Rok IV, numer 4(30) Do użytku wewnętrznego

INFORMATOR WYDZIAŁOWY

Wydział Matematyki i Informatyki UAM, ul. Matejki 48/49, 60–769 Poznań

styczeń 1997

Rada Wydziału na posiedzeniu w dniu 29.11.1996 podjęła uchwałę w sprawie rekrutacji na I rok studiów dziennych 5-letnich na kierunku matematyka i kierunku informatyka w roku 1997.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału na posiedzeniu w dniu 6.12.1996 wszczęła postępowanie o nadanie tytułu naukowego prof. drowi hab. Jerzemu Kąkolowi. Powołano następujących recenzentów: prof. dra hab. Lecha Drewnowskiego (UAM), prof. dra hab. Czesława Bessagę (Uniwersytet Warszawski), prof. dr hab. Stefana Rolewicza (Instytut Matematyczny PAN) i prof. dr Jose Boneta (Politechnika w Walencji).

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada Wydziału wszczęła postępowanie o nadanie tytułu naukowego prof. drowi hab. Józefowi Banasiowi z Politechniki Rzeszowskiej. Powołano następujących recenzentów: prof. dra hab. Andrzeja Lasotę (Uniwersytet Śląski), prof. dra hab. Kazimierza Goebla (Uniwersytet Marii Curie-Skłodowskiej) i prof. dra hab. Stanisława Szuflę (UAM).

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała pozytywnie wnioski dr hab. Krystyny Bartz, dra hab. Marka Nawrockiego, dra hab. Marka Wisły i dra hab. Macieja Wygralaka o mianowanie na stanowiska profesorów nadzwyczajnych na naszym Wydziale.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału nadała stopień doktora nauk matematycznych w zakresie matematyki mgrowi Michałowi Wiernowolskiemu. Obrona rozprawy doktorskiej odbyła się 22.11.1996.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała pozytywnie nową procedurę związaną z zatwierdzaniem tematów prac magisterskich na naszym Wydziale.

⋆ ⋆ ⋆ ⋆ ⋆

Na posiedzeniu w dniu 6.12.1996 Rada Wydziału zaopiniowała pozytywnie wniosek prof. dra hab. Tomasza Łuczaka o urlop naukowy w dniach 5.01–20.05.1997 oraz wniosek mgra Jacka Marciniaka o 6-miesięczny urlop naukowy (w ramach płatnego urlopu szkoleniowego) w okresie 1.02–31.07.1997.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaaprobowała również wniosek o indywidualny tok studiów dla Ewy Sierockiej.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała pozytywnie wniosek o zgodę na prowadzenie wykładów przez doktorów na kierunkach matematyka i informatyka.

⋆ ⋆ ⋆ ⋆ ⋆

W dniu 20.12.1996 odbyło się tradycyjne spotkanie świąteczno-noworoczne pracowników Wydziału.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału na posiedzeniu w dniu 10.01.1997 przyjęła program studiów zaocznych II stopnia, kierunek informatyka.

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada Wydziału wszczęła procedurę w sprawie przewodu habilitacyjnego dra Wojciecha Kordeckiego z Politechniki Wrocławskiej. Powołano komisję w składzie: prof. dr hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Dobiesław Bobrowski, prof. dr hab. Mirosław Krzyśko, prof. dr hab. Julian Musielak oraz prof. dr hab. Zbigniew Palka.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału wszczęła też przewód doktorski mgrowi Krzysztofowi Feledziakowi z Instytutu Matematyki Wyższej Szkoły Pedagogicznej w Zielonej Górze. Podstawą przewodu będzie rozprawa pt. „Struktura topologiczna przestrzeni funkcji wektorowych". Na promotora powołano prof. dra hab. Mariana Nowaka z Instytutu Matematyki WSP w Zielonej Górze. Ustalono też następujący zakres egzaminów doktorskich: dyscyplina podstawowa — analiza matematyczna, dyscyplina pomocnicza — filozofia matematyki, język obcy — angielski.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału zwolniła dra Grzegorza Szkibiela, pracownika Instytutu Matematyki Uniwersytetu Szczecińskiego, z postępowania nostryfikacyjnego i uznała stopień naukowy doktora uzyskany przez niego w University of New York at Buffalo (USA) za równorzędny ze stopniem doktora nauk matematycznych w zakresie matematyki nadawanym w Polsce.

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada Wydziału powołała komisję w przewodzie doktorskim mgra Tomasza Schoena. Przewodniczącym komisji została prof. dr hab. Paulina Pych-Taberska, zastępcą przewodniczącego prof. dr hab. Zbigniew Palka. Na promotora powołano prof. dra hab. Tomasza Łuczaka, a na recenzentów prof. dr hab. Jerzego Kaczorowskiego i prof. dr hab. Zbigniewa Lonca (Politechnika Warszawska). Członkami komisji zostali prof. dr hab. Paweł Domański oraz prof. dr hab. Roman Murawski (jednocześnie egzaminator z dyscypliny pomocniczej). Ustalono też następujący zakres egzaminów doktorskich: dyscyplina podstawowa — matematyka dyskretna i kombinatoryczna teoria liczb, dyscyplina pomocnicza — historia matematyki, język obcy — angielski.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału zaopiniowała pozytywnie wniosek o zatrudnienie dra Michała Wiernowolskiego na stanowisku adiunkta na naszym Wydziale.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała także pozytywnie wniosek mgra Stanisława Gawiejnowicza o przedłużenie stypendium doktorskiego o sześć miesięcy.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowąl pozytywnie korektę opłat za studia oraz stawek wynagrodzeń za prowadzenie zajęć na studiach zaocznych płatnych w semestrze letnim roku akademickiego 1996/97.

Z historii . . .

Sto lat temu, 2.01.1897 roku urodził się w Kijowie Waleri Iwanowicz Gliwienko (zmarł 15.02.1940 roku w Moskwie). W roku 1925 ukończył studia matematyczne na Uniwersytecie Moskiewskim. Pracował w Instytucie Pedagogicznym w Moskwie (od roku 1928 jako profesor). Habilitował się w roku 1936. Niezależnie i równolegle z A. Kołmogorowem i A. Heytingiem podał formalizację logiki intuicjonistycznej. Pokazał także, że logika intuicjonistyczna nie jest logiką dwuwartościową. W zakresie teorii porawdopodobieństwa pochodzi od niego m.in. aksjomatyczne ujęcie pojęcia zdarzenia.

R.M.

Na uroczystym posiedzeniu Senatu UAM w dniu 6.01.1997 wręczono nominacje na stanowisko profesora nadzwyczajnego następującym pracownikom naszego Wydziału: dr hab. Krystynie Katulskiej, dr hab. Krystynie Bartz, dr hab. Markowi Nawrockiemu, dr hab. Markowi Wiśle, dr hab. Witoldowi Wnukowi i dr hab. Maciejowi Wygralakowi.

⋆ ⋆ ⋆ ⋆ ⋆

W dniu 6.01.1997 w Instytucie Filozofii UAM odbyło się kolokwium habilitacyjne dra Kazimierza Świrydowicza z Zakładu Logiki Matematycznej naszego Wydziału. Podstawą przewodu była rozprawa *Logiczne teorie obowiązku warunkowego*, a recenzentami byli: prof. dr hab. Tadeusz Batóg (UAM), prof. dr hab. Leszek Nowak (UAM), prof. dr hab. Jerzy Perzanowski (Uniwersytet Mikołaja Kopernika) i prof. dr hab. Jan Woleński (Uniwersytet Jagielloński). W wyniku kolokwium i wykładu habilitacyjnego drowi K. Świrydowiczowi nadano stopień doktora habilitowanego nauk humanistycznych w zakresie filozofii.

⋆ ⋆ ⋆ ⋆ ⋆

Dr Wojciech Gajda z Zakładu Geometrii i Topologii otrzymał roczne stypendium Fundacji im. Alexandra Humboldta (RFN).

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Jerzy Kaczorowski został wybrany przewodniczącym Senackiej Komisji Rozwoju, prof. dr hab. Paulina Pych-Taberska — członkiem Komisji Budżetowej Senatu, a dr Ewa Marchow — członkiem Komisji Dydaktycznej.

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Julian Musielak został wybrany do grona członków Komitetu Matematyki PAN.

W sieci

Na co mam się spieszyć,
Któregoś dnia i tak dostanę się tam, gdzie trzeba.
Kubuś Puchatek

Kubusiowe zawołanie, jak zwykle olśniewające w swej mądrości, przywodzi na myśl, tak bardzo nieobecną w tym szalonym, poplątanym świecie, potrzebę stoickiego „rób swoje". Jednak nie tylko. Widać w tym również pochwałę mądrego patrzenia w przyszłość, głębokiego przeświadczenia o ukrytym sensie rzeczywistości. Lecz po pierwsze nie o interpretację Puchatka tu chodzi, a po drugie każdy (hm, może nie każdy) czuje sam niewyczerpane bogactwo misiowej filozofii życia i tłumaczenie jej zawsze pozostanie wyrywkowe i koślawe. Zatem do rzeczy.
Jak było wspomniane w sieciowym odcinku dwa miesiące temu, powstaje specjalna baza informacyjna dla matematyków w Polsce. Miło jest mi zakomunikować, iż jej pierwsza część jest gotowa — no, prawie gotowa, gdyż niektóre Uniwersytety (te bardziej leniwe) jeszcze nie zdążyły się do niej podpiąć. Jednak siedem czy osiem instytucji już wprowadziło do EMIRA (bo tak się owa baza nazywa) część swoich danych i fakt ten pozwala mieć nadzieję, że ta szlachetna idea nie umrze śmiercią naturalną w najbliższym czasie. To bardzo istotne, gdyż oczywiste jest, że owoce jej powstania będą widoczne wyraźnie dopiero za parę (optymistycznie) lat. Musi się jeszcze wiele zmienić w mentalności, a EMIR musi zaistnieć w świadomości środowiska matematycznego w Polsce jako rzecz naturalna, potrzebna i współtworzona przez to środowisko, a nie traktowana jako jeszcze jedno narzędzie, po które się sięga rzadko lub wcale. Porzeba wysiłku, by dzieło to doprowadzić do takiego stanu, który spowoduje, iż baza ta wejdzie w fazę samorozwoju, jak dobrze skonstruowana sieć neuronowa. Perspektywy, które się przed nią rysują, wykraczają poza ograniczony jej kształt pierwotny, przyjęty w zgodzie ze starą mądrością, że należy zaczynać od rzeczy małych, a dążyć ku wielkim. Inicjatorzy powstania EMIRA przyjęli, iż początkowo zawierać on będzie trzy zasadnicze części: dane osobowe o pracownikach (te są już zasadniczo wprowadzone), bazę publikacji, wraz z tekstami źródłowymi dostępnymi dla zainteresowanych, oraz bazę zawierającą informacje o wykładach i seminariach odbywających się w poszczególnych ośrodkach. Każda z nich posiada szereg oczywistych zalet i zastosowań.

Dane osobowe zawierają m.in. informacje o stopniach naukowych i zainteresowaniach badawczych (te dane na naszym Wydziale trzeba uzupełnić — patrz koniec notatki), co pozwoli, szczególnie młodszym pracownikom, jak również bardziej rozgarniętym studentom, nawiązać kontakty w dziedzinach, które są niedostępne w ośrodkach rodzimych. Umożliwi to, mam nadzieję, oprócz wspólnych badań, także delegowanie doktorantów do innych placówek, aby tam napisali prace doktorskie, a następnie inicjowali na swoich Wydziałach nowe kierunki badań. Podobny system można by stworzyć o stopień niżej i umożliwić również studentom pisanie prac magisterskich poza Wydziałem — muszą oni jednak WIEDZIEĆ, że takie możliwości istnieją oraz znaleźć sobie interesujący ich kierunek (w tym wypadku EMIR mógły odegrać kapitalną rolę). Można spojrzeć na to jeszcze szerzej i uwzględnić pomocniczą funkcję tej bazy dla kandydatów na studia (wrócę do tego później). Zasoby dotyczące publikacji pozwolą nie tylko na czytelny obraz dorobku naukowego poszczególnych osób. Możliwość łatwego dostępu do tekstów źródłowych stanowi niezaprzeczalną zaletę, a mam nadzieję, że stopień konkurencji i wzajemnej zawiści w ambitnym świecie nauki nie uniemożliwi umieszczania tam również prac świeżych, nieopublikowanych, zarysów pomysłów itp. Mogłoby się to rozszerzyć z biegiem czasu w listy dyskusyjne (patrz trochę dalej). Dane o wykładach i seminariach są tak istotne, że truizmem byłoby wyliczać ich zalety. Pominę zatem te oczywistości.

To wszystko na pewno będzie w EMIRZE, lub co najmniej jest już zaplanowane. Nie wyczerpuje to jednak potencjalnych jego zastosowań. Naturalne wydaje się, że również całą organizację, przebieg i rezultaty konferencji naukowych można by umieścić właśnie tu. Nie ma żadnych przeszkód, aby stworzyć mechanizmy dla bieżących (codziennych) relacji, z tego, co się na konferencjach dzieje, włączając w to dokumentację fotograficzną z konferencyjnego życia towarzyskiego. Również materiały pokonferencyjne mogłyby się tam znaleźć. Co prawda zmniejszyłoby to zyski organizatorów z ich sprzedaży, ale to drobiażdżek wobec zysków ogólnych. Wspomniane bazy publikacji mogłyby się rozszerzyć o elektroniczne listy dyskusyjne poświęcone interesującym zagadnieniom matematycznym, na wzór setek istniejących list dotyczących informatyki oraz tysięcy jeszcze innych. Dla niezorientowanych wyjaśniam, iż owe tzw. news-y zapewniają możliwość uczestniczenia w grupowej wymianie poglądów, pytań i odpowiedzi na określony przez użytkowników temat. Do ich czytania używa się bądź specjalnych programów, np. `rn`*, bądź bardziej uniwersalnych narzędzi, jak chociażby* `pine`*. Niektóre z nich umożliwiają automatyczne kierowanie nowych wiadomości w postaci zwykłych e-mail'i do wszystkich uczestników danej grupy dyskusyjnej.*

Jest jeszcze jedna kwestia trochę odbiegająca od EMIRA, a mianowicie użycie sieci do rekrutacji na studia, co wiąże się z koniecznością zmiany samej rekrutacji. Nie mogę o tym nie wspomnieć, gdyż dane było mi uczestniczyć w tym osobliwym spektaklu od strony administracyjnej. Absurd organizacyjny, wynikający z konieczności stosowania się do wielu bzdurnych przepisów, a wymagający najpierw od kandydatów składania wielostronicowych elaboratów, a później od komisji przerzucania ton papieru we wszystkich możliwych kierunkach, był tak dobijający, że tylko sympatyczne towarzystwo życzliwych sobie ludzi spowodowało, iż nie skończyliśmy wszyscy trwałym „bzikiem" (nie mogę nie wspomnieć w tym momencie o Pani Dziekan, dobrym duchu całej komisji — myślę, ze z nikim innym nie byłoby to możliwe do przeprowadzenia). Na szczęście na naszym Wydziale istotna część procedury rekrutacyjnej zmieniła się, miejmy nadzieję, na trwałe. Nie chroni to jednak ciągle przed kopaniem w stertach teczek i wykonywaniem masy całkowicie

BEZSENSOWNEJ pracy. Mam wrażenie, że zamiast przyjmować setki wielostronicowych podań, można by poprzestać na zgłoszeniu uczestnictwa w egzaminie wstępnym poprzez podanie tylko danych osobowych (zawartych w dwóch liniach tekstu!!!!). Wobec powszechności dostępu do sieci zorganizowanie takiej „usługi" na Wydziale wydaje się celowe, nie wspominając już o tym, że bardzo proste. Niestety przypuszczam, iż wszystko to wymagałoby zmiany wielu absurdalnych przepisów pamiętających pewnie wczesny PRL. Możliwość sieciowego zgłoszenia na studia powinna być połączona ze zorganizowaniem (np. w EMIRZE) multimedialnej bazy informacyjnej dla kandydatów na studia, która powinna być swoistą reklamą Wydziału, uwypuklającą wszystkie jego zalety (niestety żyjemy w takich reklamowych czasach). Tę litanię pobożnych życzeń można by kontynuować. Aby jednak chociaż niektóre z nich zaistniały jako fakty rzeczywiste, trzeba dokończyć tworzenie EMIRA tak, by osiągnął masę krytyczną. W związku z tym ośmielam się prosić, aby podejść do tej inicjatywy co najmniej z życzliwością i poświęcić trochę czasu na przygotowanie listy swoich publikacji, tak by mogła ona zostać wprowadzona do wspólnej bazy. Osobne pismo w tej sprawie będzie skierowane do każdego Zakładu. Jak powiedział pewien mądry człowiek: „nadzieja uczy czekać pomaleńku". Poczekajmy zatem na owoce siejąc każdy po ziarenku.

PS. EMIR jest dostępny pod adresem `http://antoni.mat.uni.torun.pl./pol-emir`. *Wszystkie informacje o znalezionych błędach, brakach itp. proszę kierować na adres*

`fraktal@math.amu.edu.pl`.

Szczegóły techniczne dotyczące wprowadzenia publikacji i uzupełnienia danych o zainteresowaniach naukowych będą zawarte w materiałach dostarczonych do Zakładów.

Mgr Wojciech Kowalewski

W Wydawnictwie Naukowym UAM ukazała się książka prof. dra hab. Andrzeja Sołtysiaka *Algebra liniowa. Wykłady z matematyki dla studentów fizyki*, ss. 240.

⋆ ⋆ ⋆ ⋆ ⋆

W tym samym wydawnictwie ukazała się również książka *Serta Mathematica Andreae Alexiewicz* pod redakcją profesorów Lecha Drewnowskiego i Zbigniewa Palki (ss. 166). Zawiera ona materiały z sesji naukowej poświęconej pamięci Profesora A. Alexiewicza, która odbyła się 27.10.1995. Obok artykułów omawiających dorobek naukowy Profesora Alexiewicza w książce zamieszczono także eseje mówiące o jego zainteresowaniach malarskich i muzycznych, jak również reprodukcje jego obrazów.

⋆ ⋆ ⋆ ⋆ ⋆

W Wydawnictwie American Mathematical Society, w serii *Contemporary Mathematics*, opublikowano książkę *Algebraic K-Theory* pod redakcją G. Banaszka, W. Gajdy i P. Krasonia (ss. 210). Zawiera ona materiały z konferencji zorganizowanej w Poznaniu w 1995 r.

⋆ ⋆ ⋆ ⋆ ⋆

W Wydawnictwie Springera (RFN) ukazała się książka *Scheduling Computer and Manufacturing Processes* (ss. 491), której jednym z pięciu współautorów jest prof. dr hab. Jacek Błażewicz.

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Jacek Błażewicz został również jednym z czterech głównych współredaktorów wydawanej przez Springera serii „International Handbook of Information Systems".

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Wacław Marzantowicz poinformował o organizowanych przez Krajowy Fundusz na Rzecz Dzieci warsztatach matematycznych, które odbyć się mają w marcu tego roku w Poznaniu.

Cytat

A man is crazy who writes a secret in any other way than one which will conceal it from the vulgar.

Roger Bacon, ok. 1250

W dniach 14–15.12.1996 w Pałacu Staszica w Warszawie odbyło się zebranie sprawozdawczo-wyborcze Polskiego Towarzystwa Logiki i Filozofii Nauki, połączone z sesją naukową, na której referaty wygłosili profesorowie Wojciech Buszkowski, Jacek Malinowski, Marcin Mostowski, Ewa Orłowska, Jerzy Perzanowski, Andrzej Skowron, Max Urchs, Jan Woleński i Ryszard Wójcicki. Zebranie i sesja były organizowane przez prof. dr hab. Wojciecha Buszkowskiego, a większość środków finansowych pochodziła z dotacji Wydziału Matematyki i Informatyki UAM. Wybrano nowe władze PTLiFN: Zarząd (5 osób), Radę (12 osób) i Komisję Rewizyjną (3 osoby). Nowym Prezesem PTLiFN została prof. dr hab. Ewa Orłowska z Warszawy. Z naszego Wydziału do władz Towarzystwa weszli: prof. dr hab. Wojciech Buszkowski jako były Prezes, dr Kazimierz Świrydowicz jako Sekretarz (ponownie), oraz prof. dr hab. Roman Murawski jako Członek Rady (ponownie).

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 10.12.1996 prof. John H. Coates z Uniwersytetu w Cambridge (Wielka Brytania) wygłosił wykład zatytułowany *The arithmetic of elliptic curves.*

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 11.12.1996, w ramach Seminarium z Algebraicznej K-Teorii prof. John H. Coates wygłosił wykład pod tytułem *Euler characteristics for elliptic curves.*

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 13.12.1996 prof. dr hab. Wiesław Kubiak z Memorial University of Newfunland (Kanada) wygłosił referat zatytułowany *Level schedules and the apportionment problem.*

⋆ ⋆ ⋆ ⋆ ⋆

Gościem Wydziału w dniach 28.11–1.12.1996 był prof. Alexander Šostak z Uniwersytetu w Rydze (Łotwa).

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 6.01–31.03.1997 na stażu naukowym na Wydziale będzie przebywać Pan Ralf Sausen.

⋆ ⋆ ⋆ ⋆ ⋆

Na Zjeździe PTM w Szczecinie, we wrześniu 1996, prof.dr hab. Henryk Hudzik wygłosił referat plenarny zatytułowany *Wybrane zagadnienia z geometrii przestrzeni Banacha*.

⋆ ⋆ ⋆ ⋆ ⋆

Na Zielonogórskich Konfrontacjach 96 we wrześniu 1996 prof. dr hab. Henryk Hudzik wygłosił referat *Formuły Amemiyi dla norm Orlicza i Luxemburga*.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 2.10–18.12.1996 prof. dr hab. Mieczysław Mastyło prowadził badania w Barcelonie (Hiszpania) w Centre de Recerca Matemática.

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Henryk Hudzik wygłosił w listopadzie 1996 r. wykłady na uniwersytetach w Madrycie, Sewilli, Walencji i Saragossie.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 21–24.11.1996 dr Cezary Suwalski jako opiekun grupy studentów przebywał w Bratysławie (Słowacja) na Międzynarodowym Konkursie Informatycznym.

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Zbigniew Palka przebywał w dniach 31.11–14.12.1996 na Uniwersytecie w Bielefeld (RFN).

⋆ ⋆ ⋆ ⋆ ⋆

Na poświęconym pamięci Profesor Heleny Rasiowej minisemestrze *Logic, Algebra and Computer Science*, który w dniach 2–22.12.1996 odbył się w Centrum Banacha w Warszawie, zaproszone referaty wygłosili: prof. dr hab. Wojciech Buszkowski (*Proof-theoretical methods in linguistics* oraz *Learning categorial grammars from linguistic data by unification*) i dr Maciej Kandulski (*Searching for a categorial grammar formalism for natural language syntax*).

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 6–11.12.1996 prof.dr hab. Zygmunt Vetulani przebywał w Salerno (Włochy), gdzie w ramach *Consorzio Lexicon* odbywał się częściowy odbiór projektu *Copernicus 625 Gramlex*.

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Zygmunt Vetulani w dniach 17–23.12.1996 przebywał w LIMSI/CNRS, Orsay (Francja), w ramach wspólnego programu badawczego.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 10–22.12.1996 prof. dr hab. Roman Murawski przebywał na Uniwersytecie w Hanowerze (RFN), gdzie wygłosił wykład oraz prowadził badania naukowe.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 15–22.12.1996 dr Krzysztof Pawałowski przebywał na Uniwersytecie w Hiroszimie (Japonia), gdzie wygłosił odczyt i brał udział w Konferencji z Topologii wygłaszając odczyt plenarny.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 1.01–30.06.1997 prof. dr hab. Jerzy Kąkol prowadzić będzie badania naukowe na Uniwersytecie North Dakota w Ground Forks (USA).

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 6.01–13.05.1997 prof. dr hab. Tomasz Łuczak przebywać będzie na Uniwersytecie w Atlancie (USA).

⋆ ⋆ ⋆ ⋆ ⋆

Prof. dr hab. Mieczysław Mastyło w dniach 6.01–31.05.1997 bedzie prowadzić badania naukowe na Uniwersytecie w Memphis (USA).

⋆ ⋆ ⋆ ⋆ ⋆

Dr Jerzy Jaworski w dniach 13.01–12.02.1997 prowadzić będzie badania naukowe w Düsseldorfie (RFN) na Uniwersytecie Heinricha Heinego.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 14.01–4.02.1996 dr hab. Grzegorz Banaszak i dr Wojciech Gajda w ramach współpracy naukowej przebywać będą na Uniwersytecie w Lozannie (Szwajcaria).

Notatka

Ze względu na objętość, artykuł dra Tadeusza Fryski na temat kryptologii publikujemy w trzech częściach. W numerze bieżącym zamieszczamy część pierwszą — M.K. & R.M.

KILKA UWAG O KRYPTOLOGII

Nieco historii

W „Encyklopedii Powszechnej" PWN znajdujemy określenie:

> **Kryptografia** — *umiejętność konsekwentnego przekształcenia tekstu pisanego, zrozumiałego dla wszystkich, w tekst szyfrowany (kryptogram) zrozumiały dla odbiorcy, znającego umówiony sposób odczytywania zwany szyfrem lub kluczem kryptograficznym.*

Pojęć kryptologia *czy* kryptoanaliza *nie ma wcale. Nieco łaskawiej traktuje sprawę „Słownik Wyrazów Obcych" PWN, w którym kryptografię nazwano już* sztuką*:*

> **Kryptografia** (kryptós = ukryty + grāphō = piszę) — *sztuka pisania znakami zrozumiałymi jedynie dla wtajemniczonych, pismo szyfrowane.*

Poza tym mamy objaśnione terminy kryptogram *oraz* kryptologia*, którą uznano już za* **naukę** *o pismach szyfrowanych, sposobach ich tworzenia i rozwiązywania. Już w tym określeniu widzimy dodatkowy człon, a mianowicie* rozwiązywanie *pism szyfrowanych. Rzeczywiście, zagadnienie to jest istotnie odrębne od tworzenia takich pism i obecnie „wyemancypowało" się już tworząc siostrzane do kryptografii odgałęzienie tej nauki (tzn. kryptologii), a mianowicie tzw.* kryptoanalizę*.*

Takie rozumienie kryptologii było uzasadnione przez całe wieki. Historia ludzkości przeniknięta jest zarówno tworzeniem tajemnic, jak i próbami ich złamania.

Jeszcze do niedawna wymyślne systemy zabezpieczeń były ograniczone w zasadzie do spraw wojskowości. Jedynie tam była wystarczająca motywacja i, przede wszystkim, zasoby finansowe do produkcji pomysłowych mechanicznych urządzeń szyfrujących. Szczególnie sławną maszyną tego typu była ENIGMA, szeroko stosowana przez Niemców w czasie II wojny światowej. Był to istotnie cud techniki swego czasu, tak jak i jej amerykański odpowiednik M-209. Jak wiemy, przy wydatnym udziale Polaków, szyfry Enigmy udało się odczytać (ośrodek brytyjski w Bletchley Park), a co więcej, utrzymać przed Niemcami ten fakt w tajemnicy. (Trzeba jednak wspomnieć, że inna z maszyn szyfrujących Geheimschreiber T-52 *pozostała bezpieczna przez cały okres wojny.)*

Okazuje się, że istnieje związek pomiędzy sukcesami kryptoanalitycznymi Anglików a początkami współczesnej techniki przetwarzania danych. W czasie II wojny światowej Anglicy rozwinęli mianowicie do tych celów szereg urządzeń tak elektromechanicznych, jak i elektronicznych, z których najsłynniejszym jest COLOSSUS, który można uważać za przodka współczesnych komputerów (o technice cyfrowej, a nie analogowej). Trzeba jednak dodać, że matematyk angielski Alan M. Turing (1912–1954), który później był jednym z pionierów w zakresie teorii maszyn obliczeniowych, a w czasie wojny stał na czele grupy kryptoanalityków z Bletchley Park, w powstaniu COLOSSUSA nie odegrał żadnej roli.

Można więc powiedzieć, że kryptologia odegrała znaczącą rolę przy narodzinach współczesnej techniki komputerowej. I musi być źródłem satysfakcji, że niejako w rewanżu rozwój tej techniki przyczynił się w olbrzymim stopniu do ponownych narodzin i rozkwitu kryptologii, jako nauki.

Nowe zastosowania

W miarę, jak elektroniczne przetwarzanie danych pojawia się na coraz to nowych obszarach — w szczególności tych związanych z telekomunikacją — pojawiają się kompletnie nowe zastosowania dla kryptologii, często bardzo odległe od swych klasycznych, militarno-dyplomatycznych źródeł.

Nie potrzeba kryształowej kuli, by przepowiedzieć, że kryptologia (która zaledwie od niedawna jest uznawana za naukę) będzie przeżywać w najbliższych latach jeszcze silniejszy wzrost. A oto jakich zastosowań możemy się spodziewać w najbliższej przyszłości:

- *Liczne rozmowy telefoniczne są już obecnie retransmitowane za pośrednictwem satelitów. Ta droga umożliwia bardzo łatwy podsłuch. W konsekwencji ważne rozmowy telefoniczne muszą być szyfrowane.*

- *Podobny do poprzedniego jest problem telewizji satelitarnej. Nie każdy użytkownik kanału telewizyjnego ma prawo oglądać audycje na nim nadawane (opłata abonamentu). Uwiarygodnienie użytkownika oparte na metodach kryptograficznych okazuje się sposobem bardzo skutecznym.*

- *Podobnie w systemach komputerowych o wielu użytkownikach, każdy użykownik musi zostać uwierzytelniony. Aktualnie robi się to za pomocą haseł; w przyszłości, przynajmniej w zastosowaniach o zwiększonym stopniu bezpieczeństwa, wymagane będzie z pewnością używanie „inteligentnych kart", które zapewnią o wiele wyższy poziom bezpieczeństwa.*

- *Wraz ze wzrostem obrotu „pieniądzem elektronicznym" i całym obrotem bankowym pojawiła się potrzeba dobrego substytutu tradycyjnego podpisu. Tak zwane podpisy elektroniczne pod wieloma względami przewyższają tradycyjny podpis ręczny.*

- *Jako końcowe zastosowanie wspomnimy jeszcze o wirusach komputerowych. Są to małe fragmenty programów wprowadzone z zewnątrz; mają one zdolność samoreprodukcji, co w rezultacie powoduje wiele szkód w programach, zbiorach danych, czy nawet całych systemach. Z grubsza mówiąc, wirus zmienia program nie mając do tego uprawnień. Zatem metody uwierzytelniania danych mogą być również rozpatrywane jako środek walki z wirusami.*

Po rozpatrzeniu tych i innych potencjalnych zastosowań każdy się zgodzi i powie: „Oczywiście, potrzebujemy bezpieczeństwa! Ale dlaczego kryptologia ma być tu polecana jako remedium? Czy nie ma innych sposobów osiągnięcia bezpieczeństwa?" Oczywiście, są inne sposoby! Wystarczy przykładowo pomyśleć o wypracowanych przez stulecia technikach zabezpieczania pieniędzy: specjalny papier, zawikłane (czasem też piękne) rysunki, precyzyjny druk, znaki wodne, specjalne srebrne nitki itd. Zatem, istotnie, dlaczego kryptologia?

Odpowiedź jest prosta: Kryptologia jest lepsza. *Powód jest jeden:* Kryptologia jest dyscypliną matematyczną! *Brzmi to może przesadnie, ale matematyka dostarcza — co najmniej w zasadzie — uzasadnień teoretycznych odnośnie siły poszczególnych algorytmów czy protokołów. Matematyka może udowodnić, że dany algorytm jest bezpieczny. Skoro bezpieczeństwo zostało wykazane matematycznie, to nie może być wątpliwości, że algorytm jest bezpieczny; nie ma potrzeby opieranie się na opiniach ekspertów (czasem sprzecznych), nie trzeba opierać osądu na „dzisiejszym stanie techniki" itp. Należy jednak wspomnieć, że takie dowody uzyskano jedynie w kilku przypadkach. Tym nie mniej, matematyka dostarcza godnych zaufania środków do systematycznego badania — to znaczy analizowania i konstruowania — algorytmów kryptograficznych. To jest wystarczający powód do preferowania mechanizmów natury kryptologicznej przed innymi systemami zabezpieczeń.*

Współczesna kryptologia wykorzystuje osiągnięcia całego szeregu dyscyplin matematycznych. Od dawna w użyciu są teoria liczb czy rachunek prawdopodobieństwa. Matematyczne uzasadnienie pewności systemu daje teoria informacji Shannona, a następnie teoria złożoności obliczeniowej. Nowe algorytmy oparte są na algebrze abstrakcyjnej i

geometrii algebraicznej. Od niedawna przebojem w licznych algorytmach kryptograficznych jest zastosowanie krzywych eliptycznych — tworu, wydawałoby się jak najdalszego od praktycznych zastosowań.

Jak wskazują wymienione zastosowania, kryptologia to nie tylko metody ukrywania informacji przed intruzem. Jedno z jej zasadniczych zadań to integralność i autentyczność informacji. Głównym celem w tym wypadku nie jest ukrywanie informacji, lecz takie jej zakodowanie, że można gwarantować jej dotarcie do adresata bez uszczerbku, niezależnie od tego, czy zamierzonego, czy też nie. Jest to właśnie to zastosowanie, dzięki któremu w ciągu ostatnich dwudziestu lat kryptologia przesunęła się z ograniczonego obszaru zastosowań wojskowych na czołową pozycję w świecie businessu. (Jeden przykład wskaże, jak oczywiście ważne jest to zastosowanie. Nie będzie końca świata, jeżeli wróg się dowie, ile pieniędzy przekazuje się co miesiąc z rachunku uniwersytetu na osobiste konta pracowników; jeśli jednak byłby on w stanie zmieniać tę liczbę, czy też numer rachunku na czeku bez pozostawienia śladu swej ingerencji, to z pewnością by to nas nieco „zdenerwowało".)

Jednym z przełomowych momentów w rozwoju kryptografii było odkrycie przez Diffie i Hellmana w 1976 roku tzw. systemów z kluczem publicznym. Była to prawdziwa rewolucja w kryptologii. Jednym ze wskaźników tej rewolucji jest następujące potem uznanie kryptologii za ważną gałąź matematyki. Ale elegancja kryptologii z kluczem publicznym dostarcza czegoś więcej, aniżeli tylko zabawkę dla matematyków: ona obiecuje być bardzo praktyczna, co faktycznie było przyczyną i racją do jej wykrycia.

Inną ekscytującą nowością są tzw. protokóły o wiedzy zerowej. Chodzi tu o takie prowadzenie dyskusji, by w jej rezultacie przekonać partnera, że jest mi znany np. dowód jakiegoś twierdzenia. Jednakże przebieg dyskusji nie powinien zawierać żadnej wskazówki odnośnie samego dowodu. (Czy jest się w stanie przekonać partnera, że znany jest nam dany sekret nie zdradzając ani cienia owego sekretu.)

Podstawowe pojęcia kryptograficzne

Celem kryptografii jest takie przesłanie informacji przez kanał, by mógł ją odczytać jedynie ten odbiorca, do którego jest ona przeznaczona. Na dodatek, gdy odbiorca już wiadomość otrzymał, to musi mieć zazwyczaj pewność, że wiadomość jest autentyczna, a więc nie jest wysłana przez kogoś, kogo celem jest oszukanie czy wprowadzenie odbiorcy w błąd. Zatem w kryptografii występuje zagadnienie ochrony poufności *informacji (tak utajnić, by odczytać mogła tylko osoba upoważniona do tego) oraz zagadnienie ochrony* autentyczności *danych (nikt nie może podszyć się pod nadawcę i celowo przesłać zafałszowanych danych). Współczesna kryptografia radzi sobie z tymi problemami przy wydatnej pomocy tak algebry abstrakcyjnej, jak i teorii liczb.*

Informacja, która ma być przesłana, nazywa się tekstem jawnym *lub* otwartym *Ten tekst jest przekształcany w* tekst zaszyfrowany *zwany też* kryptogramem. *Tak tekst otwarty, jak i kryptogram są zapisane w pewnym* alfabecie *złożonym z* liter *czy też* znaków. *Te znaki mogą zawierać nie tylko znane nam symbole liter A, B, . . . , Z i a, b, . . . , z, lecz także symbole cyfr, znaki przestankowe i odstępy. Dany* system kryptograficzny *musi przewidywać dwie zasadnicze fazy: proces przekształcania tekstu otwartego w zaszyfrowany, co nazywa się* szyfrowaniem *lub* utajnieniem *oraz proces odwrotny, polegający na przekształcaniu tekstu zaszyfrowanego w tekst jawny zwany* odtajnianiem *lub* deszyfrowaniem. *Istotą różnic między poszczególnymi systemami kryptograficznymi jest stosowany algorytm*

szyfrowania (i deszyfrowania, jako że te dwa procesy są ze sobą związane). Chodzi tu o ogólną zasadę, a nie o poszczególny, jednostkowy efekt. Szyfrowanie tego samego tekstu w danym systemie może dawać rozmaite wyniki. Pozwala to na stosowanie wspólnego systemu przez szersze grono użytkowników. Jednakże nie mogą oni czytać informacji, jeśli nie jest ona przeznaczona konkretnie dla danej osoby. Oznacza to, że dla konkretnego zastosowania danego algorytmu potrzebne są pewne parametry, zwane kluczem szyfrowania (deszyfrowania), *które już mogą ulegać zmianom w ramach danego kryptosystemu. Zatem przekształcenie szyfrujące E_K jest określone przez algorytm E oraz klucz K, zaś analogicznie przekształcenie deszyfrujące D_K jest określone przez algorytm deszyfrowania D (zdeterminowany zastosowanym algorytmem szyfrowania E) oraz klucz deszyfrowania K. Przez długi czas wydawało się, że analogicznie jak algorytmy D i E, tak samo i klucze szyfrowania i deszyfrowania są ze sobą ściśle związane i dlatego mówiło się właściwie o jednym kluczu. Jeśli osoba* A *chce przesłać ukrytą wiadomość do dwu różnych osób* B *i* C *i nie chce, by* B *rozumiał informację przesłaną do* C *(czy na odwrót), to* A *musi użyć dwu różnych kluczy. Jeden z nich jest znany tylko osobie* B*, drugi zaś tylko osobie* C*. Tak działały wszystkie systemy klasyczne. Dopiero od dwudziestu lat wiemy, że można rozłączyć klucz deszyfrowania od klucza szyfrowania w ramach tego samego algorytmu szyfrującego. W takiej sytuacji nie ma potrzeby ochrony klucza szyfrowania, gdyż za jego pomocą i tak nie można informacji odczytać ani odtworzyć klucza deszyfrowania. Ten klucz ma wyłącznie osoba, do której wiadomość jest przeznaczona i tylko ona jest w stanie ją odczytać. Dość paradoksalnie, nie może jej odszyfrować nawet osoba, która tę wiadomość zaszyfrowała, co też ma niebagatelne znaczenie. Powstały systemy z dwoma kluczami, z których jeden może być ujawniony. Dlatego noszą one nazwę* kryptosystemów z kluczem publicznym. *System taki pozwala osobom* A *i* B *na przesłanie informacji do osoby* C *przy użyciu tego samego klucza publicznego osoby* C*, ale odczytać ją potrafi jedynie* C*, gdyż tylko on zna swój klucz deszyfrowania (klucz prywatny).*

Dr Tadeusz Fryska

Opracowanie Informatora: Maciej Kandulski (mkandu@math.amu.edu.pl)
Roman Murawski (rmur@math.amu.edu.pl)