Volume 7, Number 3, 2013

Contents
MALASCHONOK, N. Symbolic Solving of Partial Differential Equation Systems and Compatibility Conditions (pp. 199–214)
RADEV, S. Test, Teachers, Quorum (Pure Populations) (pp. 215–226)
GRIGOROVA, D., E. ENCHEVA, R. GUEORGUEVA. EM Algorithm for MLE of a Probit Model for Multiple Ordinal Outcomes. (pp. 227–244)
KYURKCHIEV, N., A. ILIEV. A Refinement of Some Overrelaxation Algorithms for Solving a System of Linear Equations (pp. 245–256)
ANGELOVA, V., Y. BORISSOV. Plaintext Recovery in DES-like Cryptosystems Based on S-boxes with Embedded Parity Check (pp. 257–270)
ZANEV, V., S. TOPALOV, V. CHRISTOV. Analysis and Data Mining of Lead-Zinc Ore Data (pp. 271–280)
PETROV, P. Mapping and Merging of Anatomical Ontologies (pp. 281–270)

Abstracts

SYMBOLIC SOLVING OF PARTIAL DIFFERENTIAL EQUATION SYSTEMS AND COMPATIBILITY CONDITIONS*
Natasha Malaschonok
e-mail: namalaschonok@gmail.com

Key words: Laplace–Carson transform, systems of partial differential equations, symbolic solving, compatibility conditions.

*Supported by RFBR, No.12-07-00755-a, RusMES No.1.345.2011

Abstract. An algorithm is produced for the symbolic solving of systems of partial differential equations by means of multivariate Laplace–Carson transform. A system of \( K \) equations with \( M \) as the greatest order of partial derivatives and right-hand parts of a special type is considered. Initial conditions are input. As a result of a Laplace–Carson transform of the system according to initial condition we obtain an algebraic system of equations. A method to obtain compatibility conditions is discussed.

TEST, TEACHERS, QUORUM (PURE POPULATIONS)
Slavian Radev
e-mail: SlavianRadev@gmail.com

Key words: voting, game, observer, data mining, test, master mind.

Abstract. The “trial and error” method is fundamental for Master Mind decision algorithms. On the basis of Master Mind games and strategies we consider some data mining methods for tests using students as teachers. Voting, twins, opposite, simulate and observer methods are investigated. For a pure data base these combinatorial algorithms are faster then many AI and Master Mind methods. The complexities of these algorithms are compared with basic combinatorial methods in AI.
EM ALGORITHM FOR MLE OF A PROBIT MODEL FOR MULTIPLE ORDINAL OUTCOMES
Denitsa Grigorova, Elitsa Encheva, Ralitza Gueorguieva
e-mail: dgrigorova@fmi.uni-sofia.bg
dr.encheva@gmail.com
ralitza.gueorguieva@yale.edu

Key words: correlated probit model, EM algorithm, ordered data, polymorphism XRCC3 codon 241 (C > T) (rs861539), random effects.

Abstract. The correlated probit model is frequently used for multiple ordered data since it allows to incorporate seamlessly different correlation structures. The estimation of the probit model parameters based on direct maximization of the limited information maximum likelihood is a numerically intensive procedure. We propose an extension of the EM algorithm for obtaining maximum likelihood estimates for a correlated probit model for multiple ordinal outcomes. The algorithm is implemented in the free software environment for statistical computing and graphics R. We present two simulation studies to examine the performance of the developed algorithm. We apply the model to data on 121 women with cervical or endometrial cancer. Patients developed normal tissue reactions as a result of post-operative external beam pelvic radiotherapy. In this work we focused on modeling the effects of a genetic factor on early skin and early urogenital tissue reactions and on assessing the strength of association between the two types of reactions. We established that there was an association between skin reactions and polymorphism XRCC3 codon 241 (C > T) (rs861539) and that skin and urogenital reactions were positively correlated.

***********************************************************************************

A REFINEMENT OF SOME OVERRELAXATION ALGORITHMS FOR SOLVING A SYSTEM OF LINEAR EQUATIONS*
Nikolay Kyurkchiev, Anton Iliev
e-mail: nkyurk@uni-plovdiv.bg, nkyurk@math.bas.bg
aii@uni-plovdiv.bg, anton.iliev@gmail.com

Key words: reverse Gauss–Seidel method, or Nekrassov–Mehmke 2 method – (NM2), Successive Overrelaxation method with 1 parameter, based on (NM2) – (SOR1NM2), Successive Overrelaxation method with 2 parameters, based on (NM2) – (SOR2NM2), Refinement of (SOR1NM2) method – (RSOR1NM2), Refinement of (SOR2NM2) method – (RSOR2NM2).

*This paper is partly supported by project NI13 FMI-002 of Department for Scientific Research, Paisii Hilendarski University of Plovdiv.

Abstract. In this paper we propose a refinement of some successive overrelaxation methods based on the reverse Gauss–Seidel method for solving a system of linear equations \( Ax = b \) by the decomposition \( A = T_m - E_m - F_m \), where \( T_m \) is a banded matrix of bandwidth \( 2m + 1 \).

We study the convergence of the methods and give software implementation of algorithms in Mathematica package with numerical examples.

***********************************************************************************

PLAINTEXT RECOVERY IN DES-LIKE CRYPTOSYSTEMS BASED ON S-BOXES WITH EMBEDDED PARITY CHECK*
Vesela Angelova, Yuri Borissov
e-mail: vaa@math.bas.bg
youri@math.bas.bg

Key words: DES-like cryptosystem, S-box, affine subspace, plaintext recovery, backtracking search, language model.
This work was presented in part at the 1st International Conference Bulgarian Cryptography Days 2012, Sofia, Bulgaria, 20–21 September 2012.

Abstract. We describe an approach for recovering the plaintext in block ciphers having a design structure similar to the Data Encryption Standard but with improperly constructed S-boxes. The experiments with a backtracking search algorithm performing this kind of attack against modified DES/ Triple-DES in ECB mode show that the unknown plaintext can be recovered with a small amount of uncertainty and this algorithm is highly efficient both in time and memory costs for plaintext sources with relatively low entropy. Our investigations demonstrate once again that modifications resulting to S-boxes which still satisfy some design criteria may lead to very weak ciphers.

ANALYSIS AND DATA MINING OF LEAD-ZINC ORE DATA
Vladimir Zanev, Stanislav Topalov, Veselin Christov
e-mail: vladimir@columbusstate.edu
stopalov@gmail.com
veso@mgu.bg

Key words: data analysis, data mining, clustering, prediction, Pb-Zn ore data.

Abstract. This paper presents the results of our data mining study of Pb-Zn (lead-zinc) ore assay records from a mine enterprise in Bulgaria. We examined the dataset, cleaned outliers, visualized the data, and created dataset statistics. A Pb-Zn cluster data mining model was created for segmentation and prediction of Pb-Zn ore assay data. The Pb-Zn cluster data model consists of five clusters and DMX queries. We analyzed the Pb-Zn cluster content, size, structure, and characteristics. The set of the DMX queries allows for browsing and managing the clusters, as well as predicting ore assay records. A testing and validation of the Pb-Zn cluster data mining model was developed in order to show its reasonable accuracy before being used in a production environment. The Pb-Zn cluster data mining model can be used for changes of the mine grinding and floatation processing parameters in almost real-time, which is important for the efficiency of the Pb-Zn ore beneficiation process.

MAPPING AND MERGING OF ANATOMICAL ONTOLOGIES*
Peter Petrov
e-mail: p.a.petrov@gmail.com

Key words: ontology, anatomical ontology, ontology mapping, anatomical ontology mapping, ontology merging, anatomical ontology merging, external knowledge source, algorithm, graph, directed acyclic graph.

*This article presents the principal results of the Ph.D. thesis Intelligent systems in bioinformatics: mapping and merging anatomical ontologies by Peter Petrov, successfully defended at the St. Kliment Ohridski University of Sofia, Faculty of Mathematics and Informatics, Department of Information Technologies, on 26 April 2013.

Abstract. The problem of mapping and merging ontologies in general is an important one in the area of ontology engineering. The same problem considered within the narrower area of anatomical ontologies (AOs) is important in bioinformatics because solving it could enable the transfer of data and the application of knowledge obtained from various model organisms to other model and non-model organisms, and even to research areas such as those of human health and medicine.

This paper presents a detailed summary of the author’s PhD research done in the period 2007–2013. The paper’s main topic is the problem of mapping and merging of multiple species-specific AOs and the related approaches, methods, and procedures that can be used for solving it.

In this paper the current state of the AO merging and mapping problem is first reviewed. Then a formalization of the problem is suggested. Based on this formalization, an algorithmic procedure for mapping AOs is proposed, which utilizes both syntactic and semantic techniques, including the usage of several existing external knowledge sources (EKSs) containing anatomical information. After that a necessary and sufficient condition is outlined pertaining to the process of merging two given AOs.
Next, the computer program AnatOM developed as part of this study is described. An analysis is done of the results obtained through the use of AnatOM while mapping and merging three particular couples of species-specific AOs. A discussion is presented about the main problems encountered while doing this research. At the end, some perspectives for future development of the work are suggested, and the author’s view of this study’s contributions is presented.