LABORATORY 3

Laboratory of Data Analysis, Error Correction Codes and Cryptology

Head of Laboratory – Dr.Sci. (Technology), Prof. Victor Zyablov
Tel.: (095) 299-50-96; E-mail: zyablov@iitp.ru

The leading researchers of the laboratory include:

Dr.Sci. (Techn.)	V. Gitis	Dr.	S. Pirogov
Dr.Sci. (Math.)	V. Sorokin	Dr.	V. Sidorenko
Dr.	V. Aphanasiev	Dr.	I. Stenina
Dr.	A. Barg	Dr.	A. Trushkin
Dr.	S. Bezrucov	Dr.	A. Weinstock
Dr.	A. Davydov	Dr.	D. Zigangirov
Dr.	E. Jurkov		E. Vashenko
Dr.	V. Pereverzev-Orlov		M. Vitushko
Dr.	E. Petrova		

DIRECTIONS OF ACTIVITY:

- error control codes and information transmission;
- geoinformation technologies and systems;
- partner system design;
- theory of the speech signal.

MAIN RESULTS

ERROR CONTROL CODES AND INFORMATION TRANSMISSION

The following problems are under consideration:

- constructions, decoding and bounds for convolutional and block codes;
- combinatorial problems in vector spaces, covering codes;
- arcs, caps, and saturating sets in projective geometries over finite fields;
- graph theory.

In 2003 year as a continuation and an extension of many years works the following researches and developments are carried out.

Researches and program implementation of algorithms of Sudan, Sudan and Guruswami, for list decoding of Reed-Solomon codes over arbitrary finite fields of characteristic two with using soft decoding are continued. Modification and extending resources of the program complex for list decoding of Reed-Solomon codes "Sudan" are performed. Applying algorithms used in a statistical simulating system is provided. For this a few new functions are implemented: simulating communication channel given by the matrix of probabilities, forming random lists of symbols and their reliability on decoder input, accumulation of statistical characteristics. The work of list decoder is improved due to eliminating extra solutions, appearing because of peculiarities of polynomial factorization algorithm over extended finite fields, and speed-up of interpolation algo-

rithm and operations in finite fields with high extending degree. Connecting the complex "Sudan" with program environment "Matlab" is performed. This allows us to implement simulating concatenated code constructions including the list decoding of Reed-Solomon codes on the last stage and an arbitrary coding on the previous (inner) stage. To provide the work of Sudan algorithm a vast list of irreducible polynomials over finite fields with basis q = 16,32,64 is obtained.

Jointly with MSP ITT the program complex "CODE" for creating and simulating concatenated code constructions based on convolutional codes is developed. The complex takes as a basis a program system for simulating and researches of woven convolutional and turbo codes created in IITP RAS. The complex "CODE" is a modern means for projecting communication systems with error correcting coding. It allows specialists on communication systems to create correcting codes needed and compare them with other variants. Using this complex researches can elaborate and perform a comparative analyzes of distinct perspective coding system. The program product "CODE" is prepared to official registration.

With the help of the complex "CODE" analyzes of distinct concatenated code constructions based on convolutional codes and intended for information transmission in channels with small energy resource, e.g., space channels, is performed.

Asymptotic estimates of error probability for concatenated convolutional code constructions with changeable redundancy are obtained. Transmission algorithms for feedback systems are developed on the basis of these estimates. Computer simulating multiple-access system decoders constructed on an adaptive neural net. Estimates of error probability and adaptation rate for a neural net are obtained. A model of a concatenated construction with space-time-coding (STC) for two transmitting antennas and modulation 4-PSK and 8-PSK is developed. The simulating showed that in the Raleigh channel the construction proposed has effectiveness greater than all known constructions close to it by complexity.

A convolutional code neural net decoder based on multilayer perceptual network and neural net detector of CDMA system are analyzed. Recommendations on the choice of network parameters are obtained.

Edge isoperimetric problems for regular graphs and a new approach to Macaulay posets in graph theory are considered.

Problems connected with digital fingerprinting codes and permutation routing in optical MIN's with minimum number of stages are studied.

Jointly with Ulm University, Germany, an algorithm of finding list of the best ways on trellis is proposed. The algorithm allows us to get the list needed by a universal method with smaller complexity. Decoding concatenated codes using the algorithm proposed is investigated.

Jointly with Perugia University, Italy, constructions of 1-saturating sets in projective geometry PG(n,2) connected with covering codes in coding theory and orbits of stabilizer groups are investigated. The complete classification of 1-saturating sets in geometries with $n < 6$ is performed. New constructions of complete caps in binary projective spaces are proposed.

During 2003 laboratory was cooperated with universities of Germany and Italy. The main topics of the cooperation were continuation of many years' investigations in communication problems and combinatorial problems in vector spaces. With Ulm University (Germany) new approaches to list decoding algorithms was investigated. With Perugia University (Italy) caps and saturating sets in binary projective geometries are studied.

GRANTS FROM:

- **Ministry of Industry, Science and Technology of Russian Federation (contract No. 37.053.11.0062):** "Error correction and source coding: models and algorithms". Head of the project V. V. Zyablov, responsible executor V. B. Afanassiev.

GEOINFORMATION TECHNOLOGIES AND SYSTEMS

Geoinformation approach for forecasting and analysis of spatio-temporal processes and phenomena is under developing. The theoretical results are a base of designed network analitical geoinformation technology and systems. The main principles of the technology are remote access to geographical information (GI), high interactivity of GI analysis, intuitive understandable interface and spatio-temporal data mining facilities. The technology is realized in WWW analytical GISs GeoProcessor and COMPASS, which are problem oriented for analysis and forecasting of natural and social processes and phenomena. The GISs are designed in Java 1.1 (http://www.iitp.ru/projects/geo, http://borneo.gmd.de/and/geoprocessor) in client-server architecture.

GIS GeoProcessor is intended for publication and complex analysis of spatio-temporal characteristics of geological environment and for solving of forecasting and zonation problems in Earth sciences (natural hazard assessment, mineral and oil/gas deposits exploration). The system supports remote access to geographical information, interactive cartographic analysis of grid-based, vector and point data, spatial data mining. The system helps to evaluate the environment properties on the base of principle of analogy using the methods of multidimensional plausible reasoning: method of similarity on a precedent set, method of similarity on expert fuzzy logic knowledge, method of membership function for two classes, method of nonparametric regression.

GIS COMPASS II (Cartography Online Modeling, Presentation and Analysis System) supports analysis of vector GI. Friendly and interactive interface for multilayer vector GI cartographic representation and intuitive understandable tools for spatio-temporal data mining based on interactive analysis of complex properties of geographical objects make the system available for a wide range of the Internet users (non-professionals and specialists). Problem domains of GIS COMPASS are economy, sociology, demography, ecology, policy, marketing research, and management control.

Demonstration databases, which contain geological, geophysical, seismo-tectonic, social, economic and demographic information have been created. The total volume of the data is about 35МБ. The databases are accessible on site http://www.iitp.ru/projects/geo for interactive cartographical exploration and analysis with the help of GISs GeoProcessor and COMPASS. Exploration of the databases by the tools of GISs GeoProcessor and COMPASS confirms their efficiency. It allows to offer free of charge dissemination of GISs GeoProcessor and COMPASS to publish and analyze geographical information for scientific and educational centers of Russia, including the sites of the appropriate RFBR grants.

The methods and the algorithms of the forecast based on the complex analysis of the geodata combining statistical and logic approaches are developed. For construction of a forecast rule two methods, which supplement each other, are used: inductive training on precedents and logic expressions. So the result is empirically verified and verbalized. Methods are tested on a problem of zones allocation of strong earthquakes occurrence with the help of network analytical GIS GeoProcessor.

International cooperation

Cooperation within the framework of the Agreement on scientific and technical cooperation "Spatial-Temporary Data Mining Information Technology for Environmental

and Human Dimension Applications" with Fraunhofer AIS (Germany) is continued. New methods of the spatio-temporal analysis of grid-based and vector data were developed and some methods of GIS GeoProcessor and GIS Descartes (AIS) were integrated.

The agreement on scientific and technical cooperation with Institute of seismology of the Ministry of education and sciences of the Republic Kazakhstan "Development and application of geoinformation technology for complex seismic hazard assessment of Kazakhstan territory" is developed.

The work with Institute of the Earthquake Prediction and Analysis of Chinese State Seismolo-gical Bureau (CSB) was continued within the framework of the agreement on scientific and technical cooperation between RAS and CSB (together with UIPE RAS) "Study and physical interpretation of spatio-temporal variations of earthquake precursors in the North-East China".

The research results were reported on the international conferences and workshops. The systems GeoProcessor and COMPASS were presented with the support of RF Ministry of industry, science and technology at international exhibition on information technologies CeBit'2003 (Germany).

GRANTS FROM:

- **Russian Basic Research Foundation (07-07-90114):** "Web-GIS for interactive analysis of information on geo-referenced data".
- **Ministry of industry, science and technology of Russia: "**WWW geoinformation technology and systems for analysis and forecasting of natural and social processes and phenomena".

PARTNER SYSTEM GROUP

In the expired year in the frame of project of Partner System (PS) the development and investigation of new possibilities of knowledge technology were continued. The attention focus was directed to:

- investigation of approaches to organization of natural language like interaction with integral knowledge base
- spreading of PS technologies to creation of active learning systems
- development of PS shell for OS Windows.

One of the problems of highest interest in organization of interaction with PS is matching of user language and language of system internal knowledge representation, which are a priory different. The matching now can be realized with the use of a Concept Base where each of matched names correlates with a set of different precedents for the essence of those names (text descriptions, images, audio and video files, units of knowledge base). The new principal possibilities we connect with the using of multiple associations between different concepts, which realized in the Space of Associations of Association Hypercube.

In the Windows kernel of PS prototype we can overcome the restrictions of previously created DOS-version of PS created for medicine. This kernel allows to support:

- a process of dialogue accumulation of patients data needed for automatically creation of valuable medical patients history with the possibility of fast and comfortable access to required information parts;

– a free access to various systems help resources (up to multimedia);
– a process of forming of hypothesizes about the patient states, required investigations and treatment with taking into account the individual peculiarities of patient.

The spreading of PS knowledge technology to development of active learning systems was prolonged. The main idea of those systems is creative learning of investigated situations based on the using of examples of problem descriptions and decisions created by specialists and PS. The learning process is organized as a game and includes the training in the methods of personal knowledge formalization and new knowledge creation.

Development of information system to support researches in the field of premature birth on the basis of complex analysis of electrophysiological and clinical data was started.

GRANTS FROM:

- **Russian Foundation of Basic Research (No. 01-01-01020):** "The development of knowledge management methods for large clinical knowledge-based system".
- **Program of Presidium of Russian Academy of Sciences "Mathematical modeling and intellectual systems" (No. 10002-251/П-16/097-096/310303-035):** "Intelligent decision support within the framework of the project "Partner System".

THEORY OF THE SPEECH SIGNAL

A mathematical model of speech perception was developed. The model reproduces main effects observed in the human hearing system: adaptation to signal level; On- and Off-effects; temporal masking, both backward and forward; centre-surround mechanism (lateral suppression) in spectral-temporal area; detecting of amplitude and frequency modulation. The ability of the model to automatic segmentation of the speech signal onto quasi-stationary intervals and formant frequencies estimation was tested.

Four types of instantaneous and integral criteria of optimality in the solving of the dynamic inverse problem for the reconstruction of trajectories of some points inside of the vocal tract measured by means of X-ray microbeam system were studied. Criteria of work, full force, elastic resistance, and kinetic energy were considered. All criteria are able to compensate restriction to jaw movements ("bite-block"), while the reorganization of controls for different articulatory rate was provided only by dynamic criteria of optimality i.e., full force and kinetic energy. It was found that for non-speech movements only instantaneous criteria provide sufficient accuracy of inverse problem solution. Integral criteria are necessary for speech movements.

The accuracy of inverse solution was controlled by synthesis of vowels and diphthongs. There was found subjective similarity of the synthesized and original speech sounds.

PUBLICATIONS IN 2003

Articles

1. Ващенко Е.А., Витушко М.А., Гащенко А.В., Мачинский А.Н. Диалоговый модуль интегральной ПС // Труды конференции "Современные инфокоммуникационные технологии в системе охраны здоровья", Москва, 13-14 ноября 2003 г. С. 25-26.

2. Ващенко Е.А., Витушко М.А., Стенина И.И., Переверзев-Орлов В.С. Интегральная ПС для комплексной поддержки решений врача // Труды конференции "Современные инфокоммуникационные технологии в системе охраны здоровья", Москва, 13-14. ноября 2003 г. С. 19-21.
3. Гитис В.Г., Долгов И.В., Миронов Д.А. Информационно-аналитические проблемы ситуационных центров // Труды Международного семинара "Распределенные компьютерные и телекоммуникационные сети". М.: ИППИ РАН, Техносфера, 2003. С. 185-192.
4. Леонов А.С., Макаров И.С., Сорокин В.Н. Обучающая фонетическая система // Тезисы 4-й Международной конференции "Фонетика сегодня: актуальные проблемы и университетское образование", 2003. С. 79-80.
5. Леонов А.С., Макаров И.С., Сорокин В.Н., Цыплихин А.И. Артикуляторный ресинтез гласных // Информационные технологии в технических и социально-экономических системах. 2003. Т. 3. № 2. С. 73-92.
6. Леонов А.С., Сорокин В.Н. О вычислении команд управления по движениям артикуляторов // Труды 13-й сессии Российского акустического общества, 2003. С. 89-94.
7. Леонов А.С., Сорокин В.Н. Энергетические критерии оптимальности в речевых обратных задачах // Доклады Академии наук. 2003. Т. 392. № 5. С. 694-699.
8. Макаров И.С., Сорокин В.Н. Резонансы речевого тракта с податливыми стенками и разветвлением // Труды 13-й сессии Российского акустического общества, 2003. С. 84-89.
9. Модели и алгоритмы кодирования и сжатия информации. – Отчет о НИР по Госконтракту № 37.053.11.0062, 2003. Руководитель проекта Зяблов В.В., ответственный исполнитель Афанасьев В.Б., исполнители: Давыдов А.А., Трушкин А.В., Штарьков Ю.М., Вайнцвайг М.Н., Хованский А.В., Хованская М.А., Полякова М.П., Цветков М.А., Сидоренко А.В., Осипов Д.С., Скопинцев О.Д.
10. Репин В.Г., Цыплихин А.И. Определение точной верхней грани ошибок метода наименьших квадратов // Радиотехника и электроника. 2003. Т. 48, № 1. С. 91-99.
11. Сорокин В.Н. Модель многослойного первичного анализа речевых сигналов // Труды 13-й сессии Российского акустического общества, 2003. С. 11-16.
12. Сорокин В.Н., Ижнин А.Н., Цыплихин А.И., Чепелев Д.Н. Артикуляторно-ориентированная система распознавания речи // Труды Международного семинара "Диалог 2003". С. 657-662.
13. Сорокин В.Н., Цыплихин А.И. Аппроксимация распределений малопредставительных выборок // Труды 13-й сессии Российского акустического общества, 2003. С. 95-100.Andrienko G., Andrienko N., Gitis V. Interactive maps for visual exploration of grid
14. and vector geodata // ISPRS Journal of Photogrammetry & Remote Sensing. 2003. V. 57. P. 380-389.
15. Barg A, Blakley G.R., Kabatiansky G. Digital fingerprinting codes: Problem statements, constructions, identification of traitors // IEEE Transactions on Information Theory. 2003. V. 49. No. 4. P. 852-865.
16. Baumgartner B., Bossert M., Zyablov V. On Active Distances for Nonlinear Trellis Coded Modulation // In Proceeding of the 3rd Intern. Symposium on Turbo Codes & Related Topics. Brest, France. Sept. 1-5, 2003.

17. Bezrukov S.L., Das N., Bhattacharya B.B., Menon R., Sarkar A. Permutation routing in optical MIN's with minimum number of stages // Journal of Systems Architecture. 2003. V. 48. P. 311-323.
18. Bezrukov S.L., Elsaesser R. Edge-Isoperimetric problems for powers of regular graphs // Theoretical Computer Science. 2003.
19. Bezrukov S.L., Pfaff T., Piotrowski V.P. A new approach to Macaulay posets // Journal of Combinatorial Theory, Series A. 2003.
20. Davydov A.A., Marcugini S., Pambianco F. On saturating sets in projective spaces // Journal of Combinatorial Theory, Series A. 2003. V. 103, P. 1-15.
21. Fahrner A., Griesser H., Klarer R., Zyablov V.V. Low-Complexity GEL Codes for Magnetic Storage Systems // Submitted to IEEE Trans. On Magnetics. Oct. 2003.
22. Fahrner A., Zyablov V.V., Bossert M. Embedded Codes for Digital Magnetic Recoding. // In Proceeding of the 7th ISCTA. Ambleside, UK, July 13-18, 2003.
23. Freudenberder J., Zyablov V.V. On the Complexity of Suboptimal Decoding for List and Decision Schemes // Proceedings of Workshop Coding and Cryptography. Versailles, France. March 2003. P. 193-202.
24. Gitis V., Andrienko G., Andrienko N., Analytical web GIS for decision support in seismological problem domain // Abstracts of the XXII General Assembly IUGG, Sapporo, Japan, 2003.
25. Gitis V., Sobolev G., Ponomarev A., Kazakov V., Kurskeeva L., Belosliudtsev O. Spatio-temporal geoinformation modeling for exploration of earthquake preparation processes // Abstracts of the XXII General Assembly IUGG, Sapporo, Japan, 2003.
26. Gitis V.G. Geoinformation technologies for analysis of seismotectonic processes // National report to the International Association of Seismology and Physics of the Earth's Interior of the International Union of Geodesy and Geophysics 1999 – 2002. Presented to the XXIII General Assembly of the International Union of Geodesy and GeophysicsNevskiy M.V. (Chief Editor), Zavyalov A.D. (Deputy Chief Editor), Gliko A.O., Grachev A.F., Kuznetsov I.V., Ulomov V.I., Khrometskaya E.A. (Scientific Secretary). National Geophysical Committee, RAS, Moscow 2003. P. 42-51. http://www.wdcb.ru/NGC/NRIASPEI03.html .
27. Handlery M., Johannesson R., and Zyablov V.V. Boosting the Error Performance of Suboptimal Tailbiting Decoders // IEEE Trans. Communication. V. 48. Jan. 2003. P. 149-161.
28. Leonov A.S, Sorokin V.N. Optimality criteria in inverse problems for tongue-jaw interaction // Proc. EuroSpeech' 2003. P. 2353-2356.
29. Pavlouchkov V., Johannesson R., Zyablov V.V. On the Burst Error Detection and Erasure Correction Capabilities of Convolutional Codes // Proceedings of 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, June 29 – July 4. 2003.
30. Schmidt G., Sidorenko V., Zyablov V., Bossert M. Finding a list of best paths in a trellis. 2003 (препринт).
31. Schmidt G., Zyablov V.V., Bossert M. On Expander Codes Based on Hypergraphs // In Proceeding of 2003 IEEE Intern. Symposium on Inform. Theory, Yokohama, Japan, 2003 June 29 – July 4.
32. Sorokin V.N. Some coding properties of speech // Speech Communication. 2003. V. 40. No. 3. P. 409-423.
33. Vaschenko E., Vitushko M., Pereverzev-Orlov V. Potentials of Learning on the Basis of Partner System // Pattern Recognition and Image Analysis". 2004. V. 14. No. 1. P. 84-91.

Institute for Information Transmission Problems

In print

1. Баден П., Макаров И.С., Сорокин В.Н. Алгоритм вычисления площадей поперечных сечений речевого тракта // Акустический журнал (в печати).
2. Гитис В.Г., Андриенко Г.Л., Андриенко Н.В. Исследование сейсмологической информации в сетевых аналитических ГИС // Физика Земли (в печати).
3. Гитис В.Г., Ермаков Б.В. Основы пространственно-временного прогноза в геоинформатике // Принято на конкурс научных публикаций РФФИ. 25 п.л.
4. Гитис В.Г., Петрова Е.Н., Пирогов С.А. Модель локального взаимодействия компонент геоэкологической структуры // Информационные процессы. 2003 (в печати).
5. Макаров И.С., Сорокин В.Н. Резонансы речевого тракта с податливыми стенками и разветвлением // Акустический журнал (принято к публикации).
6. Сорокин В.Н., Чепелев Д.Н. Модель первичного анализа речевых сигналов // Акустический журнал (принято к публикации).
7. Barg A., Kabatiansky G. A class of i.p.p. codes with efficient identification // Journal of Complexity (Special issue devoted to H. Niederreiter) (в печати).
8. Barg A., Zémor G. Concatenated codes: Serial and parallel (в печати).
9. Barg A., Zemor G. Error exponents of expander codes under linear-time decoding // SIAM Journal of Discrete Mathematics (в печати).
10. Baumgartner B., Jordan R., Bossert M., Zyablov V.V. On Something Obvious and Irrelevant for Trellis Coded Modulation // To be presented on 5th Intern. ITG 2004 Conference, Jan. 14-16, 2004.
11. Bezrukov S.L. Discrete extremal problems // Invited article, Big Russian Encyclopedia (в печати).
12. Davydov A.A., Faina G., Pambianco F. Constructions of Small Complete Caps in Binary Projective Spaces // Designs, Codes and Cryptography (в печати).
13. Davydov A.A., Marcugini S., Pambianco F. Complete caps in projective spaces PG(n,q) // Journal of Geometry (в печати).
14. Davydov A.A., Marcugini S., Pambianco F. Linear codes with covering Radius 2,3 and saturating sets in projective geometry // IEEE Transactions on Information Theory (в печати).
15. Fahrner A., Griesser H., Klarer R., Zyablov V.V. Generalized Error-Locating Codes for Magnetic Storage Systems. // to be presented on 5th Intern. ITG 2004 Conference, Jan. 14-16, 2004.
16. Fahrner A., Griesser H., Klarer R., Zyablov V.V. Low-Complexity GEL Codes for Magnetic Storage Systems // To be presented on 9th joint MMM-Intermag Conference, Anaheim, California. Jan. 5-9 2004.
17. Leonov A.S., Sorokin V.N. Controls in the internal model: Score reorganization and compensation // Pattern Recognition and Image Analysis (в печати).