ_s jedného žiaka

Návrh spôsobu záznamu je vhodné ponechať na samotných žiakov. V závere ho odporúčame zjednotiť, aby sumarizácia výsledkov celej triedy prebehla čo najrýchlejšie.

Tak ako sme spomínali vyššie, strednú hodnotu náhodnej premennej T odhadneme pomocou aritmetického priemeru

$$\overline{p} = \frac{\sum_{i=1}^{n} p_i}{n},$$

kde p_i označuje počet opakovaní i-tého pokusu δ_s a n označuje celkový počet uskutočnených pokusov δ_s. Nakoľko aritmetický priemer je dobrým odhadom strednej hodnoty náhodnej premennej ([2, s. 484]), pri dostatočne veľkom n (t.j. dostatočnom opakovaní pokusu δ_s) bude s pravdepodobnosťou blízkou 1 aritmetický priemer $\overline{p}$ blízky teoretickej hodnote 14,7.

Vo fáze interpretácie teda môžeme formulovať nasledujúci úsudok: *V priemere* 15 *hodov kockou postačuje na získanie celej série čísel od* 1 *do* 6.

A teda: *Priemerne* 15 *balení cereálií kúpime, kým získame celú sériu postavičiek a tým právo na výhru.*

Matematické zdôvodnenie

V tejto časti uvádzame podstatné kroky výpočtu strednej hodnoty bez ich podrobného zdôvodnenia. Tento výpočet neodporúčame prezentovať žiakom. (Podrobnejší spôsob výpočtu čitateľ môže nájsť v [7, s. 347–348] a [3, s. 339–342].)

Opakovanie kúpy balenia s náhodnou postavičkou tak dlho, až získame celú sériu, možno rozdeliť na šesť po sebe nasledujúcich fáz. Nachádzanie sa v j-tej fáze ($j \in \{0, 1, 2, 3, 4, 5\}$) znamená, že zatiaľ sme nazbierali j rôznych postavičiek. Teda j-tá fáza je čakaním na jednu zo $6 - j$ postavičiek, ktoré ešte nemáme.

Dĺžka trvania tohto čakania je náhodnou premennou, jej hodnotou je počet opakovaní náhodného pokusu δ do získania balenia s novou postavičkou (vrátane). Označujeme ju T_j.

Dĺžka čakania, je súčtom dĺžok (trvaní) jednotlivých fáz, preto náhodná premenná T je súčtom

$$T = T_0 + T_1 + T_2 + T_3 + T_4 + T_5.$$

Keďže stredná hodnota súčtu náhodných premenných je súčtom ich stredných hodnôt ([3, s. 341, veta 9.10]), získanie $E(T_j)$ pre každé $j \in \{0, 1, 2, 3, 4, 5\}$ vedie k získaniu $E(T)$.

Bernoulliho pokus je náhodným pokusom s dvomi možnými výsledkami (jeden je označovaný ako úspech, druhý ako neúspech), ktorých pravdepodobnosti sú kladné ([3, s. 82]). Opakovanie náhodného pokusu δ v j-tej fáze ($j \in \{1, 2, 3, 4, 5\}$) je Bernoulliho pokusom. Stačí kúpu novej postavičky v j-tej fáze interpretovať ako úspech a kúpu postavičky, akú už má, ako neúspech. Ak pravdepodobnosť, že nastal úspech, t.j. v j-tej fáze sme kúpili s novým balením cereálií aj postavičku, ktorá nám chýbala, označíme u_j, potom

$$u_j = \frac{6 - j}{6}.$$

Z definície strednej hodnoty[1] určíme stredný čas čakania na prvý úspech. Pravdepodobnosť s akou náhodná premenná T_j nadobúda hodnotu $k \in \mathbb{N}$ je rovná $(1 - u_j)^{k-1} \cdot u_j$, čo zapisujeme nasledovne

$$P(T_j = k) = (1 - u_j)^{k-1} \cdot u_j.$$

[1] *Stredná hodnota náhodnej premennej* X so spočítateľným oborom hodnôt $\{x_1, x_2, \ldots\}$ je definovaná ako súčet radu $\sum_{k=1}^{\infty} x_k \cdot P(X = x_k)$ ([3, s. 339]).

Pre jej strednú hodnotu teda platí

$$E(T_j) = \sum_{k=1}^{\infty} k \cdot (1 - u_j)^{k-1} \cdot u_j.$$

Pre u_j spĺňajúce podmienku $0 < u_j < 1$ je tento rad konvergentný a jeho súčet je $\frac{1}{u_j}$ ([3, s. 341]).

Ostáva nájsť $E(T_0)$. Keďže pri prvej kúpe vždy získame novú postavičku, je doba čakania rovná 1, a teda

$$E(T_0) = 1.$$

Očakávaný čas čakania na všetky postavičky zo série je

$$\begin{aligned}\sum_{i=0}^{5} E(T_i) &= E(T_0) + E(T_1) + E(T_2) + E(T_3) + E(T_4) + E(T_5) = \\ &= 1 + \frac{6}{5} + \frac{3}{2} + 2 + 3 + 6 = 14{,}7.\end{aligned}$$

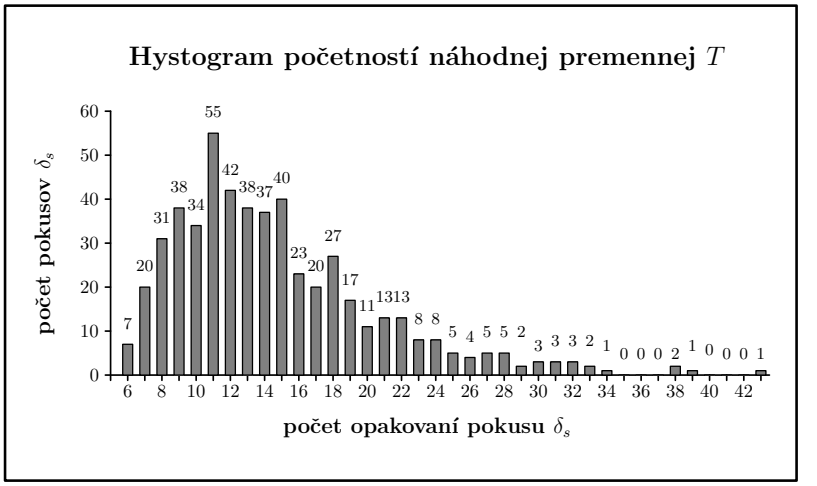
Skúsenosti z vyučovania

Tento problém sme riešili so študentami Pedagogickej univerzity, ale aj vo viacerých triedach gymnázií.

Študentom pedagogickej univerzity bol tento problém nastolený počas základného kurzu pravdepodobnosti. Išlo o študentov učiteľského štúdia. Tento problém bol riešený preto, aby sme zistili, či jeho zadanie je zrozumiteľné. Taktiež preto, aby sme zistili aké najčastejšie otázky, či postrehy odznejú a mohli sme sa na ne pripraviť, keďže v ďalšom kroku sme plánovali zadať tento problém žiakom stredných škol. Výsledky nášho pozorovania sú zachytené v celom návrhu riešenia problému predstaveného v predchádzajúcich častiach. Pre ilustráciu uvádzame výsledky z opakovania pokusu δ_s.

Na hodine bolo 52 študentov a každý z nich opakoval tento pokus 10krát. Priemerný počet doby čakania celej skupiny bol 14,68.

Nasledujúci graf zachytáva informáciu o rozdelení náhodnej premennej T.



Samotné zadanie problému a aj jeho riešenie pomocou simulácie sa stretlo s pozitívnym ohlasom. Ani v jednej triede gymnázia však tento spôsob simulácie nepatril k prvým nápadom žiakov. Domnievali sme sa, že samotná úloha, v ktorej vystupuje práve šesť postavičiek je silným vodítkom k použitiu hracej kocky. Najčastejšie nápady žiakov však boli:

- generovanie náhodných čísel pomocou softvéru MS Exel,
- losovanie šiestich označených lístkov z klobúka s ich opätovným návratom.

Domnievame sa, že aj napriek tomu, že v mnohých úlohách z pravdepodobnosti vystupujú kocky, žiaci nemajú osobnú skúsenosť s ich použitím pri simuláciách na hodine matematiky a preto ich použitie spájajú predovšetkým s hrou a hazardom.

Záver

V tomto článku ponúkame jeden z pohľadov na proces používania matematiky k riešeniu mimomatematických problémov. Ten je organizovaný v troch fázach a to vo fáze matematizácie, fáze výpočtov a dedukcie a fáze interpretácie. V prvej fáze hľadáme matematickú formuláciu mimomatematického problému, ďalej riešime už matematický problém matematickými prostriedkami a v závere ponúkame vysvetlenie získaného výsledku v pôvodnom kontexte ([2, s. 131]).

Na realizáciu fázy výpočtov a dedukcie v predloženom probléme žiaci nemajú potrebný matematický aparát. Preto sme na jeho riešenie navrhli metódu Monte Carlo. Hoci predložený problém vyžaduje len málo výpočtov, v skutočnosti je hlboko matematický a rozvíja dôležité stochastické kompetencie ([4, s. 248–249, 252], [2, s. 510]) akými sú schopnosť prekladať mimomatematický problém do jazyka matematiky, navrhovať simulácie, zbierať a organizovať štatistické údaje a v neposlednom rade formulovať úsudky typické pre stochastiku.

Literatura

[1] *Eckhardt, R.*: Stan Ulam, John von Neumann, and the Monte Carlo Method, Los Alamos Science, roč. 131 (1987), spec. č. 15.

[2] *Płocki, A*: Dydaktyka stochastyky rachunek prawdopodobieństwa, kombinatoryka i statystyka matematyczna jako nowy element ksztalcenia matematycznego, Wydawnictwo Naukowe NOVUM, Płock, 2005.

[3] *Płocki, A*: Pravdepodobnosť okolo nás stochastika v úlohách a problémoch okolo nás, Katolícka univerzita v Ružomberku, Ružomberok, 2007.

[4] *Płocki, A*: Pravdepodobnosť okolo nás stochastika v úlohách a problémoch okolo nás, Katolícka univerzita v Ružomberku, Ružomberok, 2004.

[5] *Płocki, A.*: Stochastické usudzovanie v matematike pre každého, Matematika v škole dnes a zajtra, Ružomberok, 2006.

[6] *Płocki, A., Tlustý P.*: Pravděpodobnost a statistika pro začátečníky a mírne pokročilé, Prometheus, Praha, 2007.

[7] *Płocki, A*: Stochastika dla nauczyciela, Rachunek prawdopodobieństwa, kombinatoryka i statystyka matematyczna jako matematyka in statu nascendi, Wydawnictwo Naukowe NOVUM, Płock, 2007.

Zajímavé matematické úlohy

Pokračujeme v uveřejňování úloh tradiční rubriky Zajímavé matematické úlohy. V tomto čísle uvádíme zadání další dvojice začínající třetí stovku. Jejich řešení můžete zaslat nejpozději do 1. 4. 2014 na adresu: Redakce časopisu MFI, 17. listopadu 12, 771 46 Olomouc nebo také elektronickou cestou (pouze však v TEXovských verzích, příp. v MS Wordu) na emailovou adresu: mfi@upol.cz. Zajímavá a originální řešení úloh rádi uveřejníme.

Úloha 201

V nerovnoramenném pravoúhlém trojúhelníku ABC protne osa vnitřního úhlu a osa vnějšího úhlu při vrcholu C přeponu po řadě v bodech E a F. Dokažte, že platí

$$|AE| \cdot |AF| + |BE| \cdot |BF| > |AB|^2.$$

Jaroslav Zhouf

Úloha 202

V aritmetické posloupnosti $(a_n)_{n=1}^{\infty}$ platí pro jistá přirozená čísla k a l

$$a_k = 2l + k \quad \text{a} \quad a_l = 2k + l.$$

Najděte všechny takové posloupnosti.

Stanislav Trávníček

Dále uvádíme řešení úloh 195 a 196, jejichž zadání byla zveřejněna ve třetím čísle 22. ročníku našeho časopisu.

Úloha 195

Nechť α, β, γ jsou velikosti vnitřních úhlů trojúhelníku, kde $\gamma > 90^\circ$. Dokažte nerovnost

$$\operatorname{tg}\alpha \operatorname{tg}\beta < 1.$$

Józef Kalinowski

Řešení. Ze zadání plyne $0^\circ < \alpha < 90^\circ$, $0^\circ < \beta < 90^\circ$ a $0^\circ < \alpha + \beta < 90^\circ$. Tedy $\operatorname{tg}\alpha$, $\operatorname{tg}\beta$, $\operatorname{tg}(\alpha+\beta)$ jsou kladná reálná čísla. V součtovém vzorci

$$\operatorname{tg}(\alpha+\beta) = \frac{\operatorname{tg}\alpha + \operatorname{tg}\beta}{1 - \operatorname{tg}\alpha \operatorname{tg}\beta}$$

jsou $\operatorname{tg}(\alpha+\beta)$ i $\operatorname{tg}\alpha + \operatorname{tg}\beta$ kladná reálná čísla, proto má tuto vlastnost i jmenovatel $1 - \operatorname{tg}\alpha \operatorname{tg}\beta$ zlomku na pravé straně, tj.

$$\operatorname{tg}\alpha \operatorname{tg}\beta < 1,$$

což jsme chtěli dokázat.

Jiná řešení vyžívala skutečnosti, že funkce $\operatorname{tg} x$ je pro $0^\circ < x < 90^\circ$ rostoucí. Protože $\gamma > 90^\circ$, je $\alpha + \beta < 90^\circ$, a platí tedy $\beta < 90^\circ - \alpha$. Odtud

$$1 = \operatorname{tg}\alpha \operatorname{cotg}\alpha = \operatorname{tg}\alpha \operatorname{tg}(90^\circ - \alpha) > \operatorname{tg}\alpha \operatorname{tg}\beta.$$

Správné řešení zaslali *Karol Gajdoš* z Trnavy, *Anton Hnáth* z Moravan, *František Jáchim* z Volyně, *Jozef Mészáros* z Jelky, *Filip Bialas* z G v Praze 4, Konstantinova, *Markéta Calábková* a *Petr Vincena*, oba z GJŠ v Přerově, *Antonín Češík* ze SPŠE v Pardubicích, *Martin Hora* z G v Plzni, Mikulášské nám., *Lukáš Knob* z G v Kojetíně, *Matěj Konečný* z G v Českých Budějovicích, Jírovcova 8, *Karolína Kuchyňová* z GML v Brně, *Tomáš Lysoněk* z G v Uherském Hradišti, *Viktor Němeček* z G v Jihlavě, J. Masaryka, *Tomáš Novotný* z G v České Lípě, *Martin Raszyk* z G v Karviné, *Jan Šarman* z GMK v Bílovci, *Jan Šorm* z G v Brně, tř. Kpt. Jaroše a *Martin Zahradníček* z G v Šlapanicích.

Neúplné řešení zaslali *Jan Krejčí* z GMK v Bílovci, *Marian Poljak* z GJŠ v Přerově, *Jakub Svovoda* z G V Havířově, Komenského a *Pavel Turek* z G v Olomouci–Hejčíně.

Úloha 196

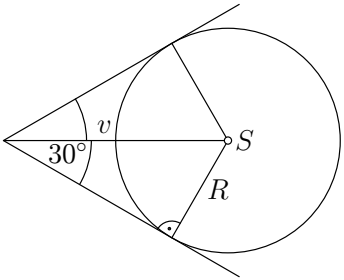
Dvě poloroviny se společnou hraniční přímkou svírají úhel $60°$ a vytvářejí *klín*. Do něj jsou umístěny dvě koule $k_1(S_1; r)$ a $k_2(S_2; r)$, které mají vnější dotyk a současně se obě dotýkají i stěn klínu. Vypočtěte poloměr ρ třetí koule k_3, která se dotýká současně obou koulí k_1 a k_2 a také stěn tohoto klínu.

Stanislav Trávníček

Řešení. Nejprve uvažujme kouli $k(S; R)$ s poloměrem R. Tato koule se dotýká dotýká stěn klínu, právě když S leží v rovině souměrnosti κ daného klínu obsahující hraniční přímku a vzdálenost v bodu S od hraniční přímky je rovna

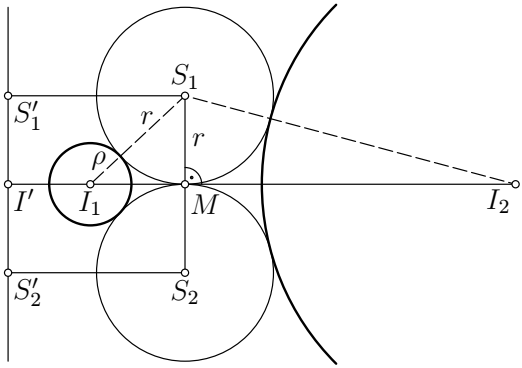
$$v = \frac{R}{\sin 30°} = 2R. \tag{1}$$

Na obr. 1 je znázorněn řez kolmý k oběma hraničním polorovinám klínu obsahující bod S.



Obr. 1

Nyní stačí uvažovat situaci v řezu klínu jeho rovinou souměrnosti κ obsahující hraniční přímku. Označme S_1', S_2' a I' kolmé průměty středů koulí po řadě k_1, k_2 a hledané koule $l(I, \rho)$ na hraniční přímku. Je zřejmé, že úloze vyhovují 2 koule, jejichž středy jsou na obr. 2 označeny I_1 a I_2. Z důvodu stejných výpočtů nechť je dále I libovolný z bodů I_1 a I_2. V rovině κ leží středy všech uvažovaných koulí a jejich body dotyku a ze shodnosti koulí k_1 a k_2 plyne souměrnost situace podle přímky $I'I$. Proto na této přímce leží i bod dotyku M koulí k_1 a k_2 (obr. 2).



Obr. 2

Podle Pythagorovy věty v pravoúhlém trojúhelníku IMS_1 platí

$$|IS_1|^2 = |IM|^2 + |MS_1|^2.$$

Podle (1) odtud dostáváme

$$(r + \rho)^2 = (2r - 2\rho)^2 + r^2,$$

což po úpravě dává

$$3\rho^2 - 10\rho r + 4r^2 = 0.$$

Proto

$$\rho_{1,2} = \frac{5 \pm \sqrt{13}}{3}\, r.$$

Existují dvě koule (viz obr. 2) dotýkající se daných koulí i stěn klínu, mající (kladné) poloměry

$$\rho_1 = \frac{5 - \sqrt{13}}{3}\, r \quad \text{a} \quad \rho_2 = \frac{5 + \sqrt{13}}{3}\, r.$$

Správné řešení zaslal *František Jáchim* z Volyně, *Antonín Češík* ze SPŠE v Pardubicích, *Martin Hora* z G v Plzni, Mikulášské nám., *Jan Krejčí* a *Jan Šarman*, oba z GMK v Bílovci, *Tomáš Lysoněk* z G v Uherském Hradišti, *Marian Poljak* z GJŠ v Přerově, *Martin Raszyk* z G v Karviné, *Pavel Turek* z G v Olomouci–Hejčíně a *Martin Zahradníček* z G v Šlapanicích.

Pavel Calábek

Dokončení ze str. 80.

První z laureátů François Englert je belgický občan. Narodil se v roce 1932 v Etterbeeku v Belgii. Doktorát PhD získal na univerzitě v Bruselu. Je emeritním profesorem na univerzitě v Bruselu.

Druhým laureátem je Peter W. Higgs. Narodil se v roce 1929 v Newcastlu upon Tyne ve Velké Británii. Titul PhD. získal na Londýnské univerzitě v roce 1954. Je emeritním profesorem na Univerzitě v Edingburghu.

Částici teoreticky předpověděl Higgs spolu s dalšími spolupracovníky v roce 1964 a experimentálně byla její existence částečně ověřena v roce 2012.

Odůvodnění nobelovské komise k udělení Nobelovy ceny za fyziku je v českém překladu následující: „Cena se uděluje za teoretický objev mechanismu, který přispívá k porozumění vzniku hmotnosti subatomárních částic, které byly v současnosti potvrzené i experimentálně na urychlovači LHC experimenty ATLAS a CMS v Evropském experimentálním centru CERN.“

Existence Higgova bozonu je podmíněná slabou interakcí, která je zodpovědná za radioaktivitu či jiné jaderné rozpady. Pomocí Higgsova bosonu lze vyložit existenci klidové hmotnosti dalších částic a v návaznosti na to postupně i vývoj všech prvků a života. Proto je Higgsův bozon označován také symbolicky jako božská částice, která po velkém třesku umožnila vznik dalších částic až po atomy, molekuly a jejich agregáty.

Higgsův bozon jakožto subnukleární částice má schopnost kondenzovat energii nehmotných částic ve hmotné částice, které jsou v dalším vývoji základem všech složitějších struktur a má základní schopnost vytvářet ze „záření“ klidovou hmotnost. V kosmu existují elementární částice jednak hmotné a jednak silových polí. Takovou částicí silového pole je právě Higgsův boson. Experimentálně bylo možné částečně potvrdit jeho existenci až po uvedení urychlovače LHC do provozu.

Higgsovou částicí se uzavírá soustava elementárních částic. Objev Higgsova bosonu jak teoretický tak i experimentálně patří mezi největší objevy fyziky, která potvrzuje tímto objevem svoji existenci jako fundamentální věda.

Literatura

[1] The Nobel Prize in Physics 2013. Nobelprize.org. Nobel Media AB 2013. Web. 8 Dec 2013. `http://www.nobelprize.org/nobel_prizes/physics/laureates/2013/`

Lubomír Sodomka

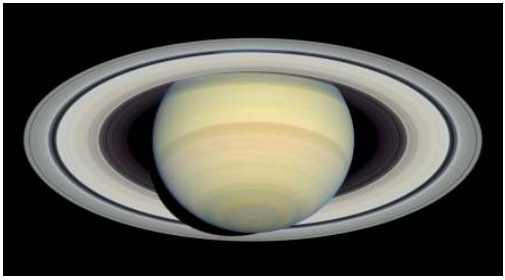
FYZIKA

Nejkrásnější planeta sluneční soustavy Saturn v úlohách

VLADIMÍR ŠTEFL

Přírodovědecká fakulta MU, Brno

Pocity krásy hrají důležitou roli při motivaci studentů a zejména studentek ve výuce méně oblíbené fyziky. Na snímcích nebo při pozorování dalekohledem vyvolává největší pocit libosti z planet ve sluneční soustavě Saturn vzhledem k jeho systému prstenců. Planeta je snadno pozorovatelná již i menšími dalekohledy, nejintenzivnější estetické dojmy vznikají při největším rozevření prstenců. Zajímavá nažloutlá barva (obr. 1), je vyvolána odrazem slunečního světla v horní vrstvě mraků planety.

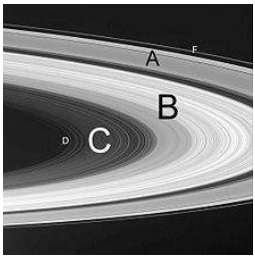


Obr. 1

Prvním, kdo systém prstenců nejen pozoroval, ale i pochopil jejich vzhled, byl *Christian Huygens* (1629–1695) v roce 1657. Mnohem později upřesnil výzkum kosmických sond Voyager I. a II. při průletech v letech 1980 a 1981 tloušťku prstenců na zhruba jeden kilometr a průměr

přibližně na 272 000 km. Prstence pozorujeme díky odrazu slunečního světla. Jsou tvořeny částečkami prachových zrn, ledem a menšími tělísky centimetrových, decimetrových až metrových velikostí. Spektrometry na zmiňovaných kosmických sondách pracující ve viditelném a infračerveném oboru zjistily, že střední rozměr částeček prstence se zvětšuje s rostoucí vzdáleností od planety. Prstence jsou staré pouze stovky miliónů roků. Není dosud spolehlivě objasněno, zda vznikly rozpadem nějakého měsíce či z původního akrečního protoplanetárního disku. V systému prstenců existují mezery, nejzřetelnější je pojmenovaná po *Giovanim Dominicovi Cassinim* (1625–1712), která jím byla objevena roku 1675 (viz obr. 1). Je způsobena gravitačním působením především měsíce Mimas, který prostor gravitačně ovlivňuje, a téměř ho „vyčistil“. Obecně i další mezery v systému prstenců jsou vyvolány gravitačním působením jednoho či více měsíců.

Jak bylo dokázáno v [1] *Jamesem Clarkem Maxwellem* (1831–1879) na základě analýzy dynamické stability, je-li hmotnost Saturnu dostatečně velká, potom prstence diskrétních vzájemně interagujících částeček na oběžné dráze kolem planety udržují stabilní tvar a nejsou tvořeny tuhými tělesy, nýbrž systémy drobných částeček. Později např. *James Edward Keller* (1857–1900) v [2] a *William Wallace Campbell* (1862–1938) proměřovali spektroskopicky relativní rychlosti vnitřních a vnějších částí prstenců k vyjasnění, který jejich okraj se pohybuje rychleji. Závislost rychlosti částic tuhého tělesa na vzdálenosti je $v \sim r$ zatímco u oběžné rychlosti pohybujícího se tělesa na kruhové dráze je dána závislostí $v \sim \sqrt{1/r}$. Bylo zjištěno, že ledové částečky tvořící převážně systém prstenců (obr. 2), se pohybují ve vnitřní oblasti rychleji než ve vnější, což je v souladu s pohybem volného tělesa a jde o tzv. keplerovskou rotaci. Modelové přiblížení problematiky lze demonstrovat následovně.

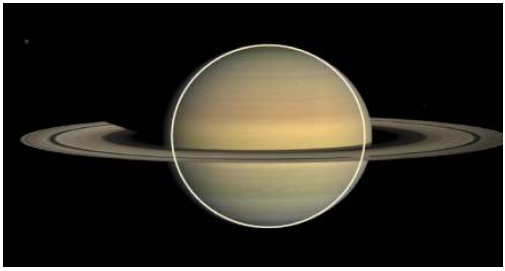


Obr. 2

Úloha 1. Určete oběžnou rychlost vnitřní části prstence D o vzdálenosti 67 000 km od Saturnu s oběžnou dobou 0,20 dne, vnitřní části prstence A o vzdálenosti 122 000 km s oběžnou dobou 0,50 dne, vnitřní části prstence E o vzdálenosti 181 000 km s oběžnou dobou 0,91 dne. Ověřte platnost závislosti $v \sim \sqrt{1/r}$.

Řešení. Dosazením do vztahu $v = \frac{2\pi r}{T}$ postupně získáme $v = 24{,}3\,\mathrm{km \cdot s^{-1}}$, $17{,}7\,\mathrm{km \cdot s^{-1}}$ a $14{,}4\,\mathrm{km \cdot s^{-1}}$, tedy s rostoucí vzdáleností od planety klesá oběžná rychlost v souladu se závislostí $v \sim \sqrt{1/r}$.

Samotná planeta je druhou největší ve sluneční soustavě a má zhruba stokrát větší hmotnost než Země. Vyznačuje se velmi rychlou rotací, která zplošťuje její tvar (obr. 3). Na rovníku dosahuje rotační perioda 10 hodin. První měření úhlových velikostí polárního a rovníkového poloměru provedl *Friedrich Wilhelm Herschel* (1738–1822) [3].



Obr. 3

Úloha 2. Ze znalosti rovníkového poloměru $a = 60\,268$ km a polárního poloměru $b = 54\,364$ km Saturnu určete hodnotu jeho zploštění.

Řešení. Velikost zploštění stanovíme ze vztahu

$$f = \frac{a-b}{a} = 1 - \frac{b}{a}$$

a dosazením obdržíme $f = 0{,}097\,96$.

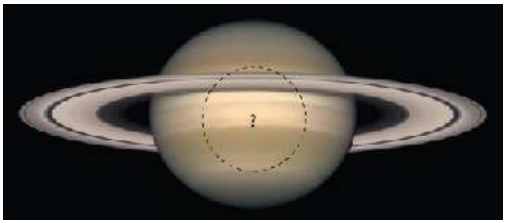
Saturn vyzařuje do svého okolí více energie, než zářením od Slunce přijímá. Nejpravděpodobnějšími dodatečnými vnitřními zdroji energie jsou gravitační smršťování, fázové přeměny vodíku v jeho nitru respektive klesání helia. Základní kvantitativní představy o energetických poměrech jsou zachyceny v následujících úlohách.

Úloha 3. Jak velká je hustota zářivého toku dopadajícího ze Slunce na Saturn?

Řešení. Porovnáním s hustotou zářivého toku tzv. solární konstantou pro Zemi obdržíme

$$K_{\mathrm{S}} = K_{\mathrm{Z}} \left(\frac{r_{\mathrm{Z}}}{r_{\mathrm{S}}} \right)^2 = 14{,}9\ \mathrm{W} \cdot \mathrm{m}^{-2}.$$

Úloha 4. Stanovte efektivní povrchovou teplotu Saturnu (obr. 4).



Obr. 4

Řešení. Pro vyjádření hledaných souvislostí použijeme vztah

$$\pi R_{\mathrm{S}}^2 (1 - A) K_{\mathrm{S}} + 4\pi R_{\mathrm{S}}^2 Q = 4\pi R_{\mathrm{S}}^2 \varrho T_{\mathrm{ef}}^4$$

(podrobněji je rozebíráno v [4]).

První výraz vyjadřuje množství energie dopadající ze Slunce na disk Saturnu, R_{S} je poloměr Saturnu, A je albedo a K_{S} je hustota zářivé energie od Slunce ve vzdálenosti Saturnu. Druhý člen charakterizuje vyzařování vnitřní energie samotným Saturnem. Člen na pravé straně zachycuje vyzařování Saturnu, kde T_{ef} je efektivní teplota. Vzhledem k rychlé rotaci Saturnu předpokládáme celým povrchem planety. Přestože planety nevyzařují úplně přesně jako absolutně černá tělesa použijeme Stefanův–Boltzmannův zákon. Při znalosti koeficientu vnitřního tepla činící u Saturnu $Q = 1{,}80$ a albeda $A = 0{,}45$ dosazení do rovnice obdržíme pro efektivní teplotu Saturnu $T_{\mathrm{ef}} = 91$ K.

Až detailní výzkum Saturnu z bezprostřední blízkosti prostřednictvím kosmických sond umožnil získat údaje, jejichž analýza vedla k chemickému složení a fyzikálním vlastnostem atmosférických vrstev Saturnu. K planetě se přiblížily kosmické sondy Pioneer II. roku 1979, Voyager I. 1980 a Voyager II. 1981, Cassini 2004.

Úloha 5. Určete práci nezbytnou k hypotetickému modelovému přesunu kosmické sondy Cassini o hmotnosti $m_{\mathrm{C}} = 5\,700\,\mathrm{kg}$ z polohy Země na její dráze k Saturnu, vše v gravitačním poli Slunce. Vzdálenost Země–Slunce činí $1{,}50 \cdot 10^{11}$ m, vzdálenost Saturnu od Slunce je $1{,}43 \cdot 10^{12}$ m.

Řešení. Práce je uskutečňována na úkor úbytku gravitační potenciální energie, tedy

$$A = G\,\frac{M_{\mathrm{Sl}}\,m_{\mathrm{C}}}{r_{\mathrm{SlZ}}}\left(1 - \frac{1}{r_{\mathrm{SlS}}}\right).$$

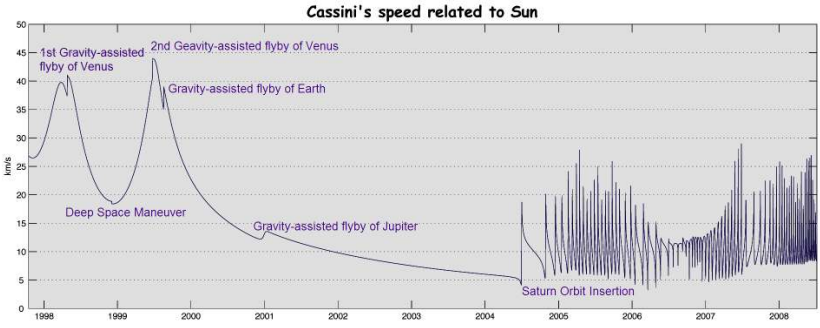
Po dosazení získáme $A \doteq 5{,}1 \cdot 10^{12}$ J.

Reálný let kosmické sondy Cassini s modulem Huygens na palubě byl komplikovanější. Po startu v roce 1997 kosmická sonda dvakrát v letech 1998 a 1999 prolétla kolem Venuše, využila jejího gravitačního pole k urychlení tzv. gravitačním prakem a po průletu kolem Země zamířila k Jupiteru, kde byla koncem roku 2000. Postupně tak při průletech kolem planet docházelo ke zrychlování pohybu kosmické sondy. Při letu kolem Jupitera se dále změnil i směr rychlosti po dráze k Saturnu. Rozeberme zjednodušenou teorii gravitačního praku – urychlení udíleného kosmických sondám planetami, podrobněji viz např. [5], [6].

Kosmická sonda Cassini při přiblížení k Jupiteru zvýšila svoji rychlost díky přitažlivé gravitační síle planety. Při průletu pericentrem ji měla největší, následně gravitace její pohyb zpomalila. V celkovém souhrnu rychlost kosmické sondy vzhledem k Jupiteru zůstala stejná. Avšak počáteční rychlost na začátku a koncová po průletu kolem Jupitera, obě vztahované k heliocentrické soustavě spojené se Sluncem, jsou rozdílné. Planeta Jupiter ztratila část pohybové energie, kterou převzala kosmická sonda Cassini (platí zákony zachování energie a hybnosti). Vzhledem k nepoměru hybností obou těles, daném značným rozdílem hmotností, je ovlivnění dráhy planety v praxi nepozorovatelné, zatímco kosmické sondy významné. Při výše popsaném manévru se rovněž změnil směr jejího letu po dráze. Průletem za Jupiterem (ve smyslu jeho oběžné rychlosti) kosmická sonda získala část oběžné rychlosti planety. V případě kosmické sondy Cassini obdržela dodatečnou rychlost $\Delta v = 2\,\mathrm{km \cdot s^{-1}}$. Na obr. 5 jsou zachyceny změny její rychlosti vzhledem k Slunci při průletech u Venuše, Země a Jupitera.

Kolem Saturnu obíhá větší počet měsíců, největším o průměru 5 150 km je Titan, objevený *Christianem Huygensem* r. 1655 [7]. Měsíc má vlastní hustou atmosféru tvořenou molekulárním dusíkem, metanem a argonem. První spektroskopické studium atmosféry Titanu provedl *Gerrit Pieter*

Kuiper (1905–1973) [8]. Po určení číselné hodnoty gravitační konstanty bylo možné prostřednictvím III. Keplerova zákona v přesném tvaru stanovit přímo nejdůležitější charakteristiku Saturnu – hmotnost.



Obr. 5

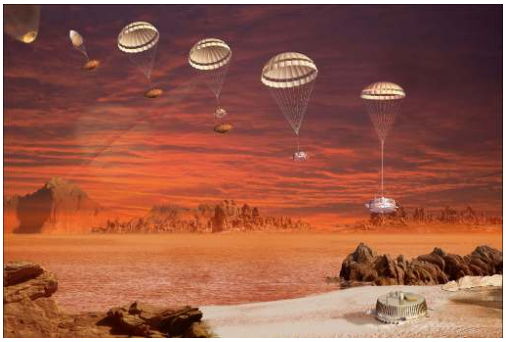
Úloha 6. Nalezněte hmotnost Saturnu, jestliže z pozorování bylo zjištěno, že měsíc Titan (obr. 6), obíhá ve vzdálenosti $a = 1\,221{,}8 \cdot 10^3$ km s oběžnou dobou $T = 15{,}945$ dne.

Obr. 6

Řešení. Úpravou III. Keplerova zákona obdržíme

$$M_{\mathrm{S}} = \frac{G}{4\pi^2}\frac{a^3}{T^2} = 5{,}7 \cdot 10^{26}\ \mathrm{kg}.$$

Spolupráce NASA, ESA a ASI vedla v roce 2004 k přistání modulu Huygens na povrchu Titanu. Modul přes hodinu úspěšně prováděl průzkum chemických a fyzikálních vlastností jeho povrchu. Ve zjednodušeném přiblížení zachycuje závěrečnou fázi přistání modulu obr. 7.



Obr. 7

Úloha 7. Při sestupu modulu Huygens o hmotnosti $m = 320$ kg na padáku na měsíc Titan rychlostí $v = 6\ \mathrm{m \cdot s^{-1}}$, došlo při dopadu modulu k jeho zaboření do hloubky $s = 12$ cm. Stanovte střední sílu F odporu materiálu hornin na Titanu. Jaké decelerační zrychlení a při tom působilo na modul?

Řešení. Kinetická energie modulu je rovna vykonané práci vynaložené při vnikání do povrchových hornin měsíce. Platí

$$Fs = \frac{1}{2}mv^2,$$

odkud po numerickém dosazení obdržíme $F = 57\,600$ N. Dále ze vztahu $mv = Ft$ stanovíme $t = 0{,}033$ s. Odtud

$$a = \frac{2s}{t^2} = 218\ \mathrm{m \cdot s^{-2}}.$$

Druhým největším měsícem Saturnovy soustavy je tzv. ledový Rhea s průměrem 1 530 km. Jeho povrch je pokryt krátery. Dokážeme určit jeho vzdálenost od Saturnu, jestliže známe údaje o pohybu Titanu?

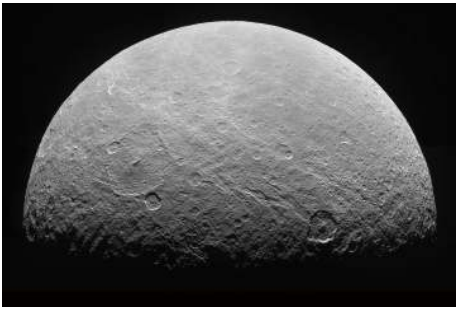
Úloha 8. Jak jsme uvedli, největší Saturnův měsíc Titan obíhá kolem planety po dráze s velkou poloosou $1{,}22 \cdot 10^6$ km za 15,945 dne. Nalezněte střední vzdálenost měsíce Rhea od Saturnu, jestliže jeho oběžná doba činí 4,518 dne.

Řešení. Dosadíme do III. Keplerova zákona

$$\frac{a_\mathrm{T}^3}{T_\mathrm{T}^2} = \frac{a_\mathrm{R}^3}{T_\mathrm{R}^2},$$

odtud vyjádříme $a_\mathrm{R} = 526 \cdot 10^3$ km.

Úloha 9. Případní obyvatelé měsíce Rhea (obr. 8), který má pro pozemský život svým složením příhodnou kyslíkovou atmosféru, bohužel však velmi řídkou s nízkou teplotou 50–100 K, by pozorovali Saturn pod středním úhlovým průměrem $\alpha = 0{,}216\,3$ rad.



Obr. 8

Při znalosti oběžné doby měsíce činící $T = 4{,}517\,5$ dne díky svým fyzikálním znalostem určili střední hustotu Saturnu. Zkuste je napodobit.

Řešení. Použijeme III. Keplerův zákon

$$\frac{a^3}{T^2} = \frac{G}{4\pi^2}\left(M_\mathrm{S} + M_\mathrm{R}\right).$$

Dále platí pro úhlovou velikost průměru

$$\alpha = \frac{2R_\mathrm{S}}{a}.$$

Hmotnost měsíce Rhea $M_\mathrm{R} = 2{,}5 \cdot 10^{21}$ kg můžeme oproti hmotnosti Saturna $M_\mathrm{S} = 5{,}7 \cdot 10^{26}$ kg zanedbávat. Dosazením do III. Keplerova zákona při

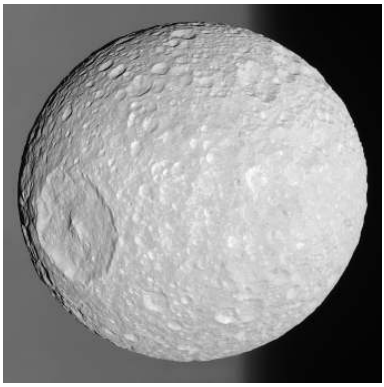
$$M_\mathrm{S} = \frac{4}{3}\pi R_\mathrm{S}^3 \varrho_\mathrm{S}$$

obdržíme pro hustotu

$$\varrho_\mathrm{S} = \frac{24\pi}{GT^2\alpha^3} \doteq 700\ \mathrm{kg \cdot m^{-3}}.$$

Nízká hustota naznačuje, že vodík a helium jsou značně zastoupeny i v nitru planety. Po chemické stránce je planeta složena z molekulárního vodíku, helia, metanu a čpavku.

Dalším zajímavým měsícem Saturnu je Mimas objevený 17. září 1789 *F. W. Herschelem*. Je nejmenším tělesem ve sluneční soustavě zformovaným do sférického tvaru o průměru přibližně 400 km. V minulosti se měsíc srazil s tělesem o průměru přibližně 10 km. Při srážce vznikl zajímavý útvar – velký impaktní kráter Herschel (obr. 9), který zaujal lineární velikostí až čtvrtinu měsíční polokoule, má průměr 130 km, hloubku 10 km s centrální horou o výšce 6,5 km. Průměrná hustota měsíce $1\,150\,\mathrm{kg}\cdot\mathrm{m}^{-3}$ napovídá, že je složen z vodního ledu s příměsí hornin. Kosmická sonda Cassini ze vzdálenosti 9 500 km upřesnila proměřením infračerveným spektrometrem povrchovou teplotu, které dosahuje nejvyšší hodnoty 92 K při průměrné teplotě 77 K. Při těchto teplotách je vodní led extrémně tvrdý.



Obr. 9

Úloha 10. Určete střední rychlost měsíce Mimas, jestliže jeho vzdálenost od planety je $r = 185{,}5 \cdot 10^3$ km a hmotnost Saturnu $M_\mathrm{S} = 5{,}7 \cdot 10^{26}$ kg.

Řešení. Dosadíme do vztahu

$$G_\mathrm{S}\frac{M_\mathrm{S}\,m_\mathrm{M}}{r^2} = \frac{m_\mathrm{M}\,v^2}{r}.$$

odkud obdržíme

$$v = \sqrt{G\frac{M_\mathrm{S}}{r}} = 14{,}1\,\mathrm{km}\cdot\mathrm{s}^{-1}.$$

V soustavě obíhajících měsíců kolem Saturnu, s větší excentricitou eliptických drah, se projevují slapové jevy.

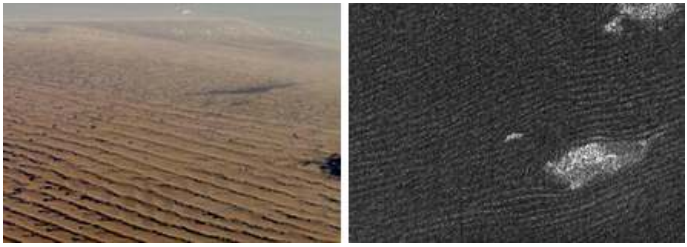
Úloha 11. Stanovte velikost slapové síly Saturnu působící na jeho měsíc Titan. Hmotnost Saturnu je $M_{\mathrm{S}} = 5{,}7 \cdot 10^{26}$ kg, měsíc Titan má hmotnost $M_{\mathrm{T}} = 1{,}35 \cdot 10^{23}$ kg, průměr $D_{\mathrm{T}} = 5\,150$ km a Saturn obíhá ve vzdálenosti $r = 1{,}22 \cdot 10^{6}$ km.

Řešení. Působící slapová síla je dána vztahem

$$F = 2G\,\frac{M_{\mathrm{S}}\,m_{\mathrm{m}}}{r^3}\,D_{\mathrm{m}}.$$

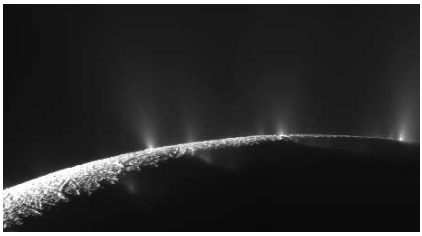
Dosadíme do vztahu parametry soustavy Saturn–Titan, $F_{\mathrm{T}} = 2{,}9 \cdot 10^{19}$ N.

Relativně velká slapová síla Saturnu, výraznější než slapová síla Měsíce působící na Zemi, vyvolává v dusíkové a metanové atmosféře Titanu značný pozorovaný vítr, který způsobuje přesuny písku na povrchu ([9], obr. 10).



Obr. 10

Dalším měsícem, kde se projevují slapové síly je Enceladus, vyznačující se nejvyšším albedem z těles ve sluneční soustavě, odráží 99 % dopadajícího světla. Byl objeven W. Herschelem roku 1789. Na jeho povrchu, byly zjištěny výtrysku vody rychlostí několik set metrů za sekundu (obr. 11). Tato aktivita je pravděpodobně vyvolána působením slapových sil měsíců Saturnu, především Dione a Mimase, jejímž důsledkem je ohřev nitra měsíce.



Obr. 11

Existují metody určování vnitřních charakteristik Saturnu?

Úloha 12. Stanovte centrální tlak v nitru Saturnu při jeho známé hmotnosti $M_{\mathrm{S}} = 5{,}7 \cdot 10^{26}$ kg a poloměru $R_{\mathrm{S}} = 5{,}7 \cdot 10^{7}$ m.

Řešení. Pro sférické planety platí rovnice hydrostatické rovnováhy

$$\frac{\mathrm{d}P}{\mathrm{d}R} = -\varrho g = -\varrho \frac{GM}{r^2}.$$

Při

$$M = \frac{4}{3}\pi \varrho r^3$$

získáme pro centrální tlak vztah

$$P_{\mathrm{c}} = -\frac{4}{3}\pi G \varrho \int_0^R r \,\mathrm{d}r = \frac{2}{3}\pi G \varrho^2 R^2 = \frac{3GM^2}{8\pi R^4}.$$

Dosazením číselných hodnot hmotnosti a poloměru Saturnu do uvedeného vztahu obdržíme $P_{\mathrm{c}} = 2{,}4 \cdot 10^{11}$ Pa.

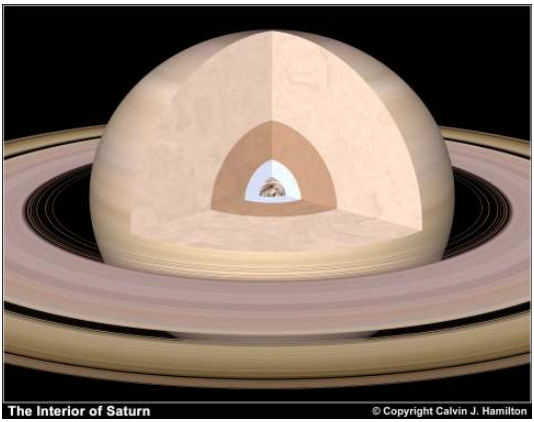
Úloha 13. Proč má obří plynná planeta Saturn horké nitro o teplotě 15 000 K?

Řešení. Menší poměr plochy povrchu k objemu

$$\frac{4\pi r^2}{\frac{4}{3}\pi r^3} = \frac{3}{r}$$

způsobuje pomalejší uvolňování tepla a následné ochlazování planety.

Stavba nitra planety je následující (obr. 12): Vnější část tvoří molekulární vodík, následuje rozsáhlá vrstva tekutého molekulárního vodíku a helia. Pod ní se nachází vrstva tekutého velmi vodivého vodíku. Zásluhou rotace jádra pohybem nabitých částic vzniká silné magnetické pole Saturnu, které objevila sonda Pioneer 11 r. 1979. Jejím zdrojem je tenká stlačená vrstva vodíku vytvářející vedení elektrického proudu v kapalině schopné generovat magnetického pole. V centrální části planety se nachází kamenné jádro. Po chemické stránce je Saturn složen z vodíku, helia, metanu a amoniaku.



Obr. 12

Úloha 14. Určete střední kvadratickou rychlost vodíku v atmosféře Saturnu a její izotermickou škálovou výšku při teplotě 90 K. Zdůvodněte existenci vodíku a helia v atmosféře.

Řešení. Pro střední kvadratickou rychlost platí vztah

$$v_{\mathrm{H}} = \sqrt{\frac{3kT}{m_{\mathrm{H}}}} = 1\,\mathrm{km}\cdot\mathrm{s}^{-1}.$$

Izotermická škálová výška je dána vztahem $h = \frac{kT}{m_{\mathrm{H}} g} = 40\,\mathrm{km}$. Vzhledem k obsahu i těžších molekul v atmosféře je skutečná hodnota škálové výšky menší.

Úloha 15. Stanovte únikovou rychlost na rovníku Saturnu při hmotnosti $M_{\mathrm{S}} = 5{,}7 \cdot 10^{26}$ kg a rovníkovém poloměru $R_{\mathrm{Sr}} = 60\,268$ km.

Řešení. Pro druhou kosmickou rychlost platí vztah

$$v_{\mathrm{Sr}} = \sqrt{2G\frac{M_{\mathrm{S}}}{R_{\mathrm{Sr}}}} = 36\,\mathrm{km}\cdot\mathrm{s}^{-1}.$$

Shrnuto s ohledem na výsledek předcházející úlohy $v_{\mathrm{Sr}} \gg v_{\mathrm{H}}$, tudíž vodík a těžší helium s ještě menší střední kvadratickou rychlostí z atmosféry neunikají. Teplo stoupající z nitra planety uvolňuje energii pro pohyb plynu v atmosféře Saturnu.

Při ukončení mise bude ekologicky kosmická sonda Cassini v roce 2017 navedena do nitra severní polokoule Saturnu. Kdyby však hypoteticky měla opustit sluneční soustavu, jakou by musela mít rychlost?

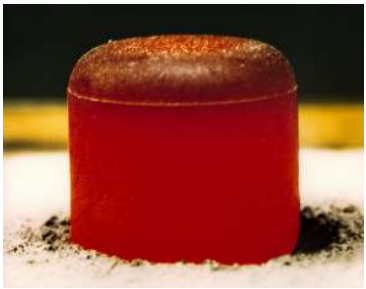
Úloha 16. Stanovte únikovou rychlost ze sluneční soustavy tělesa startujícího z oběžné dráhy Saturnu. Jeho vzdálenost od Slunce je $1{,}43 \cdot 10^{12}$ m.

Řešení. Úniková rychlost je rovna

$$v = \sqrt{2G\frac{M_{\mathrm{Sl}}}{r_{\mathrm{SlS}}}} = 13{,}8\,\mathrm{km \cdot s^{-1}}.$$

Úloha 17. Kosmická sonda Cassini (obr. 13), se pohybovala ve větších vzdálenostech od Slunce, tudíž energie získávaná solárními panely byla nedostatečná, protože hustota zářivého toku od Slunce je u Saturnu, jak jsme propočítali v předchozím textu, příliš nízká. Proto zdrojem energie o celkovém výkonu 885 W kosmické sondy byly tři radioizotopové články RTG, tableta oxidu plutoničitého PuO_2 (obr. 14). V nich bylo využíváno rozpadu plutonia $^{238}_{94}\mathrm{Pu}$, které produkuje částice α se značnou kinetickou energií, která se přeměňuje na tepelnou energii. Následný převod na elektrickou energii se uskutečňuje bez pohyblivých částí, prostřednictvím termočlánků založených na rozdílu teplot radioaktivní látky izolované uvnitř pouzdra a vnějšího chladiče. Určete nezbytné množství plutonia k zabezpečení uvedeného výkonu, průměrná účinnost je přibližně 5 %. Předpokládaná doba využitelnosti tohoto zdroje energie je nejméně 15 roků, po dobu hlavních úkolů mise Cassini.

Obr. 13



Obr. 14

Řešení. Celkovou uvolněnou energii E při reakci

$$^{238}_{94}\mathrm{Pu} \rightarrow {}^{234}_{92}\mathrm{U} + {}^{4}_{2}\mathrm{He} + E$$

stanovíme z tabulkových hodnot vazebných energií [10]

$$E = 5\,593\,\mathrm{keV} = 8{,}949 \cdot 10^{-13}\,\mathrm{J}.$$

Nezbytné množství paliva určíme následující úvahou. Pro zabezpečení celkového výkonu všech tří článků je zapotřebí $\frac{885}{8{,}95 \cdot 10^{-13}} = 9{,}9 \cdot 10^{14}$ atomů plutonia na jednu sekundu při 100 % účinnosti. Vzhledem k zadané reálné 5 % účinnosti potřebujeme 20krát větší počet atomů, tudíž $1{,}98 \cdot 10^{16}$ atomů plutonia. Jeden atom plutonia $^{238}_{94}\mathrm{Pu}$ má hmotnost $3{,}95 \cdot 10^{-25}$ kg. Celkem je zapotřebí na jednu sekundu $7{,}8 \cdot 10^{-9}$ kg, na 15 roků 3,7 kg paliva, za zjednodušujícího modelového předpokladu neklesající aktivity zářiče. Ve skutečnosti kosmická sonda Cassini nesla zhruba desetinásobně větší množství paliva ≈ 40 kg, neboť použité plutonium nebylo zcela čisté, jeho koncentrace dosahovala maximálně zhruba 70 %, aktivita zářiče s časem klesala, zdroj elektrické energie ztrácel ročně 0,8 % kapacity atd.

Článek naznačil možnosti, jak prostřednictvím motivace „transformovat fyzikální podstatu krásy“ do výuky fyziky. Jeho cílem bylo seznámení žáků a učitelů s vybranými projevy fyzikálních zákonitostí na Saturnu, jeho soustavě prstenců a měsíců. Je na učiteli, které z uvedených úloh si vybere a následně ve výuce použije.

Literatura

[1] *Maxwell, J. C.*: On the stability of the Motion of Saturn´s Rings. Macmillan and Company, Cambridge and London, 1859.

[2] *Keeler, J. E.*: A Spectroscopic Proof of the Meteorit Constitution of Saturn's Rings. The Astrophysical Journal, roč. 1 (1895), s. 416–427.

[3] *Herschel, W.*: Account of the Discovery of a Sixth and Seventh of the Planet Saturn. Phil. Trans. Royal Society of London, roč. 80 (1790), s. 1–20.

[4] *Unsöld, A., Baschek, B.*: The New Cosmos. Springer-Verlag, Berlin, Heidelberg, 2002.

[5] *Bartlett, A. A, Hord, Ch. W.*: The slingshot effect:explanation and analogies. The Physics Teacher, roč. 23 (1985), č. 8, s. 466–473.

[6] *Jones, J. B.*: How does the slingshot effect work to change the orbit of a spacecraft. Scientific American, 2005, s. 1136.

[7] *Huygens, Ch.*: De Saturni luna observatio nova. Hague, 1656.

[8] *Kuiper, G.*: Titan: A Satellite With An Atmoshere. The Astrophysical Journal, roč. 100 (1944), s. 378–383.

[9] *Dermott, S., Sagan, C.*: Tidal effects of disconnected hydrocarbon seas on Titan. Nature, roč. 374 (1994), 238–240.

[10] Ernest Orlando Lawrence and Berkeley National Laboratory: http://ie.lbl.gov/toi.html

Úlohy z termiky pro fyzikální olympioniky (2)

PAVEL KABRHEL – IVO VOLF

ÚK FO, Univerzita Hradec Králové

Na jedné straně se často hovoří o tom, že výuka fyziky je příliš teoretická, málo navazující na reálný život našich žáků i jejich rodičů a má zanedbatelný vztah k životnímu stylu a dalším předmětům přírodovědného a technického zaměření. Problematika zdrojů tepla, o níž se v dřívějších učebnicích autoři vždycky zmiňovali, jakoby z dnešních učebních programů vypadla – na základním stupni vzdělání proto, že je údajně náročná na matematické přístupy, a do učiva středoškolského se časově a rozsahem nevejde. Přesto se domníváme, že žáci právě v tomto tematickém celku se dostanou do reálných situací, které je obklopují, a tím se současně těsně propojují jejich teoretické vědomosti a praktické aplikace.

Jako zdroje tepla slouží jednak produkty přírodní aktivity – sluneční záření, voda z gejzírů, sopečná činnost, paliva aj, jednak výsledky lidské činnosti – rychlovarná konvice, boiler, vařič, tělesa ústředního topení aj. Paliva, jako zdroj tepla, mohou být pevná (uhlí, dřevo, brikety, rašelina), kapalná (petrolej, benzin, nafta, topné oleje) i plynná (metan, vodík, zemní plyn). U paliv je důležitou charakteristikou spalné teplo nebo výhřevnost H. Pod pojmem výhřevnost zvažujeme teplo, které je zmenšeno o hodnotu na odstranění vodní páry z paliva. Různá paliva se tedy liší především výhřevností: např. výhřevnost hnědého uhlí je 11 až 16 MJ/kg, benzinu 46 MJ/kg (asi 33 MJ/l). Protože potřebujeme mít srovnávací pohled na pevná paliva různého původu, zavádíme někdy tzv. měrné palivo, které má výhřevnost asi 30 kJ/kg. Horší palivo má menší výhřevnost, a tedy tepelné zařízení bude mít větší spotřebu tohoto paliva. Dále je třeba znát tepelnou účinnost zařízení, v němž se palivo spaluje (například u elektráren budeme počítat s celkovou účinností 36 % až 45 %).

Problém 1: Jaká je spotřeba měrného paliva?

Různé tepelné elektrárny mohou být porovnávány podle hmotnosti měrného paliva, které by bylo nutno spotřebovat při zajištění 1 kWh elektrické práce. Určete spotřebu měrného paliva.

Poznámky k vytvoření modelové situace. Výhřevnost měrného paliva je $H = 30$ MJ/kg, dále zvolíme tepelnou účinnost na dolní hranici uvedeného intervalu, tj. 36 %. Ke stanovení hmotnosti měrného paliva nutného k získání 1 kWh elektrické práce použijeme rovnice pro určení tepla

$$Q = mH\eta.$$

Řešení. Z rovnosti $Q = mH\eta = 1{,}0\,\text{kWh} = 3{,}6 \cdot 10^6\,\text{J}$ stanovíme hmotnost spotřebovaného paliva, $m = 333\,\text{g} = 0{,}333\,\text{kg}$. Je jasné, že při použití horšího paliva, např. hnědého uhlí o výhřevnosti 12 MJ/kg nám při stejné účinnosti vyjde spotřeba asi 830 g/kWh = 0,830 kg/kWh. Naopak s lepší technologií spalování a lepším ohřevem vody můžeme zvýšit účinnost na 45 % a při užití hnědého uhlí nám vychází hodnota asi 0,670 kg/kWh.

Problém 2: Denní a roční spotřeba uhlí v české tepelné elektrárně.

Instalovaný výkon tepelná elektrárny v Chvaleticích je 800 MW a využívá méně kvalitní uhlí o výhřevnosti 12 MJ/kg. Kdyby elektrárna „běžela na plný výkon“ po celý den, stanovte jednodenní, týdenní a roční spotřebu uhlí, za předpokladu že celková účinnost elektrárny je 36 %.

Poznámky k vytvoření modelové situace. Nejprve si všimneme podmíněného tvrzení „kdyby elektrárna běžela na plný výkon“. Poté určíme dobu činnosti elektrárny za 1 rok, tedy $t = 365{,}25 \cdot 24\,\text{h} = 8\,766\,\text{h}$. Odtud stanovíme celkovou práci, kterou elektrárna poskytla za rok, a potom stanovíme hledanou spotřebu uhlí o dané výhřevnosti. Jako reálnou účinnost vezmeme 36 %. Stejně provedeme výpočet pro jeden den a jeden týden.

Řešení. Při spálení 1,0 kg uhlí o výhřevnosti 12 MJ/kg získáme do elektrické sítě práci hodnoty 4,32 MJ = 1,2 kWh. Za 1 den dodá chvaletická elektrárna práci $800\,\text{MJ} \cdot 24\,\text{h} = 19\,200\,\text{MWh}$. Spotřebu uhlí stanovíme

$$m = \frac{19\,200 \cdot 10^3\,\text{kWh}}{1{,}2\,\text{kWh}} \cdot 1\,\text{kg} = 16 \cdot 10^6\,\text{kg} = 16\,000\,\text{t}.$$

Při nákladu 40 t uhlí ve vagónu to představuje spotřebu 400 vagónů uhlí denně, týdně 2 800 vagónů a 146 100 vagónů za rok, proto se také přistoupilo k lodní přepravě uhlí do chvaletické elektrárny. Plyne z toho také, že je lepší stavět tepelné elektrárny v blízkosti povrchových dolů, kde se těží hnědé uhlí, protože transport elektřiny je oproti transportu uhlí snazší, ekologičtější a také levnější.

Problém 3: Roční spotřeba tepelné elektrárny.

Stanovte denní, týdenní a roční spotřebu hnědého uhlí polské tepelné elektrárny Bełchatów, jejíž instalovaný výkon je 5 354 MW, včetně nového energetického bloku o výkonu 858 MW, který byl uveden do provozu v roce 2011. Charakteristický pohled na elektrárnu vidíme na obr. 1.

Obr. 1: Tepelná elektrárna Bełchatów, jeden z největších producentů oxidu uhličitého ve střední Evropě

Poznámky k vytvoření modelové situace. Tepelná elektrárna je postavena přímo v blízkosti hnědouhelného dolu, proto pro výpočty zvolíme stejné parametry (výhřevnost paliva, celková účinnost) jako v minulé úloze. Když vyhledáme informace na Wikipedii, získáme další údaje – roční výroba elektřiny představuje asi 27,5 TWh a do atmosféry chrlí elektrárna 1,09 kg oxidu uhličitého ovšem při výrobě 1 kWh.

Řešení. Denní výroba elektřiny je $5\,354\,\mathrm{MW} \cdot 24\,\mathrm{h} = 128\,496\,\mathrm{MWh}$, což představuje spotřebu přibližně 107 000 tun hnědého uhlí denně neboli asi 2 680 vagónů. Současně se však do ovzduší denně dostane asi 140 000 tun oxidu uhličitého. Za týden to představuje asi 18 740 vagónů uhlí a produkci přes 980 000 tun oxidu uhličitého. Roční spotřeba uhlí potom představuje hodnotu přibližně 980 000 vagónů hnědého uhlí, ale také produkci více než 51,1 miliónu tun oxidu uhličitého. Podívejme se však na realitu – skutečná roční produkce elektřiny je $27{,}5\,\mathrm{TWh} = t \cdot 5\,354\,\mathrm{MW}$, odtud doba činnosti tepelné elektrárny „na plný výkon“ je pouze 5 136 h ročně, denně to je asi 14 h, tedy 58,6 %. Uvedené vypočtené hodnoty musíme tedy násobit

přibližně 0,6, takže dostaneme pro roční údaje spotřebu asi 588 000 vagónů uhlí a přes 30,6 miliónů tun oxidu uhličitého.

Problém 4: Kolik pevného paliva ušetří denně (ročně) jaderná elektrárna?

Jaderná elektrárna získává teplo ochlazováním reaktorů, které se pak využívá k ohřevu vody a ke vzniku přehřáté páry. Jaderná elektrárna Temelín má instalovaný výkon $2 \times 1\,000$ MW a koeficient využití asi 79 %, jaderná elektrárna Dukovany má instalovaný výkon 1 877 MW a koeficient využití asi 85 %. Pomocí spotřebovaného tzv. měrného paliva stanovte spotřebu tepelné elektrárny, která by nahradila obě jaderné elektrárny, a vyjádřete výsledek i spotřebou hnědého uhlí o výhřevnosti 12 MJ/kg.

Obr. 2: Jaderná elektrárna Temelín

Poznámky k vytvoření modelové situace. Tento problém můžeme řešit pomocí kombinace úloh předcházejících. Koeficient využití nám stanoví, kolik elektrické práce lze získat během roční činnosti elektráren. Určíme také, kolik oxidu uhličitého by se při stejné produkci do ovzduší dostalo z tepelných elektráren o stejném výkonu. Podle informací na internetu můžeme zjistit, že v elektrárně Dukovany se vyrobilo v roce 2011 celkem 14 369 GWh, v Temelíně 13 914 GWh.

Řešení. Ověříme nejprve reálnost koeficientu využití obou elektráren. Kdyby elektrárny měly aktivní produkci po dobu plného roku, tedy 365,25 dne po 24 h, tj. 8 766 h, potom při výkonu 2 000 MW v Temelíně by museli produkovat celkem 17 532 GWh, koeficient využití je $13\,914/17\,532 \doteq 0{,}79$, pro Dukovany vycházejí hodnoty 16 454 GWh, koeficient přibližně 0,87, což je poněkud více než uváděná hodnota. Celková produkce elektřiny v obou

dvou jaderných elektrárnách představuje asi 28 280 GWh $\doteq$ 28,3 TWh. Na základě řešení problému 1 jsme zjistili, že na produkci 1 kWh je třeba 0,333 kg měrného paliva. Protože celková roční produkce obou jaderných elektráren je 28,3 TWh = $28{,}3 \cdot 10^9$ kWh, byla by spotřeba měrného paliva v tepelné elektrárně asi $9{,}4 \cdot 10^9$ kg, neboli 9,4 miliónů tun. Pokud jde o produkci oxidu uhličitého, v tepelných elektrárnách připadá na 1 kWh asi 1,09 kg CO_2. Produkce 28,3 TWh v jaderných elektrárnách představuje skutečnost, že se do ovzduší na rozdíl od tepelných elektráren nedostane za rok skoro 31 milionů tun tohoto tzv. skleníkového plynu, z něhož mají ekologové stále větší hrůzu.

Problém 5: Spotřeba paliva u osobního automobilu.

Spotřeba paliva se udává pomocí objemu benzínu (nafty), který by motor vozidla spotřeboval při ujetí vzdálenosti 100 km, tedy například 8 litrů/100 km. Zjistěte, jak se mění spotřeba paliva u osobního automobilu, který jede po dálnici stálou rychlostí mezi 90 km/h a 130 km/h.

Poznámky k vytvoření modelové situace. Pohyb osobního automobilu jako reálného silničního vozidla je velmi složitý, a proto musíme tento problém řešit v modelové situaci. Budeme předpokládat, že automobil pojede po určitou dobu stálou rychlostí v, při čemž na něj působí stálá tahová síla, překonávající síly odporové (odpor vzduchu a valivý odpor). Po spotřebě objemu V paliva získáme teplo $Q = VH$, kde H je výhřevnost udávaná v MJ/l. Toto teplo je využito k mechanické práci pouze částečně (závisí na účinnosti η) a automobil vykoná práci $W = Fs$, kde F je celková síla nutná k udržení rovnoměrného pohybu. Příslušné hodnoty najdeme ve fyzikálně-technických tabulkách, případně na internetu.

Řešení. Najdeme nejprve potřebné hodnoty: $H = 46$ MJ/kg $= 34$ MJ/l, velikost síly valivého odporu je $F = \xi mg/r$, ξ pro pohyb pryžové pneumatiky po asfaltu je 0,001 6 m, hmotnost automobilu vezmeme 1 200 kg, velikost tíhového zrychlení 9,80 m/s^2, poloměr pneumatiky asi 0,30 m. Odtud velikost síly valivého odporu je přibližně 63 N a nezávisí dle výše uvedeného vztahu na rychlosti pohybu vozidla (což bude zase jeden z předpokladů v našem modelu). Síla spojená s překonáváním odporu prostředí se stanoví $F = \frac{1}{2}CS\varrho v^2$, kde tvarový součinitel C zvolíme podle tabulárních hodnot 0,36, obsah příčného kolmého čelního řezu S určíme podle lineárních rozměrů vozidla (šířka 1,6 m, výška 1,5 m) asi 2,4 m^2, hustotu vzduchu $\varrho = 1{,}25$ kg/m^3, takže vztah pro velikost odporové síly napíšeme $F = kv^2$, kde $k = \frac{1}{2}CS\varrho$, $k = 0{,}54\,\mathrm{N} \cdot \mathrm{s}^2/\mathrm{m}^2$. Velikost odporové síly bude

potom závislá jen na rychlosti pohybu vozidla oproti nehybnému vzduchu, neboli závisející na vzájemné rychlosti pohybu vozidla a proudění vzduchu ve směru či proti směru pohybu automobilu. Jednotlivé rychlosti zvolíme 25 m/s a 36 m/s. Síla, jíž působí vzduch na automobil, je potom rovna 338 N a 700 N, síly nutné k udržení pohybu vozidla stálou rychlostí jsou přibližně 400 N a 763 N. Mechanická práce získaná motorem při účinnosti 22 % na základě spotřeby objemu V paliva je $W = \eta VH$, ale současně $W = Fs$, kde za dráhu, po níž by stálá síla působila, zvolíme 100 km. Vykonaná mechanická práce bude v krajních případech rovna 40 MJ a 76,3 MJ. Musíme zajistit teplo 182 MJ, 347 MJ, čemuž odpovídá spotřeba 5,4 litru/100 km, při větší rychlosti 10,2 litru/100 km. Zatímco rychlost se zvýšila 1,44 krát (a doba nutná k dosažení určité vzdálenosti se 1,44 krát snížila), spotřeba paliva se zvýšila 1,9 krát. Lze říci, že rychlost se zvýšila o necelou polovinu (a doba jízdy se zkrátila asi o třetinu), spotřeba se však zvýšila na dvojnásobek. Majitel vozidla pak musí svou volbu přizpůsobit okolnostem, zda mu zvýšené náklady stojí za to.

Problém 6: Jak lze snížit spotřebu paliva při jízdě automobilu?

Majitel vozidla se snaží zmenšit ekonomické nároky na jeho provoz. Vymezte podmínky a stanovte, jak se mu to může podařit. Prostudujte si řešení Problému 5 a uvažte, které hodnoty se dají jednoduchým způsobem snížit.

Poznámky k vytvoření modelové situace. Snížit hodnotu síly, překonávající valivý odpor, je možno volbou jiné pneumatiky, případně jiné vozovky (obojí je málo reálné), dále zvětšením průměru pneumatiky (což naruší design vozidla a prodraží výrobu) a nakonec zmenšením hmotnosti vozidla, což má zase určitá omezení, spojená s jízdními vlastnostmi. Nebudeme se proto o snížení této síly snažit. Ponecháme-li obě krajní rychlosti stejné, můžeme snižovat jen hodnotu $k = \frac{1}{2}CS\varrho$, tedy zmenšovat obsah příčného řezu (zúžit vozidlo či zmenšit jeho výšku) nebo snížit hodnotu odporového součinitele – jsou již známa vozidla, u kterých je $C = 0{,}29$, tedy o 20 % nižší, což vede ke snížení odporové síly. Další cestou je zvýšení mechanické i tepelné účinnosti vozidla z 22 % na 25 %, tedy zvýšení tahové síly a užitečné mechanické práce, která se využije pro pohon vozidla.

Řešení. Ponecháme tedy sílu valivého odporu na hodnotě 63 N, odporová síla způsobená vzduchem při pohybu vozidla se sníží o 20 %, tedy na hodnoty 270 N, 560 N, celková síla nutná pro udržení pohybu vozidla bude 333 N a 623 N, práce při jízdě po dráze 100 km nám vychází 33,3 MJ

(snížení na 0,83 původní hodnoty), 62,3 MJ (snížení na 0,82 původní hodnoty). Zvýšení účinnosti motoru vozidla z 22 % na 25 % znamená snížení spotřeby na hodnotu 0,88 původní hodnoty. Budeme-li počítat s průměrnou hodnotou 82,5 %, vyjde nám 72,6 %, a tedy celkové snížení spotřeby paliva vychází pro nižší hodnotu rychlosti asi 3,9 litru na 100 km, pro větší hodnotu rychlosti 7,4 litru/100 km.

Problém 7: Proč je v České republice tolik tepelných elektráren?

V České republice se vyskytují elektrárny různého druhu – tepelné, vodní, větrné, jaderné atd., které mají různý vliv na znečišťování životního prostředí. Proč nevystačíme třeba s vodními elektrárnami? Odhadněte, jak ekologicky nevýhodná je například nepříliš výkonná elektrárna v Opatovicích nad Labem, jejíž výkon na výstupu je 363 MW a ročně vyrobí 2 116 GWh, poté určete parametry hydroelektrárny s objemovým tokem 50 m^3/s při účinnosti 80 %, která by ji mohla nahradit.

Obr. 3: Tepelná elektrárna Opatovice nad Labem

Poznámky k vytvoření modelové situace. Nejprve stanovíme střední dobu, po kterou vyrábí elektrárna ročně na plný výkon:

$$\frac{2\,116\,000\,\text{MWh}}{363\,\text{MW}} = 5\,830\,\text{h},$$

tedy využitelnost elektrárny na plný výkon je 66,5 %. Protože má elektrárna Opatovice oproti Chvaleticím instalovaný výkon asi poloviční, bude

asi také spotřeba uhlí i zatížení ovzduší poloviční. Jestliže elektrická práce této elektrárny představuje 2 116 GWh, potom elektrárna dosahuje středního dlouhodobého výkonu jen 241 MW.

Řešení. Jestliže elektrická práce této elektrárny představuje 2 116 GWh, pak tato elektrárna dosahuje středního dlouhodobého výkonu jen 241 MW. Při objemovém toku 50 m^3/s je hmotnostní tok 50 000 kg/s, poté výkon hydroelektrárny o výškovém rozdílu jen 1 m bude

$$P = 50\,000 \cdot 9{,}8 \cdot 0{,}8 \text{ W},$$

tedy pouze 392 kW. K dosažení příslušného výkonu by musela být postavena přehradní hráz o výšce $h = 615$ m. Takto vysokých přehradních hrází nelze v horní části našich řek dosáhnout.

Literatura

[1] Výhřevnost. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://http://cs.wikipedia.org/wiki/Výhřevnost

[2] Měrné palivo. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://cs.wikipedia.org/wiki/Měrné_palivo

[3] Elektrárna Chvaletice. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://cs.wikipedia.org/wiki/Elektrárna_Chvaletice

[4] Elektrownia Bełchatów. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://pl.wikipedia.org/wiki/Elektrownia_Bełchatów

[5] Jaderná elektrárna Temelín. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://cs.wikipedia.org/wiki/Jaderná_elektrárna_Temelín

[6] Jaderná elektrárna Dukovany. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://cs.wikipedia.org/wiki/Jaderná_elektrárna_Dukovany

[7] Elektrárna Opatovice nad Labem. In: Wikipedia: the free encyclopedia [online]. Dostupné z: http://cs.wikipedia.org/wiki/Elektrárna_Opatovice_nad_Labem

Zdroje vyobrazení

Obr. 1: Belchatow power station by Petr Štefek
http://commons.wikimedia.org/wiki/File:20051029_Belchatow_power_station.jpg

Obr. 2: Jaderná elektrárna Temelín by Japo
http://commons.wikimedia.org/wiki/File:JETE2.JPG

Obr. 3: Tepelná elektrárna Opatovice nad Labem by Vojtech.dostal
http://commons.wikimedia.org/wiki/File:Opatovice_nad_Labem_power_plant_Czech_republic.jpg?uselang=cs

Ako funguje hard disk

PETER KOLLÁR – MARIÁN KIREŠ

Prírodovedecká fakulta UPJŠ, Košice, Slovensko

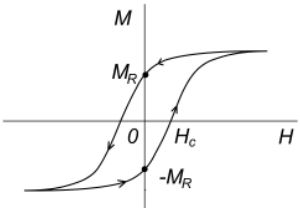
Digitálne technológie nadchýnajú takmer každého z nás svojimi možnosťami, používateľským komfortom, dostupnosťou a neustále napredujúcou technickou vyspelosťou. Ich funkčnosť je založená na fyzikálnych princípoch, ktoré ostávajú pred bežným používateľom častokrát neodkryté. Ako rozpoznáva display pohyb prstov? Ako akumulátor uskladňuje elektrickú energiu potrebnú pre napájanie daného zariadenia? Ako si pamäťové média uchovávajú zaznamenané informácie?

V snahe zvýšiť záujem o fyzikálne vzdelávanie sa ako jedna z ciest ukazuje prezentácia a priblíženie základných fyzikálnych princípov zariadení, pričom jedným z nich je aj hard disk. Pripravili sme názornú ukážku princípu záznamu, snímania a uchovávania digitálnej informácie pomocou magnetického záznamu. Experiment je možné realizovať ako interaktívnu demonštráciu riadenú vyučujúcim [1], alebo ako žiacke riadené bádanie [2].

Magnetizmus v hard disku

Hard diskom nazývame zariadenie na zaznamenávanie a uchovávanie dát, ktoré v stave uchovávania informácie nepotrebuje prijímať energiu zvonku. Princíp zaznamenávania dát je založený na existencii dlhodobo stabilného remanentného stavu magnetických materiálov. História hard disku sa začala písať v roku 1956 keď prvý hard disk bol vyvinutý vo firme IBM mal kapacitu 3,75 MB (megabajtov), ktorá dosahuje v dnes už bežných hard diskoch 1 TB (terabajt). V hard diskoch sa zaznamenáva informácia v binárnom kóde, teda zariadenie si pamätá len sled logických núl a jednotiek.

Významnou vlastnosťou fero- a ferimagnetických materiálov je skutočnosť, že ich magnetizácia M nie je jednoznačnou funkciou magnetického poľa, ale závisí od intenzity magnetického poľa podľa funkcie nazývanej hysterézna slučka (obr. 1).



Obr. 1: Hysterézna slučka

Po aplikovaní relatívne intenzívneho magnetického poľa a jeho následnom vypnutí si látka zachová remanentnú magnetizáciu M_{R}, teda stane

sa zdrojom trvalého magnetického poľa (stane sa permanentným magnetom). Ak bola látka vystavená účinku magnetického poľa v opačnom smere, tak po jeho vypnutí ostane zmagnetovaná na hodnotu magnetizácie M_{R}. Týmto dvom z časového hľadiska stabilným stavom, môžeme priradiť v binárnej sústave hodnoty 0 alebo 1 napr. tak, že remanentnej magnetizácii M_{R} priradíme hodnotu 1 a $-M_{\mathrm{R}}$ hodnotu 0.

Z uvedeného vyplýva, že magnetický materiál sa dokáže správať ako pamäťové médium. Veličina H_{c} sa nazýva koercivita a predstavuje odolnosť materiálu voči strate informácie pod vplyvom nežiaduceho magnetického poľa, ktorá má v skutočných hard diskoch (obr. 2) dosahovať primerane vysoké hodnoty.

Obr. 2: Pohľad na hard disk diskovej jednotky

Z hľadiska princípu činností hard disku je potrebné vedieť, že samotný magnetický materiál je v tenučkej vrstve nanesený na magneticky neaktívnej (najčastejšie hliníkovej alebo sklenenej podložke). Magneticky aktívna vrstva je ďalej pokrytá ochrannou vrstvou uhlíka.

Magnetický materiál (obvykle oxidy železa, alebo kobaltu hrúbky 10 nm až 20 nm) vykazuje anizotropiu, vďaka ktorej ľahký smer magnetizácie je kolmý na smer povrchu kruhovej platne. Zmenu stavu magnetického materiálu možno vykonať magnetickým poľom, ktorého zdrojom je maličká cievka tesne nad povrchom feromagnetika (obr. 3).

Obr. 3: Pohľad záznamovú a čítaciu hlavu hard diskovej jednotky

Čítanie informácie sa vykonáva pomocou hlavy v ktorej sa nachádza prvok, ktorého odpor je citlivý na magnetické pole na základe javu magnetorezistencie.

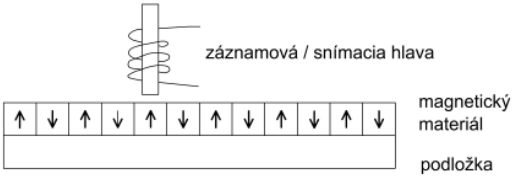
Záznam informácie v binárnom kóde

Všetky informácie sú na hard disku zaznamenané v binárnom kóde. Tab. 1 ilustruje spôsob zápisu čísel dekadickej sústavy 0 až 15 pomocou štyroch údajov v binárnej sústave.

číslo v binárnej sústave				číslo v dekadickej sústave		číslo v binárnej sústave				číslo v dekadickej sústave	
2^3	2^2	2^1	2^0	10^1	10^0	2^3	2^2	2^1	2^0	10^1	10^0
0	0	0	0	0	0	1	0	0	0	0	8
0	0	0	1	0	1	1	0	0	1	0	9
0	0	1	0	0	2	1	0	1	0	1	0
0	0	1	1	0	3	1	0	1	1	1	1
0	1	0	0	0	4	1	1	0	0	1	2
0	1	0	1	0	5	1	1	0	1	1	3
0	1	1	0	0	6	1	1	1	0	1	4
0	1	1	1	0	7	1	1	1	1	1	5

Tab. 1: Čísla v binárnej a dekadickej sústave.

Údaje v binárnej sústave sú zaznamenané pomocou malých magnetických buniek nanometrických rozmerov v lokalitách povrchu disku (obr. 4). Každá z týchto buniek môže byť priečne zmagnetovaná buď nahor (hodnota 1) alebo nadol (hodnota 0).

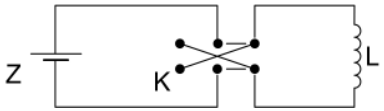


Obr. 4: Priečny záznam informácie

Demonštrujeme magnetický záznam

Záznam binárnej informácie môžeme demonštrovať modelom magnetickej vrstvy hard disku vytvoreným sústavou štyroch klincov. Klince zatlčené do drevenej doštičky predstavujú štyri pamäťové bunky s rádom 2^3,

2^2, 2^1, 2^0 nesúce informáciu o čísle v binárnej sústave. Vzdialenosť klincov je volená tak, aby sme na jednotlivé klince ľahko nasunuli cievku (napr. zo školského rozkladného transformátora). Klince sú zhotovené s ocele, ktorá z magnetického hľadiska predstavuje magneticky materiál s nie príliš vysokou koercivitou, takže ho bude možné premagnetovať pomocou relatívne nízkeho magnetického poľa. Pre nastavenie remanentného stavu pamäťovej bunky – klinca – použijeme cievku s 900 závitmi napájanú zo zdroja jednosmerného napätia 30 V/10 A cez komutátor (obr. 5).



Obr. 5: Schéma zapojenia napájania magnetizačnej cievky

Pri zápise informácie cievku nasunieme na klinec a na krátku chvíľu zapneme komutátor do jednej z krajných polôh. Komutátorom zopnutý príslušný smer prúdu cez cievku, vytvorí magnetické pole želanej orientácie, zodpovedajúce napr. stavu 1. Po vypnutí magnetického poľa pamäťová bunka ostane v remanentnom stave odpovedajúcom číslu 1.

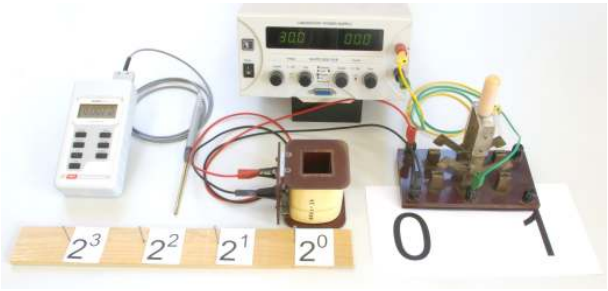
Po vypnutí komutátora cievku postupne presunieme na ďalšie pamäťové bunky (klince) a zapíšeme želanú informáciu. Ak je komutátor v druhej krajnej polohe, zmenili sme smer prúdu v cievke a tým aj smer magnetického poľa produkovaného cievkou. Magnetizáciou klinca pri tejto polohe komutátora dosiahneme stav 0.

Dbáme na to, aby sme počas experimentu nemenili zvislú orientáciu cievky.

Informáciu zapísanú v pamäťových bunkách prečítame teslametrom s axiálnou sondou, ktorú postupne pritlačíme na hlavičky jednotlivých klincov. Kladná hodnota remanentnej magnetizácie odpovedá číslu 1 a záporná číslu 0. Na absolútnej hodnote magnetizácie pri digitálnom zázname a snímaní informácie nezáleží. V školskej praxi je vhodné použiť aj sondy magnetického poľa pripojené na niektorý zo systémov pre počítačom podporované meranie (CoachLab II, ISES, Vernier a pod.). Pohľad na nami zostrojenú experimentálnu zostavu je na obr. 6.

Na overenie pochopenia fyzikálneho princípu uvedeného zariadenia je vhodné pripraviť aj ďalšiu drevenú doštičku s klincami, ktoré boli vopred zmagnetované pre zápis vybraného čísla. Úlohou študentov je ozrejmiť experimentálnu zostavu, princíp jej činnosti a meraním určiť hodnotu za-

písaného čísla. O trvácnosti zápisu sa ľahko presvedčíme na niektorej z nasledujúcich hodín premeraním magnetizácie klincov.



Obr. 6: Pohľad na experimentálnu zostavu

Záver

Máme v praxi overené, že opísaný demonštračný experiment predvádzaný učiteľom je možné viesť ako interaktívnu demonštráciu využívajúc prvotné poznatky študentov gymnázia z magnetizmu, pričom postačuje úroveň informácií ako je uvedené v časti 1. Pri práci viacerých skupín postačuje vybavenie: zdroj napätia, komutátor, cievka doska s klincami a prepojovacie vodiče. Študenti v skupinách po troch zostavia experimentálnu aparatúru, prediskutujú navzájom jej princíp a zmagnetizujú klince na jednej doske. Použitím magnetickej sondy (postupne koluje medzi skupinami) v záverečnej fáze cvičenia overia správnosť svojho postupu a prezentujú svoj magnetický záznam spolužiakom.

Poďakovanie

Príspevok vznikol pri riešení APVV projektov zameraných na popularizáciu vedy: APVV LPP-0093-09 Nanomateriály pre environmentálne aplikácie: budúcnosť je v rukách študentov a APVV LPP-0223-09 Veda na scéne Slovensko.

Literatura

[1] *Wenning, C.*: Levels of Inquiry: Hierarchies of pedagogical practices and inquiry processes. Journal of Physics Teacher Education Online, roč. 2 (2005), č. 3, s. 3–11.

[2] Projekt ESTABLISH. www.establish-fp7.eu.

INFORMATIKA

Téměř dokonalá šifra

PETR VOBORNÍK

Přírodovědecká fakulta, Univerzita Hradec Králové

Princip dokonalé šifry je znám již téměř celé století. Podmínky, které musí být při jejím používání dodrženy, však praktické nasazení stále komplikují. Šifra je tedy vhodná tam, kde se vyžaduje extrémně vysoké utajení a kde nevadí mimořádně vysoké náklady spojené s výrobou a distribucí klíčů. [1]

V tomto článku shrneme princip dokonalé šifry a na jeho základě se s využitím moderních hashovacích algoritmů pokusíme navrhnout jednu z možných modifikací práce s klíči tak, aby byly odstraněny zásadní faktory znemožňující praktické používání šifry.

Základní pojmy

V následujícím textu budou používány známé výrazy, které ovšem mohou mít v různých kontextech různé významy. Upřesněme si tedy, co je pod jejich označením míněno zde. Ostatní pojmy budou vysvětleny přímo v článku.

Data – zdrojová data, která jsou třeba ochránit šifrováním před jejich přečtením a zneužitím třetími osobami.

Zpráva – je soubor informací zasílaných mezi dvěma komunikujícími stranami. Skládá se z dat (zašifrovaných) a dalších údajů, jako jsou identifikátor odesílatele, určení příjemce, datum a čas odeslání, apod.

Klíč – tajná sada dat, s jejichž pomocí budou výpočetní operací zdrojová data šifrována a následně dešifrována.

Heslo – slovo, fráze nebo kombinace znaků, které umožňuje zašifrovaná data dešifrovat a naopak. Tzn. heslo se buď použije přímo jako **klíč**, nebo se klíč vygeneruje na jeho základě, což bude i případ tohoto článku.

Dokonalá šifra

Roku 1917 *Američan Gilbert Sandford Vernam* (1890–1960) zkonstruoval zajímavý šifrovací systém. Ten vycházel z Vigenerovy šifry z roku 1586 [2], ovšem obsahoval několik zásadních změn údajně inspirovaných německým kryptologem Hermannem z roku 1892 [3]. Systém byl založený na použití jednorázového náhodně vygenerovaného hesla, které má stejnou délku jako zpráva sama. Fakt, že je Vernamova šifra, zvaná též „one-time pad“ (jednorázová tabulka), absolutně bezpečným (neprolomitelným) šifrovacím systémem matematicky prokázal v roce 1949 *Claude Elwood Shannon* (1916–2001) [4]. Této dokonalé nerozluštitelnosti šifry lze dosáhnout ovšem pouze při dodržení tří přísných podmínek spolehlivosti:

1. Klíč musí být stejně dlouhý jako přenášená zpráva.
2. Klíč musí být dokonale náhodný.
3. Klíč nesmí být použit opakovaně. [5]

Jsou-li podmínky spolehlivosti dodrženy, je tato šifra zcela bezpečná proti jakémukoli pokusu o prolomení, včetně útoku hrubou silou. Není-li totiž znám správný klíč, neexistuje způsob proveditelný ani v libovolně dlouhém časovém horizontu, jak zprávu rozluštit. Je sice možné najít takový klíč, který by dokázal zašifrovaná data převést na srozumitelný text téže délky, ovšem takovýchto klíčů lze nalézt tolik, že tato data mohou v podstatě dávat smysl libovolný, přičemž nelze odhadnout, která z takovýchto zpráv byla tou odesílanou.

Vernam ve svém následném patentu [6] navrhl i jednoduchý přístroj, který pracoval již s 31 znaky – 26 písmen, mezera, znaky návrat vozíku (CR) a posun o řádek (LF) a signály „následují číslice“ a „následují písmena“, což pokrývalo 5 bitů, jež přístroj šifroval náhodným klíčem pomocí operace XOR.

Operace XOR

Logická operace exkluzivní disjunkce, v originále „exkluzive or“, zkráceně XOR se značí takto: $\oplus$. Výsledkem je 0, pokud jsou obě vstupní hodnoty shodné, a 1, jsou-li rozdílné (viz tab. 1).

$\mathtt{A} \oplus \mathtt{B} = \mathtt{C}$

A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

Tab. 1: Stavová tabulka hodnot operace XOR

XOR je komutativní operace, tj. nezáleží na pořadí jednotlivých hodnot s nimiž se operace XOR provádí.

$$(\mathtt{A} \oplus \mathtt{B} = \mathtt{C}) \Leftrightarrow (\mathtt{B} \oplus \mathtt{A} = \mathtt{C})$$

Poznámka: Místo operace XOR lze také použít funkci modulo 2 ze součtu obou hodnot:

$$(\mathtt{A} \oplus \mathtt{B} = \mathtt{C}) \Leftrightarrow ((\mathtt{A} + \mathtt{B}) \bmod 2 = \mathtt{C})$$

Z výsledku operace XOR lze následně další operací XOR s jednou z výchozích hodnot dopočítat tu druhou.

$$(\mathtt{A} \oplus \mathtt{B} = \mathtt{C}) \Leftrightarrow (\mathtt{C} \oplus \mathtt{A} = \mathtt{B}) \Leftrightarrow (\mathtt{C} \oplus \mathtt{B} = \mathtt{A})$$

Pokud tedy i-tý datový bit $\mathtt{D}_i$ zašifrujeme operací XOR s i-tým bitem klíče $\mathtt{K}_i$ do zašifrovaného znění $\mathtt{C}_i$, pak z $\mathtt{C}_i$ zpětně dešifrujeme výchozí datový bit $\mathtt{D}_i$ opětovným provedením operace XOR s i-tým bitem klíče $\mathtt{K}_i$.

$$\textit{Zašifrování: } \mathtt{D}_i \oplus \mathtt{K}_i = \mathtt{C}_i \qquad \textit{Dešifrování: } \mathtt{C}_i \oplus \mathtt{K}_i = \mathtt{D}_i$$

Je-li zároveň klíč náhodný, pak pravděpodobnost, že $\mathtt{K}_i = 0$, je stejná jako pravděpodobnost, že $\mathtt{K}_i = 1$, je rovna $1/2$ (tj. 2^{-1}), čili 50 %. Stejně tak je tomu i u zašifrované hodnoty $\mathtt{C}_i$. Není-li tedy znám klíč $\mathtt{K}_i$, je pravděpodobnost „uhodnutí“ správné hodnoty přesně poloviční. Pro celý znak skládající se z 8 bitů (1 byte) je pak za těchto okolností pravděpodobnost určení správného znaku již jen 2^{-8} (tj. $1/256$), čili cca 0,4 %.

Princip Vernamovy šifry

Těmto písmenům A až Z se přiřadila čísla 0 až 25 a pro i-tý znak utajovaných dat $\mathtt{D}_i$ s klíčem $\mathtt{K}_i$ (klíč se také skládal pouze ze znaků této abecedy) se znak šifrovaných dat $\mathtt{C}_i$ určil následujícím způsobem [2]:

$$\mathtt{C}_i = (\mathtt{D}_i + \mathtt{K}_i) \bmod 26$$

Dešifrování pak proběhlo opačnou operací:

$$\mathtt{D}_i = (26 + \mathtt{C}_i - \mathtt{K}_i) \bmod 26$$

Například slovo „AHOJ“ by se s použitím náhodného klíče „SMHZ“ šifrovalo jako je tomu v tab. 2.

	Znaky				Čísla			
Data	A	H	O	J	0	7	14	9
Klíč	S	M	H	Z	18	12	7	25
Zašifrovaná data	S	T	V	I	18	19	21	8
Dešifrovaná data	A	H	O	J	0	7	14	9

Tab. 2: Ukázka postupu šifrování znaků původní Vernamovou širou

Vylepšená verze této šifry pracuje s binární reprezentací dat. Jednotlivé bity dat převedených do binární podoby jsou šifrovány operací XOR s jednotlivými bity klíče. Výhodou byla možnost strojového zpracování této šifry. Vernam ve své době používal vlastní převodní tabulku pro znaky základní abecedy do binární formy, kterou místo hodnot 0 a 1 označoval znaky + a −. [6] V současnosti, kdy jsou data uchovávána a přenášena v elektronické formě bitů standardně, je situace pro podobný styl šifrování ještě daleko jednodušší.

Stejná data jako v předchozím případě by při binárním kódování (pro převod znaků na bity je použita standardní ASCII tabulka znaků) vypadala tak, jak ukazuje tab. 3.

	Znaky				Bity			
Data	A	H	O	J	01000001	01001000	01001111	01001010
Klíč	S	M	H	Z	01010011	01001101	01001000	01011100
Zašifrovaná data	18	5	7	22	00010010	00000101	00000111	00010110
Dešifrovaná data	A	H	O	J	01000001	01001000	01001111	01001010

Tab. 3: Ukázka šifrování dat Vernamovou šifrou na binární úrovni

Zašifrovaná data v příkladu jsou uvedena ve formě indexu znaku v ASCII tabulce, jelikož tyto jsou v textovém formátu nezobrazitelné. V tomto případě by zároveň náhodný klíč neměl využívat pouze byty znaků písmen, ale vybírat z celé tabulky všech 256 znaků, resp. generátor klíče by měl pracovat na úrovni bitů (náhodně volit sekvence 0 a 1), a na výsledné znaky vůbec nehledět.

Důsledky porušení podmínek spolehlivosti

Porušení podmínek spolehlivosti vede k nedostatečné bezpečnosti šifry a umožňuje její prolomení. Konkrétně nedodržení každé jednotlivé podmínky má následující důsledky.

V případě *opakovaného použití klíče* je možné tento klíč snadno určit pouze ze znalosti dvou zachycených zpráv šifrovaných týmž klíčem. Platí totiž následující vztah:

$$\mathtt{D1}_i \oplus \mathtt{K}_i = \mathtt{C1}_i \qquad \mathtt{D2}_i \oplus \mathtt{K}_i = \mathtt{D2}_i \qquad \mathtt{C1}_i \oplus \mathtt{C2}_i = \mathtt{D1}_i \oplus \mathtt{D2}_i$$

kde $\mathtt{D1}_i$ je i-tý znak 1. dat, $\mathtt{D2}_i$ je i-tý znak 2. dat, $\mathtt{K}_i$ je i-tý znak klíče, $\mathtt{C1}_i$ je i-tý znak zašifrovaného znění 1. zprávy a $\mathtt{C2}_i$ je i-tý znak zašifrovaného znění 2. zprávy. Výsledkem operace XOR dvou zašifrovaných dat je tedy XOR dvou původních dat. Tím dojde k odstranění veškeré náhodnosti klíče a z výsledku lze jednoduchou statistickou kryptoanalýzou získat oboje původní data a tím pádem i klíč. [7]

$$\mathtt{K}_i = \mathtt{C1}_i \oplus \mathtt{D1}_i = \mathtt{C2}_i \oplus \mathtt{D2}_i$$

Díky tomu lze následně každou další zprávu zašifrovanou týmž klíčem dešifrovat již v reálném čase, bez nutnosti dalších kryptoanalýz. Po prvním použití každého klíče je tedy třeba jej celý bezpečně „zničit“, jak na straně příjemce, tak na straně odesílatele.

Pokud by klíč *nebyl stejně dlouhý jako přenášená zpráva*, muselo by dojít k jeho opakování pro šifrování částí dat, které nepokryl. To by mělo za následek týž efekt jako opakované použití klíče. V případě že by útočník znal některou z částí dat, získal by tak zpětným provedením operace XOR část nebo dokonce celý klíč a mohl jej použít na zbylé části dat, jež nezná.

Znalost části dat útočníkem je celkem běžný fakt. V dopisech bývá na začátku obvykle uvedeno „Dobrý den“, „Ahoj“ apod., na konci zase podpis odesílatele. Při posílání binárních dat je situace ještě jednodušší, protože většina formátů souborů má vlastní hlavičku, která je vždy shodná (JPEG, ZIP, WAV, DOC, ...) nebo je alespoň z konečné množiny možností. Struktura dokumentů textových editorů (RTF, XML, HTML, ...) pak navíc opakovaně obsahuje známé formátovací sekvence znaků, které se dají frekvenční analýzou snadno detekovat.

Předpoklad *dokonalé náhodnosti celého klíče* stejně jako jeho dostatečná délka zaručuje, že každý jednotlivý znak (bit) dat je zašifrován zcela nezávisle na ostatních znacích. Znalost jakékoli části dat tedy útočníkovi z výpočetního hlediska neprozradí nic o kterémkoli jiném jemu neznámém znaku dat ani klíče.

Pro dokonalou bezpečnost šifry nelze použít ani pseudonáhodné hodnoty. Ty jsou totiž generovány dle určitého algoritmu a jejich vygenerování je tak při dodržení stejných podmínek zopakovatelné. Data jsou pak rozluštitelná v konečném čase, resp. lze nalézt takový klíč, který převede zašifrovanou zprávu na srozumitelná data a zároveň u něho bude možné prokázat vztah mezi jeho jednotlivými částmi nebo k nějaké výchozí hodnotě (seedu[2]) a tak identifikovat, která z možných rozluštění zpráv je ta pravá. Pro generování klíče je nejvhodnější užití fyzikálních metod, např. radioaktivity, o níž je prokázáno, že její charakter je skutečně náhodný [1].

Kvantová kryptografie

Kvantová kryptografie využívá bezpečného komunikačního kanálu (optického vlákna) mezi dvěma komunikujícími stranami. Pro přenos jednotlivých bitů jsou použity ve smluveném směru polarizované fotony. Ty totiž nelze odposlouchávat jako klasický elektrický signál, jehož intenzitu je možné změřit, aniž by byl tok dat narušen. Foton je dále nedělitelná a neklonovatelná částice a jakákoli interakce s ním jej zásadně ovlivní. Případný odposlech lze tedy snadno odhalit [8].

Aby se předešlo zachycení dat případným útočníkem odposlouchávajícím komunikaci (tzv. *Man in the middle*), je nejprve poslán tímto kanálem klíč, který splňuje požadavky spolehlivosti na jeho délku a náhodnost. Pokud přenos klíče proběhne v pořádku (nedošlo k jeho odposlechu), jsou teprve pak odeslána data zašifrovaná tímto klíčem. V opačném případě je klíč „zapomenut“ a zkusí se poslat jiný. Přenos dat již poté ani nemusí probíhat přes zabezpečený kanál, jelikož ta jsou bez klíče, při dodržení požadavků spolehlivosti, absolutně nedešifrovatelná [5]. Tento princip přináší možnost zcela bezpečné komunikace, ovšem vyžaduje přímé spojení nepřerušovaným optickým kabelem mezi oběma stranami, což je podmínka splnitelná jen v některých výjimečných případech. Při komunikaci prostřednictvím veřejné sítě internet tedy globálně použít nelze.

Jinou možností bezpečného přenosu klíče je osobní předání datového média (např. CD) obsahujícího data klíče pro budoucí použití. Podobným způsobem je například zabezpečena horká linka spojující prezidenty Ruska a USA [1].

[2]Seed je výchozí hodnota generátoru pseudonáhodných hodnot, v němž je každá následující hodnota odvozena od hodnoty předchozího kroku. Při zadání téhož seedu lze tudíž zopakovat vygenerování stejné sady pseudonáhodných hodnot.

Dlouhý a náhodný klíč

Podmínky spolehlivosti zaručují šifře nerozluštitelnost, zároveň však také komplikují její užívání. Konkrétně požadavek dokonalé náhodnosti klíče znesnadňuje jeho automatické softwarové generování. Také nutnost, aby jeho délka byla shodná s délkou šifrovaných dat, přináší (pomineme-li kvantovou kryptografii) týž problém, jako přenos dat samotných, na čemž se podílí i jednorázovost každého klíče. Může tedy být žádoucí, byť za cenu ztráty absolutní neprolomitelnosti šifry, aby klíč resp. heslo mohlo být kratší, ne zcela náhodné (zapamatovatelné) a opakovaně použitelné.

Jak již bylo uvedeno, klíč složený z pseudonáhodných hodnot nezabrání v rozluštění zašifrovaných dat v konečném čase. Bude-li však tento klíč „kvalitně náhodný“ a zároveň splňovat ostatní podmínky spolehlivosti, zůstane vyloučena možnost použití jakýchkoli výpočetních a statistických kryptoanalýz, s výjimkou útoku hrubou silou. Ten může útočník například použít na určení klíčů, které zašifrovaným datům (nebo jejich částem) dávají smysl, a následně k hledání souvztažnosti mezi jednotlivými částmi klíče. Účinnější formou útoku hrubou silou by pak bylo, v případě znalosti algoritmu generátoru pseudonáhodných hodnot pro klíče, určení výchozí hodnoty generátoru – seedu, resp. hesla. Bude-li toto dobře zvoleno, lze data rozluštit pouze „uhodnutím hesla“ s použitím „hrubé síly“ a onen konečný čas rozluštění dat tak může být nereálně dlouhý.

V případě, že budou pro účely šifrování přínosné výše zmíněné výhody ohledně hesla (krátké, nenáhodné a opakovatelné) a zároveň nebudou nepřekonatelnou překážkou uvedená omezení dokonalosti šifry (při „uhodnutí“ hesla budou data dešifrovatelná), pak již zbývá jen vytvořit algoritmus, který z krátkého hesla dokáže opakovaně vytvořit libovolně dlouhý klíč, jenž bude statisticky prokazatelně náhodný v rovnoměrném rozdělení. To znamená, aby všechny hodnoty v rozsahu bytu (rozsah bytu je 0–255, tedy 256 (2^8) možných hodnot) byly generovány se stejnou pravděpodobností, resp. generovaná sekvence bitů byla sama o sobě náhodná. Popsané vlastnosti přímo zapadají do definice hash funkce a při jejím vhodném užití lze s její pomocí docílit veškerých požadovaných vlastností klíče.

Hash

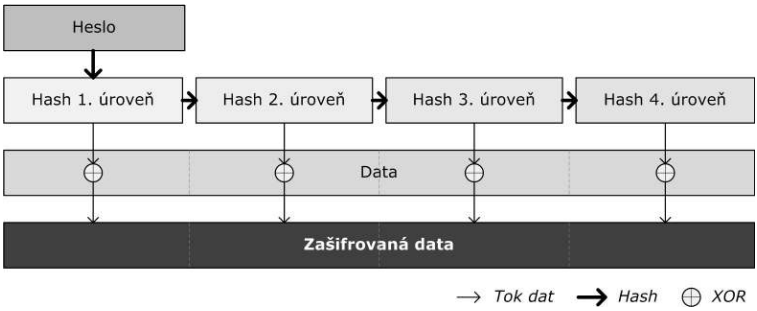
Hash je jednosměrná (ireverzibilní) výpočetně efektivní funkce mapující binární řetězce libovolné délky na řetězce pevné délky, tzv. hash-hodnoty. Základní myšlenkou je, že hash-hodnota slouží jako kompaktní zástupce vstupního řetězce. Při kryptografickém použití, je hash funkce `H`

zvolena tak, že je výpočetně nemožné nalézt dva různé vstupy, jejichž hash-hodnota by byla shodná, (tj. nelze nalézt `X` a `Y` takové, aby platilo $(\mathtt{H(X)} = \mathtt{H(Y)}) \wedge (\mathtt{X} \neq \mathtt{Y})$), a zároveň je také výpočetně nemožné určit vstup `X` pro danou hash-hodnotu `Y` (tj. $\mathtt{H(X)} = \mathtt{Y}$). Pravděpodobnost, že n-bitová hash-hodnota (např. $n = 128$ nebo 160) náhodně vybraného řetězce bude mít konkrétní n-bitovou hash-hodnotu je tedy 2^{-n} [7].

Statistické testy náhodnosti hash-kódu generovaného užitím algoritmu SHA-1[3] dle [9], [10] prokázaly, že jím generovaná sekvence bitů vyhovuje ze statistického hlediska podmínkám rovnoměrného náhodného rozdělení. Jiné hashovaní algoritmy (např. MD5, SHA-256, SHA-512, atd. nebo připravovaný SHA-3 [11]) by samozřejmě dle své definice měly mít tytéž vlastnosti, což je možné ověřit například dle postupů uvedených v [7] pomocí software popsaného v [9].

Heslo a klíč, délka klíče

Pomocí hash algoritmu lze tedy z libovolného hesla vytvořit klíč vyhovující podmínce náhodnosti a neumožňující zpětný výpočet hesla. Jeho délka je ovšem předem určena na konstantní počet bitů dle konkrétního užitého algoritmu. Zapotřebí je však klíč mnohem delší, než je hash-kód. Jednou z možností je použít jako klíč víceúrovňový hash. V tomto případě by byl hash původního hesla použit na zašifrování prvního bloku dat a následně posloužit jako vstupní hodnota pro vygenerování nového hash-kódu (hash 2. úrovně). Jím by se opět zašifroval další blok dat a znovu by z něho byl vygenerován hash 3. úrovně jako klíč pro další blok dat a tak dále, až by byla pokryta celá datová zpráva (viz obr. 1).

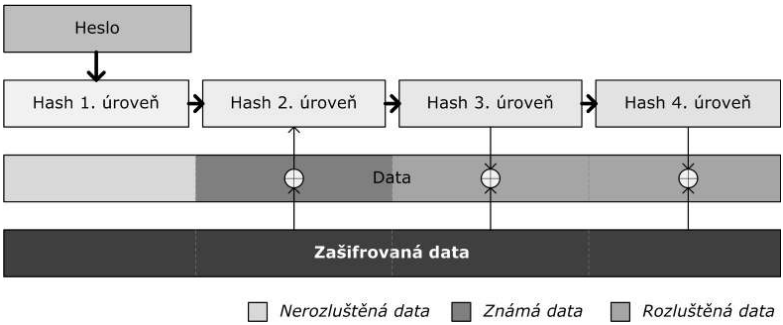


Obr. 1: Schéma šifrování dat operací XOR, kde klíč tvoří prostý víceúrovňový hash hesla

[3]SHA-1 – Secure Hash Algorithm, vracející hash-kód o délce 160 bitů, který byl navržen institutem NIST pro americké vládní aplikace [7].

Zamezení útoku při znalosti části dat

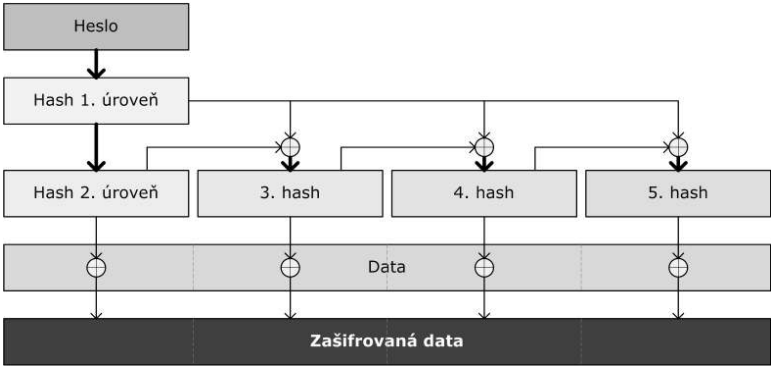
V uvedeném případě je ovšem útočník, který zná část dat, schopen rozluštit i jejich další neznámé části. Pokud by například znal data zašifrovaná hashem 2. úrovně, stačilo by mu provést operaci XOR mezi těmito a zašifrovanými daty a získal by část klíče (hash 2. úrovně). Z něho by sice nedokázal dopočítat hash 1. úrovně ani heslo, ovšem mohl by vygenerovat hash 3. úrovně, z něho pak 4. úrovně atd. Díky tomu by byl schopen dešifrovat data od bloku, jehož obsah znal, či např. slovníkovým útokem odhalil (viz obr. 2).



Obr. 2: Schéma rozluštění části dat zašifrovaných pomocí klíče z prostého víceúrovňového hashe hesla

Jednou z možností, jak takovémuto útoku zabránit, je modifikovat před generováním hash-kódu každé další úrovně vstup hash funkce (předchozí úroveň hashe) způsobem, který útočník nedokáže zopakovat, ovšem dešifrovací proces znalý správného prvotního hesla ano. Tato modifikace tedy musí přímo vycházet a záviset na tomto heslu. Lze například k hash-kódu hesla každé úrovně před generováním hashe další úrovně přičíst heslo samotné, avšak mnohem účinnější, bezpečnější a výpočetně efektnější je hash zkombinovat s jiným hashem. Oba totiž obsahují pseudonáhodné znaky z celé škály bytového rozsahu a také mají stejnou délku. Díky tomu lze opět využít operaci XOR.

Vzniklý blok bytů poslouží pouze jako vstup pro vytvoření hashe následující úrovně a sám o sobě nebude nikde použit. Pro tento účel ideálně poslouží hash hesla 1. úrovně, který by v tomto případě neměl být sám o sobě použit pro šifrování žádného z bloků dat a sloužil pouze pro kombinování s hashi vyšších úrovní (viz obr. 3).



Obr. 3: Schéma šifrování dat pomocí klíče z kombinovaného víceúrovňového hashe hesla

Pokud tedy útočník bude znát určitou část dat, dokáže sice rozluštit klíč, kterým byla tato část zašifrována, ale již nedokáže určit klíč pro následující (a samozřejmě ani předchozí) blok dat. K tomu by potřeboval znát buď hash hesla 1. úrovně nebo zdroj hashe pro klíč následujícího bloku dat. Oba požadavky by znamenaly určení reverze hashe, což je již dle základní definice této funkce výpočetně nemožné.

Jediný způsob, jak neznámé části dat určit, je „uhodnout“ heslo, popřípadě jeho hash 1. úrovně. Zde již závisí hlavně na „síle“ zvoleného hesla, tj. jak dokáže odolat před slovníkovým útokem a útokem hrubou silou. Pro volbu snadno zapamatovatelných hesel odolávajících těmto druhům útoku existuje řada postupů (např. viz [12]).

Heslo delší než hash-kód nemá u jednorázového použití smysl, jelikož v takovém případě se útočníkovi vyplatí spíše určit 1. hash-kód tohoto hesla, neboť heslo samotné k rozluštění dat nepotřebuje. Pokud by však heslo mělo být používáno opakovaně, útočníkovi se vyplatí hledat spíše heslo než jeho hash-kód, i když jeho určení bude o něco náročnější.

Jedinečný klíč pro každou zprávu

Posledním úskalím je požadavek na jedinečnost klíče pro každou komunikaci (každá data). Pro dosažení tohoto požadavku existuje několik možností. Je-li například souběžně s rychlým datovým potencionálně odposlouchávaným kanálem soustavně otevřen i další zabezpečený, byť třeba pomalý kanál, může být před zasláním každé datové zprávy tímto kanálem zasláno i nové heslo.

Druhou možností je, v případě souvislé komunikace mezi dvěma účastníky, používat stále další a další úrovně původního hesla a nezačínat je generovat vždy znovu od začátku. Klíčem pro šifru pak bude neustále jiný klíč. Nevýhodou ovšem je nezbytnost pamatovat si úroveň hashe, na které komunikace skončila a nemožnost zapojení více účastníků (při architektuře klient–server) do komunikace, aniž by neustále museli zbytečně dopočítávat příslušnou úroveň hashe dosaženou ostatními.

Jinou možností je využití faktu, že na kompletní změnu celého klíče sestávajícího z moha úrovní hashe stačí změna jediného bitu v heslu či hashe 1. úrovně. Při tomto druhu změny může být její popis součástí zprávy obsahující i zašifrovaná data. Může se jednat například o dodatečný textový řetězec, který byl k heslu přičten před výpočtem hashe první úrovně. Takovýto přídavek hesla se nazývá „salt“ a je zároveň dobrou pomůckou proti slovníkovým útokům postaveném na předgenerovaných hashových slovnících. Jeho zveřejnění přitom nijak nesnižuje obtížnost dešifrování dat, neboť pro výpočet klíče je stále nezbytné znát i původní část hesla.

Díky saltu je klíč pro data pokaždé kompletně jiný a ani případné určení jeho části, nebo i klíče celého, v některém z minulých datových přenosů, nesnižuje zabezpečení přenosu dat budoucích, aniž by muselo dojít ke změně hesla. Je pouze třeba zabezpečit, aby byl salt pokaždé jiný, čehož lze například dosáhnout pomocí generátoru tzv. GUID hodnot (*Globally Unique IDentifier*. Náhodně vygenerovaná hodnota se zanedbatelně malou pravděpodobností, že by někde někdy byly vygenerovány dvě stejné hodnoty).

Způsobů jak heslo a salt zkombinovat je nespočet. Například, pokud heslo bude `heslo` a salt `SALT` lze použít tyto způsoby:

- `hesloSALT`
- `SALTheslo`
- `hSeAsLlTo`
- `HASH(heslo)` $\oplus$ `HASH(SALT)`
- ...

Dlouhodobé uchovávání saltu

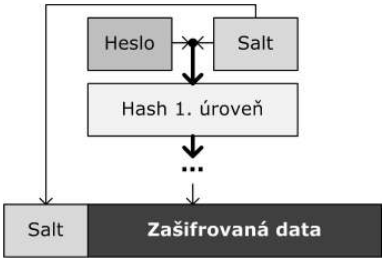
Pokud není zaručeno, že pro každá šifrovaná data bude použito jiné heslo, je pro originalitu každého klíče nezbytné použít salt. Při komunikaci dvou stran může být salt jedním z předávaných parametrů zprávy. V případě použití šifry na dlouhodobě samostatně uchovávané soubory je

třeba salt uložit tak, aby byl při potřebě soubor dešifrovat kdykoli dohledatelný a konkrétnímu souboru přiřaditelný, tedy nejlépe přímo do tohoto souboru.

Ani pozice saltu uloženého v souboru šifrovaných dat nemusí být vždy stejná, tím se také dále znesnadňuje prolomení šifry. Salt totiž nemusí být přidán pouze na začátek nebo konec zašifrovaných dat, ale i na libovolnou pozici. Je také možné salt rozdělit na jednotlivé byty a ty různě mezi data rozmístit. Jejich pozice, případně saltu jako celku, i způsobu rozmístění by pak měla být jednoznačně určitelná na základě hesla, aby ho bylo možné při dešifrování zpětně dohledat a oddělit od dat. Jelikož by salt měl být zcela náhodný, stejně jako zašifrovaná data, nemělo by dojít k jeho identifikaci a pokusu o dopočítávání hesla.

Každopádně nic nebrání použití zpětně nevypočitatelného postupu (rozmísťování saltu na základě hodnot hash-kódu hesla). Také je možné salt před uložením k datům zašifrovat pouze pomocí hashe hesla (náhodné bity zašifrované náhodnými bity bez klíče dešifrovat nelze). V případě uchování saltu u dat ovšem již nejde o šifru $1:1$, kdy jeden bit zdrojových dat je zašifrován právě do jednoho bitu zašifrovaných dat, ale o šifru $1:(1+\texttt{délka saltu})$.

Tento postup také komplikuje blokové zpracování dat. Dešifrovací algoritmus musí nejprve přečíst salt a až po té s jeho pomocí může postupně dešifrovat data. Aby tedy nebylo nezbytné dvojí zpracování dat, je nejvýhodnější salt uložit hned na jejich začátek (viz obr. 4).



Obr. 4: Schéma šifrování dat se zapojením saltu

Při takto uloženém saltu může šifrování i dešifrování dat probíhat obvyklým blokovým i proudovým způsobem. Začátek dat, kde je uložen salt, ovšem musí být přečten vždy a nelze tak dešifrovat pouze určité úseky dat nezávisle na pořadí.

Rychlost

Navržený šifrovací algoritmus tedy přímo staví na specifickém klíči, jenž tvoří víceúrovňový hash, který je navíc v každé úrovni znovu kombinován s hashem 1. úrovně. Výpočet hashe není samozřejmě triviální výpočetní operací, ale komplikovaným algoritmem, který zabírá určitý výpočetní čas. Je tedy zřejmé, že na rychlosti, či spíše pomalosti šifry, bude mít nevětší podíl právě výpočet tohoto klíče. Jelikož šifra dokáže pracovat s libovolným hashovacím algoritmem, pokusili jsme se pro ni zvolit ten nejrychlejší.

Za tímto účelem, bylo provedeno následující srovnání (tab. 4). V něm byly pomocí jednotlivých hashovacích algoritmů (řádky tabulky) výše uvedenou metodou vypočteny víceúrovňové klíče daných délek (sloupce tabulky). Pokus byl opakován vždy třikrát a výsledný průměr (buňky tabulky) je čas potřebný na výpočet každého klíče vyjádřený v milisekundách. Základní vlastnost hash-kódu (ireverzibilita a náhodnost) byla již brána jako dále netestovaná samozřejmost.

Měření bylo prováděno za identických podmínek, tj. na stejném počítači při týchž běžících procesech. Parametry testovacího stoje byly tyto: CPU 2,5 GHz, RAM 4GB, HDD 7 200 RPM, OS Windows 7 64bit. Pro výpočet klíče byly použity algoritmy integrované v programovacím prostředí Microsoft.NET Framework 4.0, jazyk C#, ve kterém byl implementován i následně testovaný šifrovací algoritmus.

	1 MB	2 MB	3 MB	5 MB	10 MB	20 MB	30 MB	50 MB	100 MB
MD5	519	1 034	1 539	2 532	5 060	10 084	15 105	25 206	50 313
SHA-1	430	842	1 272	2 098	4 216	8 410	12 613	21 016	42 006
SHA-256	291	560	890	1 406	2 820	5 682	8 648	14 168	28 523
SHA-384	295	560	862	1 368	2 757	5 549	8 225	13 734	27 379
SHA-512	211	420	655	1 046	2 083	4 221	6 309	10 496	20 874

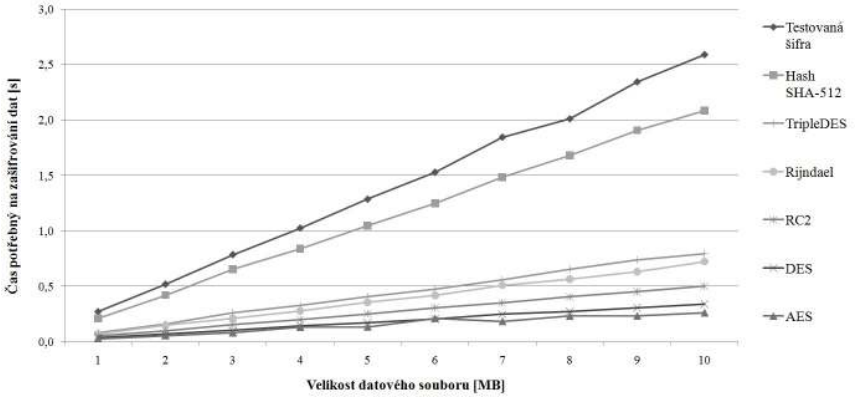
Tab. 4: Porovnání rychlostí výpočtů [ms] víceúrovňového hashe dané délky jednotlivými algoritmy

Z porovnání v tab. 4 plyne, že nejrychlejším z testovaných hashovacích algoritmů je SHA-512. Ten byl tedy následně použit i pro test srovnání rychlostí tohoto a již existujících šifrovacích algoritmů (tab. 5). Porovnání bylo provedeno podobným testem a za stejných podmínek jako srovnání rychlostí hashovacích algoritmů. Tentokrát ovšem již nešlo pouze o výpočet hodnot v rámci paměti počítače, ale zdrojová data byla čtena ze souboru na pevném disku a výsledná zašifrovaná data na disk znovu ukládána. Data byla načítána, zpracována a ukládána proudově, po blocích o velikosti 5 kB.

	1 MB	2 MB	3 MB	5 MB	10 MB	20 MB	30 MB	50 MB	100 MB
AES	28	54	79	133	264	531	818	1 263	2 797
DES	35	68	101	172	340	703	1 030	1 709	3 476
RC2	52	101	153	252	501	1 012	1 523	2 547	5 114
Rijndael	71	148	211	357	723	1 452	2 147	3 581	7 557
TripleDES	82	160	264	406	795	1 620	2 403	4 013	8 300
Testovaná šifra	270	518	785	1 285	2 590	5 113	7 703	12 764	25 825

Tab. 5: Porovnání rychlostí šifrování [ms] datových souborů dané velikosti jednotlivými algoritmy

Porovnání v tab. 5 a na obr. 5 ukazuje, že navržený šifrovací algoritmus je oproti ostatním výrazně pomalejší. Zhruba 81 % tohoto času ovšem zabírá výpočet klíče, byť nejrychlejším z testovaných hashovacích algoritmů SHA-512. Použitím rychlejšího hashovacího algoritmu by tedy mohlo dojít i k výraznému zrychlení této šifry. Tuto vlastnost by mohl přinést připravovaný hashovaní algoritmus SHA-3 (Soutěž o SHA-3 viz `http://csrc.nist.gov/groups/ST/hash/sha-3/`).



Obr. 5: Graf porovnání rychlostí šifrování datových souborů dané velikosti jednotlivými algoritmy. Zahrnuta je i rychlost generování klíče pomocí hashovacího algoritmu SHA-512.

Rychlost šifrování tedy limituje použití při klasickém šifrování v reálném čase, například při on-line komunikaci dvou stran, kde je rychlost spojení jedním z hlavních parametrů. Její využití by tak mohlo být spíše v případech, kdy má úroveň zabezpečení vyšší prioritu, nežli čas potřebný na zašifrování.

Závěr

V článku byl shrnut původní princip Vernamovy dokonalé šifry a na jejím základě navržena modifikace práce s klíči, jejichž správa zatím velmi komplikuje její praktické využití. Při kombinaci s moderními hashovými algoritmy lze šifrovat data pomocí matematicky prokazatelně zpětně nevypočitatelných postupů a přitom i opakovaně používat „jednoduchá“ hesla. Síla šifry je pak vždy přímo úměrná síle zvoleného hesla.

Implementace uvedeného postupu je přitom programově velmi snadná. Rychlost šifrování a dešifrování dat nejvíce závisí na rychlosti výpočtu hash-kódu, tedy na zvolené hash funkci. Připravovaná funkce SHA-3 přitom slibuje mnohem rychlejší výpočet a zároveň i vyšší bezpečnost než ty stávající, byť dosud neprolomené [11].

Navrženou šifru lze, díky své stávající nižší rychlosti, používat pro ochranu přenosu dat přes veřejnou síť internet zatím pouze v případech, kdy nevadí zpomalení potřebné pro šifrování dat. V případě šifrování archivů a souborů pro dlouhodobou úschovu, kde je obvykle přednější jejich bezpečnost před časem potřebným na zašifrování, může tato šifra nalézt své uplatnění již nyní.

Literatura

[1] *Singh, S.*: Kniha kódů a šifer. Dokořán a Argo, Praha, 2009.

[2] *Piper, F., Murphy, S.*: Kryptografie: Průvodce pro každého (překlad). P. Mondschein – Dokořán, Praha, 2006.

[3] *Janeček, J.*: Gentlemani nečtou cizí dopisy. Books, Brno, 1998.

[4] *Shannon, C. E.*: Communication Theory of Secrecy Systems. Bell System Technical Journal, 1949.

[5] *Hála, V.*: Kvantová kryptografie. Aldebaran Bulletin 4 (2005), č. 14. Dostupné z www [http://aldebaran.cz/bulletin/2005_14_kry.php].

[6] *Vernam, G. S.*: Secret signaling system. 1310719 U.S. Patent, 22. červenec 1919.

[7] *Menezes, A. J., Oorschot van, P. C., Vanstone, S. A.*: Handbook of Applied Cryptography. CRC Press, Boca Raton, 1996.

[8] *Dušek, M.*: Kvantová kryptografie [online]. Koncepční otázky kvantové teorie [cit. 23. 8. 2010]. Dostupné z www [http://muj.optol.cz/dusek/predn/kokt/krypt.htm].

[9] *Andrew, R. a kol.*: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [online]. NIST Special Publications (800 Series) [cit. 21. 8. 2010]. SP 800-22 Rev 1a.
Dostupné z www [http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf].

[10] *Pierre, L., Richard, S.*: TestU01: A C Library for Empirical Testing of Random Number Generators. Université de Montréal: ACM Trans. Math. Softw. 33, 4, Article 22, 2007. DOI=10.1145/1268776.
[11] *Klíma, V.*: Blue Midnight Wish, kandidát na SHA-3 aneb poněkud privátně o tom, jak jsem k BMW přišel. Crypto-World. roč. 11 (2009), č. 2.
[12] *Musílek, M., Hubálovský, Š.*: Počítačová bezpečnost ve výuce informatiky (Tvorba hesel a steganografie).
[13] *Musílek, M., Hubálovský, Š.*: Počítačová bezpečnost ve výuce informatiky. Jednoduchá záměna (monoalfabetické šifry). MFI roč. 20 (2010/11), č. 6.
[14] *Musílek, M., Hubálovský, Š.*: Počítačová bezpečnost ve výuce informatiky (Luštění jednoduché záměny, frekvenční analýza). MFI roč. 20 (2010/11), č. 9.

Simulace elektronických obvodů programem Multisim a možnosti využití jeho speciálních funkcí vhodných pro výuku

PETR MICHALÍK – PAVEL BENAJTR

Fakulta pedagogická, Západočeská univerzita, Plzeň

Simulační programy patří mezi moderní výukové prostředky. Jedním z jejich představitelů je program Multisim, který vytvořila mezinárodní společnost National Instruments. Společnost je zaměřena na výzkum i vývoj měřicí a řídící techniky. Na rozdíl od velké většiny jiných výrobců není zaměřena pouze na firemní oblast. Zajišťuje podporu pro školy v podobě seminářů i jiných aktivit, např. soutěže a veletrhy. Uvedený simulační program je určen pro simulaci a návrh elektronických obvodů. Využívají jej nejen profesionální firmy, ale také velmi často odborné školy a univerzity, např. na Pedagogické fakultě ZČU v Plzni. Vzhledem k několikaletým zkušenostem s uvedeným simulačním programem na Pedagogické fakultě, lze zhodnotit výsledky simulací jako velmi dobré v porovnání s reálným měřením v laboratoři.

Pro výukové účely obsahuje Multisim množství rozšíření, která mohou být využita při simulaci elektronických obvodů. Tato rozšíření je možné označit za funkce simulačního programu vhodné pro výuku. Před samotným výběrem funkcí, které by mohly být označeny za „vhodné pro výuku“, je vhodné sestavit zobecněnou definici. Prostřednictvím definice bude možné lépe zhodnotit jednotlivé funkce simulačního programu z edukačního hlediska. U každé z nich vznikne popis vlastností, způsob použití, cíle a očekávané výstupy. Rozsah využití funkcí ve výuce může být rozsáhlý. Návrhem možného využití funkce ve zvoleném příkladu bude možné získat lepší představu o využití těchto funkcí.

Definice funkcí simulačního programu vhodných pro výuku

Vybrat funkce, které by byly jednoznačně vhodné pro výuku, je obtížné. Množství funkcí nebo jejich modifikace, které jsou běžně využívány, by mohlo být rovněž považováno za výukové funkce. V mnoha případech lze s úspěchem využít i takové, které nejsou jednoznačně vhodné pro výuku. Jejich použitím je možné nakonec dosáhnout obdobných výsledků v porovnání s tzv. výukovými funkcemi. Aby bylo možné rozlišit, o jaký typ se jedná, je nutné sestavit popis v podobě definice. S využitím definice bude následně možné vytvořit příklady pro výuku, které v závislosti na zvolené funkci „vhodné pro výuku“ dosáhnou očekávaných výsledků.

Rozdělíme si k tomu účelu funkce simulačního programu do několika skupin. Do první skupiny budou patřit základní funkce, které umožňují realizaci obvodového zapojení a následnou simulaci bez ohledu na výukový proces. Tato skupina netvoří pro nás v tomto článku zájmovou skupinu.

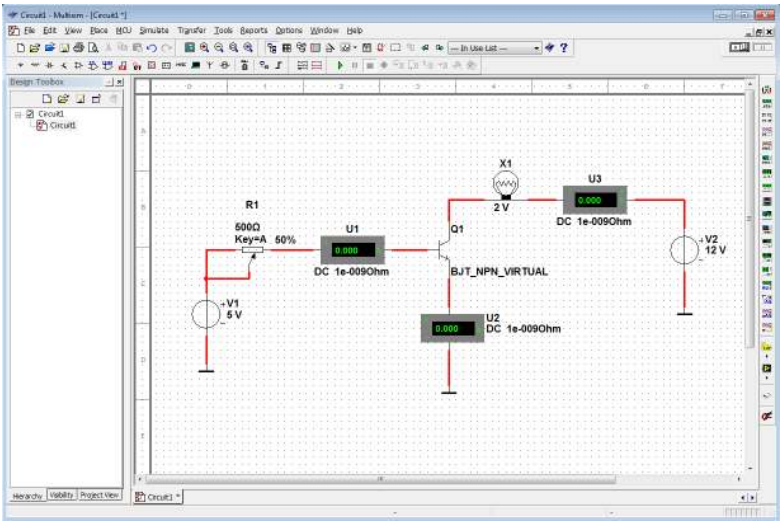
Druhá skupina sdružuje funkce simulačního programu, které lze po případné modifikaci využít jako výukové z hlediska zjednodušení probíraného výukového tématu. Např. pokud bychom chtěli studenty seznámit pouze s konkrétními částmi elektronického zapojení nebo jeho výstupy, je vhodné využít funkce, které umožní zvolit rozsah probírané látky. Můžeme následně výuku upravit na požadovanou úroveň, od úplných základů až po celkové porozumění zapojeného elektronického obvodu. Tyto funkce by bylo možné definovat dle následujícího popisu. „Funkce simulačního programu, které usnadňují a pomáhají s tvorbou elektronického obvodu. Jsou využívány především studenty, případně vyučujícím pro vstupní nastavení parametrů nebo sestavení obvodu.“ Do této kategorie lze zařadit využití ideálních součástek, tvorbu subobvodů a hierarchických funkčních bloků, kontrolu zapojeného obvodu a průvodce vytvoření zadaného obvodu.

Třetí skupina funkcí zahrnuje funkce simulačního programu, které mohou sloužit k prohloubení znalostí studenta a jejich testování. U studentů, kteří se s těmito funkcemi setkají, je vyžadována určitá úroveň znalostí. Před využitím těchto funkcí je potřebná příprava na výuku, kdy vyučující vybere zapojení obvodu a připraví vhodné vstupními parametry. Tyto funkce by bylo možné definovat dle následujícího popisu. „Funkce simulačního programu, které prohlubují a ověřují znalosti studenta. Pro jejich použití je důležitá příprava vyučujícího na výuku, který zvolí vhodné využití funkce v konkrétním případě." Do této kategorie lze zařadit např. funkce zadávání chyb simulačních modelů konkrétních součástek nebo uzamčení a znepřístupnění některých přístrojů a funkcí. K této definici by bylo možné přiřadit také několik typů analýz elektronického obvodu.

Charakteristika funkcí simulačního programu vhodných pro výuku

Ideální součástky jsou modely reálných součástek, které zahrnují pouze charakteristické parametry bez ohledu na parazitní parametry součástky. Např. ideální rezistor zahrnuje charakteristický parametr rezistenci, model reálného rezistoru obsahuje navíc indukčnost přívodů a parazitní kapacitu. Využití modelů ideálních součástek je pro výukové účely velmi vhodné, neboť, jak je známo, zjednodušením modelu lze dosáhnout efektivnějším způsobem stanovených výukových cílů. Jejich využití ve výuce je vhodné zejména u elektronických obvodů s důrazem na jejich porozumění. Získané výsledky z těchto simulací s velkou přesností odpovídají předpokládaným výsledkům a zjednodušeným matematickým výpočtům. U těchto součástek a v závislosti na jejich typu, lze nastavit velké množství parametrů, které ovlivňují výsledné chování zapojeného obvodu. V simulačním programu jsou pojmenovány jako virtuální součástky. Na obr. 1 je příklad s využitím virtuálních součástek bipolárního tranzistoru NPN a žárovky zapojené v kolektorovém obvodu. Studenti se zde mohou seznámit s principem bipolárního tranzistoru a ověřit platnost charakteristických rovnic bipolárního tranzistoru.

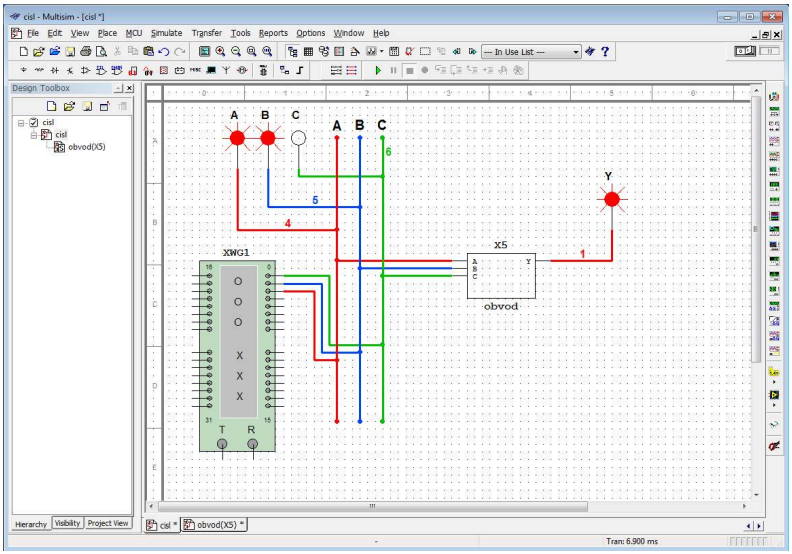
Využitím subobvodu je možné rozšířit pracovní plochu simulačního programu a hlavně zjednodušit složitější zapojení rozsáhlého elektronického systému. Subobvod je považován za vlastní součástku, která obsahuje různý počet vývodů, v závislosti na jejím vnitřním zapojení. Do subobvodu lze umístit libovolnou část zapojení. Lze jej přirovnat k integrovanému obvodu.



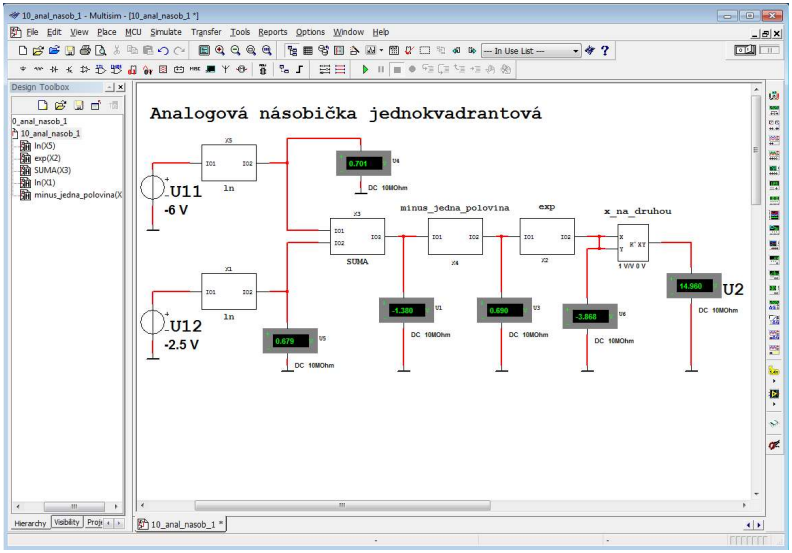
Obr. 1

Studenti mohou některé části obvodu integrovat do subobvodů a získat tím přehlednější zapojení, které částečně eliminuje množství chyb při jeho realizaci. Vyučující prostřednictvím subobvodů mohou zjednodušit nebo rozdělit výsledný obvod, u kterého bude tak možné lépe pochopit jeho princip. Obr. 2 ukazuje příklad využití subobvodu v simulačním programu. Logická funkce zapojená pomocí diskrétních logických členů byla integrována do subobvodu. Vznikla tím jediná součástka a došlo k zpřehlednění zapojení obvodu. Studenti se prostřednictvím toho příkladu naučí sestavit logickou funkci a pracovat s pravdivostní tabulkou.

Hierarchický blok je obdobou subobvodu s rozdílným způsobem uložení vloženého elektronického obvodu. V případě subobvodů je jejich obsah ukládán do souboru společně s celým obvodem. Hierarchické bloky jsou charakterizovány stejně jako subobvody, avšak jsou uloženy v samostatném souboru. To nabízí řadu využití. Vyučující poskytne studentům hierarchický blok, případně více bloků, které studenti vhodně sestaví a doplní o další součástky a přístroje. Nebo naopak doplní sestavený obvod o vhodné zapojení do hierarchického bloku, který odevzdají vyučujícímu. Využití je také možné v případě, kdy je výuka založena na použití elektronických obvodů vytvořených v předchozích vyučovacích hodinách. Studenti jednotlivé obvody integrují do hierarchických bloků, které později využijí v další výuce. Na obr. 3 je vidět zapojení s hierarchickými funkčními bloky.


cisl - Multisim - [cisl *]
File Edit View Place MCU Simulate Transfer Tools Reports Options Window Help
Design Toolbox
cisl
obvod(X5)
A B C
A B C
Y
XWG1
X5
obvod
T R
Hierarchy Visibility Project View
cisl *
obvod(X5) *
Tran: 6.900 ms

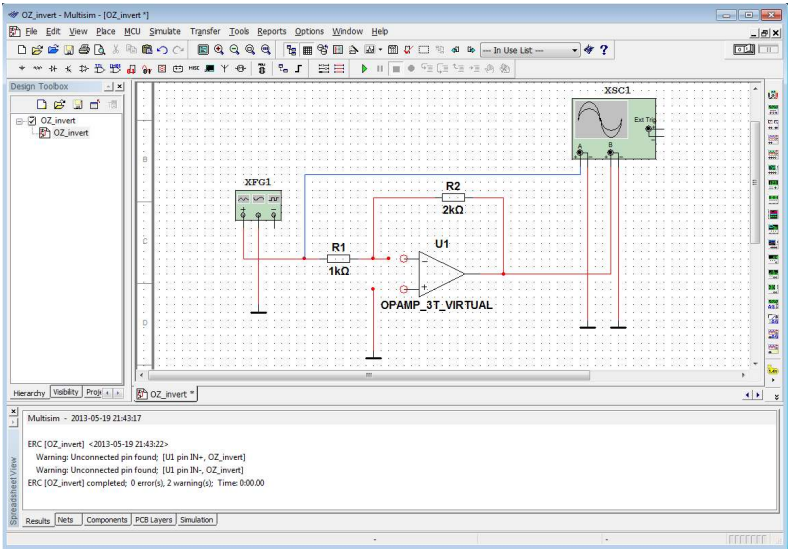
Obr. 2


10_anal_nasob_1 - Multisim - [10_anal_nasob_1 *]
File Edit View Place MCU Simulate Transfer Tools Reports Options Window Help
Design Toolbox
0_anal_nasob_1
10_anal_nasob_1
ln(X5)
exp(X2)
SUMA(X3)
ln(X1)
minus_jedna_polovina(X
Analogová násobička jednokvadrantová
U11
-6 V
U12
-2.5 V
ln
SUMA
minus_jedna_polovina
exp
x_na_druhou
U2
DC 10MOhm
Hierarchy Visibility Proje
10_anal_nasob_1 *

Obr. 3

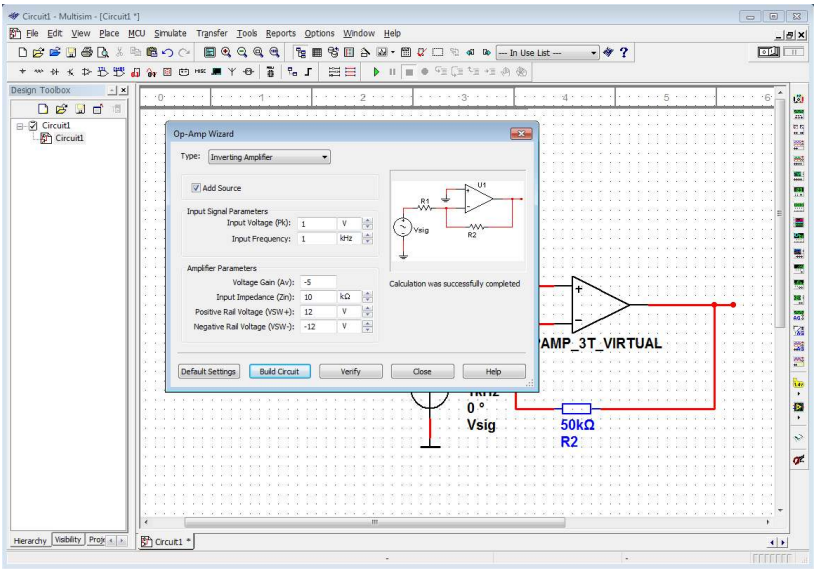
Studenti při sestavování jednokvadrantové násobičky umístili její hlavní části do samostatných bloků. Využili zapojení, sestavované v předchozích hodinách. Zapojený obvod je následně přehlednější, je snazší pochopit činnost zapojení a nezanedbatelný z hlediska výuky je také fakt, že lze snáze vyhledat případné chyby v zapojení. Při vícenásobném využití shodných bloků, jako je např. logaritmický zesilovač, se projeví případná změna nebo oprava v celém zapojení obvodu. Dojde tak k zefektivnění práce studenta.

Kontrola zapojeného obvodu je funkcí simulačního programu, která prověří zapojený obvod z hlediska možných chyb. Nalezené chyby jsou indikovány přímo v zapojeném obvodu a popsány v příslušném okně programu. V nastavení této kontroly je možné zvolit jaké chyby kontrolovat a jakým způsobem je indikovat. Lze například zjistit nevhodné spojení dvou vývodů součástky nebo odhalit nezapojenou součástku. Studenti zde mohou před spuštěním simulace ověřit, zda zapojený obvod neobsahuje základní chyby, které by negativně ovlivnily průběh měření. Obr. 4 ukazuje příklad, který obsahuje nezapojené vývody operačního zesilovače. Spuštěním automatické kontroly chyb jsou označeny nezapojené části obvodu s textovým popisem v dolní části obrazovky. Před spuštěním simulace student nalezne chyby, které by způsobily chybné výsledky při měření nebo třeba i znemožnily simulaci.



Obr. 4

Součástí simulačního programu je také průvodce vytváření obvodů. Průvodce má k dispozici několik jednodušších často používaných zapojení. Nastavením vstupních parametrů lze vygenerovat zapojení obvodu, které je např. možné využít během realizace zadaného rozsáhlejšího zapojení. V mnoha případech je vhodné využít rychlého generování části obvodu, které student již porozuměl v předchozích hodinách a zaměřit se pouze na určitou část probírané látky podle tematického cíle výuky. Simulační program nabízí různé varianty zapojení s operačními zesilovači, tranzistory nebo časovými obvody. Na obr. 5 je zobrazen průvodce pro vytvoření zvoleného obvodu.

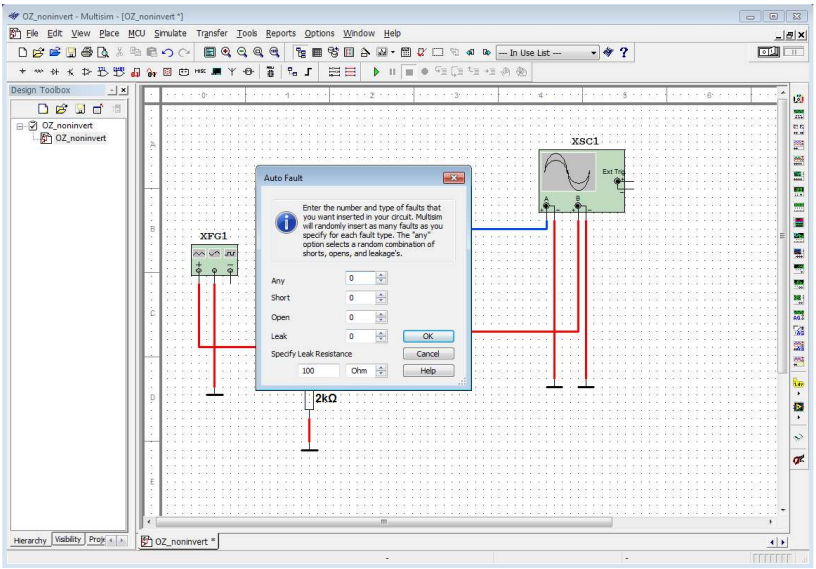


Obr. 5

Pomocí průvodce student rychle vytvoří na pracovní ploše simulačního programu např. invertující zapojení s operačním zesilovačem. V průvodci zvolí požadované parametry obvodu a následně jej umístí na vhodné místo. Pak připojí k vytvořenému zapojení další potřebné součástky a přístroje.

V simulačním programu můžeme u jednotlivých součástek nastavit chyby, které by mohly nastat v reálném obvodu. Vyučující tak může nastavením chyb ověřit úroveň znalostí a dovedností analýzy obvodu u studenta. Chyby lze generovat automaticky v celém obvodu nebo je nastavit u sou-

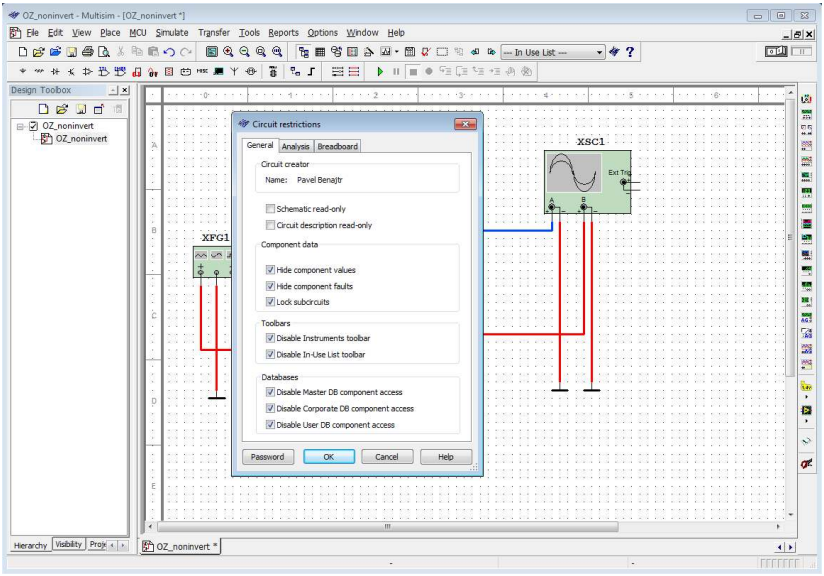
částek jednotlivě. Všechna tato nastavení se ukládají do souboru s obvodem, ve kterém byla vytvořena. K dispozici máme chybu typu odpojení vývodu součástky od vodiče, chybu typu zkrat nebo chybu typu propustnost, u které lze specifikovat velikost odporu. Využití této funkce vyžaduje určité vstupní znalosti studentů, aby bylo možné správně identifikovat nastavené chyby. Obr. 6 zobrazuje okno s volbami pro nastavení automatických chyb v celém obvodu. Lze takto vygenerovat jedinečné zapojení s rozdílným počtem a typem chyb.



Obr. 6

Uzamčení možností a funkcí simulačního programu je určeno zejména pro vyučující. V případě, že nechceme, aby student znal obsah subobvodu nebo hierarchického funkčního bloku, můžeme jej uzamknout pomocí hesla. Obdobně tomu může být u hledání chyb součástek, které jsme nastavili k ověření analytických znalostí. Uzamčením různých funkcí a možností lze zajistit, že studenta nasměrujeme k nalezení vhodného řešení. Využití této funkce je vhodné zejména při testech a hodnocené samostatné práci. Na obr. 7 je zobrazeno okno s nastavením parametrů pro uzamčení funkcí a nabídek simulačního programu. Vyučující v zadaném příkladě umístí na plochu potřebné součástky a uzamkne přístup do jejich databáze. Student

následně sestaví obvod pouze na základě dostupných součástek. V případě uzamčení jejich parametrů, nelze měnit jejich hodnoty nebo je prohlížet.

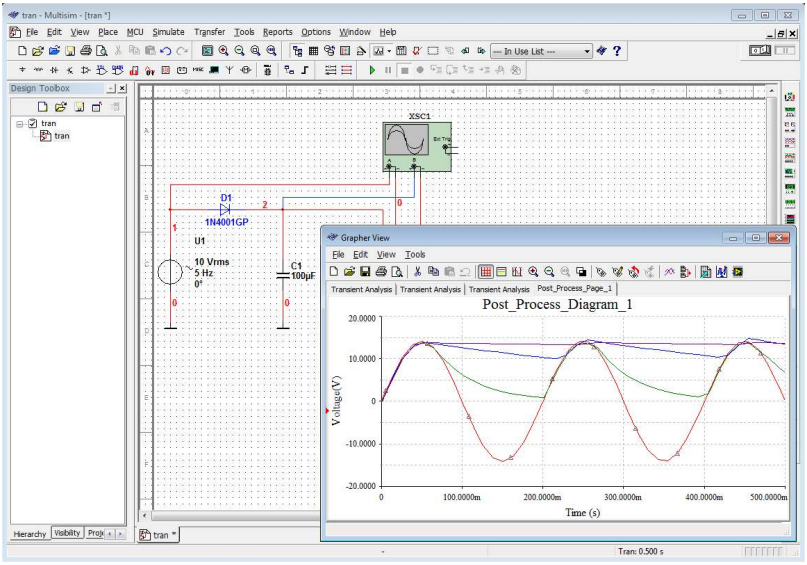


Obr. 7

Simulační programu obsahuje řadu analýz obvodů. Ke správnému použití analýzy sestaveného obvodu jsou nutné předchozí znalosti. Požadované výsledky tak závisí na vhodném využití a výběru analýzy. Nalezneme zde například analýzu stejnosměrného pracovního bodu, přechodovou analýzu, parametrickou analýzu nebo teplotní analýzu. Přiřazení analýz ke druhé skupině funkcí využitelných ve výuce je zvoleno zejména z důvodu již zmíněné požadované úrovně znalostí studenta. Opakováním analýz při změně vstupních parametrů může student lépe porozumět vlastnostem „zkoumaného“ obvodu. Obr. 8 ukazuje provedení přechodové analýzy pro obvod jednocestného diodového usměrňovače. Opakováním analýzy pro různé hodnoty součástek získá student představu o chování obvodu. Zobrazený graf obsahuje vstupní a výstupní signál. Využitím zvolených funkcí lze odečíst příslušné hodnoty ze zobrazených průběhů a ověřit získané výsledky.

Závěr

Funkce simulačního prostředku Multisim, kterými program disponuje, mohou být považovány za výukové v závislosti na jejich použití a vhodnosti. Pomocí rozdělení do několika skupin je možné určit, do které z kategorií danou funkci zařadit. V některých případech může být jednoznačné zařazení problematické a je nutné posoudit funkci z více hledisek. Jedním z nich může být úroveň požadovaných znalostí, potřebných k využití funkce. Dalšími například možnosti pro ověřování znalostí nebo cílené zjednodušení zapojeného elektronického obvodu. Případné modifikace jednotlivých funkcí umožní jejich rozšířené využití.



Obr. 8

Předložené charakteristiky a definice slouží především k orientačnímu rozdělení. Před zařazením do výuky je nejprve nutné analyzovat použitelnost funkce a její přínos pro výuku. Zejména v začátcích, kdy se studenti seznamují se simulačním programem, je vhodné využívat základní funkce. Pro složitější zapojení a prohloubení získaných znalostí lze zařadit do výuky rozšíření v podobě funkcí vhodných pro výuku. Využitím simulačního programu získají studenti možnost ověřit teoretické znalosti a získat zkušenosti a určité specifické dovednosti při práci s elektronickým obvodem.

Literatura

[1] *Benajtr, P.*: Multisim – výukový elektronický materiál. Plzeň, 2010. 40 s., Bakalářská práce. Západočeská univerzita v Plzni, Fakulta pedagogická, Katedra Výpočetní a Didaktické techniky.

[2] *Michalík, P.*: Příspěvek k počítačové simulaci elektronických obvodů. Školská fyzika roč. 9 (2012), č. 3, s. 27–32.

[3] *Juránek, A.*: MultiSIM : Elektronická laboratoř na PC. 1. vydání. BEN – technická literatura, Praha, 2008.

[4] *Vacík, V.*: Využití simulačního programu Multisim ve výuce. Plzeň, 2009. 58 s., I s. Diplomová práce. Západočeská univerzita v Plzni, Fakulta Pedagogická, Katedra Výpočetní a Didaktické techniky.

ZPRÁVY

Středoevropská olympiáda v informatice CEOI 2013

Ve dnech 13.– 19. 10. 2013 se v chorvatském městě Primošten konal jubilejní 20. ročník Středoevropské olympiády v informatice (CEOI 2013). Vedle sedmi tradičních účastnických středoevropských států (Česká republika, Chorvatsko, Maďarsko, Německo, Polsko, Rumunsko, Slovensko) se jako hosté zúčastnila také družstva ze Slovinska a Švýcarska. Jako obvykle soutěžilo také druhé družstvo pořadatelské země. Celkem se soutěže zúčastnilo 38 studentů z 9 zemí.

Reprezentační družstvo České republiky bylo sestaveno na základě výsledků, kterých dosáhli soutěžící v ústředním kole 62. ročníku Matematické olympiády – kategorie P. Na celosvětovou soutěž IOI 2013 konanou v Austrálii byli vysláni čtyři nejlepší řešitelé posledního ústředního kola MO-P, pro účast na CEOI 2013 pak byli vybráni další čtyři nejlepší studenti, kteří ale v té době ještě nestudovali v maturitním ročníku. Naši mladší soutěžící tak dostali příležitost získat na CEOI cenné zkušenosti, které mohou následně využít při úspěšné reprezentaci České republiky na IOI v příštím roce. Letos se CEOI zúčastnili tito studenti: *Martin Hora*, student gymnázia na Mikulášském nám. v Plzni, *Václav Volhejn*, student gymnázia Jana Keplera v Praze 6, *Michal Punčochář*, student gymnázia Jírovcova v Českých Budějovicích. Náš čtvrtý vybraný reprezentant Jan-Sebastian Fabík, student gymnázia na tř. Kpt. Jaroše v Brně, bohužel na poslední chvíli onemocněl, takže se soutěže nemohl zúčastnit. Vedoucími české delegace byli jmenováni *RNDr. Zbyněk Falt* a *Filip Hlásek*, oba z Matematicko-fyzikální fakulty Univerzity Karlovy v Praze.

Soutěž CEOI 2013 se tradičně uskutečnila v průběhu dvou soutěžních dnů. V každém dni soutěžící řešili tři úlohy, na které měli vždy pět hodin času. Každý

soutěžící pracuje na přiděleném osobním počítači s nainstalovaným soutěžním prostředím, které umožňuje vyvíjet a testovat programy a odesílat je k vyhodnocení. Výsledné programy jsou testovány pomocí připravené sady testovacích dat a se stanovenými časovými limity. Tím je zajištěna nejen kontrola správnosti výsledků, ale pomocí časových limitů se také odliší kvalita použitého algoritmu. Při testování každé úlohy se používají sady testovacích dat různé velikosti, takže teoreticky správné řešení založené na neefektivním algoritmu zvládne dokončit výpočet pouze pro některé, menší testy. Takové řešení je potom ohodnoceno částečným počtem bodů. Večer před soutěží vedoucí všech delegací společně vyberou soutěžní úlohy z návrhů předložených pořadatelskou zemí, upraví podle potřeby jejich formulace a přeloží je pak do mateřského jazyka studentů. Čeští studenti tedy dostali jak anglickou, tak i českou verzi zadání úloh.

Kromě vlastní soutěže je pro účastníky CEOI vždy připravován také doprovodný program. Letos měli účastníci možnost prohlédnout si nejen město Primošten, ale i národní park Krka a historická centra měst Šibenik, Split a Trogir.

Poslední den proběhlo slavnostní zakončení soutěže s vyhlášením výsledků. Každá ze soutěžních úloh byla hodnocena maximálně 100 body, takže celkově bylo teoreticky možné získat až 600 bodů. Vítězem se stal slovenský reprezentant Eduard Batmendijn, který dosáhl výsledku 355 bodů. Letos byly na CEOI uděleny 3 zlaté, 7 stříbrných a 11 bronzových medailí. Středoevropská olympiáda v informatice je soutěží jednotlivců, žádné pořadí zúčastněných zemí v ní není vyhlašováno.

Naši studenti dosáhli velmi dobrých výsledků: 8. Martin Hora, 238 bodů, stříbrná medaile, 19. Václav Volhejn, 160 bodů, bronzová medaile, 22. Michal Punčochář, 128 bodů.

Veškeré informace o soutěži, texty soutěžních úloh i podrobné výsledky všech medailistů lze nalézt na adrese `http://ceoi2013.hsin.hr/`.

Příští 21. ročník CEOI se bude konat 18.–24. června 2014 v Německu ve městě Jena, následující ročník soutěže CEOI 2015 uspořádá Česká republika. Zástupci Slovinska projevili zájem stát se řádnými členy CEOI a slíbili uspořádat soutěž v roce 2016.

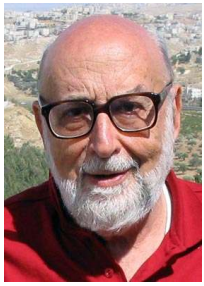
Pavel Töpfer

Nobelova cena za fyziku míří do femtofyziky

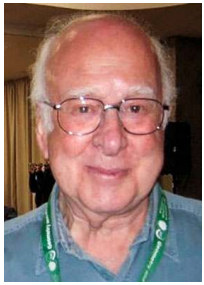
Jako každý rok počínaje rokem 1901 jsou v říjnu zveřejňovány návrhy na Nobelovy ceny za fyziku, chemii, fyziologii a medicínu, literaturu a mír, které jsou laureátům předány 10. prosince. V roce 2013 šlo již v podstatě o 113letou tradici udělování Nobelových cen (NC).

V roce 2013 byla Nobelova cena udělena za teoretickou předpověď a po experimentálním důkazu za potvrzení existence jaderné částice nazývané Higgsův boson. Na jeho experimentální důkaz musel být sestrojen v Evropské organizaci pro jaderný výzkum (CERN) velký urychlovač označovaný jako LHC (*Large Hadron Collider*). Experimenty na tomto urychlovači se potvrdila teoreticky předpověděná existence Higgsova bozonu.

Laureáti NC za fyziku pro rok 2013 [1]:



François Englert



Peter W. Higgs

Pokračování na str. 26.