Šesta nacionalna konferencija "Verovatnosne logike i njihove primene"

Beograd, Srbija, 6. oktobar 2016.

Knjiga apstrakata

ORGANIZATOR:

Matematički institut, SANU

KONFERENCIJU FINANSIRAJU:

Projekat Razvoj novih informaciono-komunikacionih tehnologija, korišćenjem naprednih matematičkih metoda, sa primenama u medicini, telekomunikacijama, energetici, zaštiti nacionalne baštine i obrazovanju, III 044006

Projekat Reprezentacije logičkih struktura i formalnih jezika i njihove primene u računarstvu, ON 174026.

Šesta nacionalna konferencija
"Verovatnosne logike i njihove primene"

Beograd, Srbija, 6. oktobar 2016.

TEME KONFERENCIJE:
Verovatnosne logike, problemi potpunosti, odlučivosti i složenosti; logičke osnove u zasnivanju verovatnoće; bayes-ove mreže i drugi srodni sistemi; programski sistemi za podršku odlučivanju u prisustvu neizvesnosti; primene verovatnosnog zaključivanja u medicini; teorija informacija; mere informacija i složenosti; teorija kodiranja; sigurnost u sajber-prostoru; složeni i dinamički sistemi i donošenje odluka; kauzalnost u kompleksnim sistemima; analiza i simulacija kompleksnih sistema; ali i sve srodne teme koje nisu navedene.

PROGRAMSKI KOMITET:
Miodrag Rašković (Matematički institut SANU), predsednik
Zoran Marković (Matematički institut SANU)
Zoran Ognjanović (Matematički institut SANU)
Nebojša Ikodinović (Univerzitet u Beogradu)
Aleksandar Perović (Univerzitet u Beogradu)

ORGANIZACIONI KOMITET:
Miodrag Rašković (Matematički institut SANU)
Ivan Čukić (Univerzitet u Beogradu)

ORGANIZATOR:
Matematički institut, SANU

KONFERENCIJU FINANSIRAJU:

Projekat Razvoj novih informaciono-komunikacionih tehnologija, korišćenjem naprednih matematičkih metoda, sa primenama u medicini, telekomunikacijama, energetici, zaštiti nacionalne baštine i obrazovanju, III 044006

Projekat Reprezentacije logičkih struktura i formalnih jezika i njihove primene u računarstvu, ON 174026.

Program konferencije:

6. 10. 2016.

11:00 *Otvaranje*

11:15 *Modal quantum logic with probability*, A. Ilić-Stepić, Z. Ognjanović

11:35 *Compact fragment of* LPP_2, A. Perović

11:55 *Correctness of the Chord Protocol*, B. Marinković, Z. Ognjanović, P. Glavan, A. Umek

12:15 *Reasoning with the Ontologies*, M. Todorović, A. Zdravković. B. Marinković

12:35 *Deductions of Probabilistic Formulas*, M. Boričić

12:55 *The System for the Decision Support for Autoimmune Diseases*, N. Glišović, M. Rašković

13:15 *Pauza*

14:00 *A Method for Extracting SBS movies from Virtual Reality Tesla Laboratories*, V. Vučkovic, A. Stanišić

14:20 *Method for generating pseudo-random numbers with unique values in output sequence*, V. Vučkovic, N. Stojiljković

14:40 *On the Computational Efficiency of the Galois Field and the Reed-Muller-Fourier Transforms of Multiple-Valued Logic Functions*, D. Gajić, R. Stanković

15:00 *Predavanje po pozivu*, Zvonimir Šikić

15:45 *30 years of Rašković's middle-model construction*, N. Ikodinović

16:05 *Computer assisted exploration of first order properties of finite structures*, Ž. Mijajlović, A. Pejović

16:25 *Experimental Evaluation of Time-Memory Trade-Off Attack*, A. Arsić, A. Zdravković

16:45 *Generating diagnostic criteria by a clinical decision support system: 3 case study in systemic connective tissue disorders*, V. Srdanović, M. Šošić, M. Rašković, S. Rašković, A. Perić-Popadić, V. Djurić, Ž. Jovičić, N. Srdanović

Apstrakti

Sadržaj

Experimental Evaluation of Time-Memory Trade-Off Attack

Aleksandra Arsić
Aleksandra Zdravković
Mathematical Institute SASA, Belgrade, Serbia

Keywords:

encryption, security evaluation, Time-Memory-Data Tradeoff attack, Trivium

This paper addresses certain issues of a generic approach for inversion of an one-way function which is of interest in different domains of mathematics including mathematical logic and its applications, and particularly regarding security evaluation of cryptographic algorithms. There are the following two straightforward approach for recovering the argument given the corresponding image generated by one-way function where the inversion is a hard problem: (i) exhaustive search over all possible arguments; (ii) employing a code-book with all possible argument-image pairs. The main problem with the both approaches is the exponential complexity of implementation. Helman has proposed a technique which reduces the required time and memory complexities. Using pre-computation time of N, Hellman showed that the online time T and memory M satisfy the relation $TM^2 = N^2$, where $N = 2^n$. Consequently, the attack is called a time/memory trade-off (TMTO) algorithm. This attack on stream ciphers is a serious security threat and the resistance to this class of attacks is an important criterion in the design of a modern stream cipher. This paper provides certain experimental evaluation of the considered TMTO paradigm. Main goal is to provide illustrative experimental evidences on a particular quantitative feature of two TMTO design approaches. For one-way function, authors choose Trivium cipher. Trivium is stream cipher designed to generate keystream from 80-bit secret key and an 80-bit initial vector (IV). Process of generating keystream bits consists of two phases. First phase aims to initialize key and IV into 288-bit initial state s. Next phase is generating keystream vector z. In this phase 15 specific bits are used for updating 3 bits of the state s and to compute 1 bit of z. The state register is then rotated and the process repeats itself until complete keysteam vector has been generated.

First phase for TMTO attack is preprocessing phase. Goal of preprocessing phase is matrix initialization.

According to computation power and technical opportunities, our matrix and the number of all possible solutions for key vector are not the same. We try to guess only 20 bits and the other 60 bits of key and 80 bits of IV are initialized by random values and stay fixed all time. In that way, number of all permutations is smaller, so time and memory space for computing matrix are smaller, too.
Preprocessing phase is described as:
Form a $m \times t$ matrix that tries to cover the whole search space which is composed of all the possible permutations with guessed 20 bits of key vector as follows:
1. Randomly generate m startpoints of the chains, each point is represented like vector of 20 bits length.
2. Make it the next point in the chain which is the output from Trivium function and update the s register with this point.
3. Iterate Step (2) t times on each startpoint respectively.
4. Store the pairs of startpoints and endpoints (SP_j, EP_j), $j = 1, ..., m$ in the matrix.

Our first experiment was to generate matrix for TMTO Attack and check if there are duplicate states. Dimensions of our matrix were $m \times t$ where $m = 2^{15}$ and $t = 2^5$. First, startpoints for each row was random initialized, keeping in the mind there are no duplicate startpoints. Next step was to fill all states in matrix. Every state in chains, except first one, is result from 20 iterations of Trivium algorithm with initialization of the register with previous state's bits from the same row in matrix. After filling the matrix, content of matrix was analyzed.

Experiments were repeated 50 times. Experiments showed that some states in matrix occur more than one time. The conclusion is the matrix does not contain all the elements of search space. Average repetition rate in all experiments was in range from 57.14 to 64.43 percents of number of all matrix states.

Our next experiment consists of constructing several tables. To construct each table, the attacker chooses t random vectors, one for each table. Described matrices have the same number of columns like first matrix, but number of rows is less than the number of rows in the single matrix. In that case, numbers of rows in all tables are equal and total number corresponds to the number of rows in the single matrix. Algorithm for matrix filling is the same, but every time when Trivium function gives us a new state vector as output, we translate it for random vector corresponding to table in which we put it. For translation we use XOR operation on its state. These tables can be generated in parallel, but statistical analysis follows the merging of all

tables in single table.

Authors did some experiments when single matrix was divided on 2, 4 and 8 smaller tables. Experiments shown that in case when we generate two tables with two random vectors, repetition rate was in range from 54.71 to 61.57 percents of size of search space. If we construct eight tables for search space and assign eight random translation vectors for each one, repetition rate will be in range from 35.19 to 41.62 percents of size of search space.

Results shown that in case of using more small tables, the total number of distinct points which cover search space is bigger. This technique reduces the number of collisions in the table, and hence allows to cover most of the points by a single table. The larger the table is, the higher is the probability that a new chain has an intersection with previous chains. Each state's repetition reduces the number of distinct keys which are actually covered by a table. The efficiency of a single table rapidly decreases with its size. To obtain a high probability of success it is better to generate multiple tables using a different reduction function for each table. In our case, as reduction function XOR operator is used. Chains of different tables can have intersection. Using more reduction functions which are applied in different tables leads to smaller number of intersections.

This paper has provided certain, particular, quantitative insights regarding design of the tables which employs TMTO approach for inverting of an one-way function.

Deductions of Probabilistic Formulas

Marija Boričić
Faculty of Organizational Sciences,
University of Belgrade
marija.boricic@fon.bg.ac.rs

Inspired by the theory of probabilized inference rules considered by Frisch and Haddawy [3], and Wagner [6], we introduce a system **NKprob** [1], an extension of Gentzen's natural deduction system **NK**, making it possible to manipulate with probabilized formulas of the form $A[a, b]$, with the intended meaning that 'the probability c of truthfulness of a sentence A belongs to the interval $[a, b] \subseteq [0, 1]$'. Formula $A[1, 1]$ is an axiom of a system **NKprob**, for every propositional formula A provable in classical logic. In our system, it is possible to introduce and eliminate each of the connectives, using at least one of the inference rules. For example, the following rules are for introduction and elimination of the implication:

$$\frac{A[a,b] \quad B[c,d]}{(A \to B)[\max(1-b,c), 1-a+d]} \ (I \to)$$

$$\frac{A[a,b] \quad (A \to B)[c,d]}{B[a+c-1,d]} \ (E_1 \to) \qquad \frac{B[a,b] \quad (A \to B)[c,d]}{A[1-d, 1-c+b]} \ (E_2 \to)$$

Further, there is the additivity rule, specific for a probabilistic system:

$$\frac{A[a,b] \qquad B[c,d] \qquad (A \wedge B)[e,f]}{(A \vee B)[a+c-f, b+d-e]} \ (ADD)$$

The system **NKprob** is sound and complete with respect to the Carnap–Popper–type models (see [2], [4] and [5]).

References:

[1] M. Boričić, *Inference rules for probability logic,* **Publications de l'Institut Mathematique,** (to appear)
[2] R. Carnap, **Logical Foundations of Probability,** University of Chicago Press, Chicago, 1950.
[3] A. M. Frisch, P. Haddawy, *Anytime deduction for probabilistic logic,* **Artificial Intelligence** 69 (1993), pp. 93–122.

[4] H. Leblanc, B. C. van Fraassen, *On Carnap and Popper probability functions,* **The Journal of Symbolic Logic** 44 (1979), pp. 369–373.
[5] K. R. Popper, *Two autonomous axiom systems for the calculus of probabilities,* **The British Journal for the Philosophy of Science** 6 (1955), pp. 51–57, 176, 351.
[6] C. G. Wagner, *Modus tollens probabilized,* **British Journal for the Philosophy of Science** 54(4) (2004), pp. 747-753.

On the Computational Efficiency of the Galois Field and the Reed-Muller-Fourier Transforms of Multiple-Valued Logic Functions

Dušan B. Gajić
Faculty of Technical Sciences, University of Novi Sad
dusan.b.gajic@gmail.com

Radomir S. Stanković
Faculty of Electronic Engineering, University of Niš
radomir.stankovic@gmail.com

Spectral transforms, performed over finite (Galois) fields of order p, denoted as GF(p), or ring of integers modulo p, as, e.g., the Galois field (GF) transform and the Reed-Muller-Fourier (RMF) transform, are of significant interest in areas like multiple-valued logic (MVL), signal processing, and information theory [6]. This is due to a close resemblance of some of their properties to the corresponding properties of the Fourier transform. [6]. Time required for the computation of spectral transforms is often the main limiting factor in their practical applications [3, 6]. Therefore, analysis of the complexity of arithmetic operations involved in fast algorithms for the computation of different spectral transforms is of considerable importance.

We present a comparison of the computational efficiency of the GF and the RMF transforms of MVL functions, performed on central processing units (CPUs) and graphics processing units (GPUs) [2, 5, 6]. We also discuss the impact of arithmetic operations carried out while computing these transforms using Cooley-Tukey fast Fourier transform-like (FFT) algorithms [4]. The cases of ternary ($p = 3$) and quaternary ($p = 4$) logic functions are experimentally examined, using the C/C++ and the CUDA C programming languages for developing the respective CPU and GPU implementations [1]. It is noticed that both the nature of arithmetic operations required by the two transforms and the chosen computational platform have substantial impact on performance. It is shown that the RMF transform has significant computational advantage over the GF transform when the later is performed in finite fields of non-prime order. The computational benefit offered by the RMF transform

is even more pronounced on novel computing architectures such as GPUs.

Acknowledgment

The research reported in the paper is partly supported by the Ministry of Education and Science of the Republic of Serbia, projects ON174026 (2011-2016) and III44006 (2011-2016).

References

[1] Cheng, J., Grossman, M., McKercher, T., *Professional CUDA C Programming Guide*, Wrox Press, 2014.

[2] Gajić, D. B., Stanković, R. S., "Computing spectral transforms used in digital logic on the GPU", in Astola, J., Kameyama, M., Lukac, M., Stanković, R. S. (eds.), *GPU Computing with Applications in Digital Logic*, Tampere International Center for Signal Processing - TICSP Series # 62, Tampere, Finland, 2012, ISBN 978-952-15-2920-7.

[3] Gajić, D. B., Stanković, R. S., "Computation of the Vilenkin-Chrestenson transform on a GPU", J. Multiple-Valued Logic and Soft Computing, vol. 24, no. 3-5, pp. 317-341, Old City Publishing, Philadelphia, USA, 2015.

[4] Karpovsky, M. G, Stanković, R. S., Astola, J. T., *Spectral Logic and Its Applications for the Design of Digital Devices*, Wiley-Interscience, 2008.

[5] Stanković, R. S., "Some remarks on Fourier transforms and differential operators for digital functions", *Proc. 22nd IEEE Int. Symp. on Multiple-Valued Logic*, Sendai, Japan, 1992, DOI: 10.1109/ISMVL.1992.186818, 365-370.

[6] Stanković, R. S., Astola, J. T., Moraga, C., *Representation of Multiple-Valued Logic Functions*, Morgan & Claypool Publishers, 2012.

The System for the Decision Support for Autoimmune Diseases

Nataša Glišović
State University of Novi Pazar,
Department of Mathematical Sciences

Miodrag Rašković
Mathematical Institute of the
Serbian Academy of Sciences and Arts (SANU)

Abstract - It is often required to establish how the data are connected, how certain data differ or do not go together with each other and what the measure of their comparison is. An important part in detecting the similarities and grouping the data into clusters has the choice of metrics and the accuracy of the cluster algorithm operation. The aim of this paper is to show the system for making a decision in the diagnostics of the patients with autoimmune diseases. In this research we proposed likelihood ratio for value analysis in cluster optimization. The support system in the diagnostics uses these proposed methods implemented in the program language *c#*.

Keywords: Systemic diseases, likelihood ratio, decision support, systemic lupus erythematosus, Sy Sjogren, systemic sclerosis

I Introduction

For clustering, we use the machine learning. The machine learning can be observed as determining the dependence on the available data [4]. The methods of the classification machine learning according to the examples do the estimation of copying the unknown dependence between the input (of the data) and the system output (of the classification) according to the available examples of the right classification. In our paper the method uses the likelihood ratio which have an aim that according to the patients' base, which consists of patients ill with three systemic autoimmune diseases (SLE, Sy Sjogren and Sclerosis systemica), decides for a new patient to which group of diseases they belong [9].

II Mathematics model

The Metric learning has become a popular issue in many learning tasks and can be applied in a wide variety of settings, since many learning problems

involve a definite notion of distance or similarity [1]. A metric or distance function is a function which defines a distance between the elements of a set [7]. A set with a metric is called a metric space. In many data retrieval and data mining applications, such as clustering, measuring the similarity between the objects has become an important part. Normally, the task is to define a function , where and are two objects or sets of a certain class, and the value of the function represents the degree of "similarity" between the two [8]. The proposed system (see the algorithm) uses the technique of clustering [10]. In order to carry out the analysis of clustering at all, it is necessary to define the measures of closeness of the two objects on the basis of their characteristics. The concept of "similarity" is determined according to the data themselves. For weight of each of the analysis this research used likelihood ratio. Let A be analysis, D diseases weight proposed to analyze A in the disease D is: ?D=P(A—D)/P(A—?D)

III The description of the base

In our paper we used the database of the patients with one of the mentioned three systemic autoimmune diseases: systemic lupus erythematosus (SLE), Sy Sjogren and systemic sclerosis (SScl).Every patient was diagnosed on the basis of appropriate criteria. The selection of variables is established by the expert committee but is also under the strict influence of the statistical analyses. The classification criteria for SLE were established by the American College of Rheumatology from 1982. Later, in 1997 the criteria were revised [6]. Systemic Lupus International Collaborating Clinics (SLICC) set up the new classification criteria in 2012 [11]. The diagnostic criteria for Sy Sjogren and the systic sclerosis [5], are given in a similar way. The data set consists of 45, at random, chosen patients with the systemic autoimmune diseases, among them, 15 of the subjects were diagnosed as SLE, 19 as Sjogren's syndrome, 11 as progressive systemic sclerosis and 3 had both SLE and Sjogren's syndrome. These patients are diagnosed and treated at the Clinic for Allergology and Immunology Clinical Centre Belgrade during the period of 2012-2014. We used a set of 87 variables, formed on the basis of 'availability' and 'prices' of the diagnostic methods. The first group of 33 variables consisted of the data obtained by anamneza and clinical check-up of patients, that is 'the most available group of data'. The second group of variables of 37-70 consisted of the data obtained by the labaratory treatment. The third group of 71-87 consisted of the variables obtained by the clinical check-ups which included invasive diagnostic procedures such as a biopsy of salivary glands, a biopsy of kidneys.

IV The conclusion of the research

In the medicals' opinion, who had tested the proposed system in practice, this system is useful because the results were very reliable and enabled giving

the suggestions of an adequate therapy. For this class of disease there is an additional therapy which can be, on the basis of the proposed system, determined.

References:

[1] Agrawal R., Faloutsos C., Swami A. Efficient similarity search in sequence databases. Proc. 4th Int. Conf. On Foundations of Data Organizations and Algorithms, 1993. - Chicago. pp. 69-84.
[2] Bezdek JC. A converegence theorem for the fuzzy ISODATA clustering algorithms. IEEE Trans Pattern Anal Mach Intell. 1980;2:1-8.
[3] Chan EZ, Ching WK, Ng MK, Huang JZ. An optimization algorithm for clustering using weighted dissimilarity measures. Pattern Recognit. 2004; 37: 943-952.
[4.] Cherkassky V., Mulier F. M., Learning from Data: Concepts, Theory, and Methods, 2nd Ed, John Wiley-IEEE Press, 2007.
[5] Frank van den Hoogen, Dinesh Khanna, Jaap Fransen,Sindhu R Johnson, Murray Baron, Alan Tyndall,et al. 2013 classification criteria for systemic sclerosis: an American college of rheumatology/European league against rheumatism collaborative initiative Ann Rheum Dis 2013;72:1747-1755.
[6] Gladman DD, Urowitz MB. Prognosis, mortality and morbidity in systemic lupus erythematosus. In: Wallace DJ, Hahn BH. Dubois' lupus erythematosus. 7th ed. Philadelphia: Lippincott Williams & Wilkins; 2007:1333-53.
[7] Goronzy JJ, Weyand CM. The innate and adaptive immune systems. In: Goldman L, Ausiello D, eds. Cecil Medicine . 23rd ed. Philadelphia, Pa: Saunders Elsevier;2007: chap 42.
[8] Li M., Chen X., Ma B., Vitanyi P. The similarity metric. IEEE Transactions on Information Theory, 2004, vol.50, No. 12, pp.3250-3264.
[9] Nadashkevich O, Davis P, Fritzler MJ. A proposal of criteria for the classification of systemic sclerosis. Med. Sci. Monit. 2004 Nov;10(11):CR615-21. Epub 2004 Oct 26.
[10] Pang-Ning Tan et al. Introduction to data mining. Pearson Education India, Chapter 8, 2007.
[11] Petri M, Orbai AM, Alarcn GS, Gordon C, Merrill JT, Fortin PR, et al. Derivation and validation of the Systemic Lupus International Collaborating Clinics classification criteria for systemic lupus erythematosus. Arthritis Rheum. 2012 Aug;64(8):2677-86.

30 years of Rašković's middle-model construction

Nebojša Ikodinović
Faculty of Mathematics
ikodinovic@matf.bg.ac.rs

In this talk we present very fruitful method introduced by Rašković in [1]. The method is developed for solving Keisler's problem about probabilistic logics with two measures μ_1, μ_2 such that μ_1 is absolutely continuous with respect to μ_2.

After the paper [1], the method becomes a very powerful technique for producing new results - the completeness theorems for classes of structures which involved 'higher order' notions, such as probabilistic or topological structures. In the heart of the method is the Barwise compactness theorem (based on a suitable generalization of finiteness).

References

[1] M. Rašković, *Completeness theorem for biprobability models*, J. Symb. Logic, Vol. 51, No. 3, 1986, 586-590.

Modal quantum logic with probability

Angelina Ilić Stepić,
Zoran Ognjanović
Mathematical Institute of the
Serbian Academy of Sciences and Arts
{*angelina,zorano*}*@mi.sanu.ac.rs*

Abstract

In this paper we present the logic L_{QM} designed for reasoning about quantum observations. L_{QM} extends Bouwerian modal logic with probability formulas $CS_{z_1,\rho_1;z_2,\rho_2;\ldots z_m,\rho_m}\Box\alpha$ whose meaning is always related to some world (vector) w and it is the following: $w = c_1 \cdot w_1 +, \ldots, +c_m \cdot w_m$ for some $c_i \in \mathbf{C}$ such that $\|c_1 - z_1\| \leq \rho_1, \ldots \|c_m - z_m\| \leq \rho_m$ and hence the probability of measuring α in a state w is equal $\|c_1\|^2 + \ldots + \|c_m\|^2$. We express the notion of measurement by modal operator and hence using formulas of the form $\Box\varphi$ we overcome well known "non distributivity problem" of quantum mechanics. Precisely, since $\Box$ not distributes over $\vee$ "it already catches non-distributity", so we do not need non-distributive structure (like non-distributive lattice) and we are satisfied with Boolean logic with some modal laws. We only need axiom of classical logic plus three modal lows instead of many axioms or rules which are normally used in quantum logics. By iterating modal operators we can express something like "it is measured that it is measured..." .This is suitable in situations (experiments) when we perform some measurement on a individual system (for instance single atom) and we relied on our knowledge about the possible outcomes, but this knowledge is consequence of the previous measurement that we performed on the ensemble of the concerned systems. Here we discuss the famous example of Schrdinger's cat and indicated how this thought experiment is actually a situation of this type. Using formulas with iterated modal operators and some performance within the logic L_{QM} we can express a distinction between different measurements in the experiment (which are often identified). In this way, by logical means we have helped to shed light on a mentioned paradox.

Formulas are interpreted in Kripke-like models called **B**- realization which can be transformed into standard Kripkean realization for quantum logic and vice versa. We prove the corresponding soundness and completeness theorems and we also show that the logic L_{QM} is decidable.

Correctness of the Chord Protocol

Bojan Marinković
Mathematical Institute of the
Serbian Academy of Sciences and Arts
bojanm@mi.sanu.ac.rs

Zoran Ognjanović
Mathematical Institute of the
Serbian Academy of Sciences and Arts
zorano@mi.sanu.ac.rs

Paola Glavan
Faculty of Mechanical Engineering and Naval Architecture,
University of Zagreb
pglavan@fsb.hr

Anton Umek
Faculty of Electrical Engineering,
University of Ljubljana
anton.umek@fe.uni-lj.si

The cloud computing has emerged in the recent years. Unfortunately, traditional SQL databases did not performed well in the new situation. The modern web applications demand high availability, speed and fault tolerance and non-relational database systems (NRDBMS) can offer the solution. Some of NRDBMS are realized in the form of a Distributed Hash Tables (DHTs). The Chord protocol is one of the first, simplest and most popular DHTs.

We need to guarantee correctness of the Chord protocol by defining a minimal set of deterministic constraints. Our aim is to provide axiomatization and to prove the strong completeness for the logic of time and knowledge for the Chord Protocol. Using the presented logic our goal is to prove the correctness of the Chord protocol, with the respect of the fact that nodes are not allowed to departure the system after they join it.

Computer assisted exploration of first order properties of finite structures

Žarko Mijajlović
Mathematical Institute SASA
zarkom@matf.bg.ac.rs

Aleksandar Pejović
Mathematical Institute SASA
pejovica@mi.sanu.ac.rs

We will show a method that will allow us to answer some nontrivial questions about finite structures. It is a combination of probabilistic method and direct solving of low cardinality cases by use of specialized software that we have developed. Specifically, we will show how we used it to explore some interesting first order properties of Tournament graphs.

Compact fragment of LPP_2

Aleksandar Perović
Faculty of Transport and Traffic Engineering,
University of Belgrade
pera@sf.bg.ac.rs

We say that an LPP_2–formula ϕ is closed iff its DNF has a form

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} P_{\geq r_{i,j}} \alpha_{i,j}.$$

Firstly we prove that compactness theorem is satisfied for the fragment of closed LPP_2–formulas. Using this fact we show that the predicate $Prob(p) < Prob(q)$ is not ω–definable in LPP_2, i.e. that for any consistent LPP_2–theory T the corresponding class of models $Mod(T)$ is not equal to the class $Mod(Prob(p) < Prob(q))$ of all models of the predicate $Prob(p) < Prob(q)$.

Generating diagnostic criteria by a clinical decision support system: case study in systemic connective tissue disorders

V. Srdanović *M. Šošić* *M. Rašković* *S. Rašković*
A. Perić-Popadić *V. Djurić* *Ž. Jovičić*
N. Srdanović

A clinical decision support system, BELART, has been developed addressing the notorious problem of knowledge acquisition by taking an approach of integrating knowledge and data (Srdanović, V., and Šošić, M., 2013).

The system employs powerful heuristics for extracting key attributes, which presents core of its inductive inference algorithm. The heuristics can easily cope with attributes having differing number of values, concurrent values, and missing values, as well as with noise. It is being used to restructure system's knowledge base, so it can be adequately applied to solving problems within a given domain. There are two main directions the system makes use of the heuristics: a) to direct consultation process adaptively, and eventually suggest possible diagnosis, and b) to automatically derive criteria for diagnosing (suspecting) a disease from a given domain.

The system was successfully applied to several medical domains, most recently to the domain of autoimmune systemic connective tissue disorders (Srdanović, V., et al., 2015).

The autoimmune systemic diseases can be very difficult to diagnose in practice, requiring a broad picture of the patients medical history, usually assessed through a large number of variables. Even for clinical specialists it can be a challenge. The additional problem lies in the fact that many autoimmune diseases patients suffer from more than one condition at a time. This is why for the correct diagnosis of these diseases a large number of different parameters are typically needed. The diagnostic process typically varies among the individual patients depending on their condition, so not all of the diagnostic procedures were needed for all patients.

The American College of Rheumatology had developed the Classification criteria for systemic lupus erythematosus in 1982. In 1997 these criteria were

revised. Systemic Lupus International Collaborating Clinics (SLICC) proposed new classification criteria, (Petri, M., et al., 2012). The SLICC variables were selected after statistical analysis, using logistic regression analyses, has been performed by experts on patients medical records.

To evaluate the systems performance, three of the autoimmune systemic diseases systemic lupus erythematosus (SLE), Sjgren's syndrome (SS), and progressive systemic sclerosis (PSS) were considered. 44 patient case histories from the Clinic of Allergology and Immunology of the Clinical Center of Serbia were used. All of the patients were in-patients at the CAI during the period 2012-2015 and all were diagnosed with some form of systemic connective tissue disorder. Patients data were thoroughly reviewed and diagnoses confirmed by expert clinicians. Out of the total of 44 patients, 15 were diagnosed SLE, 18 with SS, and 11 with PSS.

A total of 87 different manifestations (symptoms, signs, findings, ...) were selected for the study. It has to be noted that not all of manifestations had their values established for each of the patients in the study. On average, patients case histories had 65 (out of the total of 87) manifestations whose values were established. As expected, typically values of the more costly manifestations (those requiring more expensive and/or invasive procedures) have not been established.

Evaluation of the system which focused more on its diagnostic accuracy was discussed in (Srdanović, V., et al., 2015). Diagnostic strengths are assigned to each diagnosis-manifestation pair, which can be interpreted as a generalized sensitivity estimate of a particular manifestation for a given disease. Those manifestations that are being manifested with significantly different diagnostic strengths with various diseases within the domain are being designated by the system as key ones. For a given margin D by which diagnostic strengths differ, key manifestations are selected that discriminate the most among two diseases. So, for each pair of diseases and a given margin D, a set of key manifestations is formed. Table 1. below shows the diagnostic accuracy of the system for different values of D.

Table 1. Diagnostic Accuracy:

	margins for selecting key manifestations						
	0.2	0.3	0.4	0.5	0.6	0.7	0.8
average # of manifestations considered	64	47	35	30	20	13	5
diagnostic accuracy [%]	84	84	93	91	86	41	73

The highest diagnostic accuracy of the system of 93% was achieved with this group of patients for D=0.4, when the system selected 35 key manifestations (out of a total of 87). These results were used here as a basis for evaluating systems potential to automatically generate criteria for diagnosing Systemic Lupus Erythematosus. The paper (Petri, M., et al., 2012) provided a ready test bed for this evaluation.

Out of the 35 key manifestations a manifestation was selected to the group of diagnostic criteria for SLE only if its value that was highly associated with SLE was not normal, i.e. if pathology of some sort was present. That resulted in BELART system suggesting 7 manifestations representing criteria for diagnosing SLE at the level D=0.4. Both BELART and SLICC criteria are presented in Table 2. below.

It has to be noted that all 7 manifestations suggested by BELART as diagnostic criteria were also on the list of SLICC. The apparent absence of Elevated IgG and/or IgM: present is only a consequence of the fact that this manifestation is a more general equivalent of the more specific four manifestations, Antinuclear antibody, Anti-double-stranded DNA, Anti-Sm, and Antiphospholipid antibody, that are all present in the SLICC list.

Table 2. Diagnostic criteria for SLE suggested by BELART (D=0.4) and those of SLICC.

BELART	SLICC
Photosensitivity: present	Malar rash/photosensitive rash/acute cutaneous lupus
	Discoid rash
	Oral ulcers
	Nonscarring alopecia
	Arthritis
	Serositis
	Renal
Pyuria: sterile	Neurologic
Anemia: 100<Hb<120	Hemolytic anemia
	Leukopenia
	Lymphopenia <1,500mm3
	Lymphopenia <1,000mm3
	Thrombocytopenia
ANA: positive >1:80	Antinuclear antibody
Anti ds DNA: high	Anti-double-stranded DNA
	Anti-Sm
	Antiphospholipid antibody
Low complement: present	Low complement
Elevated IgG and/or IgM: present	

The systems diagnostic accuracy and robustness as well as its capability

of automatic generation of diagnostic criteria makes it convenient for possible future use in educational environments, or field tests by general practitioners in medically underserved areas, where no specialist consultation, or more complex, pathognomonic tests are available.

References

Srdanović, V. and Šošić, M. 2013. Integrating Knowledge and Data in a Medical Decision Support System, in Verovatnosne logike i njihove primene, Mathematical Institute SANU, Belgrade, 27-29.

Petri, M., Orbai, A. M., Alarcn, G. S., Gordon, C., Merrill, J. T., Fortin, P. R. et al. 2012. Derivation and validation of the Systemic Lupus International Collaborating Clinics classification criteria for systemic lupus erythematosus. Arthritis Rheum.; 64(8):2677-86.

Srdanović, V. et al. 2015. Evaluating Diagnostic Accuracy of a Clinical Decision Support System: Case Study of Systemic Connective Tissue Disorders, in Verovatnosne logike i njihove primene, Mathematical Institute SANU, Belgrade, 15-18.

Reasoning with the Ontologies

Milan Todorovi
Mathematical Institute of the
Serbian Academy of Sciences and Arts
mtodorivic@mi.sanu.ac.rs

Aleksandra Zdravkovi
Mathematical Institute of the
Serbian Academy of Sciences and Arts
alekzdravkovic@mi.sanu.ac.rs

Bojan Marinkovi
Mathematical Institute of the
Serbian Academy of Sciences and Arts
bojanm@mi.sanu.ac.rs

During the last four years the members of Mathematical Institute of the Serbian Academy of Sciences and Arts participated in realization of COST project Colour and Space in Cultural Heritage (COSCH), particularly in the activities concerning developing COSCH^{KR} application.

With the colleagues from University of Applied Sciences, Mainz (Germany) we took part in the developing of the ontology, which gathers the knowledge about process of 3D scanning. Information stored in ontology was collected with the other members of this COST action, and was structured into the ontology.

It was decided that would be useful to develop an application that will bring closer this knowledge to the scholars from the fields of social sciences and humanities. This application will, trough the iterating process of asking questions and getting the answers, provide the examples from the best practices, i.e. which instruments and techniques to use for solving the problems related to 3D scanning of the object(s) they have, and how to use the obtained results.

The developed program consists from two parts. First part, front end of the application, consists of the standard web interface that allows an user to instantiate the values of the given parameters from drop down lists. After that, the system takes these values and based on their values choose the next parameters that will be offered to the user in the next iteration, if this

possible. Otherwise, the system will mark those parameters that create the contradiction, and will ask user to change at least one of these values, if it meets user's criteria.

The process of reasoning consists of the transformation of the mentioned ontology into the Prolog syntax, and to search the knowledge base by the Prolog system. The choice of the parameter for the next iteration is chosen as the one with the minimum of the classes of equivalences of possible solutions from the set of uninstantiated parameters.

Method for generating pseudo-random numbers with unique values in output sequence

Vladan Vučković
Faculty of Electronic Engineering,
University of Niš, Serbia
vladan.vuckovic@elfak.ni.ac.rs

Nenad Stojiljković
Faculty of Electronic Engineering,
University of Niš, Serbia
nenad.jiggy.stojiljkovic@gmail.com

Abstract

Generating pseudo-random numbers is one of the computer science fields of study that matured together with computer science. With desire to create mathematical simulations of nature that is everywhere around as, we often find a need to describe some non deterministic behavior. Many of natural phenomena are looking like they have non deterministic behavior, without clear patterns. Is this true, or are we just looking at those phenomena forms from the wrong point of view that can not give us possibility to notice some patterns? Maybe nature it self is one big random number generator but we can not realize this. For example, if we are looking at simple model of an hydrogen atom, we can assume that electron is moving on cyclic orbit around nucleus. But if there is only one electron in one cyclic orbit why than we can not know the exact position of that electron? The latest research in this field give as the proof that when we are watching electron movement in hydrogen atom we can see one noise ring. This can lead as to assumption that hydrogen atom is also one random generator itself, that position of electron is determined by precise natural random generator that create ideal noise when we watch output specter of his values. If we want to create mathematical model of hydrogen atom, unique, homogeneous random sequence will be ideal to simulate electron movements. There are a lot of examples like this why no overhead generators are important in computer science. The last few years there are a lot of researches which goal is to improve existing and to create new searching

algorithms. Interesting fact is that the importance of generated random sequence that is used in those algorithms is being neglected. We can see from tests [2] that default generators are having high percentage of overheads in output sequences. We can get a major improvements in performances of searching algorithms if we use pseudo-random number generators without overhead, because every time we have overhead in output values, searching algorithm tries to go back to the same path. In this paper we consider method for generating unique homogeneous pseudo-random values using Latin square as base structure. It appears that this method produces values with negligibly small linear correlation coefficient and also satisfy principle of homogeneous distribution of values over the entire set.

References

[1] 'Introduction to Statistic', accessed 29 June 2016, http://onlinestatbook.com/Online_Statistics_Education.pdf

[2] Stojiljković, N., Vučković, V.: 'Efficient Pseudo-Random Generator for Homogeneous Filling of 2D arrays'. Proc. Int. Conf. SYM-OP-IS 2015: XLII International Symposium on Operations Research, Silver Lake Resort, Serbia, September 2015, pp. 265–268

[3] Knuth, D.E.: 'The Art of Computer Programming, Seminumerical Algorithms' (Addison Wesley Longman, 1997, 3 rd edn.)

[4] Knuth, D.E.: 'The Art of Computer Programming, Introduction to Combinatorial Searching' (Addison Wesley Longman, 2007, 4 th edn.)

[5] Riley, T., Goucher, A.: 'Beautiful Testing' (O'Reilly Media, 2010.)

[6] Merkle, M.: 'Verovatnoća i statistika za inženjere i studente tehnike' (Akademska Misao, 2006.)

[7] Smith, J.D.H, Romanowska, A.B.: 'Post-modern algebra' (Wiley-Interscience, 1999.)

[8] Radivojević, V.: 'Classification of Latin squares'. MSc thesis, Faculty of Mathematics, University of Belgrade, 2009

[9] Stojiljković, N.: 'Graphical representation of pseudo-random numbers'. Final thesis, Faculty of Electronic Engineering, University of Niš, 2014

A Method for Extracting SBS movies from Virtual Reality Tesla Laboratories

Vladan Vučković
Faculty of Electronic Engineering,
University of Niš, Serbia
vladan.vuckovic@elfak.ni.ac.rs

Aleksandar Stanišić
Faculty of Electronic Engineering,
University of Niš, Serbia
ciandre23@gmail.com

In this paper we present original method for generate SBS movies from UDK and construct VR room of Tesla's original patents in Unreal engine 4.

We use following components: Hardware: OS WINDOWS 10 64, PC Athlon FX 4200, 8Gb RAM, 6870 2GB VRAM, VR SAMSUNG GEAR, SAMSUNG GALAXY E7 and software: UDK (Unreal 3 engine), Unreal 4 engine, Nvidia CodeWorks for Android, Oculus Rift Tools. Digital movies of Colorado Springs and Tesla Long Island laboratory were firstly finished in Matinee UDK.

UDK is excellent tool but with no ability to represent VR, or to create SBS movies, so we took different approach. First, we create walkthrough in UDK with no depth. Next step was to create depth in our movies by SBS technique.

The basic technique of stereo displays is to present offset images that are displayed separately for the left and right eye. Both of these 2D offset images are then combined automatically to give the perception of 3D depth. Although the term "3D" is ubiquitously used, it is important to note that the presentation of dual 2D images is distinctly different from displaying an image in three full dimensions. The most notable difference to real 3D displays is that the observer's head and eyes movements will not increase information about the 3-dimensional objects being displayed, it's more "aquarium" feeling.

Software for this in our case is FonePaw Converter Ultimate. After importing normal movie in program we put 3D settings. For our use was : Split Screen Side By Side (Full),Depth 10, Encoder H.264, Resolution 2560x1440, Video bitrate 6000kbps, Samsung Galaxy Edge settings.

In Unreal 4 engine we created a scene with some of the famous Tesla patents, Tesla induction motor, Tesla coil, Colombo's egg of Nikola Tesla with magnetic tube, Nikola Tesla's boat with remote controller. We were choosing Project for Android devices, maximum Graphics quality, with support for VR Oculus Rift. We put Antialiasing option on, Bloom and all the effects. Also we put ETC2 texture compression.

With the release of OpenGL ES 3.0 in 2013 (and full OpenGL 4.3), the ETC2 format became a standard, with backwards compatibility and important new features. First, it added full alpha support like DXT3/5 (in 8bpp), as well as 1-bit "punch-through" alpha (in 4bpp). Second, it brought the EAC format, which supports 1 and 2-channel data (R and RG, in 4 and 8bpp respectively). Third, it added sRGB data support. And last but not least, it claimed to offer better quality than competitors at the same bitrate. The biggest issue with ETC2 are complaints about its extremely slow compression tools.

After that we create intro 3-D Matinee. Now, sequence from Matinee becomes full VR.

References

[1] Knuth, D.E.: 'The Art of Computer Programming, Seminumerical Algorithms' (Addison Wesley Longman, 1997, 3 rd edn.)

[2] Knuth, D.E.: 'The Art of Computer Programming, Introduction to Combinatorial Searching' (Addison Wesley Longman, 2007, 4 th edn.)

[3] Choi, SangSu, Kiwook Jung, and Sang Do Noh.: 'Virtual reality applications in manufacturing industries: Past research, present findings, and future directions.' (Concurrent Engineering, 2015)

[4] Lanier, Jaron, and F. Biocca: 'An Insider's View of the Future of Virtual Reality' (Journal of Communication, 42(4), 150, 1992)

[5] Warwick, K., Gray, J. and Roberts, D. eds.: 'Virtual Reality in Engineering' (Peter Peregrinus, 1993)

[6] Zhai, Philip: 'Get Real: A Philosophical adventure in Virtual Reality' (Rowman and Littlefield Publishers, New York and Oxford, 1998)

[7] Robles-De-La-Torre G.: 'The Importance of the Sense of Touch in Virtual and Real Environments' IEEE Multimedia 13(3) (Special issue on Haptic User Interfaces for Multimedia Systems, pp. 2430, 2006)

[8] Kelly, K., A. Heilbrun and B. Stacks: 'Virtual Reality; an Interview with Jaron Lanier'(Whole Earth Review, no. 64, pp. 108(12), 1989)