Institute for Information Transmission Problems

LABORATORY 3

Laboratory of Information Technologies and Data Protection

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.	V. Potapov
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		J. Makarov
Dr.	V. Pereverzev-Orlov		A. Tsyplikhin
Dr.	E. Petrova		E. Vashenko
Dr.	S. Pirogov		M. Vitushko

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 and decoding for convolutional, block and concatenating codes;
- combinatorial problems in vector spaces and projective geometries over finite fields, covering codes;
- graph theory;
- cryptography.

In 2004 year as a continuation and an extension of many years works the following researches and developments are carried out.

Researches and program implementation of the algorithm of Sudan-Guruswami for the list decoding of Reed-Solomon codes with using soft decoding are continued. Modification and improving characteristics of the program complex "Sudan's Algorithm" are performed. A cardinal method of reducing algorithm labor intensiveness, connected with search of common divider of two interpolation polynomials with the least weighted degree, is proposed. New methods forming random lists of symbols and their reliability on decoder input are developed and investigated. To reduce the complexity of the computing process approaches decreasing weights of irreducible polynomials over arbitrary finite fields of the characteristic two are created.

The program complex "CODE", developed jointly with International union of instrument-makers and specialists for information and telecommunication technologies in 2002 – 2004, is modified. The complex is a modern means for creating and simulating communication systems with concatenated error correcting coding on the base of convolutional codes. The abilities of the complex are extended essentially. As components the convolutional codes with rate from 1/4 up 8/9 and memory from 2 up 6 can be used. It give us performance capabilities to project and to research concatenated constructions in the wide region of rates from 1/7 up 8/9 and memory up 7.

The program complex "CODE" was presented on the exhibition CeBIT in the part "Computer Science of Russia" in Hanover city (FRG) and official registered in All-Russian science-technical information center (VNTIC) of Ministry of education, industry, science and technologies of Russian Federation.

For main lines of information transmission by optical channel the method of error correcting coding based on generalized concatenated codes with error localization is developed. The method allows us to reach reliability needed for redundancy 3.3%. The best coding system developed in USA has redundancy 7% and works for rate up 10 Gbit. Implementation of codes proposed is essentially simpler and therefore it is possible to obtain the rate 40 Gbit.

Investigations of characteristics of neural net detector of asynchronous DS-CDMA system based on a Hopfield network are performed and recommendations on the choice of its parameters are developed. An algorithm for finding the starting state of a feedback tailbiting encoder is proposed, based solely on the properties of the encoder state diagram.

Jointly with Ulm University, Germany, investigations of an algorithm of finding list of the best ways on trellis are continued. It is proved that the algorithm proposed forms the code word list by the optimal manner and allows us to estimate the reliability of the list obtained. Jointly with Ulm University generalized codes with error localization for protection of information on magnetic tape are developed too. The protection method developed provides the best reliability for redundancy given. Its implementation complexity is smaller than that of the known methods. Jointly with Lund University, Sweden, on the base of the graph theory the analyze of effectiveness of protection of code and information symbols for convolutional codes is developed. It is shown that the unequal protection of code and information symbols can be designed basing on the woven convolutional codes.

The first known family of concatenated codes whose distance asymptotically exceeds the product bound for all rates different from 0 and 1 is constructed. New results for the error exponent of distinct classes of codes are obtained. A new segment of code rates in which the reliability function of the binary symmetric channel is known exactly is provided. It improves over the result of P. Elias of 1955. A class of codes is constructed with positive rate and a polynomial-time identification procedure.

In the graph theory the survey of the Macaulay posets is performed and new explicit constructions of Macaulay posets are proposed. Their order is obtained.

Jointly with Perugia University, Italy, the new concept of linear locally-optimal covering codes (similar to saturating sets in projective geometry) is introduced. New combinatorial and extremal problems are formulated. Ways of their solving are proposed. The known extremal problems are studied in framework of the new concept.

In cooperation with Ulm University (Germany), there is shown that every multidimensional cyclic Gray code can be uniquely represented as the direct product of one-dimensional those. The interrelation between multicarrier spread spectrum (MC-SS) transmission and multilevel coding is revealed. It is shown that MC-SS systems

can be interpreted as a multilevel code with repetition codes in all levels. An algorithm for error and erasure correction of interleaved Reed-Solomon codes based on a modified algorithm of Bleichenbacher et al. is proposed. Bounds on the cardinality of a polyalphabetic code are obtained. Constructions of polyalphabetic codes based on monoalphabetic ones and allowing to reach Singleton type bound are suggested. A metric modification for the Viterbi decoder improving characteristics of trellis-coded modulation is developed.

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".

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.

The model describing process of interaction a component of complex spatial structure is offered. The structure can consist both of geographical objects, and from the conditionally allocated region fragments. The basic assumption of model is that - the components of structure interact only locally, that is only at presence of direct spatial or functional connections.

A grid based simulation model of surface waterflow dynamics in the urbanized territory is created. The model describes the quantity of moving water as a function of spatial coordinates and digital fields of surface heights, soil infiltration coefficients, locations of asphalt covering and buildings. The model belongs to the class of models with distributed parameters, i.e., input parameters of the model are essentially spatially non-homogeneous geological and geophysical data. The model is a basis

for a new model simulating the process of transference and accumulation of a pollutant with surface waterflow. The model of surface waterflow dynamics is prog-rammed by means of MatLab package and is tested on the data simulated in such a way that it reflects the main features of real geo-ecological processes.

The relationships between tidal force and seismicity at global and local levels caused by a lunar attraction were investigated. As a result of research with use of model of interaction 2 bodies (Eart-Moon) is revealed statistical relationships between some components tidal forces and seismic characteristics. In particular, the relationship between daily variation of the tidal force and frequency of earthquakes for separate latitudinal sectors is revealed. Examples of areas on the Earth seismically sensitive to various components of tidal force are specified. Correlations between magnitude and longitudinal component tidal force for separate sectors are found out.

The technology of the spatial-temporal analysis of the geology-geophysical information is improved; the complex of software including intensive use of statistical estimation methods and hypotheses testing in a combination with the cartographical data analysis is developed. It has allowed to carry out the complex analysis of the seismic and astrometry data and to facilitate revealing a number of relationships connecting tidal force with seismic process.

The GIS project COMPASS-RFBR for monitoring and complex analysis of the Russian science is developed on the basis of network system "COMPASS". The indicators (statistical parameters) are calculated on a database of the Russian fund of basic researches (RFBR). DB includes the information contained in the annual competitive proposals and the reports on the accepted projects. The indicators allow to estimate creative activity and efficiency of scientific researches of the institutes, departments, fields of knowledge and regions, and also to analyze dynamics of change of scientific interests.

The analysis of methods of the geoinformation analysis of stationary geophysical fields is executed on the basis of network system the Geoprocessor. The geoinformation resourcese of RAS scientific station are analyzed, the GIS-projects for RAS scientific station and Central Asia region are prepared.

The results are published in the papers and were reported at the international conferences and seminars.

The systems Geoprocessor and COMPASS were demonstrated at the International exhibition of information and telecommunication technologies CeBit '2004 (Germany) with support Minpromnauki of Russian Federation

GRANTS FROM:

- **Russian Basic Research Foundation (07-07-90114):** "Web-GIS for interactive analysis of information on geo-referenced data".
- **Russian Basic Research Foundation** (№ 03-07-90114): "Network geoinformation technology for spatial-temporal analysis of geo-ecological state of urbanized territory".
- **Basic researches program of Presidium of RAS № 21, section "Electronic Earth":** "Development the geoinformation technology and network instrumental tools for revealing of the essential information and knowledge on processes and phenomena in the Earth sciences".
- **Basic researches program of Presidium of RAS № 21, section "Electronic Earth":** "Methods, technology and network analytical GIS for the complex analysis of geophysical fields on example of RAS scientific station".

Institute for Information Transmission Problems

PARTNER SYSTEM GROUP

The work was conducted on two directions of researches: development of methods of active interaction of the user with integrated knowledge base within the framework of the project on creation of partner system for the medical applications and creation of information system of information system to support researches in the field of premature birth based on the analysis of clinical data and data of uterine activity monitoring.

The research prototype of the program for interactive graphic support of knowledge acquisition process was created. The new version of the dialogue module ensuring coordinated usage of the independent parts of input data and corresponding local and integral knowledge bases for general conclusion forming was developed. The new method of adaptive dialogue scenario forming was proposed. It is based on the choosing of the most activated elements in the knowledge base that match the key symptoms selected by the user.

The information system for in-depth analysis of biophysical and clinical data to solve several obstetrical problems of current importance is under development. The re-search was carried out on prospects of vibratory sensors as a data source of contractive uterus and fetal heart activity. This type of sensors seems to be more secure, space-saving and economical compared with other known means of obstetrical monitoring. The preliminary results obtained allows one to rate vibratory sensors as acceptable instruments to get the initial data for the contrived tasks of recognition of various pregnancy and delivery anomalies.

The experimental versions of hardware system for registration of the data and program system of accumulation, visualization both analysis of signals and clinical descriptions are created. The signal analysis program package to be built will include methods of automatic contraction marking, estimates of their frequency and depth, methods of estimation of mother and fetal heart rate and decomposition methods of complex vibration signal into its components complying with basic vibration sources (breathing, mother and fetal heart rate, etc).

GRANTS FROM:

- **Russian Foundation of Basic Research (No. 04-07-90225)**: "Development of information system to support researches in the field of premature birth on the basis of complex analysis of electrophysiological and clinical data".
- **Program of Presidium of Russian Academy of Sciences "Mathematical modeling and intellectual systems":** "Intelligent decision support within the framework of the project "Partner System".

THEORY OF THE SPEECH SIGNAL

An inverse problem with respect to the shape of the vocal tract and articulatory parameters for the fricative sounds of the Russian and English was investigated.

Taking into account the inclination of the solution of the inverse problem to the instability, it was necessary to find such acoustic parameters of the spectrum of the fricative sounds which would little depend on a type of the microphone and the distance to it. The search for these parameters was carried out with the use of a vast database for the Russian language, recorded for 69 speakers, while 47 speakers' speech was simultaneously registered by two different types of the receivers, placed

at the different distances from the speaker's mouth. Totally, 4 types of the microphones and the 2 two types of telephone sets were used, and the part of the database was passed across a simulator of telephone channel.

The statistical analysis has allowed to find the most stable parameters of the fricative sounds. The parameters include: the tilt of regression line for the average spectrum of the fricative; the frequency of the spectrum center gravity in the high frequency region with energy, exceed regression line; the frequencies of the first intersection "up – down" of spectrum envelope the regression line counting from low frequency and from high frequency. These parameters were used in a solution of the inverse problem for the fricatives of the English /*s, sh, f, θ, ð, h, z, zh*/ for which there was a database with a synchronous recording of a trajectory of the motions of 8 pellets on the inner surfaces of the vocal tract, measured on the X-ray microbeam.

In one task, only acoustic parameters of the speech signal were used as the input data, and the trajectories of the pellets motions together with the acoustic parameters were used for another task. In both tasks the error of the estimation of the measured coordinates of the points was, on the average, fewer 3%, and a difference between the solutions in a space of the articulatory parameters was about 3.6%. The perceptive control of the quality of the solution of an inverse problem was executed by a synthesis of the syllables "vowel-fricative-vowel" by the articulatory synthetizer. The vocal tract shape and the areas of its cross-section, obtained as the solution of the inverse problem served as the initial data for a synthesis. The sounding of the synthesized syllables has turned out very close to the original syllables.

PUBLICATIONS IN 2004

Books

1. Гитис В.Г., Ермаков Б.В. Основы пространственно-временного прогнозирования в геоинформатике. М.: Физматлит, 2004.

Articles

1. Баден П., Макаров И.С., Сорокин В.Н. Алгоритм вычисления площадей поперечных сечений речевого тракта. *Акустический ж.*, 2004, т. 50, № 6, стр. 739-745.
2. Гитис В.Г., Андриенко Г.Л., Андриенко Н.В. Исследование сейсмологической информации в сетевых аналитических ГИС. *Физика Земли,* 2004, № 3, стр. 43-53.
3. Гитис В.Г., Петрова Е.Н., Пирогов С.А. Модель локального взаимодействия компонент геоэкологической структуры. *Информационные процессы,* 2004, том 4, № 1, стр. 1-7.
4. Зяблов В.В., Йоханнессон Р., Павлушков. В.А. Обнаруживающие и корректи-рующие способности сверточных кодов. *Проблемы передачи информации*, 2004, т. 40, № 3, стр. 3-13.
5. Кузнецов Н.А., Гитис В.Г. Сетевые аналитические ГИС в фундаментальных исследованиях. *Информационные процессы,* 2004, том 4, № 3, стр. 221-240.
6. Леонов А.С., Макаров И.С., Сорокин В.Н., Цыплихин А.И. Артикуляторный ресинтез фрикативных. *Информационные процессы*, 2004, т. 4, № 2, стр. 141-159.
7. Макаров И.С., Сорокин В.Н. Резонансы разветвленного речевого тракта с податливыми стенками и разветвлением. *Акустический ж.*, 2004, т. 50, № 3, стр. 389-396.

8. Сорокин В.Н. Структура проблемы автоматического распознавания речи. *Информационные технологии и вычислительные системы*, 2004, № 2. стр. 25-40.
9. Сорокин В.Н., Цыплихин А.И. Сегментация и распознавание гласных. *Информа-ционные процессы*, 2004, т. 4, № 2, стр. 202-220.
10. Afanassiev V.B., Davydov A.A., Podzorov S.V. Some hints on implementation of soft Sudan decoding. *Proc. Ninth International Workshop on Algebraic and Combinatorial Coding Theory. ACCT-IX*. Kranevo: 2004, pp. 7-13.
11. Barg A. Improved error bounds for the erasure/list scheme: the binary and spherical cases. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 10, pp. 2503-2511.
12. Barg A., Kabatiansky G. A class of IPP codes with efficient identification. *Journal of Complexity*, 2004, vol. 20, no. 2-3, pp. 137-147.
13. Barg A., McGregor A. Distance distribution of binary codes and the error probability of decoding. *Preprint. Arxiv. org/cs. IT/0407011*, 2004.
14. Barg A., McGregor A. List decoding of concatenated codes: improved performance estimates. Proc. *IEEE International Symposium on Information Theory.* Chicago: 2004.
15. Barg A., Zemor G. Error exponents of expander codes under linear complexity decoding. *SIAM Journal on Discrete Mathematics*, 2004, vol. 17, no. 3, pp. 426-445.
16. Baumgartner B., Sidorenko V., Bossert M. Multicarrier spread spectrum: a coding perspective. *Proc. Eighth IEEE International Symposium on Spread Spectrum Techniques and Applications. Sydney, Australia,*2004, pp. 61-66.
17. Bezrukov S.L., Pfaff T., Piotrowski V.P. A new approach to Macaulay posets. *Journal of Combinatorial Theory*, Series A, 2004, vol. A-105, no. 2, pp. 161-184.
18. Davydov A.A., Marcugini S., Pambianco F. Complete caps in projective spaces PG(n,q). *Journal of Geometry*, 2004, vol. 80, no. 1-2, pp. 23-30.
19. 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*, 2004, vol. 50, no. 3, pp. 537-541.
20. Davydov A.A., Marcugini S., Pambianco F. Minimal 1-saturating sets and complete caps in binary projective geometries. *Proc. Ninth International Workshop on Algebraic and Combinatorial Coding Theory. ACCT-IX*. Kranevo: 2004, pp. 113-119.
21. Fahrner A., Griesser H., Klarer R., Zyablov V. Low Complexity GEL Codes for Digital Magnetic Storage Systems. *IEEE Transactions on Magnetics*, 2004, vol. 40, no. 4, pp. 3093-3095.
22. Handlery M., Johannesson R., Zyablov V.V. On error exponents for woven convolutional codes with one tailbiting component code. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 8, pp. 1809-1811.
23. Jordan R., Host S., Johannesson R., Bossert M., Zyablov V.V. Woven convolutional codes II: Decoding aspects. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 10, pp. 2522-2529.
24. Jordan R., Pavlushkov V., Zyablov V.V. Maximum slope convolutional codes. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 10, pp. 2511-2522.
25. Korobkov D., Potapov V., Sidorenko V. Decoding of trellis coded modulation with shaping. Proc. International Symposium on Information Theory and its Applications. ISITA 2004. Parma, Italy. 2004, pp. 1503-1506.
26. Leonov A.S., Sorokin V.N. Controls in the internal model: Score reorganization and compensation. *Pattern Recognition and Image Analysis*, 2004, v.14, no. 3, pp. 407-420.

27. Pavlushkov V., Johannesson R., Zyablov V.V. On unequal error protection for code symbols via active distances. *Proc. Ninth International Workshop on Algebraic and Combinatorial Coding Theory. ACCT-IX*. Kranevo: 2004, pp. 319-326.
28. Schmidt G., Sidorenko V., Zyablov V., Bossert M. Finding a list of best paths in a trellis. Proc. International Symposium on Information Theory. ISIT 2004. Chicago, USA. 2004, pp. 555.
29. Sidorenko V., Starykh. M. Decomposition of multidimensional Gray codes. *Proc. Ninth International Workshop on Algebraic and Combinatorial Coding Theory. ACCT-IX*. Kranevo: 2004, pp. 355-361.
30. Trushkin A.V. State diagram approach to feedback encoders for tailbiting codes. *Информационные процессы*, 2004, vol. 4, no. 1, pp. 8-12.

In print

1. Вайншток А.П., Гитис В.Г., Либкинд А. Н., Либкинд И.А., Минин В.А., Фадеев В.Ю. Геоинформационные аспекты мониторинга российской науки: индикаторы и инструментарий. *Информационные процессы.*
2. Сорокин В.Н., Чепелев Д.Н. Модель первичного анализа речевых сигналов. *Акустический ж*.
3. Юрков Е.Ф., Гитис В.Г. Области, сейсмически чувствительные к приливной силе. *Физика Земли.*
4. Barg A., Zemor G. Multilevel expander codes. *Algebraic Coding Theory and Information Theory. AMS-DIMACS series.* Providence: AMS.
5. Schmidt G., Sidorenko V.R., Bossert M. Error and erasure correction of interleaved Reed-Solomon codes, accepted to International Workshop on Coding and Cryptography, WCC 2005, 2005, Bergen, Norway

Reports and preprints

1. Модели и алгоритмы кодирования и сжатия информации. *Итоговый отчет о НИР по Госконтракту № 37.053.11.0062*, 2004. 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.
2. Barg A. On the asymptotic accuracy of the union bound. *Preprint. Arxiv. org/cs. IT/0412111,* 2004*.*
3. Barg A., Zemor G. Distance properties of expander codes. *Preprint. Arxiv. org/cs. IT/0409010*, 2004.
4. Sidorenko V., Schmidt G., Gabidulin E., Bossert M., Afanassiev V. On polyalphabetic block codes. Preprint. Ulm University, 2004.

Abstracts

1. Беликова Т.П., Стенина И.И. Получение знаний для поддержки интерпретации изображений. *IV Специализированная выставка и конфере-нция "Информционные технологии в медицине*. М.: ВК ВВЦ ,2004, стр. 118-121.
2. Сорокин В.Н. Верификация диктора по его голосу. 6 Международная конф. *"Комплексная защита информации",* 2004, стр. 119-120.
3. Gitis V.G. Experience of spatio-temporal seismotectonic data mining in multi-dis-ciplinary measurements. *Proceedings of European Seismological Commission XXIX General Assembley*, Potsdam, 2004, pp. 146-147