JUPIM Bilten

godina IV, broj 1, maj 2001.

Bilten Jugoslovenskog Udruženja za Primenjenu i Industrijsku Matematiku

1. Uvodne napomene

U ovom izdanju Biltena prvo ukazujemo na zaključke European Mathematical Society vezane za razvoj primenjene matematike. Napominjemo da je jedan od koautora ovih zaključaka i prof. dr Zoran Marković. Zatim pažnju posvećujemo kandidatima i dobitniku povelje JUPIM-a za 2000. godinu. U nastavku obavešavamo o aktuelnostima sa X kongresa Matematičara i planiranoj Skupštini JUPIM-a.

2. Zakljuci European Mathematical Society o Primenjenoj Matematici

Report on the Workshop on Applied Mathematics in Europe Berlingen, Switzerland, 4-6 May, 2001, Sebastià Xambó-Descamps.

This workshop can be seen as the first major initiative taken by the European Mathematical Society (EMS) in order to address the problem of making sure that "applied mathematicians can feel that the Society is also their home". The main result of the workshop is the "Berlingen declaration", which was agreed upon and signed by all participants. It consists of the following nine points:

1. The presence of applied mathematics in EMS bodies and policy decision making should be significantly increased.
2. The applied mathematics committee must be kept an active body for the time being. Its mission statement should be adapted to the new role of the committee. The chair should be invited to the Executive Committee meetings.
3. Pure and applied mathematics should be equitably represented in the publications of the EMS.
4. Special interest groups should be created gradually.
5. EMS should consider increasing its activities by collaborating with international, national and regional societies in organising meetings.
6. The EMS should further develop its Summer School Programme. It is noted with satisfaction that the existing programme includes topics in both pure and applied mathematics.
7. EMS should work towards the goals that
(a) the students majoring in mathematics should be exposed to applications of mathematics in sciences or other areas;
(b) high school teachers have adequate education in applied mathematics and mathematical modelling.
8. EMS should formulate a position with regard to the Bologna declaration of 1999.
9. It is noted with satisfaction that the EMS established a committee to raise public awareness of mathematics. EMS should promote local initiatives, encourage collaboration with various organisations, and collect and disseminate information on initiatives of member societies in this area.

3. Povelja JUPIM-a za 2000. godinu

Da bi potstaklo orijentaciju istrazivača na primene matematike, Predsedništvo JUPIM-a je ustanovilo Povelju JUPIM-a za naučni rad ili naučnu monografiju koja se dodeljuje jedanput godišnje za delo objavljeno u protekloj godini iz oblasti primenjene i industrijske matematike.

Predsedništvo je u decembru 2000. godine obavestilo članove JUPIM-a i druge zainteresovane stručnjake da se otvara konkurs za drugu Povelju JUPIM-a.

Na konkurs za dodeljivanje Povelje JUPIM-a za naučni rad ili naučnu monografiju u 2000. godini prijavljeni su sledeći naučni rezultati:

1. O. Du Merle, P. Hansen, B. Jaumard, N. Mladenović, "An Interior Point Algorithm for Minimum Sum-of-Squares Clustering", SIAM J. Sci. Comput., 21(2000), No. 4, pp. 1485-1505.

Predlagači: D. Cvetković, V. Kovačević-Vujčić.

2. I. Gutman, Ž. Tomović, "Relations Between Distance-Based Topological Indices", J. Chem. Inf. Comput. Sci., 40(2000), pp. 1333-1336.

Predlagač: D. Cvetković.

3. J. Golić, "Ctyptanalysis of Three Mutually Clock-Controlled Stop/Go Shift Registers" IEEE T. Inform. Th. 46(May 2000), pp. 1081-109.

Predlagač: M. Mihaljević.

4. B. Kovačević, M. Milosavljević, M. Veinović, M. Marković, "Robusna digitalna obrada govornog signala", Akademska misao, Beograd, 2000.

Predlagači: B. Lazić, S. Valjić, D. Cvetković

3. 1 Dobitnik Povelje JUPIM-a za 2000. godinu

Odlukom Predsedništva JUPIM-a, Povelja JUPIM-a za 2000. godinu je dodeljena prof. dr Jovanu Goliću za naučni rad "Ctyptanalysis of Three Mutually Clock-Controlled Stop/Go Shift Registers" IEEE T. Inform. Th. 46(May 2000), pp. 1081-1089.

OBRAZLOZENJE:
Predmet prijavljenog rada je matematička analiza sigurnosti kriptografskog algoritma poznatog pod imenom A5 koji se koristi u okviru GSM standarda za digitalnu mobilnu telefoniju sa širokim primenama i u našoj zemlji. Osnovni doprinosi rada sastoje se u definisanju i teorijskoj analizi više algoritama za rekonstrukciju internog stanja automata u odredjenom vremenu, početnog stanja automata i 64-bitnog tajnog ključa. Algoritmi su zasnovani na originalnoj primeni elemenata teorije automata, algebre, teorije verovatnoće i posebno teorije granajućih procesa. Pored rezultata vezanih za konkretni kriptografski algoritam A5, rad ima i širi značaj u kriptologiji, naročito u pogledu uvodjenja teorije granajućih procesa i koncepta vremensko-memorijskog kompromisa u oblast sekvencijalnih šifarskih sistema. Rad je objavljen u medjunarodnom naučnom časopisu vrhunskog renomea, kako po značaju tako i po strogim kriterijumima, a koji je posvećen matematičkim metodama u obradi i prenosu informacija. Rad predstavlja plod višegodišnjih istraživanja istog autora u oblasti kriptologije, koja su, pored ostalih, rezultovala i sledećim radovima takodje objavljenim u vrhunskim medjunarodnim časopisima u toku 2000. godine:
- J. Dj. Golić, M. Salmasizadeh, E. Dawson, "Fast correlation attacks on the summation generator", J. of Cryptology, 13(2), pp. 245-262, 2000.
- J. Dj. Golić, A. Clark, E. Dawson, "Generalized inversion attack on nonlinear filter generators", IEEE T. on Computers, Vol. 49, pp. 1100-1109, Oct. 2000.
- M. Mihaljević, J. Dj. Golić, "A method for convergence analysis of iterative probabilistic decoding", IEEE T. on Inform. Th., Vol. 46, pp. 2206-2211, Sept. 2000.

4. Okrugli sto o primenjenoj matematici na X kongresu Matematičara

U Beogradu je od 21-24. januara 2001. godine (nakon dvostrukog odlaganja) održan X kongres matematičara Jugoslavije u organizaciji Matematičkog fakulteta, Beograd, Društva matematičara Srbije, Saveza društava matematičara Jugoslavije i Instituta za matematiku, PMF, Novi Sad. Učestvovalo je oko 900 matematičara. Održana su dva uvodna predavanja, 14 predavanja po pozivu i prikazan 181 rad u okviru 12 sekcija. Organizovana su 4 okrugla stola, od kojih je jedan bio posvećen industrijskoj matematici i informatici. Na njemu su učestvovali neki članovi JUPIM-a, medju kojima je bilo i članova Predsedništva i Nadzornog odbora. Planirano je značajno učešće kolega iz privrede, ali je odlaganje kongresa svelo njihovo prisustvo na nekolicinu, medju kojima su zapažene Olivera Stanković, rukovodilac Informacionog centra Privredne komore Jugoslavije i Dinić Miroslava, Bakar, Bor. Kao uvod u diskusiju, koordinatori prof. Žarko Mijajlović i prof. Gordana Pavlović-Lažetić, postavili su nekoliko načelnih pitanja (Da li je našoj industriji potrebna industrijska matematika? Da li je potrebno obrazovati kadrove iz oblasti primenjene i industrijske matematike? Da li je neophodno posredovanje države izmedju matematičara i industrije? i dr.) Diskusiji su značajno doprineli istraživači iz oblasti primenjene matematike koji su imali prilike da saradjuju sa privredom, bilo kod nas, bilo u inostranstvu. Pozivu da prisustvuje okruglom stolu odazvao se i prof. Smile Markovski, Institut za informatiku, PMF, Skopje koji je učesnicima preneo svoja iskustva u saradnji sa italijanskom kompanijom TELECOM. Članovi JUPIM-a su predstavili svoje udruženje i odgovarajuće evropsko udruženje sa kojim nam je ponudjena saradnja. Od strane g-dje Olivere Stanković je potekla inicijativa o sklapanju sporazuma o poslovno-tehničkoj saradnji izmedju Privredne komore Jugoslavije i JUPIM-a koji bi, izmedju ostalog, omogućio šire propagiranje delatnosti JUPIM-a i njegovo povezivanje sa privredom.

5. Skupština JUPIM-a

Sadašnji organi JUPIM-a su izabrani na osnivačkoj skupštini JUPIM-a održanoj u junu 1997. godine. Po statutu JUPIM-a došlo je vreme da se održi Skupština JUPIM-a i izaberu novi organi. Planirano je da to bude na ovogodišnjem PRIM-u, ali kako konferencija još nije zakazana, Predsedništvo je odlučilo da se Skupština održi u Sali 2 Matematičkog instituta u Beogradu 12. juna u 14 časova (termin Seminara za primenjenu i industrijsku matematiku).

Molimo članove JUPIM-a da prisustvuju Skupštini, kao i da nam dostave svoje predloge za sastav organa JUPIM-a, a posebno za predsednika JUPIM-a, potpredsednika i sekretara Predsedništva i predsednika Nadzornog odbora.

6. Tekuće informacije

- Očekuje se skoro raspisivanje konkursa za novi ciklus projekata od strane Ministarstva za nauku, tehnologiju i razvoj Republike Srbije. Posebna pažnja poklanja se primenjenim istraživanjima, što otvara velike mogućnosti za intenziviranje delatnosti JUPIM-a.

- XXVIII jugoslovenski simpozijum o operacionim istraživanjima (SYM-OP-IS 2001) održaće se u Beogradu, 02-05. oktobra 2001. godine. Koordinator je Sektor za školstvo, obuku, naučnu i istraživačku delatnost VJ.
E-mail: symopis@vj.yu
Home page: http://www.vj.yu/symopis/

- Prof. Pierre Hansen, direktor Instituta GERAD iz Montreala, kanadski akademik i jedan od prošlogodišnjih dobitnika Povelje JUPIM-a prihvatio je poziv za gostovanje u Matematičkom institutu SANU. Njegov dolazak planiran je za poslednju nedelju septembra. Predvidjeno je da održi dva predavanja (teme su kombinatorna optimizacija i verovatnosne logike) i eventualne konsultacije sa zainteresovanim slušaocima.

- Članovi JUPIM-a se pozivaju da izvrše uplatu članarine za 2001. godinu na osnovu dostavljenih uplatnica, a posebno da iniciraju aktivnosti JUPIM-a i Predsednistvu JUPIM-a dostavljaju predloge i sugestije.
Adrese JUPIM-a: JUPIM, Matematički institut SANU, Kneza Mihaila 35, 11000 Beograd
E-mail: jupim@mi.sanu.ac.yu
Home-page: www.mi.sanu.ac.yu/jupim.htm.