



Peta nacionalna konferencija  
“Verovatnosne logike i njihove primene”  
Beograd, Srbija, 29-30. oktobar 2015.

Knjiga apstrakata

ORGANIZATOR:

Matematički institut, SANU

KONFERENCIJU FINANSIRAJU:

Ministarstvo prosvete i nauke Republike Srbije

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.





Peta nacionalna konferencija  
“Verovatnosne logike i njihove primene”  
Beograd, Srbija, 29-30. oktobar 2015.

TEME KONFERENCIJE:

Verovatnosne logike, problemi potpunosti, odluivosti i slozenosti; logike osnove u zasnivanju verovatnoe; bayes-ove mreze i drugi srodni sistemi; programski sistemi za podrku odluivanju u prisustvu neizvesnosti; primene verovatnosnog zakljuivanja u medicini; teorija informacija; mere informacija i slozenosti; teorija kodiranja; sigurnost u sajber-prostoru; slozeni i dinamicki sistemi i donosenje 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 (Matematički institut SANU)

ORGANIZATOR:

Matematički institut, SANU

KONFERENCIJU FINANSIRAJU:

Ministarstvo prosvete i nauke Republike Srbije

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

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



## Program konferencije:

### 29. 10. 2015.

- 11:00 *Otvoranje*
- 11:15 *Evaluating diagnostic accuracy of a clinical decision support system: case study of systemic connective tissue disorders*, V. Srdanović, M. Šošić, M. Rašković, S. Rašković, A. Perić-Popadić, V. Djurić, Ž. Jovičić, A. Srdanović
- 11:35 *The System for the support of the clinical decision making based on the comparison of patients on the basis of clinical and laboratory parameters by using the expanded the hamming distance...*, Nataša Glišović, Miodrag Rašković, Sanvila Rašković, Aleksandra Perić-Popadić, Vojislav Djurić
- 11:55 *First-Order Probabilistic Common Knowledge Logic*, Siniša Tomović, Zoran Ognjanović, Dragan Doder
- 12:15 *Augmented Reality as a Tool for Maintaining and Repairing Complex Industrial Systems*, Dušan Tatić, Bojan Tešić
- 12:35 *Music Genre Classification Based On Signal Rhythmic Segmentation*, Miloš Djurić, Milena Stanković
- 12:55 *Pauza*
- 14:00 ..., Aleksandar Perović
- 14:20 *On the generalized thermostatics for generalized entropies*, Miomir Stanković, Velimir Ilić
- 14:40 *Random coefficient bivariate INAR(1) model with dependent innovation processes*, Predrag Popović, Miroslav Ristić, Aleksandar Nastić
- 15:00 *Generation of Random Numbers by Exploiting Indetermination Caused by Race Effect of Multi-Threading Processes, Memory Content and Process State Information*, Vladan Vučković, Nikola Savić, Nenad Stojiljković
- 15:20 *Implementation of VoIP Encryption using RC4 Algorithm*, Vladan Vučković, Milan Randjelović, Nenad Stojiljković
- 15:40 *Models for sequent calculus with high probabilities*, Marija Boričić

**30. 10. 2015.**

- 11:00 *Probabilistic groupoids*, Smile Markovski
- 11:30 *What is Probability Logic?*, Zvonimir Šikić
- 12:30 *Elements of mathematical phenomenology and logical analogies: Some results on the basis of the logical analogies*, Katica Hedrih
- 13:00 *Ultrametric information*, Branko Dragović
- 13:20 *Intelligent building efficiency assessment using multiattribute utility theory*, Aleksandar Janjić, Lazar Velimirović, Miomir Stanković
- 13:40 *Ad hoc dynamic systems in emergencies*, Jelena Ranitović, Vesna Nikolić

# Apstrakti





# Sadržaj

<b>Ad hoc dynamic systems in emergencies</b>	<b>11</b>
<i>Jelena Ranitović, Vesna Nikolić</i>	
<b>Augmented Reality as a Tool for Maintaining and Repairing Complex Industrial Systems</b>	<b>12</b>
<i>Dušan Tatić, Bojan Tešić</i>	
<b>Elements of mathematical phenomenology and logical analogies: Some results on the basis of the logical analogies</b>	<b>14</b>
<i>Katica Hedrih</i>	
<b>Evaluating diagnostic accuracy of a clinical decision support system: case study of systemic connective tissue disorders</b>	<b>15</b>
<i>V. Srdanović, M. Šošić, M. Rašković, S. Rašković, A. Perić-Popadić, V. Djurić, Ž. Jovičić, A. Srdanović</i>	
<b>First-Order Probabilistic Common Knowledge Logic</b>	<b>19</b>
<i>Siniša Tomović, Zoran Ognjanović, Dragan Doder</i>	
<b>Generation of Random Numbers by Exploiting Indetermination Caused by Race Effect of Multi-Threading Processes, Memory Content and Process State Information</b>	<b>20</b>
<i>Vladan Vučković, Nikola Savić, Nenad Stojiljković</i>	
<b>Implementation of VoIP Encryption using RC4 Algorithm</b>	<b>22</b>
<i>Vladan Vučković, Milan Randjelović, Nenad Stojiljković</i>	
<b>Intelligent building efficiency assessment using multiattribute utility theory</b>	<b>24</b>
<i>Aleksandar Janjić, Lazar Velimirović, Miomir Stanković</i>	
<b>Models for sequent calculus with high probabilities</b>	<b>25</b>
<i>Marija Boričić</i>	
<b>Music Genre Classification Based On Signal Rhythmic Segmentation</b>	<b>27</b>
<i>Miloš Djurić, Milena Stanković</i>	
<b>On the generalized thermostatics for generalized entropies</b>	<b>29</b>
<i>Miomir Stanković, Velimir Ilić</i>	

<b>Probabilistic groupoids</b>	<b>32</b>
<i>Smile Markovski</i>	
<b>Random coefficient bivariate INAR(1) model with dependent innovation processes</b>	<b>33</b>
<i>Predrag Popović, Miroslav Ristić, Aleksandar Nastić</i>	
<b>The System for the support of the clinical decision making based on the comparison of patients on the basis of clinical and laboratory parameters by using the expanded the hamming distance</b>	<b>35</b>
<i>Nataša Glišović, Miodrag Rašković, Sanvila Rašković, Aleksandra Perić-Popadić, Vojislav Djurić</i>	
<b>Ultrametric information</b>	<b>38</b>
<i>Branko Dragović</i>	
<b>What is Probability Logic?</b>	<b>40</b>
<i>Zvonimir Šikić</i>	

# Ad hoc dynamic systems in emergencies

*Jelena Ranitović, Vesna Nikolić* \*†‡

## Abstract

The accelerated growth of Information and Communication Technologies (ICTs), especially the expansion and use of social media, has significantly influenced the flow of information in emergencies. Virtual organizations are becoming increasingly interconnected [1]. Dynamic systems, such as Ushahidi crisis mapping platform, allow ad hoc virtual collaboration and enable its users - first responders, digital volunteers, private and non-profit organizations to gather and disseminate useful information in near real-time [2]. Therefore, a complex system created in this way collects big crisis data from various sources. The effectiveness of the collective action and organized behavior, apart from providing an opportunity for a timely emergency response, greatly contributes to better decision-making in dynamic environments [3].

## References

- [1] Marsden, Janet Hinda Watkins. "Developing a Framework for Stigmatic Human Collaboration with Technology Tools: Cases in Emergency Response." (2015).
- [2] Meier, Patrick. "Crisis mapping in action: How open source software and global volunteer networks are changing the world, one map at a time." *Journal of Map and Geography Libraries* 8.2 (2012): 89-100.
- [3] Comfort, Louise K., et al. "Complex systems in crisis: Anticipation and resilience in dynamic environments." *Journal of contingencies and crisis management* 9.3 (2001): 144-158.

---

\*Jelena Ranitović is with the Faculty of Occupational Safety, University of Niš, Čarnojevića 10 A, 18000 Niš, Serbia, e-mail: jelena.ranitovic85@gmail.com

†Vesna Nikolić is with the Faculty of Occupational Safety, University of Niš, Čarnojevića 10 A, 18000 Niš, Serbia, e-mail: vesnik08@gmail.com

‡This work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under Grant III 44006.

# Augmented Reality as a Tool for Maintaining and Repairing Complex Industrial Systems

*Dušan Tatić*

*Faculty of Electronic Engineering, University of Niš  
dule\_tatic@yahoo.com*

*Bojan Tešić*

*Mine and Power Plant Ugljevik  
bojan\_pupi@hotmail.com*

## **Abstract**

Augmented reality (AR) is a technology that combines in real time pictures from the real world with virtual elements in order to provide users additional information about their surroundings [1]. This technology is widely used in different areas of research such as medicine, cultural heritage, architecture, etc. It also finds numerous uses in the field of industry. There is great number of applications of these technologies used for the maintenance and repair [2] or manufacturing process [3].

In this paper, we discuss the usage of augmented reality from the point view of complex systems implemented in industry. Complex industry systems are usually characterized by a large number of subsystems with different functionality and a variety of technologies combined into a global system that is hard for one human being to comprehend and understand in details [4]. The augmented reality could be used for visualization of certain steps of maintaining and repairing tasks and providing guidelines for performing related procedures in the form of video and audio signals, and when convenient also 3D models. Another related aspect is improvement of occupational safety conditions, due to a remotely controlled application of augmented reality supported interactive check lists of tasks.

A case study is presented on the example of particular maintenance and repair processes in the Thermal plant Ugljevik, Bosnia and Herzegovina. Usually, workers knowledge is gathered from specific courses and printed books. Also, big portion of this knowledge is transferred from more experienced workers to new ones. We provide an AR tool for helping less experienced workers to learn how new tasks should be performed in the form of strict guidelines that have to be followed. The

transition to the next subtask is strictly controlled and possible if the previous task is completely performed, which is verified by a check list integrated with a remote controller. Due to that, the time, cost, and error rate of maintaining and repairing procedures is reduced.

We provide a structure, application, and data layer, of the system which describes a concrete maintenance and repair instruction flow. This structure has to be followed by the worker in realization of a specific task. By capturing the surrounding environment with camera, the worker is capable to follow instructions by using the AR tool on the display of his mobile device. By recognizing specific markers, at the exact working place in the industry space, the worker gets video information how he should realize the given task. Each step in the implementation of a task is recorded and confirmed in an interactive check list, which controls the proper implementation of tasks, reducing in this way possibility for human caused errors.

## References

- [1] Carmigniani, Julie, Borko Furht, Marco Anisetti, Paolo Cervolò, Ernesto Damiani, and Misa Ivkovic. "Augmented reality technologies, systems and applications." *Multimedia Tools and Applications* 51, no. 1 (2011): 341-377.
- [2] Fiorentino, Michele, Antonio E. Uva, Michele Gattullo, Saverio Debernardis, and Giuseppe Monno. "Augmented reality on large screen for interactive maintenance instructions." *Computers in Industry* 65, no. 2 (2014): 270-278.
- [3] Nee, A. Y. C., S. K. Ong, G. Chryssolouris, and D. Mourtzis. "Augmented reality applications in design and manufacturing." *CIRP Annals-Manufacturing Technology* 61, no. 2 (2012): 657-679.
- [4] Bliudze, Simon. "A Framework for Studying Complex Industrial Systems: An Example Based on the UMTS Infrastructure." PhD diss., Ph. D. Thesis, Ecole Polytechnique, 2006

# Elements of mathematical phenomenology and logical analogies: Some results on the basis of the logical analogies

*Katica R. (Stevanovi) Hedrih*  
*Mathematical Institute SANU*  
*e-mail: khedrih@sbb.rs*

Starting with Petroviš Elements of mathematical phenomenology, the elements of logical analogies are presented. Some results on the basis of the logical analogies are listed with corresponding explanations and its importance for science and applications. One of these obtained results is logical and mathematical analogy between vector models of rigid body mass moment vectors coupled for axis and pole and vector model of cross co-relation between three stochastic processes and mathematical and logical analogies between rigid body mass moment state around a point and state of cross co-relation between three stochastic processes around a pole. Also is possible to identify logic analogies with stress state and strain state in a point of the stressed and deformed deformable body. Logical analogy is, also, visible between kinetic elements of collision between two translator bodies and two rolling balls in collision.

# Evaluating diagnostic accuracy of a clinical decision support system: case study of systemic connective tissue disorders

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

A fundamental problem in knowledge base system design is that of explicitly formulating knowledge relevant to the specific domain. Significant portion of that knowledge, however, is often implicitly contained in data related to the domain. In medical domain such data are relatively well systematized and easily accessible in the form of patient case histories. Paper discusses some strategies for integrating medical expert knowledge with data from clinical practice, built in BELART clinical decision support system (Srdanovi, 1986), that has been originally designed to address the problem. The system was successfully applied to several medical domains. Recently, the new version of the system has been ported to a new platform, and has been applied to the domain of systemic connective tissue disorders.

Autoimmune systemic diseases like systemic lupus erythematosus, progressive systemic sclerosis and Sjgren's syndrome 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 the 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 facilitate communication BELART has an interface developed to let expert clinician define his domain by selecting manifestations/attributes that are relevant to the domain. He/she defines attribute types, values they could take on, their formats and constraints, their costs, etc.

Domain definition allows for a clinical data base formation, to which the system is linked. Analyses performed on these data provide the knowledge about associations among entities in the knowledge base and the estimates of their strength. This new knowledge is in the form of simple production (or IF-THEN) rules, with manifestations as their IF parts, and diagnoses as their THEN parts. Associated with each rule are special attributes: diagnostic strength, source and reference. Corresponding diagnostic strengths are estimated by relative frequencies of occurrence of particular manifestations with the given diagnosis. Diagnostic strengths can take on values from 0 to 1, with 0.1 increments (0 meaning that manifestation does not occur with the particular disease, while 1 means that it is pathognomonic for the disease). It can thus be interpreted as a generalized sensitivity estimate for a particular manifestation.

Clearly, knowledge base consisting of rules entered by expert clinician, and particularly, those generated by the system in the way described here, can potentially be very large. To resolve that, the system employs several heuristic procedures to restructure its knowledge base additionally, and prepare it for the consultation process.

In order that a specific manifestation be a key one for diagnosing certain disease within the domain, it is not sufficient that it is manifested with high diagnostic strength with that disease. It is quite possible that the same manifestation attribute is associated with a high diagnostic strength with all of the diseases within a particular domain. Such manifestation may be very important, though, in case domain in question is a much larger one, containing many subdomains. It will then play a role of constrictor, a concept introduced by Pople (1982). Within a single domain, however, key manifestations will be those that are being manifested with significantly different diagnostic strengths with various diseases within the domain. For a given margin by which diagnostic strengths differ key manifestations are selected that discriminate the most among two diseases. For each pair of diseases and a given margin  $D$ , a set of key manifestations is formed. Obviously, selection of higher or lower margin, effects in more or less strict selection of key manifestations. Heuristics for extracting the key manifestations is a core reasoning strategy of the system.

To evaluate the systems performance, and specifically its diagnostic accuracy, 44 patient case histories from the Clinic of Allergy 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 with Systemic Lupus Erythematosus, 18 with Sjgren’s Syndrome, 11 with Systemic Sclerosis.

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 were missing, i.e. have not been established.

The evaluation process proceeds as follows. The patient case history for which the system is to suggest a diagnosis is taken out from a set of all case histories and a value for D is selected. The remaining n-1 (in our study 43) case histories are then presented to the system. The system analyzes presented case histories and prepares for consultation process by restructuring its knowledge base accordingly as described above. The consultation for the selected patient case history is then performed by using its initial data to establish working hypothesis of the possible disease(s) encountered. The system is directing the further information-gathering procedure by first asking questions about the patient that would discriminate the most among the alternative diagnoses. Also, the less costly questions are asked first. After each question is answered, i.e. value of the manifestation attribute is established for the patient in question, data are evaluated and new scores are formed for each disease category considered. In case that during a course of consultation a need to include a new disease entity in the working hypothesis becomes evident, the system would do so and continue with asking questions relevant to this new situation. Eventually the diagnosis is suggested. The process is repeated for all patient case histories at the selected level D.

Table 1. bellow shows the diagnostic accuracy of the system for different values of D. The highest diagnostic accuracy in this study of 91

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

Table 1. Diagnostic accuracy

It is worth noting here that the systems accuracy was somewhat lower for both higher and lower values of D. For higher values (D=0.6,...,0.8) the

explanation is that corresponding sets of key manifestation are very restricted and in fact derived from often a small number of degenerate data. For example, for  $D=0.8$  the system has suggested diagnoses after considering only 5 manifestations, while practically no case history participating in the study had all of the manifestation in question established. On the other hand, for lower values of  $D$  diagnostic accuracy was 84

The systems diagnostic accuracy and robustness 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

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.

Pople, H. E. 1982. Heuristic methods for imposing structure on ill-structured problems: the structuring of medical diagnostics. In Szolovits, P. (Ed.), *Artificial Intelligence in Medicine*, AAAS Symposium Series, Boulder, Colo.: Westview Press, 119-185.

Srdanovi, V. and oi, M. 2013. Integrating Knowledge and Data in a Medical DecisionSupport System, in *Verovatnosne logike i njihove primene*, Mathematical Institute SANU, Belgrade, 27-29. Srdanovi, V. 1986. BELART A Consultation System Integrating Knowledge and Data, MEDINFO-86, (Salamon/Blum/Jrgensen, eds.), North-Holland, 228-231.

# First-Order Probabilistic Common Knowledge Logic

*Tomović Siniša      Zoran Ognjanović      Dragan Doder*

We introduce a first-order probabilistic epistemic logic with common knowledge which allows a group of infinitely many agents. We provide its syntax and semantics, and prove the strong completeness property.

# Generation of Random Numbers by Exploiting Indetermination Caused by Race Effect of Multi-Threading Processes, Memory Content and Process State Information

*Vladan Vučković*

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

*Nikola Savić*

*Faculty of Electronic Engineering, University of Niš, Serbia  
savic.nikola@elfak.rs*

*Nenad Stojiljković*

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

## **Abstract**

Random number generators are widely used and exploited in computer science and applications. Usually, the pseudo-random number generators are being used as their properties are good enough for majority of applications. However, these methods have flaws and limitations which are primarily based on their ability to fairly well approximate the sequences of random numbers but not to produce truly random values. In this paper, novel methods for generating random numbers are proposed. These three new methods include generators of random numbers which exploit the processes states, memory content and indetermination caused by race effect of multi-threading processes for generation of random numbers.

## **1 Introduction**

Random numerical values are necessary and key component within many cryptographic and general purpose algorithms and therefore their generation, as

well as properties of algorithms used for generation of random numerical values is of uttermost importance in computer science. Flaws within random number generators may lead to easier cryptanalysis of confidential data. Today, the most widely used method for generating random numbers are pseudo random number generators or PRNGs [1]. These methods are fast and reliable however flawed in a sense that the PRNG-generated sequence is not truly random, because it is completely determined by a relatively small set of initial values. Furthermore it is quite possible to predict all the generated sequences produced by PRNG by simply knowing the initial values or by inspecting the series of produced random values over time. Main goal of this paper is to show the prospects of utilization of new ways of generating random numbers by non-arithmetic methods. This would be achieved by exploiting the state of computer system memory and processes as source of randomness as well as by exploiting of indeterminism caused by race effect of multi-threading processes.

## References

- [1] F. James. A review of pseudorandom numbers generators. *Computer Physics Communications*, Vol. 60, Issue 3, 1990, pp. 329344.
- [2] D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*. Addison Wesley Longman, Massachusetts, 1998.
- [3] S. N. Mehmood, N. Haron, V. Akhtar, Y. Javed. Implementation and Experimentation of Producer Consumer Synchronization Problem. *International Journal of Computer Applications (0975 8887)*, Vol. 14, Issue 3, 2011, pp. 32-37.
- [4] W. Stalling. *Operating Systems*. Pearson Education, USA, 2006.
- [5] N. Stojiljković, V. Vučković. Efficient Pseudo-Random Generator for Homogeneous Filling of 2D arrays. *Zbornika radova, XLII Internacionalni simpozijum o operacionim istraivanjima, Matematiki Institut SANU*, 2015, pp. 265-268.
- [6] N. Stojiljković. *Grafičko predstavljanje generatora pseudo-slučajnih brojeva*. Elektronski fakultet, Univerzitet u Nišu, 2014.

# Implementation of VoIP Encryption using RC4 Algorithm

*Vladan Vučković*

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

*Milan Randjelović*

*Faculty of Electronic Engineering, University of Niš, Serbia  
mail*

*Nenad Stojiljković*

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

## **Abstract**

In era of information technologies one of the most considered question is information security. With rapid expansion of Internet technologies, we came up with many security problems and vulnerabilities. Voice over Internet Protocol (VoIP) is one very popular technology that is used for voice communications and multimedia sessions over Internet Protocol (IP) networks, such as Internet itself. So the question is how to make VoIP communication secure and reliable? In this paper we discuss method for VoIP encryption using RC4 encryption algorithm.

## **1 Introduction**

Security is one of the most important segments of modern communication technologies. When we talk about VoIP communication, security takes the most important part in the design of VoIP system. Because of the time-critical nature of VoIP communication most of the conventional security measures currently implemented in today's data networks could not be used without enormous impact on system performance. So the objective of this research is to find a possible way of data encryption that could be easily applied to VoIP data stream and be implemented in real VoIP systems. Because of the stream based nature of VoIP we will be using stream ciphers as natural selection for this type of data communication. In this paper we will purpose

one efficient method for VoIP data transfer encryption based on RC4 stream cipher algorithm.

## References

- [1] Alaa M. Riad, Alaa R. Shehata, Elminir K. Hamdy, Mohammed H. Abou-Alsouad, Taha R. Ibrahim. Evaluation of the RC4 algorithm as a solution for converged networks. *Journal of ELECTRICAL ENGINEERING*, Vol. 60, Issue 3, 2009, pp. 155-160.
- [2] Mr. Sachin C Malke, Mr. Girish Talmale. The Design and Development of Low Cost Voip Device Using Linux. *Int. Journal of Engineering Research and Applications*, Vol. 4, Issue 3( Version 1), 2014, pp. 96-98.
- [3] M. Susheel Kumar, M. Sudhakar. Implementation of a voip media stream encryption device. *International Journal of Engineering Science and Advanced Technology*, Vol. 3, Issue 4, pp. 160-164.
- [4] Alaa E Din Riad, Hamdy K. Elminir, Alaa R. Shehata, Taha R. Ibrahim. Security evaluation and encryption efficiency analysis of RC4 stream cipher for converged network applications. *Journal of ELECTRICAL ENGINEERING*, Vol. 64, Issue 3, 2013, pp. 196-200.
- [5] Ashraf D. Elbayoumy, Simon J. Shepher. Stream or Block Cipher for Securing VoIP. *International Journal of Network Security*, Vol. 5, Issue 2, 2007, pp. 128-133.
- [6] Kaustubh Lohiya, Narendra Shekokar, Satish R. Devane. End to End Encryption Architecture for Voice over Internet Protocol. *International Journal of Computer Applications (0975 - 8887)*, Vol. 41, Issue 14, 2012, pp. 31-34.

# Intelligent building efficiency assessment using multiattribute utility theory

*Aleksandar Janjić, Lazar Velimirović, Miomir Stanković* \*†‡§

## Abstract

The successful automation of an intelligent building relies on the ability of the smart home system to organize, process, and analyze different sources of information to drive the automation decision-making according to different criteria defined by the user [1-3]. To this end, a strong and formal support for the knowledge base is central to the system design. In this approach, the new methodology for discrete stochastic multiple criteria decision making problem in intelligent building efficiency assessment, with different types of tradeoffs among criteria has been presented [4]. The advantage of this approach is the usage of compensatory aggregation, which is more suitable for conflicting criteria or the human aggregation behaviour.

## References

- [1] D. H. Stefanov, Z. Bien, W. C. Bang, 'The Smart House for Older Persons and Persons With Physical Disabilities: Structure, Technology Arrangements, and Perspectives', *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 12, no. 2, pp. 228-250, 2004.
- [2] M. Chan, E. Campo, D. Esteve, J. Fourniols, 'Smart homescurrent features and future perspectives', *Maturitas*, vol. 64, no. 2, pp. 9097, 2009.
- [3] T. Gentry, 'Smart homes for people with neurological disability: state of the art', *Neuro Rehabilitation*, vol. 25, pp. 209225, 2009.
- [4] A. Janjic, A. Andjelkovic, M. Docic, 'Multi-attribute Risk Assessment using Stochastic Dominance', *International Journal of Economics and Statistics*, vol. 1, no. 3, pp. 105-112, 2013.

---

\* Aleksandar Janjić is with the Faculty of Electronic Engineering, Univeristy of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia, e-mail:Aleksandar.Janjic@elfak.ni.ac.rs

† Lazar Velimirović is with the Mathematical Institute of the Serbian Academy of Sciences and Arts, Kneza Mihaila 36, 11001 Belgrade, Serbia, e-mail:velimirovic.lazar@gmail.com

‡ Miomir Stanković is with the Faculty of Occupational Safety, University of Niš, Čarnojevića 10 A, 18000 Niš, Serbia, e-mail: miomir.stankovic@gmail.com

§ This work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under Grant III 42006 and Grant III 44006.



# Models for sequent calculus with high probabilities

*Marija Boričić*

*Faculty of Organizational Sciences, University of Belgrade*

*marija.boricic@fon.bg.ac.rs*

In order to formalize the notion of deduction relation in probability logic, we introduce a system **LKprob**( $\varepsilon$ ) for some fixed small real  $\varepsilon > 0$ , a generalization of Gentzen's sequent calculus for classical propositional logic **LK**, where the probabilized sequents are of the form  $\Gamma \vdash^n \Delta$  meaning that 'the probability of truthfulness of the sequent  $\Gamma \vdash \Delta$  is greater than or equal to  $1 - n\varepsilon$ ' (see [3]). Our approach is based on two great ideas in logic – Gentzen's sequent calculus for classical propositional logic on one hand (see [5]), and Suppes' concept regarding propositions with high probabilities on the other hand (see [10] and [11]).

For every connective, there are two types of logical rules in our system (see [3]) – one introducing the connective in antecedent, and the other in consequence, for example:

$$\frac{\Gamma AB \vdash^n \Delta}{\Gamma A \wedge B \vdash^n \Delta} (\wedge \vdash) \quad \frac{\Gamma \vdash^n A \Delta \quad \Gamma \vdash^m B \Delta}{\Gamma \vdash^{m+n} A \wedge B \Delta} (\vdash \wedge)$$

Also, there are structural rules, where we point out the cut rule:

$$\frac{\Gamma \vdash^n A \Delta \quad \Pi A \vdash^m \Lambda}{\Gamma \Pi \vdash^{m+n} \Delta \Lambda}$$

and the additivity rule, which is characteristic for probability logics:

$$\frac{AB \vdash^0 \quad \vdash^m A \quad \vdash^n B}{\vdash^{m+n-k} AB}$$

where  $k\varepsilon = 1$ .

Models for **LKprob**( $\varepsilon$ ) are defined as a mapping  $p : Seq \rightarrow I \cap [0, 1]$  satisfying the following conditions:

- (i)  $p(A \vdash A) = 1$ , for any formula  $A$ ;
- (ii) if  $p(AB \vdash) = 1$ , then  $p(\vdash AB) = p(\vdash A) + p(\vdash B)$ , for any formulae  $A$  and  $B$ ;

(iii) if sequents  $\Gamma \vdash \Delta$  and  $\Pi \vdash \Lambda$  are equivalent in **LK**, in sense that there are proofs for both sequents  $\bigwedge \Gamma \rightarrow \bigvee \Delta \vdash \bigwedge \Pi \rightarrow \bigvee \Lambda$  and  $\bigwedge \Pi \rightarrow \bigvee \Lambda \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$  in **LK**, then  $p(\Gamma \vdash \Delta) = p(\Pi \vdash \Lambda)$ , where  $I = \{1 - n\varepsilon | n \in \mathbf{N}\}$  and  $Seq$  is the set of all sequents in **LK**. We say that the sequent  $\Gamma \vdash^n \Delta$  is satisfied in a model  $p$ , i.e.  $\models_p \Gamma \vdash^n \Delta$ , if and only if  $p(\Gamma \vdash \Delta) \geq 1 - n\varepsilon$  (see [2], [3], [4], [6], [7], [8] and [9]).

Our system is sound and complete with respect to the given models (see [1], [2] and [3]).

## References:

- [1] M. Boričić, *Hypothetical syllogism rule probabilized*, **Bulletin of Symbolic Logic**, 20, No. 3, 2014, pp. 401–402, Abstract, Logic Colloquium 2012, University of Manchester, 12th–18th July 2012.
- [2] M. Boričić, *Models for the probabilistic sequent calculus*, **Bulletin of Symbolic Logic**, 21, No. 1, 2015, p. 60, Abstract, Logic Colloquium 2014, European Summer Meeting of Association for Symbolic Logic, Vienna University of Technology 14th–19th July.
- [3] M. Boričić, *Suppes–style sequent calculus for probability logic*, **Journal of Logic and Computation**, (to appear) doi:10.1093/logcom/exv068
- [4] R. Carnap, **Logical Foundations of Probability**, University of Chicago Press, Chicago, 1950.
- [5] G. Gentzen, *Untersuchungen über das logische Schliessen*, **Mathematische Zeitschrift** 39 (1934–35), pp. 176–210, 405–431 (or G. Gentzen, **Collected Papers**, (ed. M. E. Szabo), North–Holland, Amsterdam, 1969).
- [6] T. Hailperin, *Probability logic*, **Notre Dame Journal of Formal Logic** 25 (1984), pp. 198–212.
- [7] H. Leblanc, B. C. van Fraassen, *On Carnap and Popper probability functions*, **The Journal of Symbolic Logic** 44 (1979), pp. 369–373.
- [8] H. Leblanc, *Popper’s 1955 axiomatization of absolute probability*, **Pacific Philosophical Quarterly** 69 (1982), pp. 133–145.
- [9] 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.
- [10] P. Suppes, *Probabilistic inference and the concept of total evidence*, in J. Hintikka and P. Suppes (eds.), **Aspects of Inductive Inference**, North–Holland, Amsterdam, 1966, pp. 49–55.
- [11] C. G. Wagner, *Modus tollens probabilized*, **British Journal for the Philosophy of Science** 54(4) (2004), pp. 747–753.

# Music Genre Classification Based On Signal Rhythmic Segmentation

*Miloš Djurić*

*Mathematical Institute SANU*

*djura042@gmail.com*

*Milena Stanković*

*University of Niš,*

*Faculty of Electronic Engineering*

*milena.stankovic@elfak.ni.ac.rs*

In this discussion we propose a new approach of recognition and classification of music according to genres, based only on audio content of the signal. Our previous work [?] showed that classification results achieved by Support Vector Machine (SVM) [?] method using features proposed by Tzanetakis-Cook [?] are in rank with already developed classifiers, but in a case of smaller number of possible classification sets, and training vectors.

The main novelty of presented method is in different signal segmentation based on the, most likely, changeable intrinsic rhythm of the music. Musical rhythm can be perceived as a combination of strong and weak beats [?]. Beat spectrum is a measure to automatically characterize rhythm and tempo of the music. Highly repetitive music will have strong beat spectrum peaks at the repetition times, therefore both tempo and the relative strength of particular beats are revealed. A stronger beat usually corresponds to the first and third quarter note and the weaker beat corresponds to the second and forth quarter note in a measure, in case that musical tact value is  $4/4$ . So, if the strong beat constantly alternates with the weak beat, the inter-beat-interval (which is the temporal difference between two successive beats) would correspond to the temporal length of a quarter note in music theory terms.

After the autocorrelation of the signal, the beat-tracking system can recognize the hierarchical beat structure comprising the quarter-note level (almost regularly spaced beat times and  $4/4$  musical tact), the half-note level ( $2/4$  musical tact). If neither is recognized in first iteration, the algorithm will move further through signal and after three more iterations, musical tact will either be recognized as one of mentioned above, or else be declared as  $3/4$  tact.

As for the issue of feature selection, four new features are added to the nine already existing in [?], represented as mean and variance for both maximal and minimal beat energy values for every frame. The purpose of signal segmentation according to intrinsic rhythm is to eliminate or to reduce the influence of signal parts with insufficient musical content, pauses and atypical rhythmic structure on the classification process.

Classification method for presented research compared to the previous one [?] has two main differences:

1. The non-linear SVM classifier is used. If we are given a set of training data  $(x_1, x_2, \dots, x_n)$  and their class labels  $(y_1, y_2, \dots, y_n)$ , where  $x_i \in \mathbb{R}^n$  and  $y_i \in -1, +1$ , to construct a non-linear SVM classifier inner product  $\langle x, y \rangle$  is replaced by a polynomial kernel function of degree  $d$   $K(x, y) = (\langle x, y \rangle + 1)^d$
2. Two additional classification genres: Rock-60-80s and Jazz, with total of five classification sets.

The results are presented in table , and can be compared with other classifiers that operate with similar problem [?, ?, ?, ?].

Future work will include unsupervised machine learning experiment, by using hidden Markov models. In the first step, segmentation based on music intrinsic rhythmic structure will be performed, and features extracted. Then, based on these features, hidden Markov model will be trained for every music piece. In the second step, a distance matrix will be constructed from the distances between every pair of music pieces (hidden Markov models) and clustering to make desired clusters will be performed. The mel-frequency cepstrum has proven to be highly effective in automatic speech recognition and in modeling the subjective pitch and frequency content of audio signals [?, ?], so signal cepstral analysis could also be included in future work.

N	Classical	Dance	Metal	Rock	Jazz
Training Vectors	100	100	100	100	100
Test Vectors	80	80	80	80	80
Correct Hits	80	78	75	61	59
Misses	0	2	5	19	21
Classification Accuracy	1	0.98	0.94	0.76	0.74

Table 1: Music genre SVM classification results

# On the generalized thermostatics for generalized entropies

*Miomir Stanković*

*Faculty of Occupational Safety, Niš  
miomir.stankovic@gmail.com*

*Velimir Ilić*

*Mathematical Institute SANU  
velimir.ilic@gmail.com*

In the past, there was extensive work on defining the information measures which generalize the Shannon entropy [6]. One of the first generalization was given by Rényi [10], who proposed a parameterized entropy,

$$\mathcal{R}_\alpha = \begin{cases} -\sum_{k=1}^n p_k \ln(p_k) & \text{for } \alpha = 1 \\ \frac{1}{1-\alpha} \ln \left( \sum_{k=1}^n p_k^\alpha \right), & \text{for } \alpha > 0, \alpha \neq 1. \end{cases}$$

which reduces to the Shannon entropy in the case  $\alpha = 1$ . Recently, we introduced and characterized new type of generalized entropy [4], which can be given as a transformation of Rényi entropy

$$\mathcal{H}(P) = h(\mathcal{R}_\alpha(P)),$$

where  $h : \mathbb{R} \rightarrow \mathbb{R}$  is an increasing and continuous function such that  $h(0) = 0$ . Beside Shannon and Rényi entropies, the generalized entropy covers the case of Sharma-Mittal entropy [11], which is defined as  $\mathcal{SM}_{\alpha,q} = h_q(\mathcal{R}_\alpha(P))$ , where

$$h_q(x) = \begin{cases} x & \text{for } q = 1 \\ \frac{e^{(1-q)x} - 1}{1-q}, & \text{for } q \neq 1. \end{cases}$$

Special cases of Sharma-Mittal are: Shannon entropy  $\mathcal{S}(P) = \mathcal{SM}_{1,1}(P)$  [6], Rényi entropy  $\mathcal{R}_\alpha = \mathcal{SM}_{1,\alpha}(P)$  [10], Tsallis entropy  $\mathcal{T}_q(P) = \mathcal{SM}_{q,q}(P)$  [12] and Gaussian entropy  $\mathcal{G}_q(P) = \mathcal{SM}_{q,1}(P)$  [2].

In this talk we derive generalized thermostatics and thermodynamical stability condition (TSC) for the generalized entropy defined in [4]. As an instance, TSC for Sharma-Mittal entropy is derived. Thus, we unify and generalize a lot of previous results for Shannon entropy [5], [1], Rényi and Tsallis entropies [9], [13], [7], [14], Sharma-Mittal entropy [3] and Gaussian entropy [8].

## Acknowledgment

This research supported by Ministry of Science and Technological Development, Republic of Serbia, Grants No. 174026 and III 044006.

## References

- [1] H.B. Callen. *Thermodynamics and an Introduction to Thermostatistics*. Wiley, 1985.
- [2] T.D. Frank and A. Daffertshofer. Exact time-dependent solutions of the Rényi Fokker-Planck equation and the Fokker-Planck equations related to the entropies proposed by Sharma and Mittal. *Physica A: Statistical Mechanics and its Applications*, 285(3–4):351 – 366, 2000.
- [3] T.D. Frank and A.R. Plastino. Generalized thermostatics based on the Sharma-Mittal entropy and escort mean values. *The European Physical Journal B - Condensed Matter and Complex Systems*, 30(4):543–549, 2002.
- [4] Velimir M. Ilić and Miomir S. Stanković. Generalized Shannon-Khinchin axioms and uniqueness theorem for pseudo-additive entropies. *Physica A: Statistical Mechanics and its Applications*, 411(0):138 – 145, 2014.
- [5] E. T. Jaynes. Information theory and statistical mechanics. *Phys. Rev.*, 106:620–630, May 1957.
- [6] A. I. Khinchin. *Mathematical Foundations of Information Theory*. Dover Publications, June 1957.
- [7] E.K. Lenzi, R.S. Mendes, and L.R. da Silva. Statistical mechanics based on Rényi entropy. *Physica A: Statistical Mechanics and its Applications*, 280(3–4):337 – 345, 2000.
- [8] Th. Oikonomou. Properties of the "non-extensive Gaussian" entropy. *Physica A: Statistical Mechanics and its Applications*, 381(0):155 – 163, 2007.

- [9] John D. Ramshaw. Thermodynamic stability conditions for the Tsallis and Rényi entropies. *Physics Letters A*, 198(2):119 – 121, 1995.
- [10] Alfred Renyi. *Probability Theory*. Dover Publications, May 1970.
- [11] B.D. Sharma and D.P. Mittal. New non-additive measures of entropy for discrete probability distributions. *Journal of mathematical sciences*, 10:28–40, 1975.
- [12] Constantino Tsallis. Possible generalization of Boltzmann-Gibbs statistics. *Journal of statistical physics*, 52(1):479–487, 1988.
- [13] Constantino Tsallis, RenioS. Mendes, and A.R. Plastino. The role of constraints within generalized nonextensive statistics. *Physica A: Statistical Mechanics and its Applications*, 261(3–4):534 – 554, 1998.
- [14] Tatsuaki Wada. On the thermodynamic stability conditions of Tsallis' entropy. *Physics Letters A*, 297(5–6):334 – 337, 2002.

# Probabilistic groupoids

**Smile Markovski**

*Faculty of Computer Science and Engineering  
"Ss. Cyril and Methodius" University  
Skopje, Macedonia  
smile.markovski@finki.ukim.mk*

**Lidija Goračinova-Ilieva**

*Faculty of Communication and IT  
FON University  
Skopje, Macedonia  
lidija.goracinova@fon.edu.mk*

Algebraic structures are commonly used as a tool in treatments of various processes. But their exactness reduces the opportunity of their application in non-deterministic environment. On the other hand, probability theory and fuzzy logic do not provide convenient means for expressing the result of combining elements in order to produce new ones. Moreover, these theories are not developed to "measure" algebraic properties. Therefore, we propose a new concept which relies both on universal algebra and probability theory.

We introduce probabilistic mappings, whose special case is the notion of probabilistic algebra. Here we consider discrete sets with only one binary operation, additionally including the "possibility" of obtaining one particular element as a product, among all of the others. This leads to a structure that we call probabilistic groupoid. "Ordinary" groupoids are just a special type of probabilistic ones.

Let  $A$  and  $B$  be at most countable non-empty sets, and let  $\mathcal{D}_B$  be the set of all probability distributions on  $B$ . Probabilistic mapping from  $A$  to  $B$  is a mapping  $h : A \rightarrow \mathcal{D}_B$ .

Let  $A$  be a set,  $n \in \mathbb{N}$ , and let  $A^n = \{(a_1, a_2, \dots, a_n) | a_i \in A, i = 1, 2, \dots, n\}$  be the  $n$ -th power of  $A$ . Every probabilistic mapping from  $A^n$  to  $A$  is a probabilistic ( $n$ -ary) operation on  $A$ . A pair  $(A, F)$  of a set  $A$  and a family  $F$  of probabilistic operations on  $A$  is called probabilistic algebra. When  $F = \{f\}$  has one binary operation, then the probabilistic algebra  $(A, f)$  is a probabilistic groupoid. Some basic properties of such structures are considered in this paper.



# Random coefficient bivariate INAR(1) model with dependent innovation processes

*Predrag M. Popović\**, *Miroslav M. Ristić†*, *Aleksandar S. Nastić‡*

Modelling time series of counts and predicting future events is an interesting topic for many researchers. One of the main approaches in modelling time series of counts is based on defining different autoregressive models where the autocorrelation is modelled with thinning operators. When two time series are dependent arises the need for introducing bivariate models. The aim of the paper is to introduce a bivariate autoregressive model with random coefficients for nonnegative time series of counts. The model that we present here is composed of two components: survival process and innovation process. The dependence between two series is introduced through their innovation processes. The survival part of the model is the autoregressive component which has an influence on the modelled time series with some probability.

The general form of the bivariate autoregressive model with random coefficients and dependent innovations is defined with the following equations

$$X_{1,t} = U_{1,t} \circ X_{1,t-1} + \varepsilon_{1,t} \quad (1)$$

$$X_{2,t} = U_{2,t} \circ X_{2,t-1} + \varepsilon_{2,t} \quad (2)$$

where

$$U_{i,t} : \begin{pmatrix} \alpha_i & 0 \\ p_i & 1 - p_i \end{pmatrix}, \quad i = 1, 2$$

and  $\alpha_1, \alpha_2 \in (0, 1)$ ,  $p_1, p_2 \in [0, 1]$ . Binomial thinning operator is defined as  $\alpha_j \circ X_{j,t} = \sum_{i=1}^{X_{j,t}} B_{ji}$ , where  $\{B_{ji}\}$  are i.i.d. random variables with Bernoulli distribution and parameter  $\alpha_j$ ,  $j = 1, 2$ . The counting series that define  $\alpha_1 \circ X_{1,t}$  and  $\alpha_2 \circ X_{2,t}$  are mutually independent. Random variables  $\varepsilon_{1,t}$  and

---

\*Faculty of Civil Engineering and Architecture, University of Niš, Serbia e-mail: popovicpredrag@yahoo.com

†Faculty of Sciences and Mathematics, University of Niš, Serbia e-mail: miristic72@gmail.com

‡Faculty of Sciences and Mathematics, University of Niš, Serbia e-mail: anastic78@gmail.com

$\varepsilon_{2,t}$  are dependent and have a joint bivariate distribution, but also independent with respect to the counting series for all  $t \in \mathbb{N}_0$ . Also, random vector  $(\varepsilon_{1,t}, \varepsilon_{2,t})$  is independent from  $(X_{1,s}, X_{2,s})$  for  $s < t$ .

We prove the existence of the model defined by equations (1) and (2). The main statistical properties of the model are discussed. For the estimation of parameters of the proposed model we consider method of moments and conditional maximum likelihood method. The asymptotic distribution of the obtained estimates is proved.

We present two special cases of the model, one where the innovation process is generated by bivariate Poisson distribution and the other where the innovation process is generated with bivariate negative binomial distribution. Practical aspect of these models are considered on real data.

## Acknowledgment

This work was supported by the Serbian ministry of education and science of the Republic of Serbia under Grant 044006, 174026 and 174013.

**The System for the support of the  
clinical decision making based on the  
comparison of patients on the basis of  
clinical and laboratory parameters by  
using the expanded the hamming  
distance**

*Nataša Glišović*

*State University of Novi Pazar,*

*Department of Mathematical Sciences,*

*Mathematical Institute of the Serbian Academy of Sciences and Arts*

*natasaglisovic@gmail.com*

*Miodrag Rašković*

*Mathematical Institute of the Serbian Academy of Sciences and Arts*

*goca@mi.sanu.ac.rs*

*Sanvila Rašković*

*University of Belgrade, School of Medicine,*

*Clinical Center of Serbia,*

*Institute of Allergology and Immunology*

*sanvilar28@gmail.com*

*Aleksandra Perić-Popadić*

*University of Belgrade, School of Medicine,*

*Clinical Center of Serbia,*

*Institute of Allergology and Immunology*

*popaleksandra@yahoo.com*

*Vojislav Djurić*  
*University of Belgrade, School of Medicine,*  
*Clinical Center of Serbia,*  
*Institute of Allergology and Immunology*  
*vojislav.djuric@kcs.ac.rs*

When modern information technologies appeared the first ideas about their possible application for the support in medical decision making appeared as well. In medicine, different from many other areas, a great deal of relatively well systematized and homogeneous medical knowledge is implicitly contained in patients' illness history. That gives the possibility for the medical experts to formulate the frame for their knowledge and that the systems based on the effective strategies of reasoning produce useful knowledge from such formulated frames and appropriate patients illness histories.

The integrated information systems in medicine and the standardized data bases about the patients give the possibilities for the development of new systems' generations for the support in the clinical decision making which would be available to the users of such integrated systems. The systematic illnesses of the connective tissue are manifested by expressive heterogeneity, both clinical and laboratory parameters (manifestations).

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 (Agrawal et al., 1993.). A metric or distance function is a function which defines a distance between elements of a set (Li et al., 2004 and Vitanyi, 2005). A set with a metric is called a metric space. In many data retrieval and data mining applications, such as clustering, measuring similarity between objects has become an important part.

In this paper presented a proposal for extended hamming distances. The advantage of the proposed distance is what can calculate the distance between two patients with incomplete by data.

The support system enables that clinical doctors compare and find similar patients quickly and objectively according to the given clinical and laboratory parameters which are necessary for the diagnostics and therapy of each patient. By finding the pairs of patients on the basis of the least distance (in the context of the expanded hamming distance) we have the possibility:

- To compare the therapy approach for each of them.
- To follow the clinical illness course, if in further following, the clinical course of the two nearest patients will be even more similar (by bringing closer to the same or by moving away the distance).
- By throwing in the newly diagnosed patients into the system base with already existing patients, there is a possibility of determining the distance of

a new patient in relation to the existing, which make it easier for the clinical doctors to make decision about further diagnostic and therapy procedures.

- By bringing into the base of the suspect cases (without enough criteria for establishing the diagnosis SLE), with establishing the immediate distance, as well as the eventual possible occurrence of new parameters in the time course, the final diagnosis is made more easily.

- The system can be applied to other clinical branches of medicine (intern, pediatrics, infective, dermatology, neurology).

- The system is flexible, it can find similar patients according to the given parameters, either individually (for example, the level of proteinuria, the number of thrombocytes) or by combinations of more parameters (such as dcDNA, the proteinuria level, the consumption C3 and C4 complement components) for the purpose of everyday clinical work.

**ACKNOWLEDGEMENT** The work presented here was supported by the Serbian Ministry of Education and Science (project III44006).

## References

[1] 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.

[2] Siegel RM, Lipsky PE. Autoimmunity. In: Firestein GS, Budd RC, Harris Ed, et al, eds. Kelley's Textbook of Rheumatology . 8th ed. Philadelphia, Pa: Saunders Elsevier; 2009:chap 15.

[3] 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.

[4] Li M., Chen X., Ma B., Vitanyi P. The similarity metric. IEEE Transactions on Information Theory, 2004, vol.50, No. 12, pp.3250-3264.

[5] Vitanyi P. Universal similarity, ITW2005, Rotorua, New Zealand, 2005.

[6] 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.

# Ultrametric Information

*Branko Dragović*  
*Institute of Physics*  
*Belgrade University*  
*and Mathematical Institute SANU*  
*e-mail:dragovich@ipb.ac.rs*

## Abstract

Distance is a very useful concept in science and mathematically is expressed by metric. To present physical distance it is used Euclidean metric or its generalization in the form of the Riemannian metric. However, there are systems whose elements are hierarchically ordered. In a hierarchical system it may be even more important to know nearness between its elements which is not related to their physical distance but to some other characteristics, in particular to some information. We show that some information characteristics of hierarchical systems can be described by ultrametric distance. As an illustrative example of hierarchical system with ultrametries we present set of 64 codons in the genetic code. Ultrametric (also called non-Archimedean metric) is a metric with strong triangle inequality (ultrametric inequality), i.e.

$$d(x, y) \leq \max\{d(x, z), d(y, z)\}. \quad (1)$$

Ultrametric spaces have some unusual properties: all triangles are isosceles, there is no partial intersection of balls, any point of a ball can be considered as its center, and so on.

*Example 1.* As an example of ultrametric space one can take set of 125 three-digit 5-adic numbers, i.e.

$$a_0 + a_1 5 + a_2 5^2 \equiv a_0 a_1 a_2, \quad a_i \in \{0, 1, 2, 3, 4\}.$$

5-Adic distance between any two different above 5-adic numbers  $a = a_0 a_1 a_2$  and  $b = b_0 b_1 b_2$  may have one of three possible values: (i)  $d_5(a, b) = 1$  if  $a_0 \neq b_0$ , (ii)  $d_5(a, b) = 1/5$  if  $a_0 = b_0$ ,  $a_1 \neq b_1$ , and (iii)  $d_5(a, b) = 1/25$  if  $a_0 = b_0$ ,  $a_1 = b_1$ ,  $a_2 \neq b_2$ . One can easily check that inequality (1) is satisfied. It is not difficult to generalize this 5-adic example to any  $p$ -adic case with  $n$  digits. Then there will be  $p^n$  elements, which are non-negative integers.

*Example 2.* Moreover, one can take  $m^n$  strings  $a_1 a_2 \dots a_n$  of the length  $n$ , where components  $a_i$  should not be numbers, but some other

entities in  $m$  different states ( $m \geq 2$ ). Here ultrametric distance between two different elements  $a = a_1a_2\dots a_n$  and  $b = b_1b_2\dots b_n$  can be introduced as follows:  $d(a, b) = n - k + 1$  if  $a_1 = b_1, a_2 = b_2, \dots, a_k \neq b_k, 1 \leq k \leq n$ .

*Example 3.* Codons are ordered triplets  $a_0a_1a_2$  of four nucleotides (U, A, C, G). Hence, there are  $4^3 = 64$  codons. The corresponding connection between codons and 5-adic numbers in *Example 1* can be introduced by suitable identification of nucleotides and digits, namely:  $U = 1, A = 2, C = 3, G = 4$ . At **Table** is presented the genetic code of vertebrate mitochondria and codons in quadruplets are at the shortest 5-adic distance. Taking 2-adic distance within quadruplets, they separate into two doublets. It is worth noting that just these codon doublets are directly related to amino acids [1–3]. Codon quadruplets can be also obtained according *Example 2*, where  $m = 4$  and  $n = 3$ .

From *Example 3* one can conclude that ultrametric distance is appropriate to describe information content of codons – two codons code the same amino acid when their ultrametric distance is the shortest one. There are also other examples of hierarchical systems, where ultrametrics is appropriate to describe nearness which is related to some information properties.

111 UUU Phe	211 AUU Ile	311 CUU Leu	411 GUU Val
112 UUA Leu	212 AUA Met	312 CUA Leu	412 GUA Val
113 UUC Phe	213 AUC Ile	313 CUC Leu	413 GUC Val
114 UUG Leu	214 AUG Met	314 CUG Leu	414 GUG Val
121 UAU Tyr	221 AAU Asn	321 CAU His	421 GAU Asp
122 UAA Ter	222 AAA Lys	322 CAA Gln	422 GAA Glu
123 UAC Tyr	223 AAC Asn	323 CAC His	423 GAC Asp
124 UAG Ter	224 AAG Lys	324 CAG Gln	424 GAG Glu
131 UCU Ser	231 ACU Thr	331 CCU Pro	431 GCU Ala
132 UCA Ser	232 ACA Thr	332 CCA Pro	432 GCA Ala
133 UCC Ser	233 ACC Thr	333 CCC Pro	433 GCC Ala
134 UCG Ser	234 ACG Thr	334 CCG Pro	434 GCG Ala
141 UGU Cys	241 AGU Ser	341 CGU Arg	441 GGU Gly
142 UGA Trp	242 AGA Ter	342 CGA Arg	442 GGA Gly
143 UGC Cys	243 AGC Ser	343 CGC Arg	443 GGC Gly
144 UGG Trp	244 AGG Ter	344 CGG Arg	444 GGG Gly

**Table.** The vertebrate mitochondrial genetic code.

[1] B. Dragovich and A. Dragovich, “A  $p$ -adic model of DNA sequence and genetic code”, *p-Adic Numbers Ultrametric Anal. Appl.* **1**, 34–41 (2009), [arXiv:q-bio.GN/0607018v1].

[2] B. Dragovich and A. Dragovich, “ $p$ -Adic modelling of the genome and the genetic code”, *Computer Journal* **53**, 432–442 (2010), [arXiv:0707.3043v1 [q-bio.OT]].

[3] B. Dragovich, “ $p$ -Adic structure of the genetic code”, *Neuro-Quantology* **9**, 716–727 (2011), [arXiv:1202.2353 [q-bio.OT]] .

# What is Probability Logic?

*Zvonimir Šikić*  
*University of Zagreb*

We examine similarities and differences between probability as mathematical theory (Kolmogorov etc.) and probability as logic (Laplace, Boole, etc.) - from historical and factual viewpoint. Special emphasis will be on the laws of large numbers (weak and strong) and countable and uncountable probabilities (in the sense of Borel).