



31/2006

Informatika v škole č. 31 2006

ISSN 1335-616X

Informačné periodikum

O teoretických, metodických otázkach a skúsenostiach z praxe pri uplatňovaní informatiky a výpočtovej techniky v základných a stredných školách

Predseda redakčnej rady: PhDr. Peter ZVERKA
Výkonná redaktorka: Ing. Alžbeta MEGOVÁ
Jazyková redaktorka: Mgr. Gabriela AICHOVÁ

Vydáva

Ústav informácií a prognóz školstva v Bratislave

Adresa redakcie: Ústav informácií a prognóz školstva
Staré grunty 52
842 44 Bratislava
e-mail: megova@uips.sk

OBSAH

POROVNANIE NIEKTORÝCH FORIEM HODNOTENIA VEDOMOSTÍ ŠTUDENTOV Galina Horáková, Vladimír Mucha, Anna Starečková	4
PREDSTAVY ŠTUDENTOV O VYUŽÍVANÍ INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ VO VYUČOVANÍ BIOLÓGIE Milan Kubiátko	10
MULTIMEDIÁLNÍ STUDIJNÍ MATERIÁL K VÝUCE JAZYKA PHP Václav Vrbík	16
ZVÁŠTNOSTI VÝPISU REŤAZCA V JAZYKU STROJOVEJ ÚROVNE Jana Parížková	18
POUŽITIE POČÍTAČOV VO VÝUČBE ODBORNÝCH PEDMETOV ZAMERANÝCH NA SURFING, MODELOVANIE A HYDRODYNAMICKÉ SPRÁVANIE Jaromír a Katarína Audy	23
ČRIEPKY SPOMIENOK NA CESTU ŽIVOTOM A. M. TURINGA J. Zelem	34

POROVNANIE NIEKTORÝCH FORIEM HODNOTENIA VEDOMOSTÍ ŠTUDENTOV

Anotácia: Príspevok je zameraný na porovnanie hodnotenia znalostí študentov klasickým spôsobom a pomocou testov.

Kľúčové slová: testy klasické, testy počítačové, porovnanie výsledkov

Úvod

Informačné technológie sa v priebehu ostatných dvadsiatich rokov stali bežným pracovným nástrojom. Počítače výrazne menia zaužívané spôsoby práce, zjednodušujú väčšinu pracovných postupov. Počítač je neodmysliteľnou súčasťou aj pedagogickej práce učiteľa a významným pomocníkom študentov pri štúdiu. Je jasné, že mnohí učitelia využívajú výpočtovú techniku aj pri hodnotení študentov. Otázkou je, ako diagnostikovanie vedomostí zdokonaľovať, ako nájsť optimálnu stratégiu v daných podmienkach. Uvedieme niekoľko skúseností s testovaním vedomostí v predmetoch matematického zamerania.

1. Dialógové overovanie vedomostí

Didaktický test je pre učiteľa užitočný nástroj. Jeho použitím sa získavajú informácie o znalostiach, zručnostiach aj návykoch študentov v objektívnych podmienkach. Na katedre matematiky FHI EU v Bratislave už v deväťdesiatych rokoch bol využívaný systém, určený na dialógové overovanie vedomostí študentov v terminálových učebniach. Systém umožňuje učiteľovi vytváranie testových úloh. Každá z týchto úloh sa môže charakterizovať ako úloha s desiatimi podúlohami, ktoré majú podobu jednoznačných tvrdení, výrokov. Učiteľ zadá podľa potreby štruktúru testu. Podľa nej počítač náhodne generuje úlohy. Študent sa musí ku každému tvrdeniu vyjadriť. K dispozícii má tri možnosti, označiť výrok ako pravdivý, nepravdivý, alebo priznať, že nevie. V priebehu testu je študent priebežne oboznamovaný s parciálnymi výsledkami, aj s konečným hodnotením.

Z niekoľkoročných skúseností možno uviesť medzi **výhody** tohto testovania:

- ⊞ vytvorenie rovnakých podmienok pre všetkých študentov,
- ⊞ možnosť využitia variability testov, čo eliminuje opisovanie študentov a núti ich samostatne pracovať,
- ⊞ umožnenie pracovať študentovi vlastným tempom a ponúknuť mu okamžitú spätnú kontrolu,
- ⊞ preukázateľná snaha čo najlepšie uspieť medzi spolužiakmi pôsobí výrazne motivačne,
- ⊞ učiteľ šetrí čas, neopravuje písomky (aj keď na druhej strane v mnohých prípadoch čas potrebný na tvorbu jednoznačných, vyvážených, zmysluplných testov je dlhší, ako prípadné opravovanie).

Nevýhody takéhoto overovania vedomostí sú:

- ⊞ tipovanie odpovedí,
- ⊞ **absencia kontroly logických postupov riešenia úloh a diagnostika prípadných chýb, ktorých sa študent mohol dopustiť.**

V snahe eliminovať uvedené nevýhody, ale zároveň využiť množstvo cielene vytvorených úloh, boli niektoré súbory úloh dané k dispozícii študentom aj s kódmi správnych odpovedí, súbežne s inicializovanými testmi na disketách. Študentovi sa umožnilo odpovedať nielen na náhodne vybrané, ale priebežne na všetky otázky, ktoré základný súbor úloh obsahuje. Na základe pozitívnych skúseností sa tak testy stali súčasťou vzdelávacieho procesu študentov. Aktuálnu podobu práce študentov s testmi možno zhrnúť do nasledujúcich bodov:

1. zásobníky úloh nielen s kódmi odpovedí, ale aj s kľúčom správnych odpovedí sú dostupné na sieti, takže každý študent má k nim prístup,

- ak zväži, že danú problematiku zvládol, má možnosť sa sám otestovať. Na disketách sú nainicializované testy z jednotlivých tematických okruhov, ale aj dlhšie trvajúce testy z veľkovej semestrálnej látky, učiva ktoré treba k zápočtom zvládnuť,
- počítač test vyhodnotí po každej položke a urobí aj záverečné hodnotenie, študent má okamžitú spätnú väzbu o zvládnutí učiva. Teda bez stresu má možnosť sám zhodnotiť svoje znalosti, odhaliť prípadné nevedomosti, ktoré má následne možnosť konzultovať s učiteľom.

Pri takejto forme testovania sa tipovanie do značnej miery eliminuje a študent v prípade, že má záujem učivu porozumieť, zameria sa na riešenie úloh, ktoré v teste nezvládol.

2. Porovnanie výsledkov z dvoch odlišných hodnotení študentov

V pokračujúcej snahe hľadať optimálnu formu diagnostiky vedomostí študentov konkrétnych predmetov, teda formu, ktorá by v sebe spájala výhody klasického hodnotenia klasického písomného testu a vytvárala rovnaké, spravodlivé podmienky pre všetkých študentov, sme podrobili študentov nasledujúcemu experimentu.

Študentovi bol zadaný najprv klasický písomný test so šiestimi úlohami. To znamená test, pri opravovaní ktorého učiteľ berie do úvahy aj postup riešenia, čo je jeden z najdôležitejších a najsilnejších momentov obligátneho opravovania písomných prác, nielen správny, resp. nesprávny výsledok. Po uplynutí času potrebného na výpočet dostal študent to isté zadanie, ale vo forme testu, označme ho ako *test B*, v ktorom mal ponúknutých päť možných výsledkov danej úlohy, z ktorých bol vždy iba jeden správny. Na základe predchádzajúceho riešenia úloh, bez možnosti čokoľvek v ňom už meniť, vyznačil odpovede v *teste B*, ktoré považoval za správne. Tým vznikla možnosť porovnať výsledky vedomostí študentov z testu A vyhodnoteného učiteľom a *testu B* pomocou počítača. Tento postup bol odskúšaný v dvoch predmetoch, matematika A a teória pravdepodobnosti. Na ilustráciu sú ukážky testových úloh a niekoľko čísiel.

Ukážka 1. Úloha je z testu z predmetu teória pravdepodobnosti, ktorý obsahoval 6 úloh, s bodovým ohodnotením 15 bodov v klasickej forme, *Test A* a vo forme testu s možnosťou výberu správnej odpovede *Test B*.

Test A

- Z 25 žiaroviek, z ktorých je desať 100W, osem 60W a sedem 40W, náhodne vyberieme tri. Určite pravdepodobnosť, že z troch vybraných žiaroviek bez vrátenia nebudú všetky rovnakého výkonu. 3b

Test B

- Z 25-tich žiaroviek, z ktorých je desať 100W, osem 60W a sedem 40W náhodne vyberieme tri. Pravdepodobnosť, že nebudú všetky rovnakého výkonu, ak sa jedná o výber bez vrátenia je

A. $1 - \frac{V_3(10) + V_3(8) + V_3(7)}{V_3(25)}$

B. $\frac{3!}{25 \cdot 24 \cdot 23} (10 \cdot 9 \cdot 8 + 8 \cdot 7 \cdot 6 + 7 \cdot 6 \cdot 5)$

C. $1 - \frac{C_3(10) \cdot C_3(8) \cdot C_3(7)}{C_3(25)}$

D. $1 - \frac{1}{25 \cdot 24 \cdot 23} (10 \cdot 9 \cdot 8 + 8 \cdot 7 \cdot 6 + 7 \cdot 6 \cdot 5)$

E. $\left(\frac{10}{25}\right)^3 + \left(\frac{8}{25}\right)^3 + \left(\frac{7}{25}\right)^3$

3b

Testovaných bolo 137 študentov, test číslo 4, z ktorého je ukážka, absolvovalo 61 študentov. Porovnanie výsledkov hodnotenia konkrétnej úlohy dvomi spôsobmi uvádza tabuľka 1.

Tabuľka 1

Počet študentov	0	20	18	2	2	4	4	11
Body z testu A	0	1	2	3	0	1	2	3
Body z testu B	0	0	0	0	3	3	3	3
$ \Delta $	0	1	2	3	3	2	1	0

Uvedené $|\Delta|$ v poslednom riadku tab. 1 vyjadruje absolútny rozdiel bodov, ktorý je zapríčinený:

- bodmi, ktoré získa študent za parciálne riešenie v *Teste A*
- odpoveďou na otázku, aj keď nepozná riešenie v *Teste B*
- nevenovanie sa dostatočnému zváženie všetkých ponúknutých možných výsledkov v *Teste B*
- aj keď nemá celkové správne riešenie, na základe svojich vedomostí určí v *Teste B* správnu odpoveď.

Ukážka 2. Jedna z úloh testu z predmetu teórie pravdepodobnosti (6 úloh, 15 bodov) v klasickej forme a vo forme testu s možnosťou výberu správnej odpovede.

Test A

4. Nech distribučná funkcia náhodnej premennej X je daná vzťahom $F(x) = \begin{cases} 0 & x \leq 0 \\ 0,2 & x \in (0; 2) \\ c & x \in (2; 4) \\ 1 & x > 4 \end{cases}$,

$P(X = 2) = 0,4$. Určte konštantu c .

2b

Test B

4. Nech distribučná funkcia náhodnej premennej X má tvar $F(x) = \begin{cases} 0 & x \leq 0 \\ 0,2 & x \in (0; 2) \\ c & x \in (2; 4) \\ 1 & x > 4 \end{cases}$ a platí

$P(X = 2) = 0,4$. Konštantu c sa rovná

A. $c = 0,8$ B. $c = 0,6$ C. $c = 0,4$ D. $c = 0,2$ E. c je ľubovoľné číslo z intervalu $(0, 2; 1)$

2b

Test číslo 4 absolvovalo 61 študentov zo 137.

Tabuľka 2

Počet študentov	4	11	1	3	5	37
Body z testu A	0	1	2	0	1	2
Body z testu B	0	0	0	2	2	2
$ \Delta $	0	1	2	2	1	0

V ukážkach 1 a 2 sa typ úlohy aj počet možných získaných bodov za jej správne riešenie líši, čo sa premieta do hodnôt uvedených v tabuľke 2.

Ukážka 3. Jedna z úloh testu z predmetu matematika (6 úloh, 30 bodov) v klasickej forme a vo forme testu s možnosťou výberu správnej odpovede.

Test A

1. Určte definičný obor funkcie

$$f : y = \frac{5}{\sqrt{\log(x+5)}} + \sqrt{-(x^2 + x - 20)} \quad 5b$$

Test B

1. Definičný obor funkcie $f : y = \frac{5}{\sqrt{\log(x+5)}} + \sqrt{-(x^2 + x - 20)}$ je

A. $D(f) = \langle -4; 4 \rangle$ B. $D(f) = \langle -5; 4 \rangle$ C. $D(f) = \langle -4; 5 \rangle$ D. $D(f) = \langle -4; 4 \rangle$

E. $D(f) = \langle -5; 4 \rangle$ 5b

Úloha je z testu číslo 101, ktorý absolvovalo 118 študentov, výsledky hodnotenia uvádza tabuľka 3

Počet študentov	4	11	15	31	9	2	4	7	0	3	4	28
Body z testu A	0	1	2	3	4	5	0	1	2	3	4	5
Body z testu B	0	0	0	0	0	0	5	5	5	5	5	5
$ \Delta $	0	1	2	3	4	5	5	4	3	2	1	0

Rozdiely bodov v hodnotení klasickým spôsobom a vyhodnotením počítačom v tomto prípade rastú s počtom možných získaných bodov. Inak povedané, čím je vyššie ohodnotenie náročnosti riešenia úlohy, tým sa rozdiel medzi dvoma spôsobmi hodnotenia zväčšuje. V uvedenom prípade je priemerný získaný počet bodov zo zadanej úlohy

$$\bar{x}_{testA} = 2,98, \quad \bar{x}_{testB} = 1,88$$

V prípade, že úlohy testu A pretransformujeme do podoby nasledujúceho testu C tak, že parciálna operácia, úkon, úvaha potrebná k riešeniu konkrétneho príkladu, ktorej učiteľ priradí konkrétny počet bodov v teste A, sa v teste C objaví ako samostatná úloha. Tým docielime priblíženie obidvoch hodnotení. Nasledujúca ukážka je z testov, ktoré boli vytvorené na základe získaných a vyhodnotených výsledkov z testov typu B.

Ukážka 4. Úloha z testu z predmetu matematika (6 úloh, 30 bodov) v klasickej forme a vo forme testu s možnosťou výberu správnej odpovede (20 úloh, 30 bodov).

Test A

1. Určte definičný obor funkcie

$$f : y = \frac{5}{\sqrt{\log(x+5)}} + \sqrt{-(x^2 + x - 20)}$$
5b

Test C

1.1. Definičný obor funkcie $g : y = \frac{5}{\sqrt{\log(x+5)}}$ je

- A. $D(g) = (-\infty; -5)$ B. $D(g) = (-\infty; -4)$ C. $D(g) = (-4; \infty)$ D. $D(g) = (-5; \infty)$

- E. $D(g) = (-5; -4) \cup (-4; \infty)$ 2b

1.2. Definičný obor funkcie $h : y = \sqrt{-(x^2 + x - 20)}$ je

- A. $D(g) = (-\infty; -5) \cup (4; \infty)$ B. $D(g) = (-5; 4)$ C. $D(g) = \langle -5; 4 \rangle$

- D. $D(g) = \langle -4; 5 \rangle$ E. $D(g) = (-\infty; -5) \cup \langle 4; \infty \rangle$ 2b

1.3. Definičný obor funkcie $f : y = \frac{5}{\sqrt{\log(x+5)}} + \sqrt{-(x^2 + x - 20)}$ je

- A. $D(f) = \langle -4; 4 \rangle$ B. $D(f) = (-5; -4)$ C. $D(f) = \langle -4; 5 \rangle$ D. $D(f) = (-4; 4 \rangle$ E. $D(f) = (-5; 4 \rangle$

1b

Úloha je z testu číslo 101, ktorý absolvovalo 129 študentov. Pre porovnanie výsledkov z testu B a testu C sú v tabuľke 4 uvedené výsledky z náhodne vybraných 118 testov.

Tabuľka 4

Počet študentov	2	7	6	7	2	0	0	1	0	3	2	0
Body z testu A	0	1	2	3	4	5	0	1	2	3	4	5
Body z testu C	0	0	0	0	0	0	1	1	1	1	1	1
$ \Delta $	0	1	2	3	4	5	5	0	1	2	3	4

Počet študentov	2	5	11	15	3	0	1	0	0	6	4	4
Body z testu A	0	1	2	3	4	5	0	1	2	3	4	5
Body z testu C	2	2	2	2	2	2	3	3	3	3	3	3
$ \Delta $	2	1	0	1	2	3	3	2	1	0	1	2

Počet študentov	0	1	4	1	4	3	0	0	1	0	1	21
Body z testu A	0	1	2	3	4	5	0	1	2	3	4	5
Body z testu C	4	4	4	4	4	4	5	5	5	5	5	5
$ \Delta $	4	3	2	1	0	1	5	4	3	2	1	0

Porovnaním výsledkov v tab. 3 a 4 dôjdeme k záveru, že priemerný počet bodov z uvedeného príkladu *testu C* sa približuje k priemernému počtu bodov získaných v *teste A*, pretože:

$$\bar{x}_{testA} = 3,03, \bar{x}_{testC} = 2,45$$

Záver

Naším cieľom nie je zamerať sa na celkovú štatistiku získaných údajov, ale aj v neľahkých podmienkach, v ktorých sa dnešné školstvo nachádza uviesť námety na zamyslenie, ako hodnotiť veľké množstvo študentov objektívne, so spätnou väzbou, so zreteľom na snahu niektorých študentov akoukoľvek nekalou formou získať zápočet alebo skúšku. V každom prípade obrazom kvality výučby by mali byť vedomosti našich študentov. Za získané vedomosti však nenesie zodpovednosť iba učiteľ. Pokiaľ študent neštuduje, ale skôr sa spolieha na fakt, že niečo opíše, niečo „natipuje“, a tým sa mu podarí stanovené podmienky splniť, učiteľ nemôže byť so svojou prácou spokojný. Preto sa musí zamerať nielen na výučbu a na motiváciu študentov k systematickému štúdiu, ale musí hľadať také formy „odmeňovania“ študentov, aby študent mal istotu spravodlivých podmienok pre všetkých, ale aj vedomia: chcem vedieť, v horšom prípade musím vedieť, pretože neopíšem.

Ale aj uvedené a odskúšané postupy majú svoje zápory, napr.

- ⊖ tvorba najmä testov *typu C* je náročná na čas,
- ⊖ treba mať k dispozícii pre jednu skupinu viacero vyvážených testov,
- ⊖ pri veľkom počte študentov je efektívne vyhodnotiť testy scannerom, ktorý nemá každý učiteľ k dispozícii.

Z týchto dôvodov je potrebné sa zamyslieť, aké informácie chceme testovaním získať, čo platí vo všeobecnosti, nielen pre predmet matematika. Ale v každom prípade výsledky, ktoré získame pomocou počítačového vyhodnotenia testu, v plnom rozsahu nenahradia klasickú formu hodnotenia vedomostí učiteľom.

RNDr. Galina HORÁKOVÁ, CSc.

Mgr. Vladimír MUCHA

RNDr. Anna STAREČKOVÁ, PhD.

Katedra matematiky, FHI EU v Bratislave

E-mail: horakova@euba.sk

E-mail: mucha@euba.sk

Literatúra

MAZÁK, E.: Počítačové řízení a podpora výuky. ČTUT, Praha, 1997.

HORÁKOVÁ, G., STAREČKOVÁ, A.: Motivácia študentov k zodpovednejšiemu prístupu ku štúdiu. ALMA Mater, roč. 6, 1996, Praha.

Resume

The aim of the paper is to compare results from testing the students by the multiple choice test with the assessment of students by their teacher.

PREDSTAVY ŠTUDENTOV O VYUŽÍVANÍ INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLOGIÍ VO VYUČOVANÍ BIOLÓGIE

Úvod

V súčasnej dobe prechádza vzdelávanie mohutným rozvojom. Do popredia sa dostávajú nové technológie, ktoré vytlačujú také prostriedky ako spätný projektor, diaprojektor, prípadne aj epiprojektor. Používanie informačných a komunikačných technológií (IKT) je do veľkej miery ovplyvnené aj osobou učiteľa. Záleží tu na jeho schopnostiach pracovať s IKT, ale aj na tom, či je ochotný sa učiť s nimi pracovať alebo nie. IKT majú významný vplyv na vzdelávanie. OSBORNE a HENNESSY [6] napísali, že IKT zdokonaľujú účinnosť prezentovania informácií a takisto stimulujú záujem študentov o vyučovanie s použitím IKT. Podobne aj SELINGER [8] tvrdí, že IKT môžu zlepšiť kvalitu vzdelávania, pretože obsah multimédií pomáha ilustrovať a vysvetliť náročné pojmy spôsobmi, ktoré boli predtým nedostupné prostredníctvom zdrojov tradičného vzdelávania a metód. Potencionálne výhody použitia IKT vo vyučovaní sú nesmierne veľké. Nie sú len prílohou alebo doplnkom učiteľovej prípravy, ale tiež ponúkajú neohraničený prístup k poznatkom a informáciám, ktorý je dostupný vďaka internetu [2].

Metodika

V našom výskume sme ako výskumný nástroj používali dotazník. Pre tento druh výskumného nástroja sme sa rozhodli preto, lebo ide o hromadné získavanie údajov. Po vytvorení dotazníka a pred jeho odoslaním do škôl sme ho dali ohodnotiť, určiť vhodnosť a reliabilitu kompetentom, ktorí sa zaoberajú konštrukciou, používaním a hodnotením dotazníkov. Po určení vhodnosti dotazníka sme ho odoslali do škôl. Dotazník nebol zameraný len jeden problém, ale na viac, ako napríklad záujem o biológiu s používaním IKT, využívanie IKT na vyučovacej hodine, vzťah študentov k IKT, zmeny používania IKT na školách.... Z toho dôvodu boli použité aj rôzne položky v dotazníku – škálované, otvorené, uzavreté, polootvorené. Spolu sa nám vrátilo 270 vyplnených dotazníkov z deviatich gymnázií. Bol zastúpený 1. až 4. ročník. Dotazníky študenti vyplnili v priebehu troch mesiacov (apríl, máj, jún) v roku 2005. Zastúpené boli 4 kraje Slovenska – Žilinský, Banskobystrický, Trenčiansky a Bratislavský. Dotazníky sme štatisticky vyhodnocovali pomocou programu MS Excel.

Výsledky

Rozbor niektorých položiek dotazníka

V našom príspevku by sme chceli rozobrať niektoré položky z nášho dotazníka, ktoré súvisia s predstavami študentov o využívaní IKT na vyučovaní biológie, takisto, aké zmeny by navrhli vo využívaní IKT na ich škole. Zaujímalo nás, aj to, aké výhody a nevýhody má podľa študentov používanie IKT.

V jednej z položiek sme chceli od študentov vedieť, aké zmeny by navrhli vo využívaní IKT na ich škole. Očakávali sme väčšiu kreativitu žiakov, ale študentmi navrhnuté zmeny sa dali zhrnúť do siedmich kategórií, ako je uvedené v tabuľke 1. Viac ako tretina študentov napísala, že by chceli vôbec používať IKT, druhou najčastejšie uvádzanou odpoveďou bolo, že študenti chceli častejšie používať IKT na vyučovaní biológie. Na otázku neodpovedalo 8,52 % respondentov. Spokojných so súčasnou situáciou bolo 11,85 % opýtaných. Do kategórie „iné“ sme zaradili zaujímavé odpovede napr.:

„Každému jednotkárovi dať notebook.“

„Kamera pri pôrode.“

„Biológia sa mi páči aj bez IKT.“

Chceli sme ešte zistiť, či existuje štatisticky významný rozdiel medzi pohlaviami v jednotlivých možnostiach, ale výsledky Chí – kvadrát testu neukázali štatisticky významný rozdiel (tab. 1).

Tabuľka 1 Percentuálne zastúpenie odpovedí na otázku: „Aké zmeny by si navrhol vo využívaní IKT na Tvojej škole“.

Navrhnuté zmeny vo využívaní IKT	Percentuálne zastúpenie
používať IKT	36,30 %
častejšie používať IKT	20,37 %
vybaviť a obnoviť triedy IKT	10,00 %
projektové vyučovanie	5,56 %
žiadne	11,85 %
iné	7,78 %
neodpovedal	8,52 %

Ďalšou otázkou sme chceli od študentov, aby napísali čo najviac možností využitia IKT v rámci vyučovania biológie. Ich odpovede sme zhrnuli do kategórií, ktoré uvádzame v tabuľke 2. Tretina študentov uviedla, že na vysvetľovanie učiva biológie. Oproti predchádzajúcej otázke, v tejto neodpovedala až takmer pätina študentov. Použitím Chí – kvadrát testu sme zistili, že chlapci uvádzali (oproti dievčatám) vo väčšej miere využitie IKT „na všetko“. Zo zaujímavých odpovedí bola napr.:

„To je na profesorovi, ja sa dokážem prispôbiť.“

Tabuľka 2: Výsledky χ^2 - testu pri zisťovaní závislosti medzi pohlaviami v jednotlivých položkách otázky dotazníka: „Podľa Teba, na čo všetko sa dá použiť IKT v rámci vyučovania biológie“ a ich percentuálne zastúpenie

Možné využitie IKT	Chí kvadrát	Percentuálne zastúpenie
preverovanie	0,6595	14,07 %
motivácia	1,2118	9,26 %
vysvetľovanie	0,0265	34,44 %
na všetko	6,9286**	16,30 %
animácie	0,0211	3,33 %
zhrnutie	0,2192	4,81 %
iné	0,0079	5,56 %
neodpovedal	0,2439	19,26 %

** štatisticky významný rozdiel na hladine významnosti $p > 0,001$.

V nasledujúcich dvoch položkách dotazníka sme chceli, aby nám študenti uviedli, čo najviac výhod a nevýhod využívania IKT. Uvádzajú ich tabuľky 3 a 4. Pri výhodách sme zistili štatisticky významné rozdiely pri odpovedi „prístup na internet“ v prospech chlapcov a v prospech dievčat pri odpovediach: „vyššia vzdelanosť“, „predstavivosť“ a „priblíženie učiva“.

Pri nevýhodách sme takisto zistili štatisticky významné rozdiely. V prospech chlapcov to bolo pri odpovediach „spotreba energie“ a „vysoká cena“. A pri dievčatách to bolo pri odpovedi „neodpovedal“. To znamená, že chlapci mali tendenciu odpovedať na nami položenú otázku.

Tabuľka 3 Výsledky χ^2 - testu pri zisťovaní závislosti medzi pohlaviami v jednotlivých položkách otázky dotazníka: „Aké sú podľa Teba výhody používania IKT“ a ich percentuálne zastúpenie

Výhody	Chí kvadrát	Percentuálne zastúpenie
videnie neviditeľného	0,016	0,74 %
porozumenie	0,8358	2,59 %
zapamätanie	0,396	4,44 %
prístup na internet	4,8524*	1,48 %
zaujímavejšia hodina	0,2771	5,93 %
pochopenie	0,2285	11,85 %
spoznávanie	1,996	0,37 %
zvyšovanie záujmu	0,2157	2,96 %
rozvoj samostatnosti	2,4801	0,74 %
spestrenie hodiny	0,2157	0,37 %
zjednodušenie	0,5451	1,11 %
prístup k info	0,728	19,63 %
názornosť	0,5451	1,11 %
komunikácia	0,0657	2,96 %
spolupráca	1,9396	2,59 %
spätná väzba	0,2157	0,37 %
vylúčenie nebezpečných situácií	0,2157	0,37 %
motivácia	0,5451	1,11 %
vizualizácia	0,0079	5,56 %
simulácia	2,4801	0,74 %
pozorovanie pitiev	2,4801	0,74 %
interaktívnosť	0,1827	1,11 %
zdokonalenie v práci s PC	0,2157	0,37 %
zlepšenie v cudzom jazyku	2,5618	4,44 %
menšia prašnosť	0,0323	1,48 %
urýchlenie dejov	2,4801	0,74 %
vyššia vzdelanosť	5,1345*	2,22 %
predstavivosť	11,4271***	4,81 %
priblíženie učiva	5,1345*	2,22 %
doplnenie	3,3973	1,48 %
samohodnotenie	0,8398	0,37 %
väčší prehľad	2,5384	1,11 %
iné	0,0634	1,85 %
žiadne	2,5384	1,11 %
neodpovedal	0,4353	19,63 %

* štatisticky významný rozdiel na hladine významnosti $p > 0,01$.

*** štatisticky významný rozdiel na hladine významnosti $p < 0,001$.

Tabuľka 4: Výsledky χ^2 -testu pri zisťovaní závislosti medzi pohlaviami v jednotlivých položkách otázky dotazníka: „Aké sú podľa Teba nevýhody používania IKT“ a ich percentuálne zastúpenie

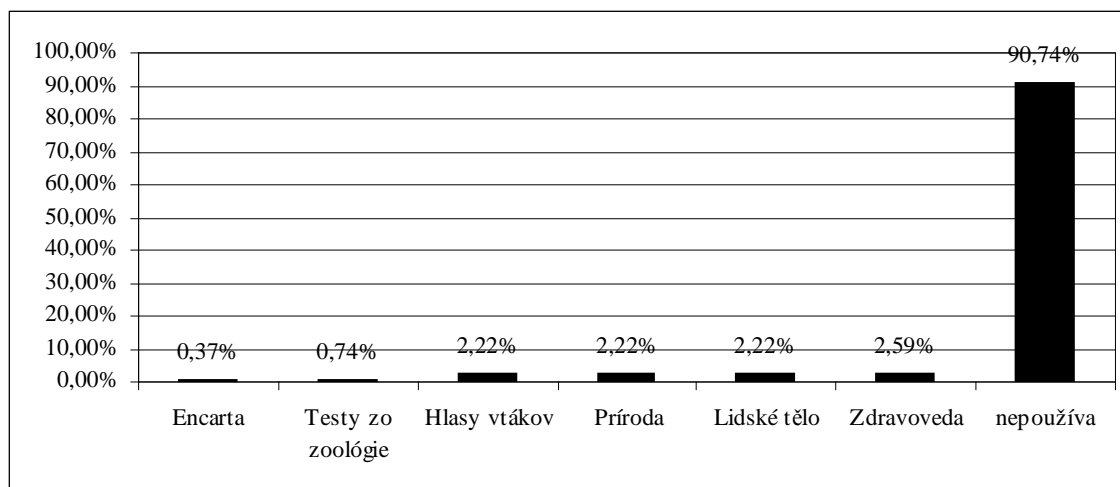
Nevýhody	Chí kvadrát	Percentuálne zastúpenie
nezaškolení učitelia	0,0165	6,30 %
slabý softvér	0,2157	2,96 %
zastaralé vybavenie	0,0827	3,70 %
pomalý internet	2,4081	0,74 %
spotreba energie	8,5884**	2,59 %
nedostupnosť pre všetkých	0,0224	5,93 %
náročné pracovanie	0,2157	0,37 %
častá údržba	3,5309	2,22 %
čas	2,5532	7,04 %
vysoká cena	6,5754**	17,78 %
strata medziľudskej komunikácie	0,3696	2,22 %
objemnosť	0,6517	1,48 %
zhoršenie zdravia	0,0657	2,96 %
info v cudzom jazyku	0,2157	0,37 %
iné	2,0437	3,33 %
závislosť	0,8398	0,37 %
žiadne nie sú	0,4353	19,63 %
neodpovedal	5,6954*	27,41 %

* štatisticky významný rozdiel na hladine významnosti $p > 0,01$.

** štatisticky významný rozdiel na hladine významnosti $p > 0,001$.

Zaujímalo nás aj to, či študenti využívajú na hodinách biológie softvér s biologickou tematikou. Preto v ďalšej položke dotazníka sme chceli zistiť v akej miere a ktoré edukačné kompaktné disky používajú učitelia na vyučovaní biológie z pohľadu žiakov. Ako vidíme v grafe 1 dohromady sa používa 6 edukačných diskov na vyučovaní biológie. Ale ich používanie uviedlo len necelých 10 % opýtaných. Ostatní uviedli, že na ich hodinách biológie učiteľ nepoužíva žiadne edukačné CD s biologickou tematikou. Použili sme Chí-kvadrát na zistenie štatistickej závislosti medzi pohlaviami, ale nezistili sme žiadne štatisticky významné rozdiely.

Graf 1: Napíšte, ktorý edukačný softvér s biologickou tematikou používate na vyučovaní biológie



Diskusia

V našom výskume sme zistili, že podľa študentov sa IKT na hodinách využívajú málo. Podobne uvádza aj PATTERSON [7]. Viac ako polovica nami oslovených študentov uviedla, že by chceli využívať na hodinách IKT, resp. viac ich využívať. Môžu to spôsobovať viaceré faktory. Buď učitelia biológie nevyužívajú IKT na svojich hodinách, čo je spôsobené strachom z používania, prípadne to môže byť nedostatočné vybavenie. Niektorí študenti ale uviedli, že miestnosti, v ktorých by mala prebiehať výučba sú neustále obsadené informatikmi. V našom výskume sme zistili veľké množstvo výhod, ktoré poskytujú informačné a komunikačné technológie. Naše výsledky sú porovnateľné so zisteniami napr. s KALAŠOM [3] alebo COX a kol. [1]. V porovnaní s NG a GUNSTONOM [5] sme zistili viaceré nevýhody, ktoré uvádzame vo výsledkovej časti. Spomínaní autori uvádzajú tieto nevýhody: časový faktor, cena, nedostatok zručností, zastaralý softvér, organizácia triedy. Zaujímavé výsledky sme zistili aj pri otázke o využívaní edukačného softvéru. Môžeme súhlasiť s LIKAVSKÝM [4], ktorý uviedol, že jedným z problémov využívania IKT v geografii na vyučovaní je slabý, prípadne žiadny softvér. K tomu nás vedie to, že viac ako 90 % respondentov označilo, nepoužívanie edukačného softvéru na vyučovaní biológie.

Záver

Cieľom nášho príspevku bolo naznačiť predstavy študentov gymnázií o využívaní informačných a komunikačných technológií vo vyučovaní biológie, o tom aké sú podľa nich výhody a nevýhody používania IKT a takisto, či sa na ich školách používa softvér s biologickou problematikou. Naš výskum naznačuje, že v biológii je problém s používaním IKT. Podľa študentov sa IKT využíva slabó prípadne vôbec nie, aj keď má veľa výhod. IKT je určite efektívnym nástrojom pri učení, zapamätávaní a riešení úloh.

Tento príspevok vznikol s podporou grantu KEGA 3/3184/05.

Literatúra

1. COX, M.; WEBB, M.; ABBOTT, C.; BLAKELEY, B.; BEAUCHAMP, T.; RHODES, V.: ICT and Pedagogy: a review of the research literature. Annesley: DfES Publications 2003. Available on http://www.becta.org.uk/page_documents/research/ICT_pedagogy_summary.pdf (2006-08-18).
2. GILMORE, A. M.: Turning teachers on to computers: evaluation of a teacher development program. Journal of Research on computing in education, vol. 27, No. 3, 1995, pp. 251 – 269.
3. KALAŠ, I.: Modely a scenáre používania IKT v školách. In: Sborník Národní konference 2003. Mezinárodní organizační výbor Poškole, 2003, s. 26-38.

4. LIKAVSKÝ, P.: PC GLOBE – Charakteristika a námety na využitie vo vyučovaní geografie. Informatika v škole, č. 7, 1992, s. 36 – 41.
5. NG, W.; GUNSTONE, R.: Students perceptions of the effectiveness of the World Wide Web as a research and teaching tool in science learning. Research in Science Education, vol. 32 No. 4, 2002, pp.1-22.
6. OSBORNE, J.; HENNESSY, S.: Literature Review in Science Education and the Role of ICT: Promise, Problems and Future Directions. Bristol, Nesta FutureLab, 2003. Available on: <http://www.nestafuturelab.org/research/reviews/se01.htm> (2006-06-12).
7. PATTERSON, M. J.: Developing an internet based chemistry class. Journal of Chemical Education, vol. 77 No. 5, 2000, pp. 554-555.
8. SELINGER, M.: Developing and using content in technology enhanced learning environments, 2004. In: I. P. A. Cheong, H. S. Dhindsa, I. J. Kyeleve and O. Chukwu (Eds), Globalisation trends in science, mathematics and technical education (pp. 24 - 37). Universiti Brunei Darussalam: Gadong.

PaedDr. Milan KUBIATKO
Prírodovedecká fakulta UK
Katedra didaktiky prírodných vied, psychológie a pedagogiky

MULTIMEDIÁLNÍ STUDIJNÍ MATERIÁL K VÝUCE JAZYKA PHP

Úvod

Před několika roky jsme si na našem pracovišti kladli otázku zda se zabývat „módními“ e-learningovými multimediálními výukovými aplikacemi. Protože jsme neměli žádné praktické zkušenosti s tvorbou multimediálních e-kurzů, bylo naší první snahou seznámit se s problematikou studiem literatury, účastí na konferencích a analýzou dostupných hotových e-kurzů. Po různých počátečních pokusech s tvorbou a nasazením vlastních e-kurzů do výuky jsme měli možnost se podílet na řešení projektu Leonardo da Vinci II BATCOS (Development & Piloting of Basic On-Line Training Courses). Partnery projektu byly relevantní organizace z České republiky, Německa, Itálie a Velké Británie. V projektu byly vyvinuty vzdělávací materiály pro 33 kurzů, uspořádaných do 4 skupin. Například ve skupině Informační a komunikační technologie v podnikové praxi jsou kurzy Elektronické podnikání nebo Teleworking, ve skupině Výrobní procesy kurz Řízení skladů nebo Softwarové systémy pro řízení průmyslových procesů. Vyvinuté vzdělávací materiály jsou v angličtině, češtině, němčině a italštině. Obsah vytvořených kurzů a ukázky z CD verze lze najít na adrese <http://athena.zcu.cz/batcos> pod odkazem DEMO. Při řešení projektu (projekt byl dokončen v roce 2003) jsme nabyli řadu zkušeností, které jsme se snažili dále rozvíjet. V dalším textu budou uvedeny konkrétní příklady kurzu Úvod do PHP.

Struktura a formální uspořádání kurzu

Pro snazší tvorbu e-kurzů je na ZČU v Plzni vyvíjen *ProAuthor*, autorský systém orientovaný především na podporu tvorby obsahových zdrojů on-line kurzů a off-line multimediálních učebnic. Umožňuje generování dat autorských zdrojů ve formátu odpovídajícím standardu SCORM 2004. Výše uvedené e-kurzy byly vytvořeny právě s podporou tohoto nástroje.

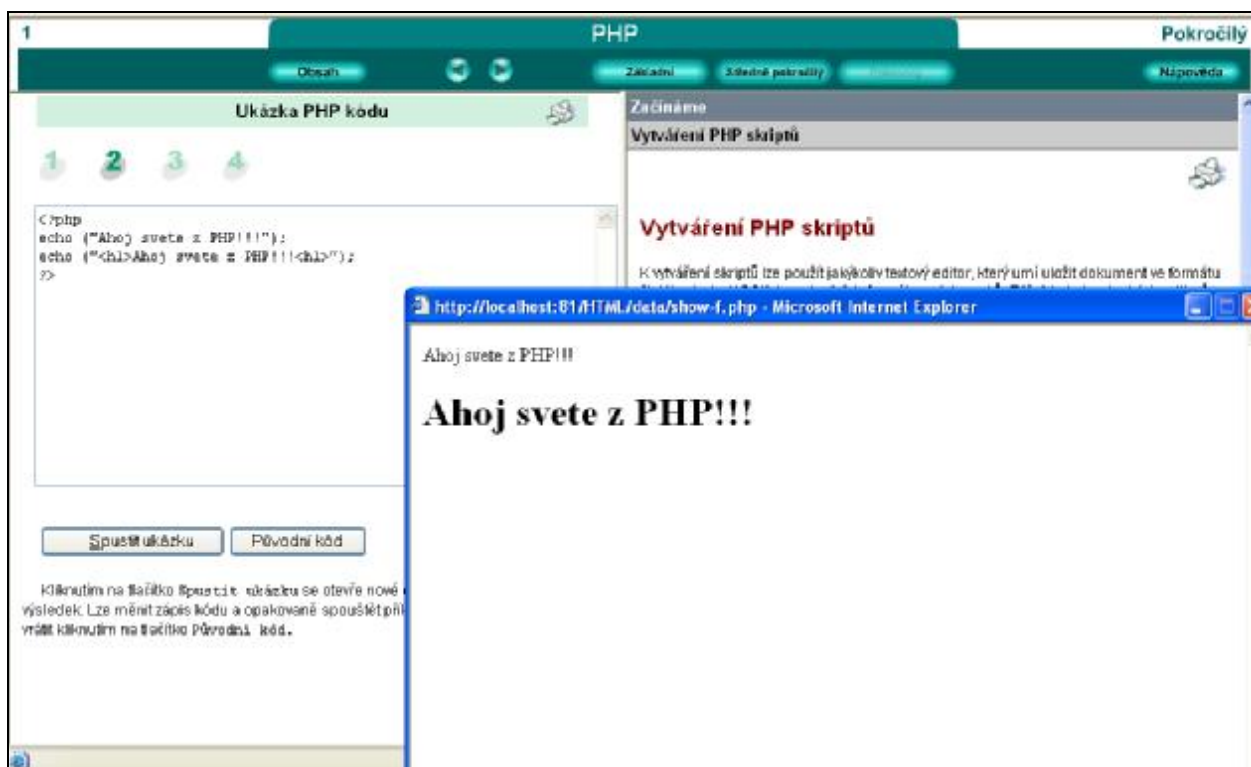
Základ každého e-kurzu je tvořen plánem kurzu. Plán kurzu je časově orientovanou sekvencí jednotlivých studijních kapitol sdružujících v sobě různé typy vzdělávacích aktivit. Základní vzdělávací aktivity jsou studijní článek (prezentace nové látky), úkol (jeho řešení se odesílá lektorovi kurzu k hodnocení), cvičení (jeho řešení se neodesílá lektorovi kurzu k hodnocení, slouží tedy pouze studentovi pro procvičení látky), diskuse, test (jeho řešení se odesílá lektorovi kurzu k hodnocení), autotest (jeho řešení se neodesílá lektorovi kurzu k hodnocení, slouží tedy pouze studentovi pro procvičení látky) a anketa.

Začlenění vhodných ilustračních příkladů k jednotlivým částem prezentované látky posiluje jejich srozumitelnost a názornost. Tímto v sobě obsahuje také výrazný motivační potenciál studia. Uvedením ilustračních příkladů má student možnost přímo sledovat aplikaci prezentované látky na praktické úrovni.

Studijní články kurzů jsou z formálního hlediska zobrazeny ve dvou svislých rámcích v okně prohlížeče (*Microsoft Internet Explorer*). V pravém rámcí je stručný vysvětlující text. V levém rámcí je ilustrace probírané látky obrázky, animacemi, simulacemi...

Kurz Úvod do PHP

Obsahuje základy programování v PHP. Studijní články jsou v levém rámcí ilustrovány obrázky ve formátu *swf* (vektorové) nebo ukázkami programů v PHP. Ukázky lze spouštět, modifikovat a tisknout. Na následující obrázku je uvedena ukázka studijního článku Vytváření PHP skriptů se spuštěnou ukázkou.



Při konfiguraci off-line verze byla snaha udělat ji maximálně jednoduchou a funkční na většině systémů Windows, pokud možno pouze s uživatelskými právy a aby nebylo nutné instalovat do systému jakékoliv programy nebo knihovny. Výsledkem je možnost spouštět kurz nejen z vloženého CD-ROM, ale také jej přímo nakopírovat na disk počítače studenta a spouštět odtud.

Ukázku vytvořeného kurzu lze nalézt na adrese (v ukázce jsou pouze studijní články): <http://www.pef.zcu.cz/pef/kvd/cz/materialy/php/php/php/index.htm>.

Závěr

Cílem příspěvku bylo uvést stručnou charakteristiku kurzu Úvod do PHP, který vznikl s podporou projektu FRVŠ 252/2006. Po zkušenostech s aplikací jiných e-kurzů ve výuce bylo rovněž vytvořeno CD s off-line verzí kurzu pro domácí studium bez nutnosti připojení k internetu (připojení k internetu z domova je obvykle pro studenty drahé). Při konfiguraci off-line verze byla snaha udělat ji maximálně jednoduchou a funkční na většině systémů Windows, pokud možno pouze s uživatelskými právy. Není nutné instalovat do systému jakékoliv programy, nebo knihovny. Použit byl Apache2 a PHP 4.3.4. Výsledkem je možnost spouštět kurz nejen z vloženého CD-ROM, ale také jej nakopírovat na disk počítače studenta a spouštět odtud.

Václav VRBÍK
Katedra výpočetní a didaktické techniky FPE, ZČU v Plzni
vrbik@kvd.zcu.cz

ZVLÁŠTNOSTI VÝPISU REŤAZCA V JAZYKU STROJOVEJ ÚROVNE

V tomto príspevku sa zameriame na zvláštnosti, ktoré sa vyskytnú pri vypisovaní reťazca pomocou programu v jazyku strojovej úrovne. Smerodajná bude vybraná technika výpisu reťazca, ktorú ponúka operačný systém svojimi funkciami či službami. Výsledky porovnáme a zhodnotíme.

Úvod

Zobrazovanie reťazcov sa dá veľmi dobre porovnať so zobrazovaním čísel. Je logické, že zobrazovanie čísel by malo trvať o trochu dlhšie. Treba totiž najskôr transformovať číslo na reťazec a ten potom vypísať. Túto skutočnosť potvrdzujú existujúce programy na prevod číselnej hodnoty daného čísla na reťazec cifier v strojovo orientovanom jazyku. Úplne iná situácia je v jazyku C. Je jedno, či vypisujeme číslo:

```
printf("%d ",cislo)
```

alebo vypisujeme reťazec nasledovným spôsobom:

```
printf("%s ",retazec)
```

prípadne takto:

```
printf("abcdeabcde ")
```

Zakaždým dostaneme rovnaký čas zobrazenia. Je to trochu prekvapujúci výsledok. Funkcia printf je zrejme naprogramovaná tak, že pracuje rovnako s reťazcami aj s číslami. Preto z tohoto pohľadu nemá zmysel hovoriť zvlášť o zobrazovaní reťazcov a zobrazovaní čísel v jazyku C. Nasledovné kapitoly sa budú zaoberať iba výpisom reťazcov programom v strojovo orientovanom jazyku (SOJ alebo ASM - hovorovo assembler) a to dvomi spôsobmi: pomocou služby, resp. funkcie operačného systému na výpis reťazca a pomocou služby, resp. funkcie operačného systému na výpis jednotlivých znakov v cykle.

Počet opakovaní jednotlivých testov sme zvolili 10, pre viacero behov (55555, 40000, 31765, 20000-krát).

Zobrazovanie reťazca v SOJ po znakoch v cykle

Nasledujúci kód ukazuje príklad 40000-násobného výpisu reťazca uloženého v pamäti na adrese test.

Kód je jednoduchý. Vnútorý cyklus CYK2 testuje znaky reťazca a pokiaľ nenarazí na koncový znak \$ pokračuje vo vypisovaní na obrazovku po jednom znaku funkciou číslo 2 operačného systému. Vonkajší cyklus CYK1 zabezpečí daný počet opakovaní.

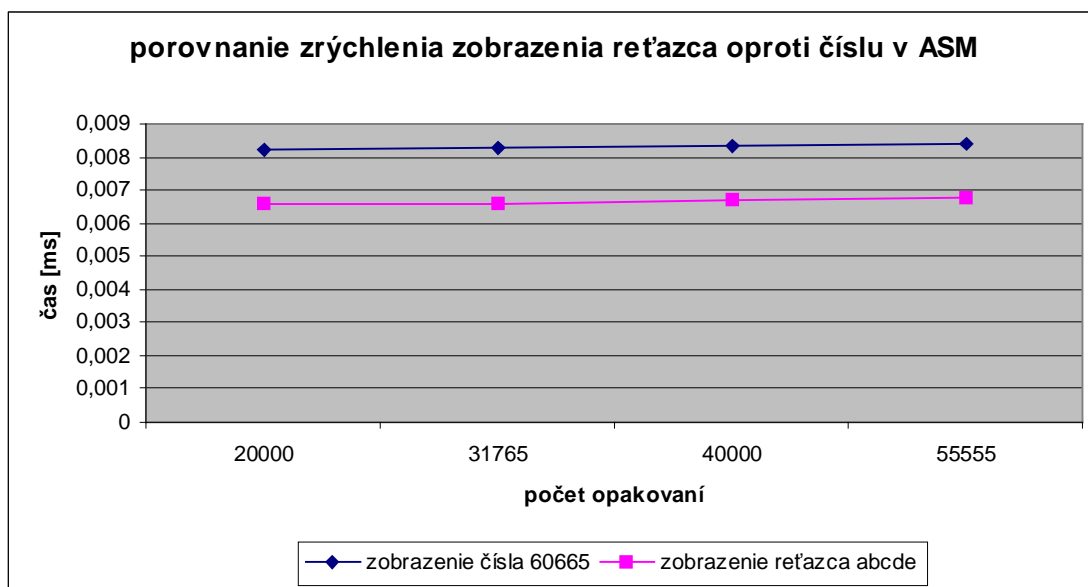
```
mov cx, 40000
CYK1:
mov si, offset test
CYK2:
mov dl, [si]
cmp dl, '$'
je dalej
mov ah, 2
int 21h
inc si
jmp CYK2
dalej:
loop CYK1
```

Zobrazovanie reťazca "abcde" v SOJ pomocou cyklu

	55555-krát	40000-krát	31765-krát	20000-krát
	1,868131868	1,373626374	1,043956044	0,659340659
	1,868131868	1,373626374	1,043956044	0,659340659
	1,868131868	1,373626374	1,043956044	0,659340659
	1,868131868	1,373626374	1,043956044	0,659340659
	1,868131868	1,318681319	1,043956044	0,659340659
	1,868131868	1,318681319	1,043956044	0,659340659
	1,923076923	1,318681319	1,043956044	0,659340659
	1,923076923	1,318681319	1,043956044	0,659340659
	1,923076923	1,318681319	1,043956044	0,659340659
priemer	1,884615385	1,346153846	1,043956044	0,659340659
priemer na znak v ms	0,006784683	0,006730769	0,006574859	0,006593407
priemer za všetky behy	0,006670929			

Tento kód vypísal na obrazovku reťazec „abcde“. Pre zaujímavosť sme týmto kódom vypísali aj číslo 60665, ktoré má rovnakú dĺžku (počet číier je 5).

Pre porovnanie je priložený nasledovný graf:



Z grafu je jasne viditeľný rozdiel v rýchlosti zobrazenia čísla a nenumerného reťazca. Znakový reťazec sa spracuje rýchlejšie ako číselný reťazec. Samotné spracovanie cifry čísla trvá približne 0,002 ms.

Pre reťazec o dĺžke 10 znakov vyzerá testovacia tabuľka nasledovne:

Zobrazovanie reťazca abcdeabcde v SOJ pomocou cyklu

	55555-krát	40000-krát	31765-krát	20000-krát
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,692307692	2,142857143	1,318681319
	3,791208791	2,747252747	2,142857143	1,373626374
	3,791208791	2,747252747	2,142857143	1,373626374
	3,791208791	2,747252747	2,142857143	1,373626374
	3,791208791	2,802197802	2,142857143	1,373626374
priemer	3,791208791	2,71978022	2,142857143	1,340659341
priemer na znak v ms	0,006824244	0,006799451	0,006745969	0,006703297
priemer za všetky behy	0,00676824			

Výsledný priemerný čas výpisu jedného znaku sa líši od predchádzajúceho testu iba veľmi minimálne. Všetky znaky sú vypisované rovnakou rýchlosťou.

Zobrazovanie reťazca v SOJ, funkciou na výpis reťazca

Vonkajší cyklus je presne taký istý ako v predchádzajúcom prípade. Vnútorý cyklus odpadá a reťazec sa zobrazuje naraz pomocou DOS služby 9 pri prerušení INT 21h.

```
mov cx, 40000
CYK1:
  mov dx, offset test
  mov ah, 9
  int 21h
  loop CYK1
```

Zobrazovanie reťazca "abcde" v SOJ, pomocou služby 9

	55555-krát	40000-krát	31765-krát	20000-krát
	1,483516484	1,098901099	0,824175824	0,494505495
	1,483516484	1,098901099	0,824175824	0,494505495
	1,483516484	1,098901099	0,824175824	0,494505495
	1,483516484	1,098901099	0,824175824	0,494505495
	1,483516484	1,098901099	0,824175824	0,494505495
	1,483516484	1,098901099	0,824175824	0,549450549
	1,483516484	1,098901099	0,824175824	0,549450549
	1,483516484	1,098901099	0,824175824	0,549450549
	1,483516484	1,098901099	0,879120879	0,549450549
	1,483516484	1,043956044	0,879120879	0,549450549
priemer	1,483516484	1,093406593	0,835164835	0,521978022
priemer na znak v ms	0,005340713	0,005467033	0,005258397	0,00521978
priemer za všetky behy	0,005321481			

Vo vyššie uvedenej tabuľke bol zobrazovaný reťazec „abcde“. V nasledovnej tabuľke pre porovnanie zobrazujeme reťazec, ktorý pozostáva z desiatich znakov:

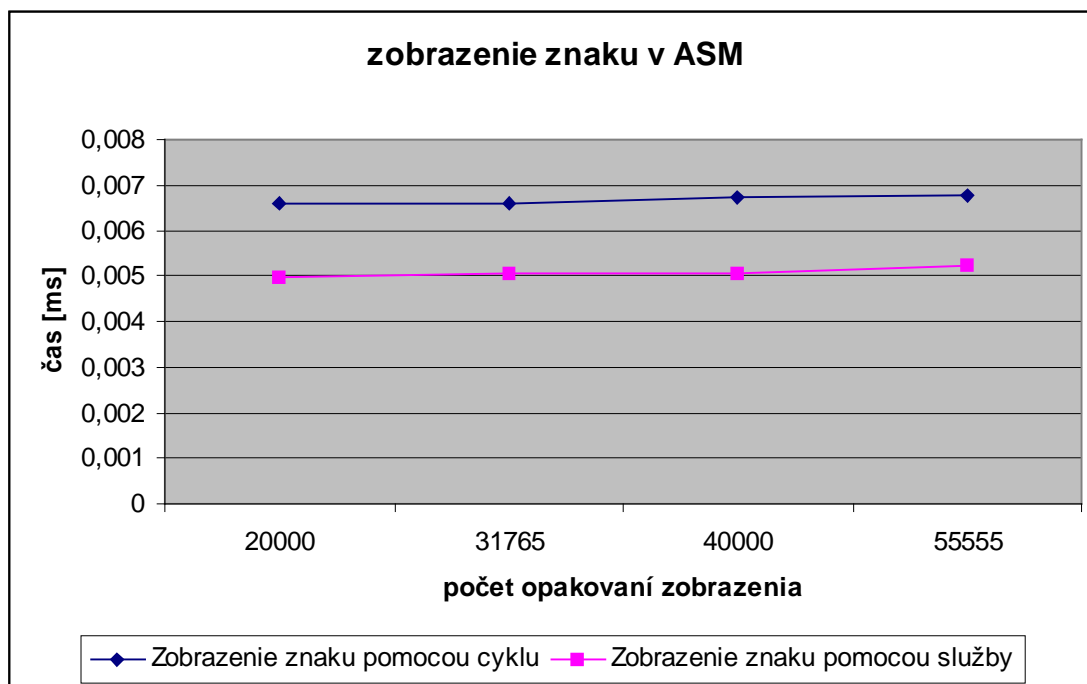
Zobrazovanie reťazca “abcdeabcde” v SOJ, pomocou služby 9

	5555-krát	4000-krát	31765-krát	20000-krát
	2,912087912	1,978021978	1,593406593	0,989010989
	2,912087912	1,978021978	1,593406593	0,989010989
	2,912087912	1,978021978	1,593406593	0,989010989
	2,912087912	1,978021978	1,593406593	0,989010989
	2,912087912	2,032967033	1,593406593	0,989010989
	2,912087912	2,032967033	1,593406593	0,989010989
	2,912087912	2,032967033	1,593406593	0,989010989
	2,912087912	2,087912088	1,593406593	0,989010989
	2,912087912	2,087912088	1,593406593	0,989010989
	2,857142857	2,087912088	1,648351648	0,989010989
priemer	2,906593407	2,027472527	1,598901099	0,989010989
priemer na znak v ms	0,00523192	0,005068681	0,005033531	0,004945055
priemer za všetky behy	0,005069797			

Je zaujímavé priemerné zvýšenie výkonnosti pri zobrazovaní dlhšieho reťazca.

Porovnanie rýchlosti zobrazenia reťazca pomocou funkcie 9 a 2

Na nasledujúcom grafe je viditeľný rozdiel medzi zobrazením reťazca pomocou funkcie či služby 9 na výpis reťazca a pomocou funkcie 2 na výpis znakov reťazca v cykle. Je badateľné, že funkcia 9 na výpis reťazca vychádza z tohoto porovnania víťazne. Je pravdepodobne lepšie optimalizovaná ako výpis znakov v cykle.



Jana PARÍZKOVÁ
Fakulta informatiky a informačných technológií STU Bratislava

POUŽITIE POČÍTAČOV VO VÝUČBE ODBORNÝCH PREDMETOV, ZAMERANÝCH NA SURFING, MODELOVANIE A HYDRODYNAMICKÉ SPRÁVANIE

Abstrakt: Od roku 2002 Edith Cowan Univerzita (ECU) v Západnej Austrálii začala ponúkať trojročné bakalárske štúdium, zamerané na výskum a technológiu v Surfingu (SST - Surf Science and Technology). Je potrebné poznamenať, že v súčasnosti je na svete len jedna podobne orientovaná katedra, a to v Plymouthu v Anglicku. Technické predmety vyučované na SST v ECU sú zamerané na modelovanie, výrobu a testovanie individuálneho surfingového športového zariadenia podľa jednotlivých potrieb študentov. Všetko si to vyžaduje rozsiahle znalosti v hydrodynamike, silách a trení pôsobiacich na surfing, v telesnej zdatnosti/obratnosti športovca (študenta) a štýlu surfovania. Zladiť a optimalizovať všetky tieto veličiny je možné len s použitím počítača a vhodného programu. Keďže pedagogická činnosť na ECU prebieha súbežne s výskumom, spolupracujeme s podnikmi, školami, a firmami výrobného, športového a ekonomického zamerania. Ak toto všetko berieme do úvahy, cieľom článku je informovať pedagógov a výskumníkov o experimentálnom využití počítačov v technologicky zameranej vede, výskume a výučbe v surfingu na vysokoškolskej úrovni.

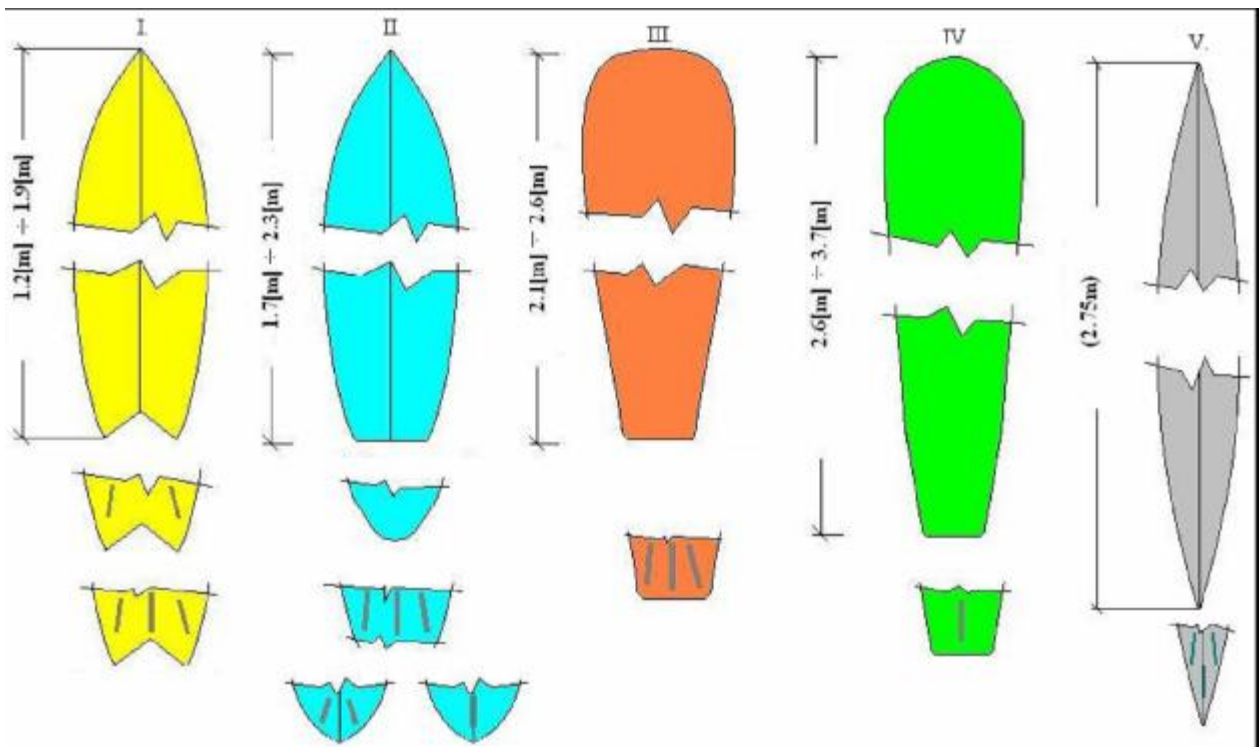
Kľúčové slová: počítačová technika, vysokoškolské vzdelávanie, výučba a výskum, modelovanie, surfing, výroba a testovanie, optimalizácia.

Úvod

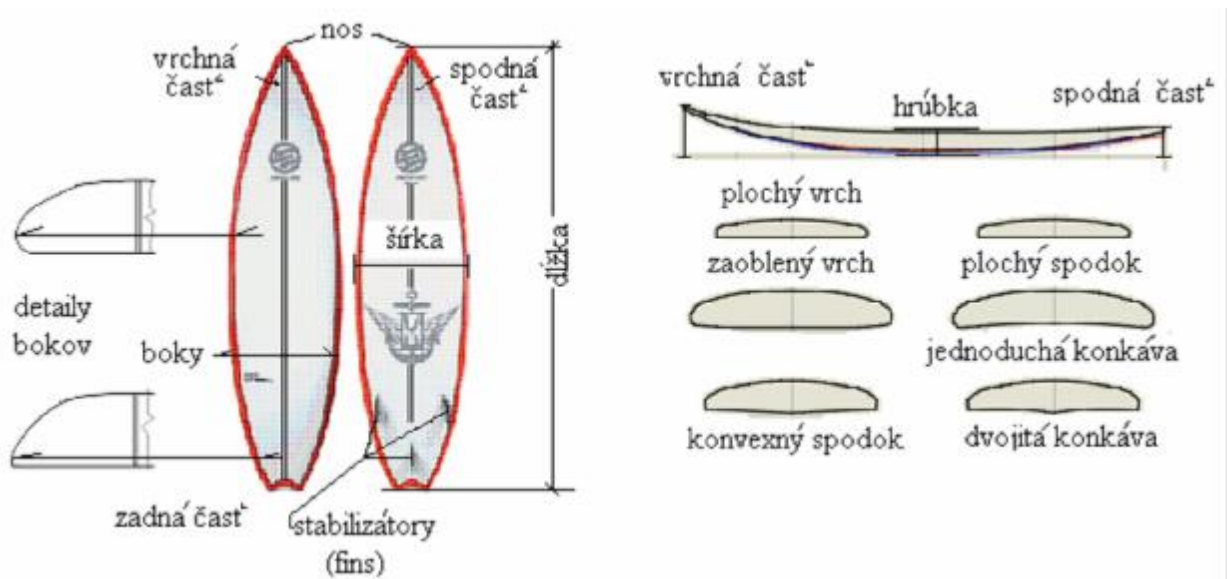
V súčasnej dobe na SST študuje asi šesťdesiat študentov. Popri domácich Austráľčanoch veľkú časť tvoria študenti zo zahraničia – Ameriky, Anglicka a Afriky. Všetci študenti sú aktívni športovci, sústavne hľadajú možnosti zlepšenia surfovacej dosky tak, aby to vyhovovalo ich štýlu a úrovni surfovania. Tradične sa takéto zlepšenia robia cez materiálové a tvarové zmeny dosky. Materiál ovplyvňuje mechanické vlastnosti a životnosť. Tvar má vplyv na stabilitu, nadľahčovanie a manévrovanie. Preto je nevyhnutné nájsť určitú bilanciáciu medzi materiálom a funkčným tvarom a zlepšiť tak ekonomické a úžitkové vlastnosti surfovacej dosky. Súčasný trend vyzerá tak, že „najlepšia“ doska je tá, ktorá „najlepšie spolupracuje“ so surfistom.

Keďže štýl surfovania je u každého odlišný, táto informácia má len malú hodnotu pre výrobcu a užívateľa. Preto je v súčasnosti kompromisom trhová ponuka piatich typov surfovacích dosiek vhodných pre surfovanie na rôzne veľkých vln (pozri obrázok 1).

Typ I surfovacej dosky sa vyrába v dĺžkach od 1,2 do 1,9 metra. Na konci má dva alebo tri stabilizátory (fíny) a všeobecne sa používa pre surfovanie na malých vlnách. Typ II je o niečo väčší. Dĺžkové miery sú od 1,7 do 2,3 metra. Môže mať jeden, dva, alebo tri stabilizátory (fíny) a je vhodný pre dynamické surfovanie na väčších vlnách. Typ III má dĺžku od 2,1 do 2,6 metra. Ukončený je zvyčajne tromi stabilizátormi a je vhodný pre začiatočníkov. Typ IV má dĺžku od 2,6 do 3,7 metra. Je vhodný pre malé vlny, má dobré nadľahčovanie a ľahko sa vesluje. Typ V dosahuje dĺžku cca 3 metre a používa sa na surfovanie veľkých vln. Na obrázku 2 sú hlavné tvarové prvky surfovacej dosky. Z hľadiska tvaru, jej vrchná časť (nos – špicatá časť) kontroluje tok vody okolo bokov, čím ovplyvňuje rýchlosť a trenie. Samotná konštrukcia dosky nadľahčuje športovca a umožňuje mu jazdiť po vlnách vďaka vztlakovej sile pôsobiacej na surfováciu dosku. Zadná časť dosky je vybavená stabilizátormi a umožňuje kontrolovať manévrovanie a stabilitu. Ďalšie tvarové veličiny ovplyvňujúce správanie sa surfovacej dosky vo vode, sú dané priečnym rezom a typom bokov. Priečny prierez môže byť plochý, konkávny, konvexný, alebo kombinovaný všetkými týmito tromi tvarmi a ovplyvňuje vztlakovú silu a trenie. Tvar bokov je pravouhlý na konci dosky pre rýchle uvoľňovanie vody a zaoblený smerom k nosu pre udržiavanie stability. Na obrázku 3 sú fotografie z testovania surfovacej dosky, vyrobenej jedným z ECU SST študentov v roku 2005.



Obrázok 1: Súčasné komerčné surfovacie dosky



Obrázok 2: Hlavné tvarové prvky surfovacej dosky



Obrázok 3: SST (ECU) študent testuje svoju individuálne navrhnutú surfovaciu dosku, vyrobenú počas materiállovej a technologickej výučby v druhom semestri druhého ročníka pod vedením dr. J. AUDYHO.

V nasledujúcich častiach článku sú ukážky z dvoch semestrálnych prác ECU SST študentky druhého ročníka Natalie FRANCIS pod vedením dr. AUDYHO, zamerané na počítačové modelovanie a výrobu surfovacích dosiek a finov.

2. Počítačové modelovanie v technicky a materiálovo orientovaných SST – predmetoch na ECU: ukážky študentských prác

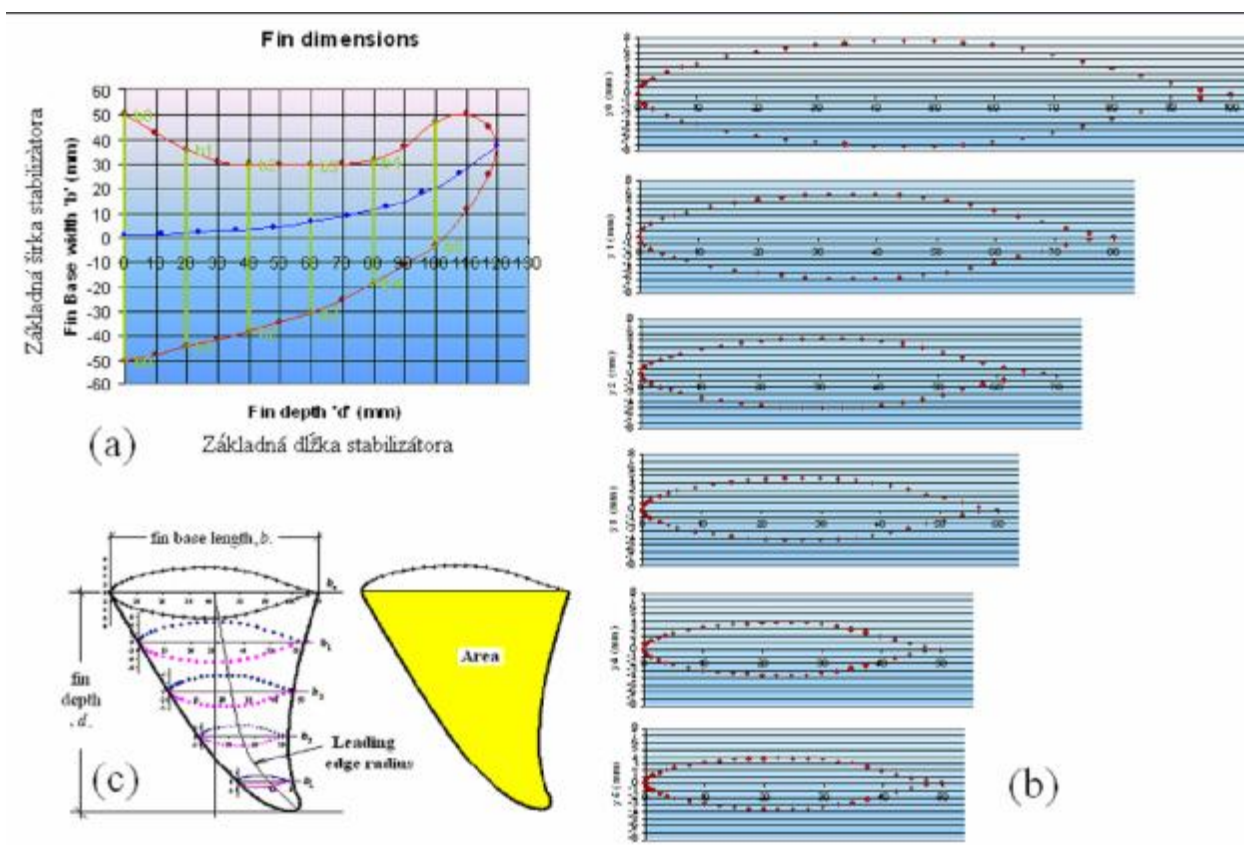
2.1. Stabilizátory (SURFING FINS): Modelovanie a výroba

Tento SST predmet je zaradený v prvom semestri druhého ročníka. Počítačové vybavenie (program a grafika) špeciálne vytvorené pre tieto účely dr. AUDYHO a jeho riešiteľskou skupinou umožňuje úplne počítačové modelovanie a „pracovné“ simulácie stabilizátorov (finov) surovacích dosiek. Študenti majú možnosť použiť CAD/CAM program (computer adaptive drawing and modelling), Excel, vzhľadom na ich skúsenosti a programovaciu/užívaciú zručnosť.

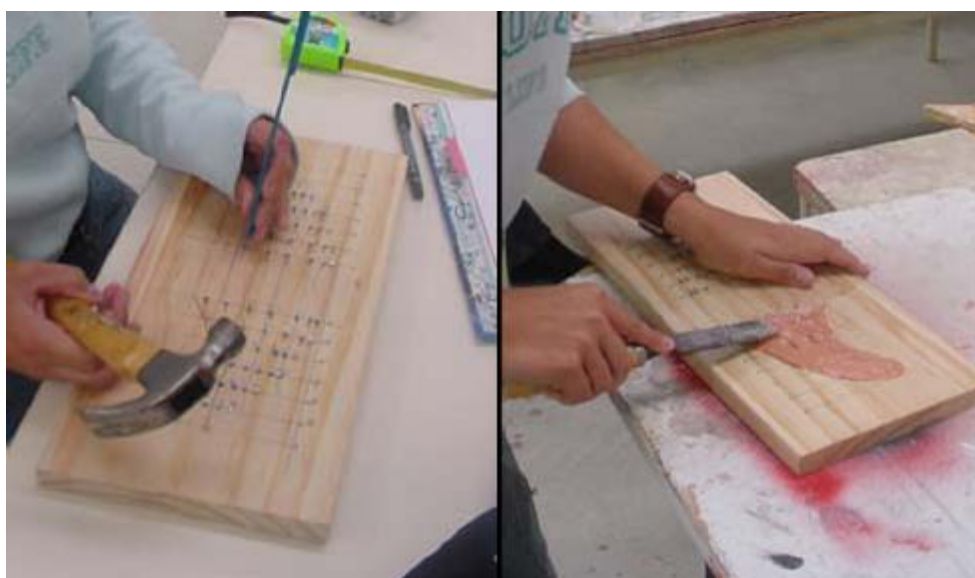
Programy umožňujú úplne optimalizovať tvar stabilizátorov, predpovedať spôsob obtekania vody okolo ich povrchu, a vyrátať tlakové a trecie sily. Princíp programovania, spolu s výsledkami programového modelovania a testov boli prezentované na konferenciách v Maroku (2006 a 2005) a v Thajsku (2004) a publikované v literatúre 1, 2 a 3, preto nie sú popisované v tomto článku. Ukážky dole sú vybrané z práce študentky Natalie FRANCIS, ktorá navrhovala a testovala svoj stabilizátor (fin) pomocou Excelu, podporeného databázou založenou na experimentálnych výskumoch NASA pre vztlakové sily, použitím metódy popísanej v literatúre 1, 2 a 3. Táto optimalizačná metóda navrhnutá AUDYM a jeho skupinou je založená na určení základnej šírky a dĺžky stabilizátora pre laminárny obtok vody (Reynoldove číslo $R=105$) a pre „maximálne možnú“ vztlakovú silu a „minimálne možné“ trenie (aspektový pomer A medzi 1 a 2), pozri literatúru 1, 2 a 3. Šírkové rozloženie stabilizátora v jeho jednotlivých prierezoch možno vypočítať pomocou percentuálnej redukcie v dĺžke jednotlivých prierezov k základnej šírke stabilizátora, pozri tabuľku 1. Grafické zobrazenie stabilizátora a jeho jednotlivých prierezov, pozri obrázok 4, umožňuje rýchlu komunikáciu medzi človekom a počítačom. Práca s Excelom pre začiatočníka zaberie asi 2 hodiny. Pracovná činnosť programu popísaného v literatúre 1 a 2 netrvá viac ako pár minút.

Tabuľka 1 Kalkulácia sekčných prierezov stabilizátora použitím Excelu (ukážka je prebratá od študentky N. FRANCIS)

b0		b1		b2		b3		b4		b5	
1		0.8		0.68		0.6		0.5		0.5	
x0	y0	x1	y1	x2	y2	x3	y3	x4	y4	x5	y5
0	0	0	0	0	0	0	0	0	0	0	0
0.5	1.122	0.4	0.8976	0.34	0.763	0.3	0.6732	0.25	0.561	0.25	0.561
0.75	1.343	0.6	1.0744	0.51	0.9132	0.45	0.8058	0.375	0.6715	0.375	0.6715
1.25	1.675	1	1.34	0.85	1.139	0.75	1.005	0.625	0.8375	0.625	0.8375
2.5	2.235	2	1.788	1.7	1.5198	1.5	1.341	1.25	1.1175	1.25	1.1175
5	3.1	4	2.48	3.4	2.108	3	1.86	2.5	1.55	2.5	1.55
7.5	3.781	6	3.0248	5.1	2.5711	4.5	2.2686	3.75	1.8905	3.75	1.8905
10	4.358	8	3.4864	6.8	2.9634	6	2.6148	5	2.179	5	2.179
15	5.286	12	4.2288	10.2	3.5945	9	3.1716	7.5	2.643	7.5	2.643
20	5.995	16	4.796	13.6	4.0766	12	3.597	10	2.9975	10	2.9975
25	6.543	20	5.2344	17	4.4492	15	3.9258	12.5	3.2715	12.5	3.2715
30	6.956	24	5.5648	20.4	4.7301	18	4.1736	15	3.478	15	3.478
35	7.25	28	5.8	23.8	4.93	21	4.35	17.5	3.625	17.5	3.625
40	7.43	32	5.944	27.2	5.0524	24	4.458	20	3.715	20	3.715
45	7.495	36	5.996	30.6	5.0966	27	4.497	22.5	3.7475	22.5	3.7475
50	7.45	40	5.96	34	5.066	30	4.47	25	3.725	25	3.725
55	7.283	44	5.8264	37.4	4.9524	33	4.3698	27.5	3.6415	27.5	3.6415
60	6.959	48	5.5672	40.8	4.7321	36	4.1754	30	3.4795	30	3.4795
65	6.372	52	5.0976	44.2	4.333	39	3.8232	32.5	3.186	32.5	3.186
70	5.576	56	4.4608	47.6	3.7917	42	3.3456	35	2.788	35	2.788
75	4.632	60	3.7056	51	3.1498	45	2.7792	37.5	2.316	37.5	2.316
80	3.598	64	2.8784	54.4	2.4466	48	2.1588	40	1.799	40	1.799
85	2.53	68	2.024	57.8	1.7204	51	1.518	42.5	1.265	42.5	1.265
90	1.489	72	1.1912	61.2	1.0125	54	0.8934	45	0.7445	45	0.7445
95	0.566	76	0.4528	64.6	0.3849	57	0.3396	47.5	0.283	47.5	0.283
100	0	80	0	68	0	60	0	50	0	50	0



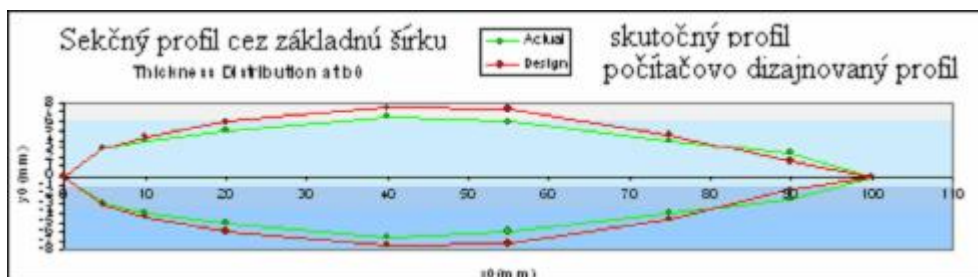
Obrázok 4: Údaje o dĺžke, šírke a hrúbke stabilizátora (finu) navrhnutého N. FRANCIS (a, b), podľa metódy navrhutej a popísanej AUDYM a jeho skupinou (c) v literatúre 1, 2 a 3. Obrázok 5 znázorňuje práce na prototypu stabilizátora (finu), navrhnutého podľa tabuľky 1 a obrázku 4. Obrázok 6 ukazuje sekčný profil stabilizátora (počítačovo modelovaného a skutočného) spolu s fotografiou prototypového stabilizátora (finu).







Obrázok.5: Výroba drevej šablóny pre stabilizátorové polovice podobne ako na obrázku 4 (c), príprava laminátového modelu (formy) pre výrobu stabilizátorových polovic z laminátu, zlepenie finových polovic použitím katalyzovaného resinu, dokončenie povrchových úprav.



Obrázok 6: Sekčný profil cez základnú šírku stabilizátora ukazujúci minimálne rozdiely medzi počítačovými a skutočne dosiahnutými hodnotami. (Ukážka je prevzatá z práce N. FRANCIS, ECU 2006.) Je potrebné podotknúť, že táto optimalizačná metóda je veľmi úspešná a populárna. Na jej základe bolo obdržaných niekoľko školských a priemyselných ocenení a viacero študentov SST sa podieľalo na počítačovom modelovaní vyššieho rozsahu. Jedným z nich bol Sam BLATCHFORD, ktorý pod vedením dr. AUDYHO zameral svoju ďalšiu kariéru na modelovanie, pozri obrázok 7.

Surf student searches for perfect fin

A BUNBURY student is making waves in the surfing community with his study into the properties of surf fins.

Edith Cowan University student Sam Blatchford is currently studying for his honours degree in surf science and technology under the supervision of lecturer Dr Jaro Audy.

Mr Blatchford said he had been researching the aspect ratio of surfboard fins, including how the depth and area affect the drag and lift properties of the board.

“We’re trying to look at the point where you can get the best lift and the least drag,” he said.

“Using regression analysis we’re hoping to produce and solve an equation, then apply that to surfboard fins.”

The 24-year-old said his love for the ocean began about 13 years ago when he lived in South Australia.

After leaving school he enrolled in an information technology and engineering course at the University of South Australia.

He said a friend alerted him to the unique surf science course at ECU Bunbury, and after some investigation Mr Blatchford enrolled and moved to WA.

Dr Audy said he enjoyed working with the honours student.

“Sam is diligent and tough, able to work under pressure and he picks up ideas about materials and design very quickly,” he said.

Mr Blatchford said he would be looking to align himself with local companies to produce an optimal fin when his research is finished.



Edith Cowan University honours student Sam Blatchford works on optimising surfboard fin design under the supervision of lecturer Dr Jaro Audy.

Obrázok 7: Novinový článok v ‘Bunbury Herald’ z augusta 2005 pojednáva o optimalizácii stabilizátorov (finov) na ECU pod vedením dr. AUDYHO.

2.2. SURFOVACIE DOSKY: Modelovanie a výroba

Tento predmet SST je zaradený v druhom semestri druhého ročníka. Surfovacía doska (tvar typu 1, pozri obr. 1) popísaná v tejto časti navrhla v roku 2005 študentka Nathalie FRANCIS, podľa návodu v literatúre 4. Jej model bol inšpirovaný 6’6 - trojstabilizátorovou surfovacou doskou, ktoré vyrába Lee BARTLETTOM pre Havajské ostrovné výrobky (Hawaiian Islands Creations HIC). Študentkiným cieľom bolo navrhnuť model s menšou dĺžkou, vhodný pre jej výšku umožňujúci surfovanie na malých vlnách, aby mal dobrú manévrovateľnosť a dostatočnú vztlakovú silu pre jej váhu. Vstupné údaje súvisiace s touto surfistkou a vlnami, pre ktoré bola doska modelovaná, sú v tabuľke 2. Optimalizované tvarové hodnoty tejto dosky sú v tabuľke 3.

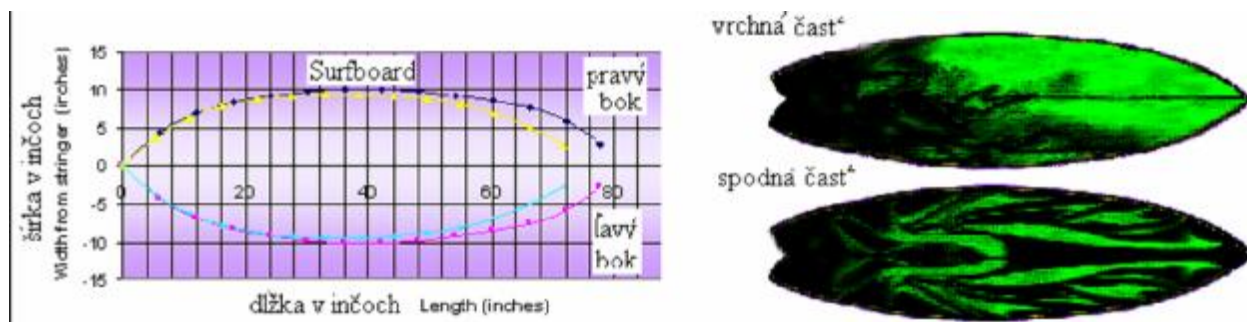
Tabuľka 2: Vstupné údaje pre modelovanie súvisiace so surfistkou a vlnami (podľa N. FRANCIS)

Surfistka – ‘študent/výrobca’ – užívateľ			Vlny pre surfovanie		
výška	skúsenosť v surfovaní	štyl surfovania	veľkosť	stupňovitosť	výkon
5’6	začiatočník/pokročilý	vysunutá noha	malé	mixovaná	malý

Tabuľka 3: Tvarové hodnoty dosky modelovanej podľa vstupných údajov v tabuľke 2 (podľa N. FRANCIS)

1 [inc] = 25.4 [mm]	Tvar surfovacej dosky
dĺžka [inc]	5'11
šírka [inc]	19 ½ (na dĺžke 33 inčoch od nosa)
boky	pravouhlého tvaru na konci @ zaokrúhlene smerom k nosu (pozri obr. 2)
nos	špicatý
zakončenie	s vybraným 1,5 inč. od konca (pozri obr. 2)
uhol vybrania	5 na nose a 2 na konci
stabilizátory (fíny)	tri (stredný fin umiestnený vo vzdialenosti 12 inčov od konca)
hrúbka surfingu [inc]	2 ½

Na obrázku 8 je počítačový výstup súvisiaci s optimalizovaním základných dĺžkových rozmerov a celkového tvaru surfovacej dosky, včítane bokov (a) a počítačovo vytvorenou grafikou (b).



Obrázok 8: Počítačovo vytvorený tvar a grafický návrh surfovacej dosky modelovanej podľa údajov v tabuľke 1 a 2.





Na obrázku 9 sú niektoré vybrané fotografie minuloročných druhákov s ich samostatne modelovanými a vyrobenými surfovacími doskami.



Obrázok 10: Novinový článok z ‘Bunbury Herald’ r. 2005 o SST ECU študentoch z technickej a materiálovej skupiny, vedenej dr. AUDYM.

3. Závery

V súčasnej dobe je nevyhnutné používať počítače vo výučbe odborných, technicky zameraných predmetov. Výučba a výskum podobne ako práce teoretického a praktického charakteru sú rovnocenné a vzájomne sa dopĺňujúce. Tento článok poukázal na možnosti uplatnenia počítačov vo výučbe tak zvláštneho a netradičného odboru ako je surfovanie. Príprava programu a optimalizačnej metódy nebola samoučelná. Vyžiadali si to potreby výučby, výskumu a priemyslu. Veríme, že v záujme aj slovenských čitateľov. Komunikácia a spolupráca je vítaná.

Literatúra

Audy K. and Audy J.: "A study of computer assisted analysis of effects of geometrical features on hydrodynamic performance of commercial surfing fins", The Maghrebian Conference on Software Engineering and Artificial Intelligence (MCSEAI), December 2006.

Audy J. & K., and Haines T.: "Human Computer Interaction in Designing Surfing Fins for Optimum Drag Lift Ratio and Hydrodynamic Performance" The 5th International Conference on Human System Learning Who is in Control?, ISBN: 2-909 285-33-2, Marrakech – Morocco, November 22-25, 2005, pp. 187 to 200.

<http://www.europia.org/edition/livres/cogn/ICHSL5.htm>

Audy J. & K., Haines T., and Killen P.: "Students Responses to New Teaching and Learning Approaches Involved in Surf Science and Technology: Making Surf-Craft Fins and Examining Their Performance", Conference on "New Challenges for Sustainability and Growth in Higher Education", Khon Kaen, Thailand, November 2004.

Haines T., Audy J. & K. and Killen P.: "Incorporation of Novel Ideas into 'Surf Equipment, Design, Materials and Construction' Course", Conference on "New Challenges for Sustainability and Growth in Higher Education", Khon Kaen, Thailand, November 2004.

Pod'akovanie

Autori článku by chceli pod'akovať Edith COWAN Univerzite za štedrú podporu výskumu a výučby, súvisiacej so Surf Science & Technology.

dr., Ing AUDY, J*. (MSc) a dr. Ing AUDY, K.
e-mail (*Corresponding author) j.audy@ecu.edu.au

Edith COWAN University, School of Enterprise and Technology

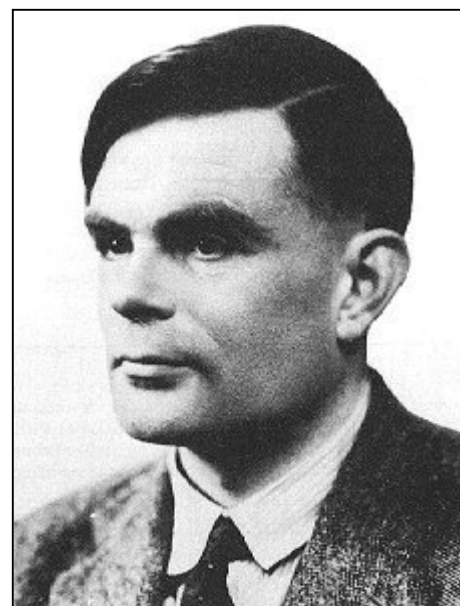
Robertson DRIVE
South West Campus Bunbury
Western Australia 6230

ČRIEPKY SPOMIENOK NA CESTU ŽIVOTOM A. M. TURINGA

V príspevku sú uvedené niektoré základné životopisné údaje významného matematika, logika, kryptoграфа a vojnového hrdinu A. M. TURINGA, jedného z „otcov“ elektronických číslicových počítačov. Vyzdvihuje sa jeho osobný prínos na výsledok druhej svetovej vojny.

Obrazne povedané, bity digitálnej logiky krúžia okolo planéty Zem obrovskou intenzitou. Prenášajú technické údaje, obchodné rozhodnutia, politické programy, ultimáta, príkazy k palbe, videokonferencie, neskoré večerné hovory a milostné odkazy. Má to na „svedomí“ jeden z geniálnych, zatiaľ najdokonalejších výtvorov človeka, elektronický číslicový počítač. Jeden z ľudí, ktorý sa podstatnou mierou zaslúžil o vznik elektronických číslicových počítačov bol Alan Mathison TURING (na obrázku vpravo).

A. M. TURING sa narodil 23. júna 1912 v Londýne. Jeho veľmi vzdelaní rodičia sa zosobášili v Indii. Od roku 1926 navštevoval školu v Sherborne. V roku 1931 začal študovať matematiku na univerzite v Cambridgi. Ako študent bol kritizovaný za svoj rukopis, zápasil s angličtinou, dokonca z humanitných predmetov prepadal. Zato z chémie si robil vlastné experimenty. Alan TURING bol neobratný, ťažko prístupný samotár, ktorému vraveli „pán profesor“. Obvykle chodil v obnosenej športovej bunde, mal váhavý hlas, zažltnuté zuby a neudržiavané nechty [1]. Mal však svoj vlastný myšlienkový svet, v ktorom mali svoje miesto aj teória relativity a kvantová mechanika. V roku 1934 promoval. Ako člen Kráľovského kolégia obhajoval v roku 1935 dizertačnú prácu na tému Základná limitná veta pravdepodobnosti. TURING bol už v čase štúdií známy originalitou a radikalizmom. Nerád používal výsledky prác svojich kolegov a radšej si teoretické základy budoval a overoval sám. Výnimkou bola azda iba NEUMANNOVA kniha o základoch kvantovej mechaniky.



V rokoch 1936 – 1938 študoval na univerzite v Princetone, spojenej s menom Alberta EINSTEINA. Jedna z prác, za ktorú TURING v tridsiatych rokoch získal vedecké ocenenie, sa týkala práve teórie relativity. Doktorát robil u A. CHURCHA [2]. Roku 1935 sa stretáva v Cambridgi s Von NEUMANOM. V priebehu nasledujúcich desiatich rokov títo dvaja géniovia nezávisle na sebe položili matematické, logické a fyzikálne základy elektronického číslicového počítača. Sú to práve ich mená, ktoré sa spájajú s fenoménom dnešnej doby.



To však už začalo besnenie druhej svetovej vojny. Nebyť TURINGA, možno by mala iný priebeh, ako ju poznáme z učebníc dejepisu. TURING ako dôstojník pre dekódovanie pracoval v Bletchley Parku, kde bol v maximálnom možnom utajení presídlený malý kolektív lúštitel'ov šifrier. Šéfom skupiny bol Naval COMMANDER a Alastair DENNISTON. Členmi boli Ian FLEMING, alias James BOND, ktorý zomrel v roku 1968, ďalej Gordon WELCHMAN, znovuobjavitel' Zygalského tabuliek a Alan TURING. Ich hlavné poslanie bolo dešifrovať správy nemeckých nacistov, ktoré boli šifrované pomocou zariadenia s názvom Enigma. Enigma mala svoj pôvod v Hebernovom stroji zostrojenom v USA v roku 1918. Tento šifrovací stroj kúpil v roku 1919 H. A. KOCH z Holandska. Hugo Alexander KOCH zapísal svoj patent šifrovacieho stroja založeného na rotoroch. O štyri roky neskôr predal patent Arthurovi SCHERBIUSOVI, nemeckému inžinierovi, ktorý ho vylepšil a nazval Enigma (obrázok vľavo).

Vo variante A bola predstavená už v roku 1923 ako komerčné zariadenie na medzinárodnom poštovom kongrese v Berne. Šifrovací stroj Enigma nemal komerčný úspech, ale bol odkúpený, vylepšený a používaný nacistickým Nemeckom. Samotný prístroj má rozmery 31 x 25,5 x 13 cm a hmotnosť vyše 10 kg. Hlavnou súčasťou Enigmy je rotor z nevodivého materiálu, na ktorom je realizovaná permutácia \tilde{p} . Jej výsledok sa kontaktom prenáša na

susedný rotor. Rotory sú uložené na spoločnej osi. Ich natočením proti smeru hodín o uhol $k \cdot 360/26$ sa realizuje tzv. Cézarovská šifra C_k . Na vnútornej strane rotora je zarážka, ktorá po otočení rotora o 360š uvedie do pohybu susedný rotor. Jeden rotor realizuje permutáciu

$$r(p,k) = C_k p C_k, \quad r^{-1}(p,k) = C_k p^{-1} C_k$$

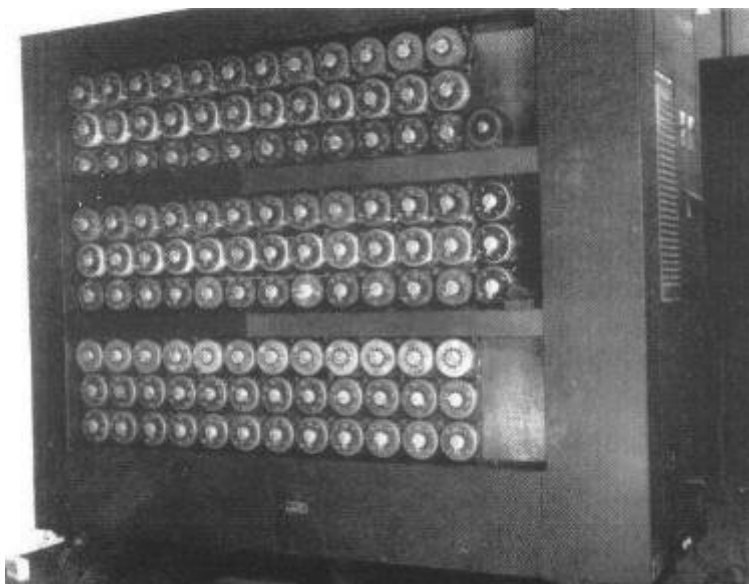
$$r(p,k)(x) = p(x+k)-k \bmod 26$$

$$r^{-1}(p,k)(x) = p^{-1}(x+k)-k \bmod 26.$$

Druhá polovica šifrovania sa realizuje spätným prepojením cez os.

Enigma bola na tú dobu špičkové šifrovacie zariadenie. Prelomenie šifrovacieho kódu Enigmy sa považovalo za nemožné. TURING zohral rozhodujúcu úlohu v tomto úsilí. Jeho matematické schopnosti, spolu s predchádzajúcim príspevkom kolektívu poľských vedcov Mariana REJEWSKEHO, ktorý zomrel ako 74-ročný v roku 1980, Jerzyho RÓZYCKEHO, ktorý sa stratil v Stredozemnom mori 9.1. 1942 na ceste z Alžírsku do Francúzska a Henryka ZYGALSKEHO, ktorý po vojne zostal v Anglicku a zomrel v roku 1978, prispeli k pochopeniu nemeckých námorných šifriera azda najviac. Na úsilí o dešifrovanie správ z Enigmy sa podieľalo aj širšie „zázemie“. Bolo to poľské Biuro Szyfrów a Hans Thilo-SCHMIDT, nemecký aristokrat, ktorý predával Poliakom cez Francúza Gustava BERTRANDA staré denné kódy do januára 1939. Kód Enigmy bol prelomený aj vďaka šťastnej náhode, keď bola zajatá nemecká ponorka, ktorá mala na svojej palube jeden prístroj Enigma. Skôr ako ju Nemci stihli zničiť dostala sa do rúk Angličanom. Už skôr sa podarilo zaistiť rotory z Enigmy. Od 8.11. 1931 boli známe vďaka SCHMIDTOVI prvé rotory I-III, od 12.2. 1942 rotory VI a VII (U 33). Rotory IV a V vylúštil TURING.

Na prelomení kódu Enigmy sa podieľali aj nedostatky samotnej Enigmy, ako niekedy aj až hrubá nedisciplinovanosť jej operátorov. Enigma bola totiž „bezpečná“ aj v prípade odcudzenia prístroja, to znamená, že sa dala použiť aj nepriateľom, ak by bola používaná správne. Mala obmedzenia pri zapojení prepojovacích káblov, poradí rotorov a reflexného rotora. Kód správy, tzv. message key bol súčasťou správy a bol 2-krát šifrovaný. Ďalej to bol ľudský faktor, najmä lenivosť operátorov, ktorí používali ako kľúč skratky mien svojich priateľiek, prípadne sprostých slov a hlavne v rozpore s predpismi ich nemenili. Tak aj náhoda pomohla k rozlúšteniu záhady neprelomiteľného kódu šifrovacieho stroja Enigma.



Odhaduje sa, že na konci druhej svetovej vojny pracovalo na strane spojencov asi 10 000 kryptoanalytikov. Medzi iným TURING pri dešifrovaní správ z Enigmy využil aj nemeckú dôslednosť. Nemci totiž každé ráno o 6:50 vysielali správy o počasí, čo v podstate znamenalo lúštiť 60 možných usporiadaní rotorov \times 17 576 nastavení rotorov 3 paralelne prepojených Enigiem, t.j. 1 054 560 možností. Ak jedno preverenie trvá 1 sec, potom by 60 \times 3, t.j. 180 Enigiem pracovalo 5 hodín. TURING presadil konštrukciu zariadenia, ktoré vedelo v krátkom čase analyzovať pravdepodobné nastavenia Enigmy. Šlo o stroj s názvom Bomba (obrázok vľavo), ktorý vážil okolo 1 tony, so šírkou 2,1 m, výškou 2 m a hĺbkou 0,6 m. Bol to v podstate počítač i keď namiesto polovodičových prvkov mal servomotory. Princíp TURINGOVHO

paralelného stroja Bomba spočíval v 3 paralelne prepojených Enigmách, ktoré overia konečný počet nastavení rotorov. Genialita TURINGA spočívala v tom, že každý, kto by si nakreslil blokovú schému Enigmy, mohol prísť na jeho nápad. Ten nápad však mal len TURING.

Dešifrovanie správ z Enigmy prinieslo spojencom jednu z rozhodujúcich výhod v boji o Atlantik a na západnom fronte. Britská ani americká vláda doposiaľ nepripustili otvorenú diskusiu o metódach, ktoré TURING používal. Jeden z jeho bývalých kolegov, ako aj mnohí historici tvrdia, že TURINGOV prínos pri dešifrovaní správ z Enigmy bol najdôležitejším príspevkom jednotlivca k víťazstvu spojencov.

Po vojne TURING pracoval na prvom skutočnom britskom digitálnom počítači Collosus. Jeho nepokojný duch ho priviedol k skúmaniu vzťahu medzi počítačmi a prírodou. Veril, že stroje môžu imitovať procesy, prebiehajúce v ľudskom mozgu. Z tohto dôvodu poslednú časť života strávil bádaním o tom, ako stovky miliárd neurónov v mozgu s pomocou elektrických impulzov spolupracujú počas učenia. Začal študovať komplexné systémy. Malú revolúciu vo

vedeckej komunite spôsobil jeho návrh uplatniť matematické metódy aj v biológii. Svojou vlastnou genialitou anticipoval psychologické problémy, ktoré môžu nastať pri kontakte ľudí s múdrymi strojmi. V národnom fyzikálnom laboratóriu pracoval od roku 1945. Neskôr, v roku 1948, prešiel na univerzitu v Manchestri. Členom Londýnskej kráľovskej spoločnosti sa stal v roku 1951.

TURING bol človek plný paradoxov. Výsostne racionálne rozmyšľajúci človek, v ktorého hlave sa zrodilo toľko spoločensky prínosných ideí, bol v podstate samotárom. Spoločnosť ľudí k svojmu životu vôbec nepotreboval. Paradoxom života je, že tento vojnový hrdina prakticky celý život pracoval pre vládu a jej inštitúcie. A bola to práve táto vláda a jej súdy, ktoré ho označili za „potenciálne bezpečnostné riziko“ pre Veľkú Britániu. Prudérne Anglicko v tej dobe nedokázalo totiž tolerovať TURINGOVU homosexualitu. Táto vyšla najavo pri vyšetrovaní lúpeže jeho bytu v roku 1952. V roku 1952 bol tiež uväznený za násilné protesty proti obmedzeniam britských homosexuálov. Stalo sa to vo Veľkej Británii, v jednej z najdemokratickejších krajín na svete. V tom čase sa homosexualita považovala za zločin alebo za psychickú chorobu. Súd TURINGA obvinil z „hrubej neposlušnosti“ a predpísal mu hormonálnu terapiu, aby lekári skrotili jeho tzv. „neprirodzenú sexuálnu túžbu“. Mal si vybrať medzi väzením alebo liečbou. Vybral si liečbu. Násilne mu boli podávané estrogenové injekcie, ktoré ho mali „vyliečiť“. Namiesto „vyliečenia“ mu však narástli prsia. TURING už nemohol ako delikvent dostať víza do USA. Táto skutočnosť ukončila akúkoľvek nádej na spoluprácu s VON NEUMANNOM. Pre homosexualitu géniovi TURINGOVI bola zakázaná práca vo vedeckom ústave. V liste priateľovi deprimovaný vojnový hrdina napísal, že čelí obvineniu zo sexuálnych priestupkov, cíti sa pošpinený, jeho práca je zničená. Verný svojmu prenikavému logickému mysleniu napísal: „TURING tvrdí, že stroje myslia. TURING spí s mužmi. Teda stroje nemyslia.“

Nečakaná smrť prišla 7. júna 1954 vo Wilmslowe, keď pani TURINGOVÁ našla svojho 41-ročného syna Alana mŕtveho. Deň predtým zjedol jablko, do ktorého si napustil pomocou injekcie kyanid. Vyšetovanie potvrdilo samovraždu otrávením za príčinu smrti. Jeho matka však tvrdila, že šlo o nehodu. Nešťastný a zdrvený TURING si odchod zo života zariadil ako scénu vytrihnutú z jeho obľúbenej rozprávky o Snehulienke. A tak až do trpkého konca zostal tento matematický génius verný symbolom, s ktorými celý život pracoval. Dá sa konštatovať, že racionálny TURING odmietol žiť v iracionálnom svete. Tak skončil príbeh veľikána, na ramenách ktorého stojí dnešná informatika, človeka, ktorý sa osobne pričínal o záchranu tisícov iných životov.

Dnes je samozrejmosťou, že ani v Anglicku, ani inde na Západe sa nepovažuje homosexualita za zločin ani za psychickú chorobu. Pre niektorých humanistov je aj tento tragický, spoločnosťou vynútený skon génia považovaný za TURINGOV odkaz [5]. Podľa nich vlastne nadväzuje na FUKUJAMOVU myšlienku, že pri vhodných vonkajších podmienkach je ľudská povaha vo svojej podstate empatická. Takýto druh humanistickej morálky sa už dnes stal inštitucionálnou súčasťou moderných spoločností. Je isté, že dnešná spoločnosť by TURINGA neutýrala, ale ocenila. To, čo TURING dokázal na poli vedy i humanity, by mu dnes stačilo na niekoľko Nobelových cien a nehynúci ohlas.

doc. Ing. Ján ZELEM, CSc.
Katedra kvantitatívnych metód a hospodárskej informatiky
FPEDaS, Žilinská univerzita

Literatúra

- [1] COVENEY, P. – HIGHFIELD, R.: Medzi chaosom a řádem, Mladá fronta, Edice Kolombus, Praha 2003, ISBN 80-204-0989-0
- [2] JEDINÁK, D.: Alan Turing – mysliaci stroj kacírkej teórie. <http://www.matmix-web.sk/archiv/200506/2/turing.pdf>
- [3] GROŠEK, O. – VOJVODA, M. – ZAJAC, P.: Vybrané kapitoly z kryptológie. Rotorové šifrátory. http://209.85.135.104/search?q=cache:igonqMHio5UJ:aladin.elf.stuba.sk/~zajacpa/ks/enigma.rtf+Enigma&hl=sk&gl=s&ct=clnk&cd=65&lr=lang_sk
- [4] http://neuron.tuke.sk/~balki/biokybernetika/povodna/krypto_historia.htm
- [5] GÁL, F.: Náboženstvo je ako depozitár hodnôt. <http://www.sme.sk/c/2905621/Nabozenstvo-je-ako-depozitar-hodnot.html>
- [6] <http://www.ellsbury.com/enigmabombe.htm>
- [7] <http://frode.home.cern.ch/frode/crypto/>