Institute for Information Transmission Problems

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 2002 year as a continuation and an extension of many years works the following researches and developments are carried out.

Researches and development of rearrangements in turbo codes and woven convolutional codes maximizing code distance and optimizing weight distribution are performed. Nonrandom rearrangements based on linear and cubic transformations modulo code length are proposed. A program system permissive to research and to choose rearrangements for turbo and woven convolutional codes efficiently is created. An analysis of concatenated schemes based on convolutional codes is executed.

A basic version of a program system for simulating and researches of concatenated code constructions based on convolutional codes is developed. This system permits to create distinct constructions from built-in sets of convolutional codes and interleaving types, to research distance characteristics of constructions, to create distinct variants of concatenated and iterative decoders, to perform a statistical simulating for estimates probability characteristics of code constructions and decoders.

Jointly with Lund University, Sweden, a construction of woven convolutional codes with one tailbiting component code is developed. This construction has better parameters than a woven convolutional code with the same convolutional codes-components but without tailbiting. Estimates of correcting properties of convolutional and tailbiting convolutional codes based on their active distances are obtained. A suboptimal decoding algorithm of tailbiting convolutional codes is proposed. This algorithm has the same probabilistic characteristics as the optimal decoder but its implementation complexity is essentially smaller. Metric characteristics of an estimate of correcting properties for window decoding of convolutional codes are obtained.

Jointly with Ulm University, Germany, researches of woven codes based on bipartite graphs and hypergraphs-extenders with block codes as components are executed. Random methods constructing codes based on bipartite graphs and hypergraphs-extenders with Read-Muller codes as components are developed. Program systems for simulating are created. Simulation results show big availability of the considered class of woven codes.

Estimates of probabilistic characteristics for decoding binary codes into a list defined by code words in a sphere of a given radius are investigated. Relations between probabilities of error and rejection of decoding are obtained. For a small radius this relations are better than known those.

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 are performed. A soft decoding for these approaches is investigated also. A basic version of a program system for simulating and researches of list decoding of Reed-Solomon codes is developed. This system includes whole and stage-by-stage implementation of the list decoding algorithm of Sudan and Guruswami with assignment of input lists with the most probable values of symbols and forming a list of the most probable output code words. The system permits to analyze work and complexity of all stages of the algorithm. It can be used in the educational programs of high Schools on professions of telecommunication and information protection.

The problem of symbol by symbol a posteriori probability decoding for information symbols of nonsystematic encoded block codes is considered. An extended trellis representation for block codes is introduced that enables the application of the known BCJR algorithm as well as trellis based decoding in the dual code space. Complexity properties of the extended trellis are investigated.

OFDM transmission over time varying mobile radio channels is considered. A class of (L, R) channels is introduced. For the (L, R) channel, the duration of the impulse response is upper bounded by L and the spectrum of the impulse response is zero except for the first R components. An algorithm for maximum likelihood estimation of the transfer function of the (L, R) channel is suggested.

By simulations in AWGN and fading channels it is shown that for certain conditions suboptimal iterative multistage decoding is very close to optimal maximum likelihood decoding and even improves it if interleaving is used.

Bounds on the covering radius of linear codes with a known dual distance, bounds on packings of spheres in the Grassmann manifolds, a low-rate bound on the reliability of a quantum discrete memoryless channel, some polynomials related to weight enumerators of linear codes, and random codes are investigated. A number of researches connected with error exponents are performed.

In graph theory the following problems are considered: edge isoperimetric problems for regular graphs, a new approach to Macaulay posets, a local-global principle for vertex-isoperimetric problems.

Institute for Information Transmission Problems

Jointly with Perugia University, Italy, relations and close properties of saturating sets in projective geometry PG(n,q) and covering codes in coding theory are investigated. With using these relations upper and lower bounds, constructions, and infinite families of codes and sets are obtained. With the help of computer many new relatively small 1-saturating sets in PG(2,q) and 2-saturating sets in PG(3,q) are constructed. New constructions of “small” complete caps in binary projective spaces are proposed.

During 2002 laboratory was cooperated with universities of Germany, Sweden 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) woven convolutional codes based on bipartite graphs and hypergraphs-extenders with block codes as components was investigated. With University of Lund (Sweden) woven convolutional codes using cyclic closed convolutional codes as one of components was created and analyzed. Royal Academy of Sweden supports these investigations. With Perugia University (Italy) arcs, caps, and saturating sets in projective geometry over finite fields 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 technology of new generation is under developing. Fundamental principles of the technology are remote access to geographical information (GI), high interactivity of GI analysis, intuitive understandable interface and spatio-temporal data mining tools.

The fundamental principles of geoinformation technology are realized in the network analyti-cal GIS GeoProcessotof and COMPASS, problem domains of which are analysis and forecasting of natural and social processes and phenomena. The GISs are designed in Java 1.1 in client-server architecture (http://www.iitp.ru/projects/geo, http://borneo.gmd.de/and/geoprocessor).

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 non-parametric 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. The database for GIS GeoProcessor contains the digital models of topography, geophysical fields, geological faults, catalogues of earthquakes and topographical elements. The database for GIS COMPASS contains examples of social and economic information on Russian Federation and World Countries, as well as an example of census data on region of Manchester.

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 analyse geographical information for scientific and educational centres of Russia, including the sites of the appropriate RFBR grants.

International cooperation.

Cooperation within the framework of the 5FP IST program under the project "Spatial mining for Data of Public Interest" (acronym SPIN!, contract IST-1999-10536) was continued. The following countries participate in the Project: Germany, Italy, Great Britain and Netherlands. Very close problems are investigated in scope of the Agreement on scientific and technical cooperation "Spatial-Temporary Data Mining Information Technology for Environmental and Human Dimension Applications" with Fraunhofer AIS.SPADE institute (former name GMD, Germany)**.** 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" was concluded.

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 CeBit'2002 (Germany).

GRANTS FROM:

- **Russian Foundation of Basic Research (No. 00-07-90100):** "Network geoinformation systems for presentation and analysis of spatio-temporal information referring to Earth Sciences and human dimension".
- **Ministry of Industry, Science and Technology of Russian Federation:** "Development of an information technology for spatio-temporal data mining for analysis and forecasting of natural and social processes and phenomena".
- **IST Program (EU IST – 10536):** "Spatial Mining for Data of Public Interest (SPIN!)".

Institute for Information Transmission Problems

PARTNER SYSTEM GROUP

Investigated the problem of knowledge and data integration with the goal of creation encyclopedic knowledge systems for decision support systems, and knowledge production and propagation.

Developed technologies get further evolution. They will be used to creation of applied intellectual systems on the base of generating them by means of projecting integral base onto particular problem area.

Windows prototype of software environment kernel for support of knowledge and data unification process on the base of conceptual network models matching is developed. Created kernel allows us to realize previously developed method for clinical information structuring with the goal of fullness providing of registered data in computer systems for physician's professional decisions supporting. This provides us by possibility for developing of software environment for supporting of physician's professional decisions in real multiple profile medical clinic when needed to process data and knowledge in multidimensional spaces of initial descriptions, users interaction, knowledge receiving from different sources, and creation of new knowledge.

Developed kernel provides us also by possibilities of multiphase learning process realization in the frame of Partner Systems concept. These processes first of all are oriented onto medicine, and allow to user to learn the professional language and knowledge in the active regime. All of this can spread the learning process up to creation of absolutely new knowledge.

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 "Intellectual Computer Systems" (№ 3.4):** "Intelligent decision support within the framework of the project "Partner System".

THEORY OF THE SPEECH SIGNAL

There were studied criteria of optimality for inverse problems "acoustic parameters – vocal tract shape", "vocal tract shape – controls", "articulatory displacements – controls" using X-ray microbeam measurements and electromyograms of internal and external muscles. Instantaneous and integral criteria of work, elastic force, kinetic energy and total force were considered. In non-speech mode and for the task "from vocal tract shape to controls", instantaneous criteria provided sufficiently accurate solutions while for the task "from articulatory displacements to controls" only integral criteria on the time interval about 100 ms were appropriate. Inverse problem solutions reproduced the effect of bite-block compensation and the reorganization of control scores for different rates of articulation.

A 3-dimensional vocal tract model was developed taking into account *sinuses piriformis*, alternative width of the pharynx and yielding walls, which considerably increased the accuracy of resonance frequencies computation.

The first version of digits recognition was tested in the speaker-independent mode, different type of microphones and channels for signal-to-noise ratio 10-20 dB. Word error rate was about 12%.

PUBLICATIONS IN 2002

Articles

1. Afanassiev V.B., Davydov A.A. Finite field towers: iterated presentation and complexity of arithmetic, // Finite Fields and their Applications. 2002. V. 8. P. 216-232.
2. Ashikhmin A., Barg A. Bounds on the covering radius of linear codes // Designs, Codes and Cryptography. 2002. V. 27. No. 3. P. 261-270.
3. Barg A. On some polynomials related to weight enumerators of linear codes // SIAM Journal on Discrete Mathematics. 2002. V. 15. No. 2. P. 155-164.
4. Barg A. A low-rate bound on the reliability of a quantum discrete memoryless channel // IEEE Transactions on Information Theory. 2002. V. 48. No. 12.
5. Barg A., Forney G.D. Random codes: Minimum distance and error exponents // J. IEEE Transactions on Information Theory. 2002. V. 48. No. 9. P. 2568-2573 (also Proc. 2002 ISIT, Lausanne).
6. Barg A., Nogin D. Bounds on packings of spheres in the Grassmann manifolds // IEEE Transactions on Information Theory. 2002. V. 48. No. 9.
7. Barg A., Zemor G. Error exponents of expander codes // IEEE Transactions on Information Theory. 2002. V. 48. No. 6. P. 1725-1729.
8. Baumgartner B., Hof A., Sidorenko V., Bossert M. Multilevel codes: maximum-likelihood versus iterative multistage decoding // Proceedings 7th International OFDM-Workshop, pp. 148-152, Hamburg, Germany, September 2002.
9. Bezrukov S.L. and Serra O. A local-global principle for vertex-isoperimetric problems // Discrete Mathematics. 2002. V. 257. No. 2-3. P. 285-309.
10. Bott R., Korobkov D., Potapov V., Sidorenko V. Two dimensional time-frequency estimation of mobile radio channels // Proceedings of Wireless 2002, Calgary, Alberta, Canada. P. 300-311.
11. Griesser H., Sidorenko V. Efficient APP decoding of nonsystematic encoded block codes // Proceedings of 2002 IEEE Int. symposium on Information Theory, ISIT 2002, Lausanne, Switzerland, June-July, 2002. P. 145.
12. Griesser H., Sidorenko V. Efficient APP decoding of nonsystematic encoded block codes // Problems of Information Transmission. 2002. V. 38. No. 3. P.182-193.
13. Хендлери М., Йоханнессон Р., Зяблов В.В. Кодер и свойства расстояний плетеных сверточных кодов с циклически замкнутым компонентным кодом // Проблемы передачи информации. 2002. Т. 38. № 1. С. 48-58.
14. Хендлери М., Йоханнессон Р., Зяблов В.В. Декодирование в окне с точки зрения расстояний // Проблемы передачи информации. 2002. Т. 38. № 3. С.3-19.
15. Хендлери М., Хост С., Йоханнессон Р., Зяблов В.В. Расстояние, приспособленное для циклически замкнутых кодов // Проблемы передачи информации. 2002. Т. 38. № 4. С. 37-55.
16. Host S., Johannesson R., Zyablov V.V. Woven convolutional codes I: Encoder properties // IEEE Transactions on Information Theory. 2002. V. 48. No. 1. P. 149-161.
17. Модели и алгоритмы кодирования и сжатия информации. – Отчет о НИР по Госконтракту № 37.053.11.0062, 2002. 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.
18. Гитис В.Г., Вайншток А.П., Андриенко Г.Л., Андриенко Н.В. Геоинформационный анализ сейсмологических данных // Труды Восьмой национальной конференции по искусственному интеллекту, Коломна, 7-12 октября, 2002. С. 78-86.

19. Gitis V., Sobolev G., Ponomarev A., Kazakov V., Kurskeeva L., Belosliudtsev O. Complex Analysis of Geodynamic Monitoring Data in Almay Prognostic Site // Proceedings of European Seismological Commission XXVIII General Assembley, Genoa, 1-6 September 2002. P. 234-235.
20. Gitis V., Yurkov E. Statistical relationships between seismicity and moon component of tidal force // Proceedings of European Seismological Commission XXVIII General Assembley, Genoa, 1-6 September 2002. P. 235.
21. Gitis V., Sobolev G., Ponomarev A., Kazakov V., Kurskeeva L., Belosliudtsev O. Geoinformation technologies for analysis of geodynamic monitoring data in Almaty prognostic site // Тезисы 2-го казахстанско-японского семинара по предотвращению последствий разрушительных землетрясений, 23-25 сентября 2002, Алматы. С. 52-53.
22. Юрков Е.Ф. Система анализа характеристик акустического процесса при разрушении образцов горных пород // Вулканология и сейсмология. 2002. № 4. С. 57-70.
23. Andrienko G., Andrienko N., Gitis V. Interactive maps for visual exploration of grid and vector geodata // ISPRS Journal of Photogrammetry & Remote Sensing. 2003. No. 57. P. 380-389.
24. Vitushko M., Gurov N., Pereverzev-Orlov V. A Syndrom as a Tool for Presenting Concepts // Pattern Recogn. and Image Anal. 2002. V. 12. No. 2. P. 194-202.
25. Макаров И.С., Баден П., Сорокин В.Н. 3-мерная модель речевого тракта и алгоритм вычисления площадей поперечного сечения // Труды Международного семинара "Диалог". 2002. С. 352-359.
26. Цыплихин А.И., Леонов А.С., Сорокин В.Н. Двумерные распределения фонетических сегментов // Труды Международного семинара "Диалог", 2002, с. 484-495.
27. Sorokin V. Internal model as a tool for inverse problems solving // International seminar NATO "Dynamics of speech production and perception", Il. Ciocco, Italy, June 24 – July 06, 2002.
28. Sorokin V., Speech inverse problems: Tasks and solutions // International seminar NATO "Dynamics of speech production and perception", Il. Ciocco, Italy, June 24 – July 06, 2002.
29. Tsyplikhin A. Two-dimensional distributions of the phonetic segment pair durations // International seminar NATO "Dynamics of speech production and perception", Il. Ciocco, Italy, June 24 – July 06, 2002.

In print

1. Barg A. Extremal problems of coding theory. – In H. Niederreiter, Ed., Coding Theory and Cryptography, World Scientific (to appear).
2. Barg A., Kabatiansky G. A class of i.p.p. codes with efficient identification // DIMACS Report 2002-36 (submitted) (also Proc. 2002 ISIT, Lausanne).
3. Barg A., Zemor G. Error exponents of expander codes under linear-time decoding // DIMACS Report 2002-32 (submitted).
4. Bezrukov S.L., Elsaesser R. Edge-Isoperimetric problems for powers of regular graphs // Theoretical Computer Science (to appear).
5. Bezrukov S.L., Pfaff T., Piotrowski V.P. A new approach to Macaulay posets // Journal of Combinatorial Theory, Series A, (to appear).
6. Davydov A.A., Faina G., Marcugini S., Pambianco F. Computer search in projective planes for the sizes of complete arcs // Journal of Geometry (to appear).

7. Davydov A.A., Marcugini S., Pambianco F. On saturating sets in projective spaces // Journal of Combinatorial Theory, Series A (to appear).
8. Davydov A.A., Marcugini S., Pambianco F. Complete caps in projective spaces PG(n,q). (Submitted).
9. Davydov A.A., Marcugini S., Pambianco F. Linear codes with covering Radius 2,3 and saturating sets in projective geometry. (Submitted).
10. Handlery M., Johannesson R., Zyablov V.V. Boosting the error performance of suboptimal tailbiting decoders // IEEE Transactions on Communication (submitted).
11. Handlery M., Johannesson R., Zyablov V.V. On the error exponents for woven convolutional codes with one tailbiting component code // IEEE Transactions on Communication (submitted).
12. Jordan R., Pavlouchkov V., Zyablov V.V. Maximum slope convolutional codes // IEEE Transactions on Information Theory (submitted).
13. Гитис В.Г., Андриенко Г.Л., Андриенко Н.В. Исследование сейсмологической информации в сетевых аналитических ГИС // Физика Земли (в печати).
14. Ващенко Е., Витушко М., Переверзев-Орлов В. Возможности обучения на основе партнерской системы // Pattern Recogn. and Image Anal. (сдано в печать)
15. Репин В.Г., Цыплихин А.И. Определение точной верхней грани ошибок метода наименьших квадратов // Радиотехника и электроника. 2003. Т. 48. № 1 (в печати).
16. Макаров И.С., Сорокин В.Н. Резонансы речевого тракта с податливыми стенками и разветвлением // Акустический журнал (сдано в печать).
17. Leonov A.S., Sorokin V.N. Controls in the internal model: Score reorganization and compensation // Speech Communication J. (to appear).