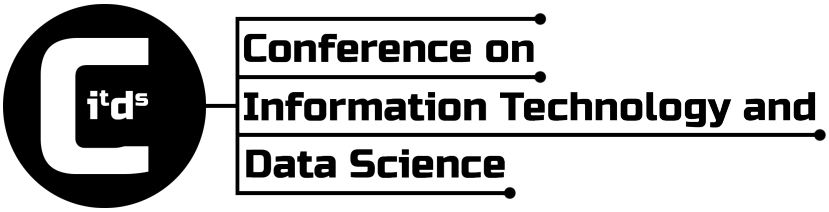
University of Debrecen

Faculty of Informatics

Debrecen, Hungary

The 1^{st} Conference on Information Technology and Data Science



Committee members
Conference Chairmen

- István Fazekas
- András Hajdu

Program Committee

Sándor Baran	István Fazekas
András Hajdu	Márton Ispány
Roland Kunkli	István Oniga
Attila Pethő	László Szathmáry
János Sztrik	György Vaszil
Erzsébet Csuhaj Varjú	Zoltán Fülöp
Miklós Hoffmann	Gábor Szederkényi
Gergely Kovásznai	Attila Kiss

Organizing Committee

Piroska Bíró	Tibor Tómács
András Czinke	Attila Gilányi
Roland Kunkli	Attila Kuki
Sándor Pecsora	Jánosné Polgár
Anett Rácz	Erzsébet Tóth

General contact e-mail: citds@inf.unideb.hu

The conference was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

Contents

Deep Learning-Based Approach for Detecting Cassini-Huygens Spacecraft Trajectory Modifications*

Ashraf ALDabbas[a], Zoltán Gál[b]

[a]University of Debrecen (Doctoral School of Informatics)
ashraf.dabbas@inf.unideb.hu

[b]University of Debrecen (Faculty of Informatics)
gal.zoltan@inf.unideb.hu

Machine learning has changed numerous domains also the path we fulfill research. Concerning GIS and spatial scope of study several approaches have been developed such as data remote sensing. This research paper provides a supervised approach for detecting changes among Cassini spacecraft orbit, a deep learning method based on recurrent neural network. Long Short-Term Memory (LSTM) and bidirectional LSTM is utilized to identify the needed patterns in time series. Mainly, change detection make practical and effective use of multi-temporal datasets to observe special events. As such, our research seeks to offer a unique perspective of the substantial processes requested concerning change detection of the Cassini orbiter around the planet Saturn.

Keywords: Cassini-Huygens interplanetary project, complex event, sensory data, big data, artificial intelligence, pattern processing, knowledge representation

Introduction

The connotation of a complex event is tied up with processing multiple events accompanied by paying attention to mark out distinct events within a timely tributary of events [2]. There are cases where the obtainable information to depict any process or system is just an inspection of the observations. There is a remarkable denomination of issue to recognize an extreme event for the scope of big data [4].
The spacecraft launched in October 1997 from the Earth arrived to the orbit around planet Saturn on 1 Jul 2004 [8]. This event is named Saturn Orbit Insertion (SOI) of the spacecraft Cassini-Huygens. It required the spacecraft 6.7 years from the Earth's launch to reach its destination (SOI) at Saturn. The data set that we conducted our research in this work can be found at the NASA reference [7].

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund. The paper was supported by the QoS-HPC-IoT Laboratory, too.

Related work and previous studies

High number of research papers are accessible in the Cassini-Huygens project field [1, 3, 5, 6, 9]. Majority of them are focused on the Saturn, its rings and moons. No detailed evaluation of the trajetory modifications of the Cassini orbiter was presented in the scientific literature yet.

Complex event detection conditions of the Cassini trajectory

The main goal behind the application of our classifier is to specify complex events from sensor-generated data. To recognize the temporal semantics for identifying complex events, we have extended the sensory data index. The trajectory of the spacecraft was modified several times but no detailed information is available publicly about these events. The accessible database of the NASA with 116 volumes contains samplings with high dispersion of the time. After the process of SOI in 2004, the spacecraft was executing several modifications of the trajectory conform to the commands sent by the supervisor team from the Earth.

Since velocity is a measured vector variable, an extreme event in the trajectory implies fulfilling one of the following two conditions: an extreme change in time of the velocity vector direction or of the velocity vector magnitude. Cardinality of the processed sets I and J, give the number of extreme events considered trajectory modifications of the Cassini orbiter. Generation of these two sets were based on fulfilling the threshold values of the conditions. The cardinality dependence of the sets I and J was analysed in function of threshold values and working point of operation was determined. The total number of extreme events based on velocity vector modification and acceleration magnitude modification are 210 and 114, respectively. These events serve to make binary classification of the samples.

Classification with recurrent neural networks

It is obvious that extreme events of the trajectory are time dependent and can be detected based on the sequences of the sampled multidimensional time series. To keep the orbiter on the complex helicoid discussed previously, automatic modifications were executed by the orbiter. Because of different scientific and astronomical targets of the project, there were sent modification commands of the trajectory by the human control team from the Earth. For better sensing the memory behaviour of the trajectory we used Bi-LSTM and LSTM layer of the tested neural networks. The confusion matrix with regard to binary classification is a 2×2 table intended to depict the grouping model performance and shows precisely the number of classified samples. Usage of the Matthews correlation coefficient MCC and F1 score gave us possibility to determine classification precision of each tested LSTM or Bi-LSTM RNN system.

References

[1] A. ALDABBAS, Z. GAL: *Cassini–Huygens mission images classification framework by deep learning advanced approach*, International Journal of Electrical and Computer Engineering (IJECE) 11.3 (2020), DOI: http://doi.org/10.11591/ijece.v11i3.pp%25p.

[2] A. ALDABBAS, Z. GÁL: *Complex Event Processing Based Analysis of Cassini–Huygens Interplanetary Dataset*, in: Intelligent Computing Paradigm and Cutting-edge Technologies: Proceedings of First international conference on Innovative Computing and Cutting-edge Technologies (ICICCT 2019), Istanbul, Turkey: Springer, 2019, pp. 51–66, DOI: https://doi.org/10.1007/978-3-030-38501-9.

[3] A. ALDABBAS, Z. GÁL: *Learning and Reasoning with structured Prediction Based on Revealing Event Complexity*, International Journal of Advanced Science and Technology 29.3 (2020), pp. 13816–13828, DOI: http://sersc.org/journals/index.php/IJAST/article/view/31723.

[4] G. DEMATTEIS, T. GRAFKE, E. VANDEN-EIJNDEN: *Rogue waves and large deviations in deep sea*, Proceedings of the National Academy of Sciences 115.5 (2018), pp. 855–860.

[5] P. HAN, W. WANG, Q. SHI, J. YANG: *Real-time Short-Term Trajectory Prediction Based on GRU Neural Network*, in: 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), IEEE, 2019, pp. 1–8.

[6] D. IZZO, M. MÄRTENS, B. PAN: *A survey on artificial intelligence trends in spacecraft guidance dynamics and control*, Astrodynamics (2019), pp. 1–13.

[7] NASA: *National Aeronautics and Space Administration of the USA, Cassini ISS Online Data Volumes, Imaging Science Subsystem (ISS), Saturn EDR Data Sets*, (Accessed on 30/10/2020), URL: %5Curlhttps://pds-imaging.jpl.nasa.gov/volumes/iss.html.

[8] J. NIETO, A. SUSÍN: *Cage Based Deformations: A Survey*, in: Deformation Models: Tracking, Animation and Applications, Netherlands: Springer, 2013, pp. 75–99, DOI: https://doi.org/10.1007/978-94-007-5446-1_3.

[9] L. SPILKER, S. EDGINGTON: *Cassini-Huygens: Recent Science Highlights and Cassini Mission Archive*, EPSC 2019 (2019), EPSC–DPS2019.

Smartwatch activity recognition using ML.net framework

Alexandru Alexan[a], Anca Alexan[a], Oniga Ștefan[a]

[a]Department of Electric, Electronic and Computer Engineering, Technical University of Cluj-Napoca, North University Center Baia Mare
alexanalexandru@gmail.com
anca.alexan@cunbm.utcluj.ro
stefan.oniga@cunbm.utcluj.ro

Wearable devices are becoming everyday objects, assisting us in many fields including healthcare [2]. One of the most popular wearable technology devices is the smartwatch, which replaced an every-day carry device with one capable of monitoring and assisting the wearer. This integrates very well with the smart house ideology [4], providing a device that can control any aspect of a smart House in an extremely small form factor. Although the initial reason for using a smartwatch[1] may not be health or IoT integration orientated, this small device can easily help in these areas and do much more. Even though these devices are not medical grade, they can help detect health problems [5] due to their multiple integrated sensor types and high wear time. Another area that can benefit from a small device that has movement sensors and is worn most of the time by the user is activity recognition. Activity recognition was extensively implemented using a smartphone [3], using one detection device that can record and process the user's movement data. Having another device, a smartwatch, that is worn by the user on his wrist, helps significantly in providing correlation data and additional information regarding the user's current activity. The data that is gathered by the smartwatch needs to be processed, and for this, we choose a .net machine learning framework, ML.Net. With this framework, we have access to complex pipelines for machine learning processing. Due to the emergence of .net Core, which can run on multiple operating systems, this library can be used on a wide number of platforms. One of the most important aspects of choosing this framework was the fact that is open source, allowing the developer to see or even alter the source code.

The data from the chosen smartwatch, a Samsung Gear S3 device, was gathered using a custom Tizen app written in c sharp. This Tizen .NET application has access to the underlying sensor layer and its values. There are multiple advantages of using the C sharp programming language, besides rapid application development, as we benefit from the Common Language Infrastructure standards and a managed runtime. This application handles the data gathering process from the smartwatch device and uses a web-socket to transfer this data to the cloud.

The gathered and processed data is comprised of accelerometer and gyroscope data for the three axes: x, y and z. The obtained data is being also displayed on the watch face as shown in figure 1 while the watch application is running.

After the data is loaded into the cloud, it is currently offline processed using the ML.NET framework to analyze the activity types. The best algorithm for this data, tested

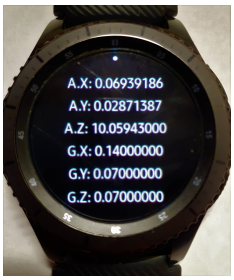


Figure 1: Sensor data displayed on the smartwatch

using a small data-set, is FastTreeRegression with a coefficient of determination of 0.9392. The chosen FastTreeRegression algorithm is an implementation of the MART gradient boosting algorithm and yielded good results on the used data-set.

Keywords: activity recognition, smartwatch, wearables, IoT, machine learning, ML.NET, sensor network

References

[1] A. Barbu, G. Militaru, I. Savu: *Factors Affecting Use of Smartwatches*, FAIMA Business & Management Journal 7.5 (Mar. 2020), pp. 44–57.

[2] B. Fong, A. Fong, C. Li: *Wearable Healthcare* (May 2020), pp. 239–256, DOI: https://doi.org/10.1002/9781119575788.ch9.

[3] A. Ismael, M. Jayabalan, D. Al-Jumeily: *A Study on Human Activity Recognition Using Smartphone*, Journal of Advanced Research in Dynamical and Control Systems 12 (May 2020), pp. 795–803, DOI: https://doi.org/10.5373/JARDCS/V12SP5/20201818.

[4] Y. Li, K. Zhao, M. Duan, W. Shi, L. Lin, X. Cao, Y. Liu, J. Zhao: *Control Your Home with a Smartwatch*, IEEE Access PP (July 2020), pp. 1–1, DOI: https://doi.org/10.1109/ACCESS.2020.3007328.

[5] L. Silva, S. Murilo, R. Lins: *Uso de SmartWatch no Auxílio a Monitoração de Arritmias Cardíacas / Usage of SmartWatch to Assist Monitoring of Cardiac Arrhythmias*, Brazilian Journal of Development 6 (Oct. 2020), pp. 75511–75525.

Multi-Resident location detecting in Smart Home

Anca Alexan[a], Alexandru Alexan[a], Stefan Oniga[a]

[a]University of Cluj-Napoca, North University Center Baia Mare
anca.alexan@cunbm.utcluj.ro
alexanalexandru@gmail.com
stefan.oniga@cunbm.utcluj.ro

Smart homes equipped with activity detection sensors, which have a binary output, can be considered low-cost activity monitored locations. Although this type of activity detection system has a low-profile and is very affordable, it can successfully be used in multiple domains such as automation, health monitoring, security and activity detection [7]. This system works very well if detecting simple actions or monitoring a single subject. However, if multiple residents live in the same smart home, correctly determining the activity type and pinpointing the correct subject can get very challenging [3], [5]. One option to improve the activity detection rate and accuracy is to use Artificial Intelligence to interpret the data gathered from the Smart House sensor networks. Since we are dealing with multiple resident scenarios, one of the most difficult roles of the artificial intelligence layer is to correctly match the sensor data to the appropriate resident [2] to correctly identify the performed activity. The amount of data and quality can greatly affect the chosen data analysis algorithm and predictions. Using machine learning algorithms (MLA) [6] can greatly increase the detection accuracy due to the multiple existing data processing functions [4]. Since MLA is a universal nonlinear tool for modeling and processing complex data [1], it is a great choice for complex activity recognition. In this article, we propose an activity detection and recognition system that is capable of operating in a multi-resident smart house. We propose to recognize complex activities and assign them to the correct resident.

Keywords: smart home, CASAS, multi-resident tracking

References

[1] A. ALEXAN, A. ALEXAN, S. ONIGA, I. PAP: *Analysis of activity detection data pre-processing*, in: Oct. 2019, pp. 282–286,
DOI: https://doi.org/10.1109/SIITME47687.2019.8990804.

[2] P. GUPTA, R. MCCLATCHEY, P. CALEB-SOLLY: *Tracking changes in user activity from unlabelled smart home sensor data using unsupervised learning methods* (Oct. 2020),
DOI: https://doi.org/10.1007/s00521-020-04737-6.

[3] M. KANEVSKI: *Advanced Mapping of Environmental Data: Introduction*, in: Feb. 2010, pp. 1–17, ISBN: 9781848210608,
DOI: https://doi.org/10.1002/9780470611463.ch1.

[4] T. MAJOROS, B. UJVÁRI, S. ONIGA: *EEG data processing with neural network*, Carpathian Journal of Electronic and Computer Engineering 12 (Dec. 2019), pp. 33–36,
DOI: https://doi.org/10.2478/cjece-2019-0014.

[5] S. RANASINGHE, F. AL MACHOT, H. MAYR: *A Review on Applications of Activity Recognition Systems with Regard to Performance and Evaluation*, International Journal of Distributed Sensor Networks 12 (July 2016),
DOI: https://doi.org/10.1177/1550147716665520.

[6] J. SÜTŐ, S. ONIGA, C. LUNG, I. ORHA: *Comparison of offline and real-time human activity recognition results using machine learning techniques*, Neural Computing and Applications 32 (Oct. 2020),
DOI: https://doi.org/10.1007/s00521-018-3437-x.

[7] T. WANG, D. COOK: *sMRT: Multi-Resident Tracking in Smart Homes with Sensor Vectorization*, IEEE Transactions on Pattern Analysis and Machine Intelligence PP (Feb. 2020), pp. 1–1,
DOI: https://doi.org/10.1109/TPAMI.2020.2973571.

Enhanced heuristic optimization of high order concentrated matrix-exponential distributions *

Salah Al-Deen Almousa[a], **Miklós Telek**[ab]

[a]Department of Networked Systems and Services, Technical University of Budapest, Budapest, Hungary

[b]MTA-BME Information Systems Research Group, Budapest, Hungary
almousa@hit.bme.hu, telek@hit.bme.hu

This paper presents a heuristic optimization method for finding high order concentrated matrix-exponential (ME) distributions.

Introduction

Highly concentrated matrix-exponential functions are useful in many research areas, for example, in numerical inverse Laplace transform (NILT) methods [3]. Recently, Akar *et al.* [1], proposed the ME-fication technique, in which a concentrated matrix exponentiation distribution replaces the Erlang distribution for approximating deterministic time horizons.

In a recent work [4], concentrated ME distributions of order N, abbreviated as CME(N), were successfully constructed in the range of $N = 369, \ldots, 2001$ based on a heuristic numerical optimization procedure optimizing 3 parameters independent of the order. In this work, we aim at improving that heuristic optimization procedure to further decrease squared coefficient of variation of the computed CME(N) distribution. The proposed enhanced optimization procedure optimizes 6 parameters (independent of the order) and we refer to it as *6-parameter optimization* method.

Matrix exponential distributions

Definition 0.1. Order N *ME functions* (referred to as ME(N)) are given by

$$f(t) = \underline{\alpha} e^{\mathbf{A}t}(-\mathbf{A})\mathbf{1}, \tag{0.1}$$

where $\underline{\alpha}$ is a real row vector of size N, $\mathbf{A}$ is a real matrix of size $N \times N$ matrix and $\mathbf{1}$ is the column vector of ones of size N.

Definition 0.2. If $f(t) \geq 0, \forall t \geq 0$, and $\underline{\alpha}$ is such that $\underline{\alpha}\mathbf{1} = 1$ then $f(t)$ is the probability density function of a *ME distribution* of order N.

According to (0.1), vector $\underline{\alpha}$ and matrix $\mathbf{A}$ define a matrix exponential function. We refer to the pair $(\underline{\alpha}, \mathbf{A})$ as *matrix representation* in the sequel.

*This work is partially supported by the OTKA K-123914 and the NKFIH BME NC TKP2020 projects.

An ME distribution is said to be concentrated when its squared coefficient of variation

$$SCV(f(t)) = \frac{\mu_0 \mu_2}{\mu_1^2} - 1, \tag{0.2}$$

is low. In (0.2), μ_i denotes the ith moment, defined by $\mu_i = \int_{t=0}^{\infty} t^i f(t) dt$. We note that the SCV according to (0.2) is insensitive to multiplication and scaling, i.e. $SCV(f(t)) = SCV(cf(\lambda t))$.

The solution of the optimization problem

$$\begin{gathered} \min_{\underline{\alpha}, \mathbf{A}} SCV(f(t)) \\ \text{subject to } f(t) \geq 0, \ \ \forall t > 0 \end{gathered}$$

is still open, and following [4], we look for concentrated ME distribution in the following subset of ME distributions which is non-negative by construction.

$$f(t) = cf^+(\lambda t), \tag{0.3}$$

where $f^+(t)$ is

$$f^+(t) = e^{-t} \prod_{j=1}^{n} \cos^2\left(\frac{\omega t - \phi_j}{2}\right), \tag{0.4}$$

where $\omega \geq 0$ and $0 \leq \phi_j < 2\pi$ for $j \in \{1, \ldots, n\}$ and the order of the associated ME distribution is $N = 2n + 1$.

Our proposed method aims at finding ME(N) with low SCV for such high orders where the optimization of all parameters of $f^+(t)$ is infeasible.

The SCV values resulted by our proposed 6-parameter optimization procedure is compared with the existing 3-parameter optimization procedure in Figure 1. The figure also plots the SCV values obtained from the optimization of all parameters of $f^+(t)$ by the CMA-ES evolution strategy based optimization method [2].

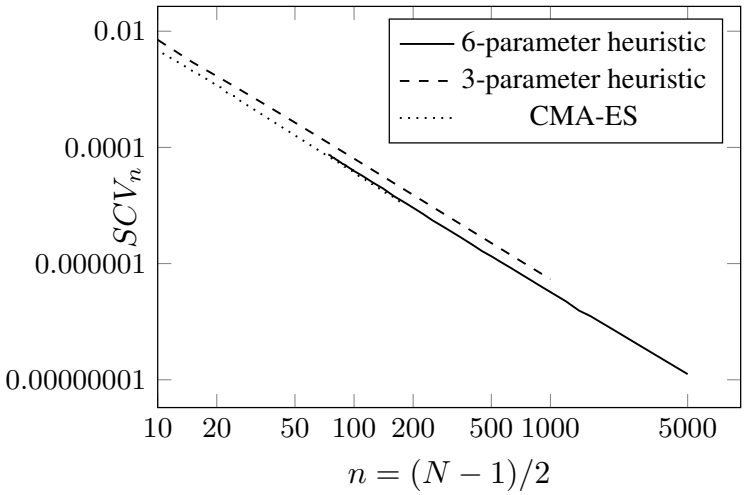


Figure 1: The minimal SCV values obtained by full optimization, 3-parameter optimization and the proposed 6-parameter optimization as a function of order n in log-log scale

Keywords: squared coefficient of variation, optimization, concentrated matrix exponential distributions.

References

[1] N. AKAR, O. GURSOY, G. HORVATH, M. TELEK: *Transient and First Passage Time Distributions of First-and Second-order Multi-regime Markov Fluid Queues via ME-fication*, Methodology and Computing in Applied Probability (2020), pp. 1–27,
DOI: https://doi.org/10.1007/s11009-020-09812-y.

[2] N. HANSEN: *The CMA evolution strategy: a comparing review*, in: Towards a New Evolutionary Computation, Springer, 2006, pp. 75–102,
DOI: https://doi.org/10.1007/3-540-32494-1_4.

[3] G. HORVÁTH, I. HORVÁTH, S. A. D. ALMOUSA, M. TELEK: *Numerical inverse Laplace transformation using concentrated matrix exponential distributions*, Performance Evaluation 137 (2020), p. 102067,
DOI: https://doi.org/10.1016/j.peva.2019.102067.

[4] G. HORVÁTH, I. HORVÁTH, M. TELEK: *High order concentrated matrix-exponential distributions*, Stochastic Models 36.2 (2020), pp. 176–192,
DOI: https://doi.org/10.1080/15326349.2019.1702058.

Preferential attachment random graphs with multiple type elements*

Ágnes Backhausz[a], Edit Bognár[a], Bence Rozner[b]

[a]ELTE Eötvös Loránd University, Budapest, Hungary
agnes.backhausz@ttk.elte.hu

[b]Alfréd Rényi Institute of Mathematics
bence.rozner@ttk.elte.hu

Introduction

One of the main motivations of studying random graphs is modelling large real-world networks. However, these large networks can be much more complex than a set of vertices and edges: both vertices and edges can have different characteristics which have an impact on the random growth of the graph. For example, in an online social network, we can separate the users in a few groups (e.g. according to age, place of living etc.) such that vertices in the same group have higher chance to be connected to each other and their membership also has an effect on their connections with other groups. Among other concepts (e.g. clustering, stochastic block models), this can be modeled by multitype versions of preferential attachment model. The graph is growing step by step, by adding always a new vertex, connecting it to some of the old vertices such that vertices with larger degree are chosen with a higher probability, and then, the type of the new vertex is chosen with probabilities proportional to the number of vertices of different types among its new neighbors. These kind of models have been studied recently in [1, 5].

It is also natural to distinguish different types of edges. For example, being friends or being colleagues can be represented by different types when we want to model an online social network. Furthermore, we can also assume certain preferential attachment type of dynamics: old vertices with larger number of edges from a given type have higher chance to get new edges from this particular type. This means that the types of edges are chosen in a way depending heavily on the random evolution of the graph, and we can see a nontrivial random structure as a result. In particular, we can be interested in the asymptotic proportion of vertices having, for example, two edges of type 1, five edges of type 2, etc. This can give us an understanding of the local behaviour of this multitype network.

Based on [2, 4], we present our results proving that this asymptotic proportion of vertices with a given edge configuration converges. This convergence is shown in a general setup, where the limits are random variables themselves, for which we can derive a recur-

*This research was supported by the project "Integrált kutatói utánpótlás-képzési program az informatika és számítástudomány diszciplináris területein (Integrated program for training new generation of researchers in the disciplinary fields of computer science) ", No. EFOP-3.6.3-VEKOP-16-2017-00002. The project has been supported by the European Union and co-funded by the European Social Fund.

rence equation. Going further, in a special case, we show that the limit becomes deterministic if we add a random perturbation to the probabilities of choosing different type of edges. The main tools for studying these questions are martingale methods and the theory of urn models, when the number of balls added to the urn is random and depends on the color of the ball chosen.

An important application of the theory of random graphs is about epidemic spread. Again, adding types as extra features to the vertices and edges of the graph can be motivated by real-world problems. For example, age has an essential role in infection and recovery from many diseases, hence it is worth introducing groups of the individuals, according to their age. Based on [3], we present the results of computer simulations, where we compare different vaccination strategies in case of epidemic spread modelled on random graphs (including preferential attachment random graphs) with multiple type vertices. We conclude that both the type and degree of the vertices are essential features for the optimal vaccination.

Keywords: random graphs, martingales, preferential attachment

References

[1] T. ANTUNOVIĆ, E. MOSSEL, M. Z. RÁCZ: *Coexistence in preferential attachment networks*, Combin. Probab. Comput. 25.6 (2016), pp. 797–822, ISSN: 0963-5483, DOI: https://doi.org/10.1017/S0963548315000383.

[2] Á. BACKHAUSZ, B. ROZNER: *Barabási-Albert random graph with multiple type edges and perturbation*, Acta Math. Hungar. 161.1 (2020), pp. 212–229, ISSN: 0236-5294, DOI: https://doi.org/10.1007/s10474-019-01005-5.

[3] Á. BACKHAUSZ, E. BOGNÁR: *Virus spread and voter model on random graphs with multiple type nodes* (2020), URL: https://arxiv.org/abs/2002.06926.

[4] Á. BACKHAUSZ, B. ROZNER: *Asymptotic degree distribution in preferential attachment graph models with multiple type edges*, Stoch. Models 35.4 (2019), pp. 496–522, ISSN: 1532-6349, DOI: https://doi.org/10.1080/15326349.2019.1624574.

[5] S. ROSENGREN: *A multi-type preferential attachment tree*, Internet Math. (2018), p. 16.

An encoding of the λ-calculus into the calculus of String Multiset Rewriting*

Attila Bagossy[a], Péter Battyányi[a]

[a]Department of Computer Science, Faculty of Informatics, University of Debrecen, Hungary
bagossyattila@mailbox.unideb.hu, battyanyi.peter@inf.unideb.hu

In the past few years many formalisms have been designed by computer scientists in order to model biological systems consisting of interacting components. Most of these systems are high level abstractions of biological phenomena with the aim of describing a complex system and the possible interactions of the constituents [4], [5], [2]. However, the implementation of efficient simulators for high level languages did not prove to be an easy task. The calculus of String Multiset Rewriting (SMSR) [1] seemed to offer a solution acceptable from both approaches: the maximal matching operator is able to represent higher level languages and the SMSR system is simple enough to enable the development of efficient simulators. SMSR is based on term rewriting. A term in SMSR consists of a multiset of strings. By the maximal matching operator we are able to manipulate tree-like structures: complete multisets can be replaced by another multiset at the same time. This is the very feature that we make extensive use of in present work.

In our presentation we define reduction rules so that we can embed the λ-calculus in the calculus of SMSR. We govern the evaluation process by introducing new constants in the calculus, which, by the matching process, restrict the number of applicable rules. We remark that SMSR is a commutative structure with respect to the order of strings forming the multisets. Hence, we have obtained a representation of the non-commutative λ-calculus in a commutative structure which is not very difficult to implement. Firstly, we prove the correctness of the translation, then propose some applications of this new approach.

The theory of the lambda calculus has some elementary and well-known results, the proofs of which might lean on an intuitive understanding of the terms little more than necessary. We examine two well-known theorems: the standardization and the finiteness of developments theorems (cf. [3]). The standardization theorem asserts that, if we have a reduction sequence from M to N, then there is a reduction sequence with the property that no redex can be used "to the left" of an already used redex. The finiteness of developments theorem roughly says that, if we start reducing the redexes of a term, the reduction sequence always terminates provided we never reduce the created redexes but only the ones obtained from the already existing redexes. Our translation allows us to give a proper representation of the lambda calculus subterms, hence a correct description of

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was co-financed by the Hungarian Government and the European Social Fund.

the β-reduction. This time, the strings in the translation act as addresses of subterms, the reduction step can be depicted as an operation on paths leading to subterms. This strict accordance is established in order to obtain a proof of the standardization theorem. The finiteness of developments theorem is proved by a reformulation of Xi's development separation method [6]. The machinery at hand provided by the translation seems to allow us a much clearer setting even for the demonstration of the development separation theorem.

Keywords: String Multiset Rewriting, lambda calculus, finiteness of developments

References

[1] R. BARBUTI, G. CARAVAGNA, A. MAGGIOLO-SCHETTINI, P. MILAZZO: *An Intermediate Language for the Simulation of Biological Systems*, Electronic Notes in Theoretical Computer Science 194 (2008), pp. 19–34,
DOI: https://doi.org/10.1016/j.entcs.2007.12.004.

[2] R. BARBUTI, G. CARAVAGNA, A. MAGGIOLO-SCHETTINI, A. TROINA: *A Calculus of Looping Sequences for Modelling Microbiological Systems*, Fundamenta Informaticae 72 (2006), pp. 21–35.

[3] H. P. BARENDREGT: *The Lambda Calculus: Its Syntax and Semantics*, North Holland, 1985.

[4] L. CARDELLI: *Brane Calculi. Interactions of Biological Membranes*, in: CMSB'04: Proceedings of the 20 International Conference on Computational Methods in Systems Biology, Berlin, Heidelberg: Springer, 2005, pp. 257–280,
DOI: https://doi.org/10.1007/b107287.

[5] V. DANOS, C. LANEVE: *Formal Molecular Biology*, Theoretical Computer Science 325 (2004), pp. 69–110,
DOI: https://doi.org/10.1016/j.tcs.2004.03.065.

[6] H. XI: *Development Separation in Lambda-Calculus*, Electronic Notes in Theoretical Computer Science 143.6 (2006), pp. 207–221,
DOI: https://doi.org/10.1016/j.entcs.2005.07.014.

Comparison of multivariate ensemble post-processing methods

Sándor Baran[a], **Mária Lakatos**[a]

[a]Faculty of Informatics, University of Debrecen, Debrecen, Hungary
baran.sandor@inf.unideb.hu
marcsilakatos1@gmail.com

Extended abstract

Compared to deterministic weather forecasting, the implementation of ensemble prediction systems (EPS) in the early 90's was a significant improvement. However, in real-life scenarios ensemble predictions tend to be underdispersed and/or biased, hence uncalibrated. Scientific literature offers multiple ways to calibrate ensemble forecasts, introducing both univariate and multivariate post-processing methods.

Although univariate approaches generally improve the forecast skill of ensemble forecasts, certain spatial and temporal dependencies, that are present in the raw ensembles, may be lost during post-processing. One of the main aspects of applying multivariate post-processing is restoring the lost spatial and temporal dependencies. Lerch et al. [6] provided a comprehensive comparison of different multivariate post-processing procedures, whose forecast skill was assessed using simulation-based data. Multivariate methods can be broadly divided into two separate groups. The first one aims to fit a multivariate distribution function, which can lead to numerical problems, due to the large number of parameters to be estimated [1]. During the second strategy, a univariate post-processing method is applied to the raw ensemble, then samples are generated from the resulted predictive distributions. Finally, these samples are reordered according to information based on the rank structure of raw forecasts, forecast errors or past observations.

We are focusing on the latter approach and our aim is to extend the study of Lerch et al. [6] by investigating the forecast skill of the different methods using real ensemble forecasts and corresponding observations. We consider temperature and wind speed forecasts for 7 major cities of Hungary produced by two different ensemble prediction systems, namely, the operational EPS of the European Centre for Medium-Range Weather Forecasts (ECMWF) and the ALADIN-HUNEPS system of the Hungarian Meteorological Service. In both case studies calibrated univariate temperature and wind speed forecasts are obtained using normal [4] and truncated normal [9] EMOS models, respectively. In the second step, various forms of the ensemble copula coupling (ECC) [7], the dual ensemble copula coupling (d-ECC) [2] and the Schaake shuffle [3] are applied. To quantify the forecast skill of the different multivariate post-processing methods we consider the energy score [5] and the variogram score [8].

According to our case studies, multivariate approaches generally improve the predictive performance of the raw ensemble forecasts, especially in the case of wind speed.

However, the selection of the best performing method is not trivial, since it strongly depends on the prediction horizon and the weather variable at hand.

Keywords: ensemble model output statistics, ensemble post-processing, multivariate calibration, probabilistic weather forecasting

References

[1] S. BARAN, A. MÖLLER: *Bivariate ensemble model output statistics approach for joint forecasting of wind speed and temperature*, Meteorology and Atmospheric Physics 129.1 (2017), pp. 99–112.

[2] Z. BEN BOUALLÈGUE, T. HEPPELMANN, S. E. THEIS, P. PINSON: *Generation of scenarios from calibrated ensemble forecasts with a dual-ensemble copula-coupling approach*, Monthly Weather Review 144.12 (2016), pp. 4737–4750.

[3] M. CLARK, S. GANGOPADHYAY, L. HAY, B. RAJAGOPALAN, R. WILBY: *The Schaake shuffle: A method for reconstructing space–time variability in forecasted precipitation and temperature fields*, Journal of Hydrometeorology 5.1 (2004), pp. 243–262.

[4] T. GNEITING, A. E. RAFTERY, A. H. WESTVELD, T. GOLDMAN: *Calibrated Probabilistic Forecasting Using Ensemble Model Output Statistics and Minimum CRPS Estimation*, Monthly Weather Review 133.5 (May 2005), pp. 1098–1118, ISSN: 0027-0644,
DOI: https://doi.org/10.1175/MWR2904.1.

[5] T. GNEITING, L. I. STANBERRY, E. P. GRIMIT, L. HELD, N. A. JOHNSON: *Assessing probabilistic forecasts of multivariate quantities, with an application to ensemble predictions of surface winds*, Test 17.2 (2008), p. 211.

[6] S. LERCH, S. BARAN, A. MÖLLER, J. GROSS, R. SCHEFZIK, S. HEMRI, M. GRAETER: *Simulation-based comparison of multivariate ensemble post-processing methods*, Nonlinear Processes in Geophysics 27.2 (2020), pp. 349–371,
DOI: https://doi.org/10.5194/npg-27-349-2020.

[7] R. SCHEFZIK, T. L. THORARINSDOTTIR, T. GNEITING, ET AL.: *Uncertainty quantification in complex simulation models using ensemble copula coupling*, Statistical Science 28.4 (2013), pp. 616–640.

[8] M. SCHEUERER, T. M. HAMILL: *Variogram-based proper scoring rules for probabilistic forecasts of multivariate quantities*, Monthly Weather Review 143.4 (2015), pp. 1321–1334.

[9] T. L. THORARINSDOTTIR, T. GNEITING: *Probabilistic forecasts of wind speed: Ensemble model output statistics by using heteroscedastic censored regression*, Journal of the Royal Statistical Society: Series A (Statistics in Society) 173.2 (2010), pp. 371–388.

Truncated generalized extreme value distribution based ensemble model output statistics model for probabilistic wind speed forecasting

Sándor Baran[a], Patrícia Szokol[a], Marianna Szabó[ab]

[a]Faculty of Informatics, University of Debrecen

[b]Doctoral School of Informatics, University of Debrecen

In recent years, ensemble weather forecasts have been provided by all major weather prediction centres, which obtain their forecasts from multiple runs of numerical weather prediction models with perturbed initial conditions or parametrizations. However, ensemble forecasts can often be underdispersive and also biased, so post-processing is needed to account for these deficiencies. One of the most popular modern post-processing techniques is the ensemble model output statistics (EMOS), which provides a full predictive distribution of the studied weather quantity. We propose a novel EMOS model for calibrating wind speed ensemble forecasts, where the predictive distribution is a generalized extreme value (GEV) distribution left truncated at zero (TGEV). The truncation corrects the disadvantage of the GEV distribution based EMOS model [2] of occasionally predicting negative wind speed values without affecting its favorable properties. The new model is tested on wind-speed forecasts of the 50-member European Centre for Medium-Range Weather Forecasts ensemble and the 11-member Aire Limitée Adaptation dynamique Développement International-Hungary Ensemble Prediction System (ALADIN-HUNEPS) ensemble of the Hungarian Meteorological Service. The forecast skill of the TGEV EMOS model is compared with the predictive performance of the truncated normal [3], log-normal [1] and GEV EMOS methods and the raw ensemble forecasts. The results verify the advantageous properties of the TGEV EMOS approach.

Keywords: Continuous ranked probability score, ensemble calibration, ensemble model output statistics, truncated generalized extreme value distribution

References

[1] S. Baran, S. Lerch: *Log-normal distribution based EMOS models for probabilistic wind speed forecasting*, Quarterly Journal of the Royal Meteorological Society 141 (2015), pp. 2289–2299, DOI: https://doi.org/10.1002/qj.2521.

[2] S. Lerch, T. L. Thorarinsdottir: *Comparison of non-homogeneous regression models for probabilistic wind speed forecasting*, Tellus A.65 (2013), p. 21206, DOI: https://doi.org/10.3402/tellusa.v65i0.21206.

[3] T. L. THORARINSDOTTIR, T. GNEITING: *Probabilistic forecasts of wind speed: ensemble model output statistics by using heteroscedastic censored regression*, Journal of the Royal Statistical Society Series A (Statistics in Society) 173 (2010), pp. 371–388,
DOI: https://doi.org/10.1111/j.1467-985X.2009.00616.x.

Radical digitization through 3D environments - Experiences in the MaxWhere 3D VR platform

Péter Baranyi[a]

[a]Széchenyi István University, Győr, Hungary
baranyi.peter@sze.hu

The goal of this paper is to draw attention to the MaxWhere 3D VR platform. MaxWhere 3D platform (www.maxwhere.com) is a desktop VR solution that can considerably decrease working and educational costs, while at the same time improves the effectiveness of students and active employees. Virtual and Augmented Reality Technology is one of the key technologies of digital transformation in industrial and non-industrial areas. MaxWhere has various features to integrate Industry 4.0 tools, e-learing tools, content, online meeting and working tools or video/audio based content. It possesses powerful features for sharing (publicly or in private groups) 3D collaboration rooms, classrooms, study rooms, mentor rooms, as well as highly interactive showrooms and laboratories.

Beyond MaxWhere, the paper discusses the possible consequences of a radical digitization using 3D spaces in general, which brings with itself a change in everyday workflow and learning processes and knowledge management in modern industrial, management and educational environments.

Our research focuses on the capabilities of MaxWhere-based on considerations behind the field of Cognitive Infocommunications (CogInfoCom) [1, 2, 9]. Cognitive infocommunications (CogInfoCom) is an interdisciplinary research field that has emerged as a synergy between info-communications and the cognitive sciences. One of the key observations behind CogInfoCom is that through a convergence process between these fields, humans and ICT are becoming entangled at various levels, as a result of which new forms of cognitive capability are appearing.

The objective is to shift the currently used VR frameworks towards the cybereducational space and workspace and to justify the viability of MaxWhere VR in achieving this.

The key observation to make with respect to these different channels of communication is that they can all be used – and moreover simultaneously – in VR environments [7]. In contrast, when using the 2D solutions that are widespread today, it is not possible to make full use of the auditory and spatial metaphors that arise naturally through relationships in 3D space. In 2D, not as many objects can be 'close' to each other, as 2D allows for less complex topologies than 3D. The distance between and size of objects in 3D acquire new connotations by virtue of their identity: a table in 3D is naturally designed for laying out and comparing documents, whereas a display on a wall is naturally designed for presentations or content laid out for all to see. The absolute size (and relevance) of different content are easier to understand in 3D because the spatial surroundings offer a natural scale by which to interpret the normative size of various displays and objects. Whereas 2D offers some kind of understanding of relative sizes, normative scale is most often ei-

ther disregarded or lost. These are just a few reasons why VR is extremely powerful in communicating a wide range of concepts [6].

The 3D visualization must be linked to the user and follow its motion, so that the 3D virtual object can be rendered in the real time according to the relative position of user to the real object [3].

In a more quantifiable sense, several recent investigations have focused on how many and what types of interactions are necessary to achieve similar results in different – 2D and 3D scenarios. Of key interest is how workflows can be communicated and shared through linguistic descriptions, digital content and technological tools.

Our tests show that users are able to complete a set of digital workflows given to them at least 50 faster in 3D, using the MaxWhere 3D environment [8, 10], than in traditional educational platforms. Further, 3D environments are capable of providing users with a much higher level of comprehension when it comes to sharing and interpreting digital workflows [4, 5].

Keywords: Cognitive Infocommunications, 3D virtual learning, digital mindset, digital twins

References

[1] P. BARANYI, Á. CSAPÓ: *Definition and synergies of cognitive infocommunications*, Acta Polytechnica Hungarica 9.1 (2012), pp. 67–83.

[2] P. BARANYI, Á. CSAPÓ, G. SALLAI: *Cognitive Infocommunications (CogInfoCom)*, Springer, 2015.

[3] F. BELLALOUNA: *Industrial Use Cases for Augmented Reality Application*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 11–18.

[4] B. BERKI: *2d advertising in 3d virtual spaces*, Acta Polytechnica Hungarica 15.3 (2018), pp. 175–190.

[5] B. BERKI: *Desktop VR as a virtual workspace: a cognitive aspect*, Acta Polytechnica Hungarica 16.2 (2019), pp. 219–231.

[6] M. BORDEGONI, F. FERRISE: *Designing interaction with consumer products in a multisensory virtual reality environment: this paper shows how virtual reality technology can be used instead of physical artifacts or mock-ups for the new product and evaluation of its usage*, Virtual and Physical Prototyping 8.1 (2013), pp. 51–64.

[7] Á. B. CSAPÓ, I. HORVÁTH, P. GALAMBOS, P. BARANYI: *VR as a medium of communication: from memory palaces to comprehensive memory management*, in: 2018 9th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2018, pp. 000389–000394.

[8] I. HORVÁTH, A. SUDÁR: *Factors Contributing to the Enhanced Performance of the MaxWhere 3D VR Platform in the Distribution of Digital Information*, Acta Polytechnica Hungarica 15.3 (Mar. 2018), pp. 149–173,
DOI: https://doi.org/10.12700/APH.15.3.2018.3.9.

[9] R. KLEMPOUS, J. NIKODEM, P. Z. BARANYI: *Cognitive Infocommunications, Theory and Applications*, Springer, 2019.

[10] B. LAMPERT, A. PONGRÁCZ, J. SIPOS, A. VEHRER, I. HORVÁTH: *MaxWhere VR-learning improves effectiveness over clasiccal tools of e-learning*, Acta Polytechnica Hungarica 15.3 (2018), pp. 125–147.

Possible neural models to support the design of Prime Convo Assistant*

Norbert Bátfai[a], Máté Szabó[a]

[a]University of Debrecen
batfai.norbert@inf.unideb.hu
szabo.mate@inf.unideb.hu

The Prime Convo Assistant initiative is a software development idea intended to examine how we could use automatic and interactive theorem provers and machine learning methods to automatically generate new sentences in an artificial visual language. The name Prime Convo Assistant comes from the name of the device of Isaac Asimov's psychohistorians called Prime Radiant on the one hand, and from, according to Julian Jaynes' theory of the bicameral mind, the internal conversation with ourselves on the other. Our idea is that the sentences of the visual language in question are initially given in the form of first-order logic formulas, as in the case of Pasigraphy Rhapsody. In the framework of the present work, we primarily conduct literature research and test existing models. On the one hand, in the field of what neural models exist whose input is a first-order logic corpus, and on the other hand, in the field of what deep learning-based solutions help the operation of automatic theorem provers. In addition, in a broader context, we examine the possible relationship between Society 5.0 and esport culture from a kind of robopsychological and robophilosophical point of view.

Introduction

The initiative called Pasigraphy Rhapsody[1] (PaRa) aims to create a first-order logic-based artificial graphical language. In our preliminary experiments, the logic formulas are represented by n-dimensional dotted hypercubes, the dotting of the hypercubes has been inspired by our previous work [3] as it can be seen in Fig 1[2]. Our motivation was to invent a Minecraft-like builder game based on such hypercubes.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

[1]Pasigraphy Rhapsody, https://gitlab.com/nbatfai/pasigraphy-rhapsody.

[2]The idea of using yslant and xslant to achieve a 3D effect like appearance is based on Stefan Kottwitz's example http://www.texample.net/tikz/examples/sudoku-3d-cube/, see https://gitlab.com/nbatfai/pasigraphy-rhapsody/-/blob/master/para/docs/prelpara.lua.

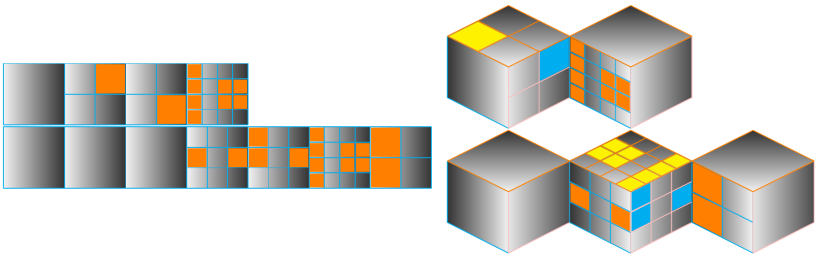


Figure 1: A detail of the PaRa formalization of Lord's Prayer in 2 and 3 dimensional LuaLaTeX visualization.
Source: https://gitlab.com/nbatfai/pasigraphy-rhapsody

Prime Convo Assistant

To develop Pasigraphy Rhapsody, in our previous work [2] we proposed to formalize standard artificial intelligence tasks (like monkey and banana) or to create a game where players formalize their everyday activities. But these are very slow processes if the latter is possible at all. Therefore, in this work, we raise the issue of examining the possibility of automatic conversion of large corpora to Pasigraphy Rhapsody such as converting the Lean Mathlib library[3]. The goal of using a game to formalize sentences is to reach the widest possible user community. That is important from two main aspects. On the one hand an esport game can shape the thinking of players widely[4], namely to teach modern mathematical logic to them. And on the other hand we could build large corpus in this way. In this work we move away from looking for possible games but we try to fulfill the latter sub-goal with a different method. Since in an axiomatic system in principle we can automatically generate new sentences easily. The Lean Matlib library a such axiomatic system. So it is worth to try to formalize it in PaRa. The first step in the PaRa formalization is to create the first-order logic form of the investigated sentences. But the following steps has already been fully automated. Therefore, in principle, such a conversion may be possible. With PaRa conversion, our goal is to study the possible neural models that receive the same input in parallel, but one model gets its input in visual (as PaRa images) form and the other in textual (as first-order logic formulas) form. In this sense the conception of Prime Convo Assistant, introduced in [2], would be transformed to a such system that has the following use cases.

1. Translating the Lean corpus to PaRa
2. Creating new sentences from the Lean logical corpus on the one hand and from the converted visual (PaRa) images on the other hand.

[3]The Lean mathematical library, https://arxiv.org/abs/1910.09336, https://github.com/leanprover-community/mathlib.

[4]But it can also be interesting to compare Society 5.0 [5] and esport culture.

Possible Neural Models

First-order Logic Input Our first question that what neural models exist whose input is a first-order logic corpus. Are there such BERT-based systems [6]? An another question is whether a soft theorem prover, such as [4] could be applied to first-order logic input?

Symbiosis of Theorem Provers and Machine Learning The DeepMind work [1] provides some answers to our questions, as it uses formulas formally derived from axioms as a training set. Therefore, a natural question is whether can we repeat their results using Lean? Can machine learning provide a Jaynesian inner voice that, for example, can say hints to the interactive theorem prover?

Keywords: robopsychology, robophilosophy, machine learning, automated theorem proving, Society 5.0, esport

References

[1] E. AYGÜN, Z. AHMED, A. ANAND, V. FIROIU, X. GLOROT, L. ORSEAU, D. PRECUP, S. MOURAD: *Learning to Prove from Synthetic Theorems*, 2020, arXiv: 2006.11259 [cs.LO], URL: https://arxiv.org/abs/2006.11259.

[2] N. BÁTFAI: *Hacking with God: a Common Programming Language of Robopsychology and Robophilosophy*, 2020, arXiv: 2009.09068 [cs.CY], URL: https://arxiv.org/abs/2009.09068.

[3] N. BÁTFAI, D. PAPP, G. BOGACSOVICS, M. SZABÓ, V. S. SIMKÓ, M. BERSENSZKI, G. SZABÓ, L. KOVÁCS, F. KOVÁCS, E. S. VARGA: *Object file system software experiments about the notion of number in humans and machines*, Cognition, Brain, Behavior. An Interdisciplinary Journal 23.4 (2019), pp. 257–280, DOI: https://doi.org/10.24193/cbb.2019.23.15.

[4] P. CLARK, O. TAFJORD, K. RICHARDSON: *Transformers as Soft Reasoners over Language*, 2020, arXiv: 2002.05867 [cs.CL], URL: https://arxiv.org/abs/2002.05867.

[5] Y. HARAYAMA: *Society 5.0: Aiming for a New Human-centered Society*, Hitachi Review 66.6 (2017), pp. 8–13, URL: https://www.hitachi.com/rev/archive/2017/r2017_06/pdf/p08-13_TRENDS.pdf.

[6] D. JACOB, C. MING-WEI, L. KENTON, T. KRISTINA: *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, CoRR abs/1810.04805 (2018), arXiv: 1810.04805 [cs.CL], URL: http://arxiv.org/abs/1810.04805.

Red Flower Hell: a Minecraft MALMÖ Challenge to Support Introductory Programming Courses[¶]

Norbert Bátfai[a], Tünde Tutor[a], Zoltán Bartha[a], András Czanik[a]

[a]University of Debrecen
batfai.norbert@inf.unideb.hu, tunde.tutor@gmail.com
barthazoli00@gmail.com, czandris98@gmail.com

The Red Flower Hell challenge is designed for undergraduate courses, such as introductory programming or artificial intelligence, in which students can learn in a competitive way. The name Red Flower Hell comes from the objective of the challenge because the agent programs to be developed must collect as many red flowers as possible in a battle royale-like gorge in Minecraft created directly for this challenge. The battle royale feature is given by that lava flows down the hillsides in the gorge. In the first round of the challenge, agents only have to deal with lava. In the second round, agents also have to fight various Minecraft monsters, such as zombies or spiders. The agent versus agent fight has not yet been implemented. We have used Project MALMÖ for implementing Red Flower Hell. It is a Minecraft mod created by Microsoft for researching artificial general intelligence. The Red Flower Hell challenge was tested at a High-level programming language course at the University of Debrecen in the spring semester of the 2019/2020 academic year. We present these experiences in this work.

Introduction

Today, it is typical that leading tech companies have their own artificial general intelligence (AGI) research platform, which is organized around a given particular well-known game. Such a platform of Microsoft is based on the Minecraft game, this is the Minecraft MALMÖ project [5].

Minecraft and AGI Research

The MALMÖ AGI research platform is also evolving through competitions with renowned universities and companies [4], [3], [2]. But our esports department called DEAC-Hackers also has a Minecraft-MALMÖ division [1].

[¶]This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

Red Flower Hell

The Red Flower Hell (RFH) is a MALMÖ project-based, battle royale-like gorge in Minecraft, shown in Figure 1, designed for undergraduate courses, such as introductory programming or artificial intelligence in order to students can learn in a competitive way. The XML file defining our gorge-like game world can be found on the project repository at `https://github.com/nbatfai/RedFlowerHell`.

Figure 1: The base task is to collect as many red flowers as possible before the lava flowing down the hillside has reached the agent. Source: https://github.com/nbatfai/RedFlowerHell

Human Intelligence agents

Before we start programming AI or simple heuristic agents, it is interesting to know how many flowers a human player can collect. This question is answered by Human Intelligence (HI) agents.

Software Agents for Introductory Programming Courses

These agents are based only on simple heuristic algorithms and do not contain standard MI solutions such as graph searching or Q-learning.

Some sample agents

The following simple heuristic example agents have been created for RFH. The GreenPill, Test Subject #40 and MrPoppy.

RFH for AI Courses

These agents must already use standard MI techniques such as Q-learning.

Keywords: Minecraft MALMÖ, programming challenge, education of programming, agent programming, artificial intelligence

References

[1] N. BÁTFAI, C. CSUKONYI, D. PAPP, C. HERMANN, E. DEÁKNÉ OSVALD, K. GYŐRI: *A DEAC-Hackers esport szakosztály mesterséges intelligencia oktatási és kutatási elképzelése a Minecraftban*, Mesterséges intelligencia – interdiszciplináris folyóirat II.1 (2020), pp. 95–109,
DOI: https://doi.org/10.35406/MI.2020.1.95.

[2] P. L. DIEGO, H. KATJA, P. M. SHARADA, K. NOBURU, K. ANDRÉ, D. SAM, D. G. RALUCA, I. DANIEL: *The Multi-Agent Reinforcement Learning in MalmÖ (MARLÖ) Competition*, CoRR abs/1901.08129 (2019), arXiv: 1901.08129,
URL: http://arxiv.org/abs/1901.08129.

[3] W. H. GUSS, C. CODEL, K. HOFMANN, B. HOUGHTON, N. KUNO, S. MILANI, S. MOHANTY, D. P. LIEBANA, R. SALAKHUTDINOV, N. TOPIN, M. VELOSO, P. WANG: *The MineRL Competition on Sample Efficient Reinforcement Learning using Human Priors*, 2019, arXiv: 1904.10079 [cs.LG],
URL: https://arxiv.org/abs/1904.10079.

[4] J. HSU: *AI takes on popular Minecraft game in machine-learning contest*, Nature 575 (Nov. 2019), pp. 583–584,
DOI: https://doi.org/10.1038/d41586-019-03630-0.

[5] M. JOHNSON, K. HOFMANN, T. HUTTON, D. BIGNELL: *The Malmo Platform for Artificial Intelligence Experimentation*, in: 25th International Joint Conference on Artificial Intelligence (IJCAI-16), AAAI - Association for the Advancement of Artificial Intelligence, 2016,
URL: https://www.microsoft.com/en-us/research/publication/malmo-platform-artificial-intelligence-experimentation/.

Measuring spatial orientation skills in MaxWhere*

Borbála Berki[a], Anna Sudár[a]

[a]Széchenyi István University, Győr, Hungary
{berki.borbala,sudar.anna}@sze.hu

A new virtual reality-based test battery is now under development as part of an aptitude test and skill development project to support human resource assessment. This test space focuses on the subjects' spatial orientation skills. Spatial orientation is defined by two parameters—directional heading and location—that are usually described relative to fixed reference points in the environment referred to as landmarks [5]. Virtual reality-based spatial orientation tests have a wide literature, as this technology enables the information incorporated into the virtual environment to be manipulated empirically.

The present research uses MaxWhere desktop virtual reality platform that capable of displaying both 2D and 3D content and becoming in the focus of several studies in the past years [1–4, 6]. The proposed study takes place in a virtual city, where the center of a small town is displayed with a suburb and a business district. In this spatial orientation task, the participants have to go to a given location space with the help of a map as fast as possible. The map is a plan view, schematic document. When the user reaches the goal, a new task is presented regardless of the correctness of the previous item. Each task takes place in the same virtual environment, but the starting and goal points are changing from item to item. After finishing the tasks the participants have to solve a spatial memory test. In this recognition, test pictures are presented about locations from the virtual space and distractor images. The task is to indicate which presented images were seen during the spatial orientation task.

The main dependent variable is the elapsed time between the start and endpoint of each item and the number of map viewing is recorded. The basic task can be extended with an aggravating condition by modifying the visibility (mist, lowlight) and as a facilitating condition, the participants can see their position on the given map.

Keywords: virtual reality, spatial orientation, spatial memory

References

[1] B. BERKI: *Experiencing the Sense of Presence within an Educational Desktop Virtual Reality*, Acta Polytechnica Hungarica 17.2 (2020), pp. 255–265,
DOI: https://doi.org/10.12700/aph.17.2.2020.2.14.

*This research was supported by the 2019-1.1.1-PIACI-KFI-2019-00149 - Supporting Market-driven Research Development and Innovation Projects of the National Research, Development and Innovation Office.

[2] I. K. BODA, E. TÓTH: *English language learning in virtual 3D space by visualizing the library content of ancient texts*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 305–311.

[3] G. BUJDOSÓ, K. BOROS, C. M. NOVAC, O. C. NOVAC: *Developing cognitive processes as a major goal in designing e-health information provider VR environment in information science education*, in: Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications: CogInfoCom 2019, ed. by P. BARANYI, IEEE, 2019, pp. 187–192,
DOI: https://doi.org/10.1109/CogInfoCom47531.2019.9089958.

[4] I. HORVÁTH, A. SUDÁR: *Factors Contributing to the Enhanced Performance of the MaxWhere 3D VR Platform in the Distribution of Digital Information*, Acta Polytechnica Hungarica 15.3 (Mar. 2018), pp. 149–173,
DOI: https://doi.org/10.12700/APH.15.3.2018.3.9.

[5] M. L. MEHLMAN, J. S. TAUBE: *In Vivo Electrophysiological Approaches for Studying Head Direction Cells*, in: Handbook of Behavioral Neuroscience, vol. 28, Elsevier, 2018, pp. 169–187,
DOI: https://doi.org/10.1016/B978-0-12-812028-6.00009-4.

[6] A. RÁCZ, A. GILÁNYI, A. M. BÓLYA, J. DÉCSEI, K. CHMIELEWSKA: *On a Model of the First National Theater of Hungary in MaxWhere*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 575–576.

English language learning by visualizing the literary content of a knowledge base in the three-dimensional space*

István Károly Boda[a], Erzsébet Tóth[b†]

[a]Debrecen Reformed Theological University, Department of Mathematics and Informatics
boda.istvan@drhe.hu

[b]University of Debrecen, Faculty of Informatics
toth.erzsebet@inf.unideb.hu

In our paper we would like to present our three-dimensional virtual library model (3DVLM) and its current implementation in the three-dimensional virtual space of the MaxWhere Seminar System. The aim of the 3DVLM is to present for the library users selected verbal and multimedia content in the 3D space (and in parallel in the hypertextual 2D space) in order to achieve two basic aims:

- first, giving an overview of the *classical heritage* which the European culture is based on. In this respect, the users can have access to texts about Callimachus who was one of the most respected Hellenistic scholar-poets of his age, as well as selected literary texts by Callimachus and other prominent authors (e.g. epigrams, lyric poems, anecdotes etc.). In addition, the library provides the readers with supporting materials (e.g. vocabulary items, concordances and quotes, selected parts of relevant Wikipedia entries etc.) which help them to understand the preprocessed primary texts. Note that the co-reference and/or intertextual relationships are represented, in the first place, by hypertext links between the primary texts (or selected parts of texts) and the supporting materials;

- second, the virtual library is intended to support *language learning* by carefully preparing and commenting the provided texts in order that the users, and especially the young members of the generation CE with supposed intermediate or advanced English language competence can acquire the accumulated knowledge and preserved values that the ancient authors created centuries ago.

The learning philosophy of the model is to help the readers understand and interpret the *primary texts* of the virtual library 'at once', supplying them with the necessary knowledge (represented by *secondary materials* covering the relevant linguistic or dictionary, generic, encyclopedic and background knowledge). Because the smooth (i.e. easy, simple, self-evident, user-friendly etc.) access to the primary texts and the associated secondary

*This research was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was co-financed by the Hungarian Government and the European Social Fund.

†The second author thanks for the opportunity to have a presentation in the CITDS conference.

materials is essential in the learning process, we tried to arrange and visualize the compiled material by using different and varied colors and typography (e.g. font and paragraph styles, images, graphics, icons, lists, tables, graphs, spatial maps, etc.). Note that exploiting the excellent and spectacular features of the 3D environment might possibly motivate the members of the generation CE, and therefore encouraging and persuading them to enhance their knowledge (being linguistic on the one hand, and general on the other hand). We firmly hope that our users will gradually improve their English language competence in the course of reading, understanding and memorizing the preprocessed material provided by our virtual library.

In our paper we would like to focus on the data structure and organization of the virtual library model selecting, introducing and illustrating typical structure patterns by visualizing them. Some of these patterns are as follows:

- the **primary texts** contain embedded hypertext links to other texts (representing encyclopedic knowledge) and vocabulary items (representing dictionary knowledge); in addition, there are links to the **thesaurus pages** organized around relevant micro-contexts, i.e. thesaurus items (semantically related words, expressions and phrases upon a specific subject or meaning) and concordances (or quotations) which belong to the corresponding thesaurus pages;

- the **category page** about ancient Greek literature including categories from the hierarchical classification scheme of the ancient Library of Alexandria invented by Callimachus (referred to as "Pinakes") in the 3rd century BC. It has hypertext links to the relevant primary texts representing a classification scheme of the 3DVLM;

- the **navigation page** which represents a kind of "navigation map" for the selected content of the virtual library. The map shows relevant connections between selected content units of the virtual library established by relevant keywords and/or "key sentences". The map has hypertext links to the exact location where each referred item can be found;

- the **reference page** which consists of the bibliographic description of all sources having been referred to from anywhere in the full content of the virtual library. It currently contains more than 350 entries.

In order that the selected texts could be easily understood and memorized we provided additional items which are necessary for language learners (e.g. vocabulary and thesaurus of rare or special words, expressions and idioms, images and illustrations, selected concordances and quotations, encyclopedia entries, referred texts etc.).

Although the current implementation of the model in the MaxWhere Seminar System uses the 3D Castle space, it is, because of the flexible organization of the 3DVLM, fully compatible with other MaxWhere 3D spaces. In our presentation we would like to show a brief overview of how the model works in the 3D environment emphasizing those features which we think can be especially useful and efficient for the possible users of the virtual library [1–5].

Keywords: three-dimensional virtual library model (3DVLM), MaxWhere Seminar System, Callimachus, text-based language learning

References

[1] I. BODA, M. BÉNYEI, E. TÓTH: *New dimensions of an ancient Library: the Library of Alexandria*, in: CogInfoCom2013. Proceedings of the 4th IEEE International Conference on Cognitive Infocommunications, New York, NY, USA: IEEE, 2013, pp. 537–542,
DOI: https://doi.org/10.1109/CogInfoCom.2013.6719306.

[2] I. BODA, E. TÓTH: *Classical Heritage and Text-Based Second Language Learning in Three-Dimensional Virtual Library Environment*, in: ICAI 2020. Proceedings of the 11th International Conference on Applied Informatics, Achen, Germany: CEUR-WS, Vol. 2650., 2020, pp. 46–56.

[3] I. BODA, E. TÓTH: *From Callimachus to the Wikipedia: an ancient method for the representation of knowledge in the WWW era*, in: CogInfoCom2018. Proceedings of the 9th IEEE International Conference on Cognitive Infocommunications, Piscataway, NJ, USA: IEEE, 2018, pp. 205–210,
DOI: https://doi.org/10.1109/CogInfoCom.2018.8639895.

[4] I. BODA, E. TÓTH, I. CSONT, L. T. NAGY: *Toward a knowledge base of literary content focusing on the ancient Library of Alexandria in the three dimensional space*, in: CogInfoCom2015. Proceedings of the 6th IEEE International Conference on Cognitive Infocommunications, New York, NY, USA: IEEE, 2015, pp. 251–258,
DOI: https://doi.org/10.1109/CogInfoCom.2015.7390600.

[5] I. BODA, E. TÓTH, F. Z. ISZÁLY: *Text-based approach to second language learning in the virtual space focusing on Callimachus' life and works*, in: CogInfoCom 2019. Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications, Piscataway, NJ, USA: IEEE, 2019, pp. 439–444,
DOI: https://doi.org/10.1109/CogInfoCom47531.2019.9089933.

Implementing a Barycentric Coordinates-based Visualization Framework for Movement of Microscopic Organisms*

Andrea Bodonyi[ab], **Győző Kuruczc**, **Gábor Holló**[c],

Roland Kunkli[b]

[a]University of Debrecen, Doctoral School of Informatics

[b]University of Debrecen, Faculty of Informatics
{bodonyi.andrea,kunkli.roland}@inf.unideb.hu

[c]University of Debrecen, Faculty of Humanities
{kurucz.gyozo,hollo.gabor}@arts.unideb.hu

In the course of a wide number of research projects, the need to deal with a large volume of research-specific generated data is frequently present. Whether looking for patterns, anomalies, or visual forms of the data, the issue more than likely demands a visualization framework. A potential precedent may be the observance of the microscopic world, allowing us to extract new knowledge regarding its nature [4].

The problem that we faced had the same requirement; the generated research-specific data could become significantly clearer if presented visually, allowing the observer to gain access to some of the higher-level properties that would be difficult to obtain otherwise. Our research aimed to analyze certain aspects of the behavior of microscopic organisms in a well-defined environment [2, 3]. The output of the simulation system used in the research was several datasets, each of which contains a description of the movement of a microscopic organism in a three-dimensional environment. However, considering the non-trivial characteristics of the data sequence, no out-of-the-box solution could be applied for our visualization purposes.

Each of the datasets is made of a frame sequence describing the step-by-step movement of the simulated organism. The non-triviality originated from the fact that the description was realized indirectly by the behavior of the environment. Given was five fixed food points in the organism's surroundings and a central moving object representing the organism itself. In each data frame, we only had information about the change of the surrounding objects in terms of the organism's point of view, which effectively means that in every moment, we only know the location vectors of five points in the central object's local coordinate system, and the object itself is positioned in the global origin.

This work aims to present the creation process and the operation of a framework for visualizing the movement and behavior of microscopic organisms. The framework solves

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

the problem of indirectness and determines the per-frame positions of the objects. We achieved these goals by building on our previous method, which relies on barycentric coordinates for the conversion process that originates from the need to go from local to global coordinates [1]. The main advantage of this method comes from the fact that the coordinate transformation process is realized entirely without building on earlier frames, yielding a higher overall precision by avoiding the propagation of floating-point errors that is a known drawback of the matrix-based approach.

The main idea is that the food positions from every frame are taken as reference points for obtaining the barycentric coordinates of the central object, using the reference points from the very first frame as a basis. Since obtaining the barycentric coordinates of a three-dimensional point requires four reference positions, the possessed data is perfectly satisfactory for these constraints. The food points had a randomly generated and fixed lifetime to simulate the consumption by other competitors. Thus, the points could disappear either when the food was consumed by the organism or when their lifetime reached their maximum value (i.e., they were "eaten" by a competitor organism). In this case, the food in question is replaced in the next data frame with a new one, positioned at a different location. This ever-changing nature of the reference points raised the problem of finding the coordinates of the newly appeared reference points to update the basis used for the central object.

Considering all the requirements mentioned above and putting our barycentric method into practice, we designed a tool for processing the existing simulation data, obtaining the necessary global positions, and visualizing the results in a three-dimensional scene. The framework was implemented in such a way that it delivers an interactive visualization environment, facilitating the efficient exploration of the input data through real-time, user-driven feedback mechanisms. Throughout the design of our proposed system, we also made sure to include several functions for the users to analyze their data from multiple aspects and get answers to their questions. The framework makes it possible to navigate in the frame sequence to any desired moment and freeze the simulation for inspecting the momentary behavior of the organism. Our application also includes the visualization of the visibility of foods to get an overview of which are accessible for consumption by the organism.

In this paper, we would like to present the starting problem, the world description, and the data creation concept. We also give a brief overview of our existing, barycentric coordinates-based approach and then provide an extension with the support of dynamic reference points. The presentation of the application of our method based on barycentric coordinates and the resulting visualization framework will also be part of our paper. Lastly, we demonstrate our results using several new test scenarios (including both artificially generated and real datasets) and present the analysis of the precision of our proposed system.

Keywords: visualization framework, animation, movement, microscopic organism, barycentric coordinates

References

[1] A. BODONYI, R. KUNKLI: *Efficient object location determination and error analysis based on barycentric coordinates*, Visual Computing for Industry, Biomedicine, and Art 18.3 (2020), pp. 1–7, DOI: https://doi.org/10.1186/s42492-020-00052-y.

[2] G. HOLLÓ: *A new paradigm for animal symmetry*, Interface Focus 5.6 (2015), pp. 1–10, DOI: https://doi.org/10.1098/rsfs.2015.0032.

[3] G. HOLLÓ, M. NOVÁK: *The manoeuvrability hypothesis to explain the maintenance of bilateral symmetry in animal evolution*, Biology Direct 7.18 (2012), pp. 1–7, DOI: https://doi.org/10.1186/1745-6150-7-22.

[4] T. ISHIKAWA: *Suspension biomechanics of swimming microbes*, Journal of The Royal Society Interface 6.39 (2009), pp. 815–834, DOI: https://doi.org/10.1098/rsif.2009.0223.

Replacing the SIR epidemic model with a neural network and training it further to increase prediction accuracy

Gergő Bogacsovics[a], András Hajdu[a], Róbert Lakatos[a], Marcell Beregi-Kovács[a], Attila Tiba[a], Henrietta Tomán[a]

[a]University of Debrecen
bogacsovics.gergo@inf.unideb.hu, hajdu.andras@inf.unideb.hu,
robert.lakatos@it.unideb.hu,
beregi.kovacs.marcell@science.unideb.hu,
tiba.attila@inf.unideb.hu, toman.henrietta@inf.unideb.hu

Researchers often use theoretical models to describe and explain various phenomena. Research in the area of natural sciences generally defines theoretical models with the help of mathematics, as well. The mathematical description of theoretical models is very useful, as it can be used to generalize and parameterize the theoretical models. Furthermore, it provides a relatively simple, yet concise and effective way of modelling complex phenomena. However, it is a well-known fact that the more complex the model, the more complex the mathematical description is. For this reason, theoretical models generally avoid large complexity and aim for the simplest possible definition. Although simplicity makes the model mathematically more manageable, it often makes it inaccurate to apply in practice, leading to sub-optimal performance. This is because the real environments are usually rather complex, and the studied phenomena and the related observations are never ideal or regular. The collected data during the observations usually contain confounding factors, for which a simple theoretical model can not prepare. Additionally, mathematical models are usually too rigid and sophisticated, and therefore cannot really deal with sudden changes in the environment.

The application of data science and artificial intelligence provides a good opportunity to develop complex models that can combine the basic capabilities of the theoretical models with the ability to learn more complex relationships. It has been shown [3] that with neural networks, which are one of the most powerful tools for machine- and deep learning, we can build such models, that can approximate mathematical functions. Trained artificial neural networks are able to behave like theoretical models developed for different fields, while still retaining their overall flexibility. In this way, the effective learning abilities of neural networks can be combined with the basic abilities of theoretical models. Through their learning capabilities and properties, trained models are capable of constant learning, and therefore have the ability to perform better than theoretical models in a complex real-world environment.

The aim of our study is to show our notion that we can create an architecture using artificial intelligence, especially neural networks, which is able to approximate a given theoretical model, and then further improve with the help of real data to better suit the

real world and its various aspects. In order to validate the functionality of the architecture developed by us, we have selected a simple theoretical model, namely the Kermack-McKendrick one [2] as the base of our research. The Kermack-McKendrick is an SIR [1] model, which is a relatively simple compartmental epidemic one, based on differential equations that can be used well for infections that spread very similar to influenza or COVID. However, on one hand, the SIR model relies too heavily on its parameters, with slight changes in them leading to drastic overall changes of the S, I and R curves, and on the other hand, the simplicity of the SIR model distorts its accuracy in many cases.

In our paper, by using the SIR model, we would like to show that the architecture described above can be a valid approach for modeling the spread of a given disease (such as influenza or COVID-19). To this end, we detail the accuracy of our models with different settings and configurations, and also outline an ensemble network constructed from these models that achieves even greater accuracy.

Keywords: deep learning, neural networks, mathematical models, SIR model

References

[1] T. HARKO, F. S. LOBO, M. MAK: *Exact analytical solutions of the Susceptible-Infected-Recovered (SIR) epidemic model and of the SIR model with equal death and birth rates*, Applied Mathematics and Computation 236 (2014), pp. 184–194.

[2] W. O. KERMACK, A. G. MCKENDRICK: *A contribution to the mathematical theory of epidemics*, Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character 115.772 (1927), pp. 700–721.

[3] Z. ZAINUDDIN, O. PAULINE: *Function approximation using artificial neural networks*, WSEAS Transactions on Mathematics 7.6 (2008), pp. 333–338.

Time Evolution Model for Classifying Files in Antivirus Testing Procedures

László Bognár[a], Antal Joós[a], Bálint Nagy[a]

[a]University of Dunaújváros
bognarl@uniduna.hu, joosa@uniduna.hu, nagyb@uniduna.hu

As business and people rely more and more on computer related devices (including smart devices and the IoT), they are increasingly vulnerable to cyber-attacks [1]. These attacks include threats of social networks [6] data phishing, malicious programs etc. The defense against malware is composed of malware detectors, systems that investigate malicious objects (mainly files and URLs). Several malware detection techniques and methods to investigate the vulnerability of systems are introduced in the literature [7].

Security solution testers use malicious files (sample set) coming from different sources to determine whether the defense is able to detect these files as malicious or not [3, 8].

One of the most important parts of the testing procedure influencing the reliability of the procedure is the correct and relevant selection of the used sample set.
How to correctly classify samples of a sample set is one the major issues for security solution testers to ensure their service to be reliable and to be able to give relevant recommendations for their client about the capabilities of security solutions [5]. Evaluating the efficiency of different antiviruses (AV), different antivirus vendors or even testing the level of security in a corporation requires reliable information about the samples [2].

Besides the main question whether a given object (file/URL) (abbreviated only file in what follows) in a sample set is "*Infected*" or "*Noninfected*" [4, 9], in case of the infected files the "freshness" of the infection is also an important issue. The starting time of operation of a malware is essential for categorizing the malware as "*New*" or "*Old*".

Sample selection can be broken down into three phases [10]: Collection, Validation and Classification. In this paper the classification phase is in focus, however some aspects of the validation phase are also incorporated. It is assumed that the collection was correct, and the sample consists of real-world, prevalent, fresh, diverse files collected independently.

The sample validation process essentially is series of tests to make sure that the sample is functional (has working malicious function). There are several methods trying to validate samples: reverse engineering, usage of automated tools or by using various specialized tools (e.g. sandboxes) to check file integrity or functionality.

Best practices show that validation is most valuable when it is based on sample functionality, but these methods are not applicable to all sample types and may need enormous efforts to pursue these kinds of activities on a daily basis with huge number of files.

In this paper a so called "*Time Evolution Model*" is suggested to help categorize each file or even a whole sample set (also called as feed).

The basic time dependent variable of this model is the *Ratio* of the "*Yes*" decisions to

the question: Is this file infected? The answers come from the members of a set of antimalware where most of these members showed reliable operations in the past in malware detection.

After the appearance of a new malware it takes less or more time for the different antimalware to detect the fact of infection. Some antimalware is simply not able to recognize some specific infections. (Possibly due to some validation issue.) Hence the ratio of "*Yes*" decisions is gradually increasing in time and reaches the state when the increase and the variation of the *Ratio* value is small enough to establish this *Ratio* as the steady state value of the time evolution.

The main goal of this study is to establish the main characteristics of these time functions. A nonlinear curve fitting method is used to fit a smooth time function on the observed *Ratio* data to estimate the steady state value (called *Asymptote*), the *Start Time* (starting time of operation) and the *Slope* at the *Start Time* for each file in a feed. These parameters can be used later to classify a file belonging to a certain category ("*Old*", "*New*", "*Infected*", "*Noninfected*", etc.).

For this estimation past *Ratio* data within a *Time Window* are used. The *Time Window* ends at the moment of investigation ("Today") and goes back in time. Obviously, the length of time, how far the *Time Window* goes back, has influence on the estimation. It is also investigated.

The reliability of the "Yes" decisions of the antiviruses is crucial. In this study it is assumed that the antimalware set consists of properly selected members. The process of selection resulting in a reliable set is discussed elsewhere.

Keywords: vulnerability, probability, relative frequency

References

[1] AMTSO: *Symantec Internet security threat report 2019*, https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf/, [Online; Accessed 2 October 2020], 2019.

[2] S. BROWN, J. GOMMERS, O. SERRANO: *From Cyber Security Information Sharing to Threat Management*, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, WISCS '15, Denver, Colorado, USA: Association for Computing Machinery, 2015, pp. 43–49, ISBN: 9781450338226,
DOI: https://doi.org/10.1145/2808128.2808133.

[3] I. BURGUERA, U. ZURUTUZA, S. NADJM-TEHRANI: *Crowdroid: Behavior-Based Malware Detection System for Android*, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '11, Chicago, Illinois, USA: Association for Computing Machinery, 2011, pp. 15–26, ISBN: 9781450310000,
DOI: https://doi.org/10.1145/2046614.2046619.

[4] M. CHRISTODORESCU, S. JHA, S. SESHIA, D. SONG, R. BRYANT: *Semantics-Aware Malware Detection*, in: June 2005, pp. 32–46, ISBN: 0-7695-2339-0,
DOI: https://doi.org/10.1109/SP.2005.20.

[5] Z. A. COLLIER, I. LINKOV, J. H. LAMBERT: *Four domains of cybersecurity: a risk-based systems approach to cyber decisions*, 2013,
DOI: https://doi.org/10.1007/s10669-013-9484-z.

[6] W. GHARIBI, M. SHAABI: *Cyber Threats In Social Networking Websites*, International Journal of Distributed and Parallel Systems 3 (Feb. 2012), pp. 1–8.

[7] F. LEITOLD, K. HADARICS: *Measuring security risk in the cloud-enabled enterprise*, in: 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), Los Alamitos, CA, USA: IEEE Computer Society, Oct. 2012, pp. 62–66,
DOI: https://doi.org/10.1109/MALWARE.2012.6461009.

[8] F. LEITOLD: *Testing Protections against Web Threats*, in: Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software, MALWARE '11, USA: IEEE Computer Society, 2011, pp. 20–26, ISBN: 9781467300315,
DOI: https://doi.org/10.1109/MALWARE.2011.6112322.

[9] A. MOSER, C. KRUEGEL, E. KIRDA: *Limits of Static Analysis for Malware Detection*, in: Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), 2007, pp. 421–430,
DOI: 10.1109/ACSAC.2007.21.

[10] C. H. TSENG, S. WANG, S. WANG, T. JUANG: *Proactive malware collection and classification system: How to collect and classify useful malware samples?*, in: 2014 International Conference on Information Science, Electronics and Electrical Engineering, vol. 3, 2014, pp. 1846–1849,
DOI: https://doi.org/10.1109/InfoSEEE.2014.6946241.

Genealogical networks: a case study from the perspective of network science*

Imre Bordán[a], Imre Varga[a]

[a]University of Debrecen, Faculty of Informatics
varga.imre@inf.unideb.hu

In this paper, the analysis of a genealogical network is presented. The source database [2] was constructed from the records of birth, marriage and death registers of a middle-sized Hungarian town covering some centuries. This genealogical network contains ca. 100.000 individuals. The topological features of this graph were analyzed by computer software in order to draw conclusions about the community. The results illustrate how networks science can help the social sciences.

Genealogy is an ancillary historical discipline. It means the study of family origins and history, and the tracing of their lineages. The word "genealogy" comes from two Greek words ("family" and "science"), thus is derived "to trace ancestry", the science of studying family history. Genealogists use historical records, genetic analysis, and other sources to get information about a family and to demonstrate ancestry and pedigrees of individuals. In the broad sense, genealogy traces the descendants and the ancestors of a person. Genealogy research is performed for historical, scholarly, or forensic purposes as well. The results of such research are often presented in pedigree charts.

Family trees or ancestry charts are usually maintained as a binary tree data structure containing the ancestors of a person. In a simple assumption, everyone has 2 parents, 4 grandparents, 8 great-grandparents, 16 great-great-grandparents, and so on. Thus the number of ancestors in a given generation can be expressed by the powers of two. For example in the 30th generation theoretically, there are more the one billion people, which can be more than the total population of the Earth at that time. This conflict can be resolved by the fact that not all ancestors are individual. In genealogy, this phenomenon is called pedigree collapse. It describes the situation caused by the reproduction between two individuals who share an ancestor. It is very rare in the short-term oral history of a family, but it is unavoidable in huge pedigree charts covering centuries. Due to pedigree collapse genealogists have use graphs instead of tree data structures.

When not just a family, but a community is in the focus of genealogical research besides the size of the data source its structure also changes. Marriages and childbirths connect families. Ancestry charts of a minor community cannot be represented by a forest of family trees, it is a directed acyclic graph. In a small settlement especially in bygone years, the society was more closed than nowadays, thus families are densely interconnected.

*The authors would like to express their sincere gratitude to Imre Szepesi for his valuable registry research and the creation of the genealogical database they used [2].

Our goal is to build a directed network of people based on only registry records (without genetic test results) and then determine different metrics of the networks [1], such as in-degree and out-degree distribution, average clustering coefficient, size of the giant component, average path length etc. In this system, they have social meaning as well. The characterization of pedigree collapse also requires network analysis. While the data set is never complete a novel quantity is defined to illustrate the scale of pedigree collapse. Our ancestor-loss coefficient was calculated for each person and we found that pedigree collapse is quite frequent within a few generations. Numerical results are interpreted from the perspective of the networks science and the social science as well.

Keywords: genealogy, networks analysis, pedigree collapse

References

[1] M. NEWMAN: *Networks: An Introduction*, Oxford University Press, 2010, ISBN: 978-0-19-920665-0.

[2] I. SZEPESI: *Hajdúböszörméni családerdő*, https://gw.geneanet.org/szepesi?i=0&lang=en &type=tree, 2020.

Post-processing methods for calibrating the wind speed forecasts in central regions of Chile*

Mailiu Díaz[a], Orietta Nicolis[b], Julio César Marín[c], Sándor Baran[d]

[a]Department of Meteorology, University of Valparaíso, Chile
mailiudp@gmail.com

[b]Faculty of Engineering, Andres Bello University, Chile
orietta.nicolis@unab.cl

[c]Department of Meteorology, University of Valparaíso, Chile
julio.marin@meteo.uv.cl

[d]Faculty of Informatics, University of Debrecen, Hungary
baran.sandor@inf.unideb.hu

In this paper we propose some parametric and non-parametric post-processing methods for calibrating the wind speed forecasts from nine WRF models around the towns of Valparaíso and Santiago de Chile (Chile). The WRF outputs were gener- ated with different planetary boundary layers and land-surface model parametriza- tions and they were calibrated using the observations from 37 monitoring stations. The post-processing statistical calibration have been implemented using EMOS and quantile regression forest (QRF) methods with a regional and semi-local approach. The best performance has been obtained by the QRF using a semi-local approach and considering some specific weather variables from WRF simulations.

Introduction

The Weather Research and Forecasting (WRF) model has been successfully used by the atmospheric science community over the years for predicting weather conditions. However, although several improvements have been implemented, the WRF outputs are often affected by bias errors especially when predicting the wind speed over complex terrain. Since last decade, some statistical post-processing models have been developed to obtain sharpness and calibration forecasts such as non- homogeneous regression or ensemble model output statistics (EMOS, [1]) which provide full predictive distribution of the future weather quantity using single para- metric distribution with parameters connected to the ensemble members. Recently, some studies have been focused on machine learning techniques for statistical fore- casting. An example is the quantile regression forests (QRF) proposed by [2].

*This research was supported by the Interdisciplinary Center of Atmospheric and Astro-Statistical Studies, University of Valparaíso, Chile.

Methodology

EMOS and QRF models were run with the regional and semi-local approach. Since the wind data are not normal the Truncated-Normal distribution was used (see [3] for more details). In the following we will denote by EMOS_C and QRF_C the models with the semi-local approach to differentiate them from regional models (EMOS and QRF). Regional EMOS for 9 members required the estimation of 12 parameters for each training period and the same number for each cluster with the semi-local approach. QRF method was implemented using two different cases. For the first one denoted as QRF we used the nine wind speed forecasts from the WRF models; and for the second case QRF_M we used the mean, the standard deviation, the minimum and maximum values of some variables (U10, V10, T2, PSFC, and RH) in addition to the orographic variance (VAR), land use (LU), HGT, and the observed altitude (Alt_st), for a total of 24 covariates. Both cases were tested with different arguments and we decided to compute the model with 300 trees and a minimum size of 5 for terminal leaves, since these arguments provided smaller scores. Further, the implementations of QRF and QRF_M differ each other in the number of variables randomly sampled as candidates at each split; one for QRF and three for QRF_M were the best options. CRPS was used to compare the univariate forecast models with the basic regional EMOS.

Results

The mean CRPS of the forecast models versus EMOS (see Figure 1) evidenced: the semi-local EMOS approach improves the calibration at each hour, QRF performances better with semi-local approach (QRF_C), and the best QRF forecasts are obtained by adding other features as predictors in the regression model (QRF_M and QRF_C_M). Similar

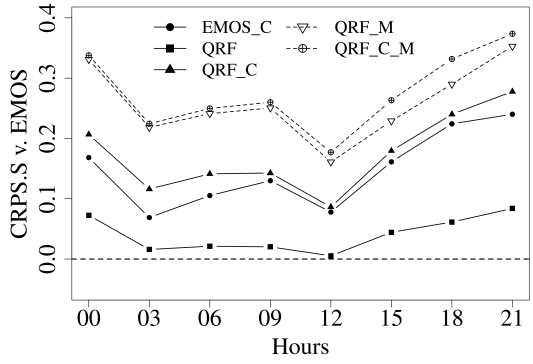


Figure 1: Mean CRPS vs. EMOS by hours for all stations.

results were obtained with the comparison of the overall scores (see Table 1), where the lowest values of univariate scores were obtained with QRF_M and QRF_C_M.

Models	CRPS	MAE	RMSE	Cover
Ensemble	1.1715	1.4470	1.9949	43.95
EMOS	0.6078	0.8333	1.2443	82.12
EMOS_C	0.5108	0.7121	1.0361	80.29
QRF	0.5794	0.7968	1.1827	89.15
QRF_C	0.4939	0.6867	0.9817	88.18
QRF_M	0.4441	0.6143	0.9021	90.69
QRF_C_M	0.4318	0.5992	0.8781	89.65

Table 1: Overall scores for the different models computed in the study.

Keywords: WRF, QRF, calibration, wind speed

References

[1] T. GNEITING, A. E. RAFTERY, A. H. WESTVELD, T. GOLDMAN: *Calibrated Probabilistic Forecasting Using Ensemble Model Output Statistics and Minimum CRPS Estimation*, Monthly Weather Review 133.5 (2005), pp. 1098–1118.

[2] M. TAILLARDAT, O. MESTRE, M. ZAMO, P. NAVEAU: *Calibrated Ensemble Forecasts Using Quantile Regression Forests and Ensemble Model Output Statistics*, Monthly Weather Review 144.6 (2016), pp. 2375–2393.

[3] T. L. THORARINSDOTTIR, T. GNEITING: *Probabilistic forecasts of wind speed: ensemble model output statistics by using heteroscedastic censored regression*, Journal of the Royal Statistical Society Series A 173.2 (2010), pp. 371–388.

Trees classification based on Fourier coefficients of the sapflow density flux*

Dmitry Efrosinin[a,b], Irina Kochetkova[b,c], Natalia Stepanova[d], Alexey Yarovslavtsev[b,e], Konstantin Samouylov[b,c], Riccardo Valentini[f,b]

[a]Johannes Kepler University Linz, Austria
dmitry.efrosinin@jku.at

[b]Peoples' Friendship University of Russia (RUDN University), Russia
gudkova-ia@rudn.ru, yaroslavtsev-am@rudn.ru, samuylov-ke@rudn.ru

[c]Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of RAS, Russia

[d]V.A. Trapeznikov Institute of Control Sciences of RAS, Russia
natalia0410@rambler.ru

[e]LAMP, Russian Timiryazev State Agrarian University, Russia,

[f]Tuscia University, Viterbo, Italy
rik@unitus.it

This work is a continuation of a previous survey related to a new sensor tree monitoring system TreeTalker© (TT) [6]. This system has been used to create a database, which is expected to be published shortly and which includes, among other things, a large amount of information on the sap density flux describing water transport process in different tree varieties that also differ in age, health status, metric characteristics, etc. Recall that in the previous paper [2] we presented a method for predicting the density flux during the day based on data on air temperature during the observed cycle. For this purpose, Fourier series and a multivariate regression model were used, establishing the functional relationship between the respective Fourier coefficients for temperature data sets and density flux values. Here we report our first experiments carried out on data sets extracted by the TT monitoring system as well as on the estimated values of the density flux and dedicated to trees classification. Classification is a very common use case of a machine learning. Artificial neural networks [3, 5] is a part of a supervised machine learning which is most popular in different problems of data classification, pattern recognition, regression, clustering, time series forecasting. We study the possibility to use NN to classify the trees of the same species but with different age groups and visual-tree-assessment (VTA) scores. As classification features we use a predicted Fourier coefficients of the sap flow density

*The work was supported by the Russian Science Foundation, project 19-77-30012 (recipients I. Kochetkova, A. Yarovslavtsev, R. Valentini). The publication has been prepared with the support of the "RUDN University Program 5-100" (recipients D. Efrosinin, K. Samouylov).

flux approximation function. In the long term, this approach which incorporates data generated by the TT with the proposed Fourier coefficient estimation method can be used to determine the anomalous state of a tree or generally monitor forest ecology.

Consider data sets with n_p observable cycles for two species of trees: *Salix albe* and *Acer platanoides*. The data of the first and second groups of trees we divide respectively into three and four subgroups according to the Table 1. We prepare a data for classification

(a)

Class N	Age group	VTA score
1	IV	2
2	IV	3
3	III	2

(b)

Class N	Age group	VTA score
1	VI	1
2	VI	2
3	VI	3
4	VI	4

Table 1: Classes of *Selix albe* (a) and *Acer platanoides* (b)

in form of the set of the following relations,

$$S = \{(\hat{\alpha}_{i,0}, \hat{\alpha}_{i,1}, \ldots, \hat{\alpha}_{i,m}, \hat{\beta}_{i,1}, \ldots, \hat{\beta}_{i,m}) \to \text{Class } N : 1 \leq i \leq n_p\}.$$

70% of sample S is referred to as training data and the rest – as validation data. We train a multilayer (6-layer) NN using an adaptive moment estimation method [4] and the neural network toolbox in *Mathematica*© of the Wolfram Research. Then we verify the classifier which should be accurate enough to be used to predict new output from verification data. The algorithm was ran many times on samples and networks with different sizes. In all cases the results were quite positive and indicate the potential of machine learning methodology for trees classification problem based on the estimated Fourier coefficients.

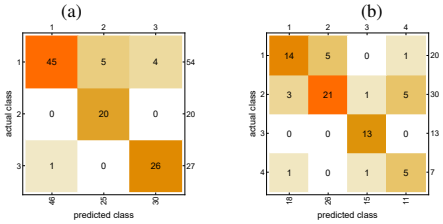


Figure 1: Confusion matrices for classification of *Salix alba* (a) and *Acer platanoides* (b)

The results of predictions are visualized in form of confusion matrices shown in Figure 1. Each row of these matrices represents the instances in a predicted value while each column represents the instances in an actual value. Different statistical measures of the performance of a binary classification, such as the overall accuracy (ACC), sensitivity (true positive rate – TPR), specificity (true negative rate – TNR) as well as $F1$-scores which is the harmonic mean of precision and sensitivity, are given in Table 2. For more details about these measures, refer to [1]. We can see that the first data can be classified with higher accuracy as the second one. It should be noticed that the main goal of the paper

Table 2: Classification performance

Metric / Data	ACC	TPR	TNR	$F1$-scores
Salix albe	0.9009	$1 \to 0.8333$ $2 \to 1.000$ $3 \to 0.9629$	$1 \to 0.9787$ $2 \to 0.9382$ $3 \to 0.9459$	$1 \to 0.9000$ $2 \to 0.8889$ $3 \to 0.9123$
Acer platanoides	0.7571	$1 \to 0.7000$ $2 \to 0.7000$ $3 \to 1.000$ $4 \to 0.7143$	$1 \to 0.9200$ $2 \to 0.8750$ $3 \to 0.9649$ $4 \to 0.9048$	$1 \to 0.7368$ $2 \to 0.7500$ $3 \to 0.9286$ $4 \to 0.5556$

was not only to make first attempts to classify subgroups of trees with the highest possible accuracy, but to check the overall expediency of using Fourier coefficients as characteristic parameters or features of different classes. As we can see, the accuracy of classification is encouraging.

References

[1] D. G. ALTMAN, J. M. BLAND: *Statistics Notes: Diagnostic tests 1: sensitivity and specificity*, BMJ 308.6943 (1994), p. 1552,
DOI: https://doi.org/10.1136/bmj.308.6943.1552.

[2] D. EFROSININ, I. KOCHETKOVA, N. STEPANOVA, A. YAROVSLAVTSEV, K. SAMOUYLOV, R. VALENTINI: *The Fourier Series Model for Predicting Sapflow Density Flux based on TreeTalker Monitoring System*, in: LNCS, NEW2AN 2020 (to be published), St. Petersburg, Russia: Springer, 2020.

[3] C. GERSHENSON: *Artificial Neural Networks for Beginners*, 2003, arXiv: cs/0308031 [cs.NE].

[4] D. P. KINGMA, J. BA: *Adam: A Method for Stochastic Optimization*, 2014, arXiv: 1412.6980 [cs.LG].

[5] S. RUSSELL, P. NORVIG: *Artificial Intelligence: A Modern Approach*, 3rd, USA: Prentice Hall Press, 2009, ISBN: 0136042597.

[6] R. VALENTINI, L. MARCHESINI, D. GIANELLE, G. SALA, A. YAROVSLAVTSEV, V. VASENEV, S. CASTALDI: *New Tree Monitoring Systems: From Industry 4.0 to Nature 4.0.* Annals of Silvicultural Research 43.2 (2019), pp. 84–88,
DOI: https://doi.org/10.12899/asr-1847.

A WebGL-based virtual puzzle game for spatial skill development purposes

Bence Dániel Erős[a,b], **Roland Kunkli**[b]

[a]University of Debrecen, Doctoral School of Informatics

[b]University of Debrecen, Faculty of Informatics
{eros.bence,kunkli.roland}@inf.unideb.hu

Because of their unique challenges, twisty puzzles and similar logical games are popular with children and adults alike. Therefore, they are one of the key tools of skill development in public opinion since their first appearance. The physical environment creates specific limitations to these games, but new tools from computer graphics and its virtual environments allow us to reach new possibilities.

We report an application that helps the users to try rotations on 3D models based on the rules of the well-known puzzle Rubik's Cube. In our solution, these models could be different from the usually used symmetric and convex shapes.

Keywords: virtual spatial puzzle, Rubik's Cube, skill development, WebGL

Motivation

In the early stages of our life, we learn the fundamental skills which help us to interact efficiently with our environment during our whole lifetime. Playing is an opportunity to make the necessary exploration and discoveries throughout this learning process, but gain them in a fun way. By now, research has shown that challenges appear in the form of 3D geometry have a measurable skill development effect on the visual-spatial intelligence of children [3]. These spatial puzzles affect those areas of our brain system that create visual representations of objects in space and develop the ability of expressing our thoughts graphically using spatial concepts [3, 7].

A shared experience is that these spatial puzzle toys are still can be a challenge not just for people at young ages, but adults. One way is the recognition of many questions that come from the theoretical background of these puzzles [4]. On the other hand, the design of a new puzzle still requires expert knowledge because of the need for rotatable pieces, and with an inaccurate plan, the construction may fall apart. In their work [5], Sun and Zheng introduce one more problem from the puzzle design domain: the collision of puzzle pieces. Here, every shape which can not meet one of the properties of symmetry or convexity can stop the playing process when some pieces of the puzzle block each other as a consequence of collision. The presented method in their article can handle the creation of the inner mechanism for putting together the rotatable pieces, but before the physical printing process, the model needs to go through some deformation steps to avoid the collision of puzzle pieces [5].

Results

In our work, we focus on the opportunities to create spatial puzzles in a virtual environment. For this purpose, we created an application that uses many tools provided by WebGL technologies. The number of web-based applications with 3D content is increasing since the beginning of the last decade. Today there is no need for the addition of plugins in web browsers, and users can reach these graphical contents on more devices with limited storage and computational capabilities like mobile phones. Thereby the most different areas can provide content to the users, for example, medical imaging, heritage, online games, and e-learning [2].

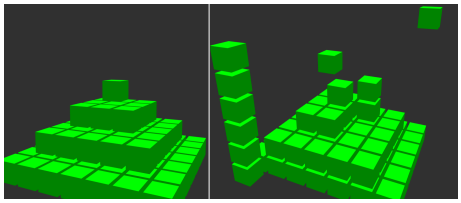


Figure 1: In our first prototype of the application, we found that floating pieces of the puzzle can enrich the possibilities of challenges.

To create a puzzle from its rotatable pieces, we defined two ways. One solution, when we draw many individual meshes at the beginning of the design process and then put these pieces together in one whole shape (see Figure 1). We found that this method is widespread because several examples are already available online, like those where sets of little cubes result in a whole one in the case of the well-known Rubik's Cube. These implementations also provided a case study [6] about display opportunities and rotation mechanics logic to reach the best possible user experience in our application.

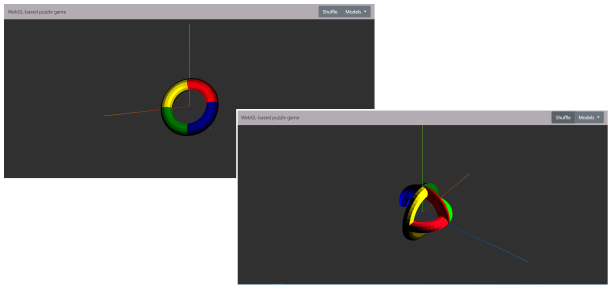


Figure 2: Rotations on a torus mesh.

After that, we examined the way where the design process starts from a mesh that has not got separable pieces. Then, we had to find a solution to perform cuts during the preparation process of puzzle pieces. For this purpose, we used the Blender graphical toolset [1]. Here, tools like the *Bisect tool* and the *Boolean modifier* can also provide a

solution to our problem. The pieces can be saved into several data-formats like OBJ or COLLADA. In our code, we defined functions that read in the vertices of the mesh from the file and display the individual puzzle pieces (see Figure 2).

References

[1] *Blender v2.79. (software)*, The Blender Foundation, Accessed: 2020-01-16.
Available online: https://www.blender.org/.

[2] A. EVANS, M. ROMEO, A. BAHREHMAND, J. AGENJO, J. BLAT: *3D graphics on the web: A survey*, Computers & Graphics 41 (2014), pp. 43–61,
DOI: https://doi.org/10.1016/j.cag.2014.02.002.

[3] H. FITRIYANI, N. TASU'AH: *The Use of Three Dimensional Puzzle as a Media to Improve Visual-Spatial Intelligence of Children Aged 5-6 Years Old*, Indonesian Journal of Early Childhood Education Studies 3.1 (2014), pp. 74–78,
DOI: https://doi.org/10.15294/ijeces.v3i1.9476.

[4] D. JOYNER: *Adventures in Group Theory - Rubik's Cube, Merlin's Machine and Other Mathematical Toys, 2nd Edition*, ISBN: 9780801890130, Baltimore, Maryland: The Johns Hopkins University Press., 2008.

[5] T. SUN, C. ZHENG: *Computational Design of Twisty Joints and Puzzles*, ACM Transactions on Graphics 34.101 (4 2015), pp. 1–11,
DOI: https://doi.org/10.1145/2766961.

[6] J. WHITFIELD-SEED: *rubik-js (software)*, 2013, Accessed: 2020-02-21.
Available online: https://github.com/joews/rubik-js.

[7] P. G. ZIMBARDO, R. L. JOHNSON, V. MCCANN: *Psychology: Core Concepts, 8th Edition*, ISBN-13: 9780134190839, New York, New York: Pearson, 2017.

Theoretical and simulation results for a multi-type network evolution model*

István Fazekas[a], Attila Barta[b]

[a]University of Debrecen, Department of Applied Mathematics and Probability Theory
fazekas.istvan@inf.unideb.hu

[b]University of Debrecen, Doctoral School of Informatics
barta.attila@inf.unideb.hu

A continuous-time network evolution model is studied. The basic units of the model are edges and triangles. The evolution of the units is governed by a continuous-time branching process. The asymptotic behaviour of the model is studied. It is proved that the number of edges and triangles have the same magnitude on the event of non-extinction, and it is $e^{\alpha t}$, where α is the Malthusian parameter.

Introduction

Network theory is one of the most popular research topics of our age. It studies both real-life networks and theoretical models. Networks are described by graphs. The nodes of the network are the vertices of the graph and the connections are the edges. One of the most famous models is the preferential attachment model introduced by Albert and Barabási. It is a discrete time model (that is the evolution events occur at time $n = 1, 2, \dots$) and it describes connections of two nodes. The meaning of connection can be cooperation or any interaction. Therefore the connections of more than two nodes are also important. For example, Backhausz and Móri in [1] describe three-interactions, Fazekas and Porvázsnyik in [4] N-interactions, or Fazekas and Perecsényi in [3] star-like connections. Continuous-time network evolution models seem to be more difficult but more realistic models than the discrete time ones. In [7] a continuous-time branching process is applied to govern the evolution mechanism. In [2] we extended the results of [7] for 3 interaction models. There we applied the general theory of branching processes [5].

The model

We shall study the following random graph evolution model. At the initial time $t = 0$ we start with a single object, it can be either an edge or a triangle. We call this object the ancestor. This ancestor object produces offspring objects which can be also edges or triangles. Then these offspring objects also produce their offspring objects, and so on. The reproduction times of any object, including the ancestor, are given by its own Poisson process with

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

rate 1. We assume that during the evolution, the reproduction processes of different objects are independent. The reproduction processes of the triangles are independent copies of the generic triangle's reproduction mechanism. Similarly, the reproduction processes of the edges are independent copies of the reproduction mechanism of the generic edge.

Results

We present the general results on our model. These are the survival function and the mean offspring number. We show asymptotic theorems on the number of triangles and the number of edges. All of them have magnitude $e^{\alpha t}$ on the event of non-extinction, where α is the Malthusian parameter. To prove our results we apply general theorems on multitype branching processes [6], [9], [8]. And last we present some simulation results supporting our theorems.

Keywords: network theory, braching process, Malthusian parameter

References

[1] A. BACKHAUSZ, T. MÓRI: *A random graph model based on 3-interactions*, Ann. Univ. Sci. Budapest. Sect. Comput. 36 (2012), pp. 41–52.

[2] I. FAZEKAS, A. BARTA, C. NOSZÁLY, B. PORVÁZSNYIK: *A continuous-time network evolution model describing* 3*-interactions*, Manuscript (2020).

[3] I. FAZEKAS, C. NOSZÁLY, A. PERECSÉNYI: *The N-star network evolution model*, J. Appl. Probab. 56 (2019), pp. 416–440.

[4] I. FAZEKAS, B. PORVÁZSNYIK: *Scale-free property for degrees and weights in an N-interactions random graph model*, J. Math. Sci. (N.Y.) 214 (2016), pp. 69–82.

[5] P. JAGERS: *Branching Processes with Biological Applications*, Wiley (1975).

[6] C. J. MODE: *Multitype branching processes; theory and applications*, American Elsevier (1971).

[7] T. F. MÓRI, S. ROKOB: *A random graph model driven by time-dependent branching dynamics*, Annales Univ. Sci. Budapest., Sect. Comp. 46 (2017), pp. 191–213.

[8] O. NERMAN: *On the convergence of supercritical general (C-M-J) branching processes*, Z. Wahrscheinlichkeit. 57 (1981), pp. 365–395.

[9] O. NERMAN: *On the convergence of supercritical general branching processes*, University of Göteborg: PhD Theses, 1979.

Ensemble noisy label detection on MNIST

István Fazekas[a], Attila Barta[b], László Fórián[c*]

[a]University of Debrecen, Department of Applied Mathematics and Probability Theory
fazekas.istvan@inf.unideb.hu

[b]University of Debrecen, Doctoral School of Informatics
barta.attila@inf.unideb.hu

[c]University of Debrecen, Doctoral School of Informatics
forian.laszlo@inf.unideb.hu

In recent years, deep neural networks have reached very impressive performance in the task of image classification. However, these models require very large datasets with labeled training examples, and such datasets are not always available. The labeling process is often very expensive, or it is very difficult even for experts in a particular field. That is what leads to the use of databases with label noise, which contain incorrectly labeled instances. Therefore, it is important to consider training on this type of datasets. According to a widely accepted assumption, deep networks learn consistent, simple patterns in the beginning [2], and then it is followed by the learning of incorrect labels. So correcting the label noise in the train set can make the difference between overfitting to the wrong examples, and a better generalization ability. A lot of studies address the noisy labels problem, for example, [1] is an extensive survey about a broad range of the existing methods.

In this presentation we use the MNIST dataset, but we suppose that it contains some inaccurately labeled instances. MNIST is a database of handwritten digits, it consists of images with 28×28 grayscale pixels. The size of the training set is 60000 examples and the test set has 10000 samples.

We classify MNIST with an ensemble of convolutional neural networks. Firstly, we train that on the original training dataset, and then we are going to apply a label noise correction technique on the training database. Finally, we take a CNN ensemble with the same structure and train it on the new dataset gained by the label noise cleansing method.

We have used the framework in [5] to correct the inaccurate labels of our dataset. The authors of this paper suggest a two-stage approach. We outline some details about it in the following. The noise correction is made in the first phase by jointly optimizing the weights of a neural network and the labels of the training data. During this joint optimization process they train a classifier and correct the wrong labels at the same time. It is made possible by repeating alternating steps of updating the network parameters and the training labels. In the early stages, the training goes in the usual way, but they use a combined loss function for this purpose. Two regularization terms are added to the cross entropy loss function to prevent certain anomalies. When the classifier has achieved a reasonable accuracy, they start the repetition of the two above mentioned steps. The

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

first is the well known update of the network weights by the stochastic gradient descent method. In the other step, they update the labels in the following way. In every epoch the target vectors of the training samples are replaced by the average of the network's softmax output in the last 10 epochs. The averaging and a relatively high momentum prevents sudden changes in the labels at this time. Once this label correction is done, the authors start the training over in the second step with the recently obtained new labels and without the two regularization terms of the loss function.

The background network of this noise correcting and training process is the PreActResNet [4]. It is a modification of the famous ResNet network [3]. Residual Networks give a simple yet groundbreaking solution to the vanishing gradient problem. They use identity shortcuts, which let the data skip one or more layers. Obviously, the error backpropagation is the point where these models can really take advantage of these shortcuts. The pre-activation residual blocks [4] let the gradients flow throughout the PreActResNet even more easily. Such networks may have hundreds of layers and researchers consider them more accurate than ResNets.

Tanaka et al. [5] made experiments on CIFAR-10 with synthetic label noise, and a real-world dataset, in which almost 40 percent of the labels are wrong [6]. Our work differs from both of them, because we use a preprocessed dataset without adding synthetic label noise. However, we do not treat it as a perfectly clean training set. We suppose the existence of a certain, but not too large amount of label noise in MNIST. As mentioned before, we train an ensemble of CNN classifiers before and after the label noise cleansing. We perform this correction with the first phase of the method seen in [5]. To further enhance this procedure, we have also used an ensemble for this label noise cleansing, too. Our goal is to examine its effect on the dataset, the learning process, and the accuracy.

We implemented our experiments with Pytorch. Pytorch is a Python-based deep learning framework, in which only the forward pass of the networks have to be defined. It also offers a high degree of freedom while creating specific models. This flexibility makes it a suitable tool for deep learning research.

References

[1] G. ALGAN, I. ULUSOY: *Image Classification with Deep Learning in the Presence of Noisy Labels: A Survey*, 2020, arXiv: 1912.05170 [cs.LG].

[2] D. ARPIT, S. JASTRZĘBSKI, N. BALLAS, D. KRUEGER, E. BENGIO, M. S. KANWAL, T. MAHARAJ, A. FISCHER, A. COURVILLE, Y. BENGIO, S. LACOSTE-JULIEN: *A Closer Look at Memorization in Deep Networks*, in: ed. by D. PRECUP, Y. W. TEH, vol. 70, Proceedings of Machine Learning Research, International Convention Centre, Sydney, Australia: PMLR, Aug. 2017, pp. 233–242, URL: http://proceedings.mlr.press/v70/arpit17a.html.

[3] K. HE, X. ZHANG, S. REN, J. SUN: *Deep Residual Learning for Image Recognition*, in: 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778, DOI: https://doi.org/10.1109/CVPR.2016.90.

[4] K. HE, X. ZHANG, S. REN, J. SUN: *Identity Mappings in Deep Residual Networks*, in: Computer Vision – ECCV 2016, ed. by B. LEIBE, J. MATAS, N. SEBE, M. WELLING, Cham: Springer International Publishing, 2016, pp. 630–645, ISBN: 978-3-319-46493-0, DOI: https://doi.org/10.1007/978-3-319-46493-0_38.

[5] D. TANAKA, D. IKAMI, T. YAMASAKI, K. AIZAWA: *Joint Optimization Framework for Learning With Noisy Labels*, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2018, pp. 5552–5560,
DOI: https://doi.org/10.1109/CVPR.2018.00582.

[6] X. TONG, X. TIAN, Y. YI, H. CHANG, W. XIAOGANG: *Learning from massive noisy labeled data for image classification*, in: 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 2691–2699,
DOI: https://doi.org/10.1109/CVPR.2015.7298885.

Wavelet and recurrent neural network-based performance analysis of fast connectionless data transfers*

Zoltán Gál[a], Péter Polgár[a], Róbert Tornai[a], Tibor Tajti[b], Gergely Kocsis[a]

[a]University of Debrecen, Faculty of Informatics
gal.zoltan@inf.unideb.hu, polgarp@mailbox.unideb.hu
tornai.robert@inf.unideb.hu, kocsis.gergely@inf.unideb.hu

[b]Eszterházy Károly University, Institute of Mathematics and Informatics
tibor.tajti@gmail.com

In this paper we focus on fast communication issues of the Big Data processing tasks shared between High Performance Computing systems and on finding optimum bandwidth solution. Because of limited performance found at the connection oriented data transfer applications, we implemented a communication tool named Fast File Transfer Manager (FFTM). In our performance evaluation framework we used tcpdump to measure traffic sent by the own developed fast file transfer tool based on connectionless transfer protocol (UDP). Parameters of the captured traffics were: maximum transfer size (MTU), transmission ratio (Bw), and L4 segment size (L). For pattern detection in time series complex wavelet filtering was applied to identify degradation of the traffic performance. Recurrent neural network variants were applied to classify communication network traffics of the FFTM system for full tensor space of orthogonal communication parameters.

Introduction

Finding algorithms with low computation processing level for PDU management is an open question in the network and transmission logical levels for high speed communication services [3]. Big Data processing requires high volume of data to be delivered between client and high performance computation systems [5]. This implies usage of applications providing fast file transmission compatible with the existing IP based stacks [1].

Related work

Best effort based datagram delivery of the protocol data unit streams provides usable time critical services just in networks having minimal bandwidth in the scale of $n \cdot 10$ Mb/s.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund. The paper was supported by the QoS-HPC-IoT Laboratory, too.

Different implementations of the TCP congestion control mechanism with divisive efficiency of the transmission speed were developed by research institutes, standardization institutes and ICT companies in the last decades [4]. Even so reduced number of traffic evaluations can be found in the UDP transport based solutions [7], [8]. Comparison and analysis of the representing high-speed communication mechanisms existing today makes possible to set configuration for best transmission performance [2], [6].

Fragmentation and encapsulation of segments

IP packets larger than the size of maximum transfer unit parameter of the network interface card should split in smaller fragments with sequential order. The maximum transfer unit $vMTU$ of the of the virtual network interface card (vNIC) is given by $vMTU = \lfloor (MTU - 20)/8 \rfloor * 8 + 20$ bytes, where $\lfloor x \rfloor$ is floor value of the argument x and MTU is the value set in the configuration command. Having the total size L of the transport layer segment the number of IP packet fragments n for $vMTU$ size is $n = \lceil L/(vMTU - 20) \rceil$.

In virtual machine environment packet fragment payloads $P_{3,1}, ..., P_{3,N-1}$ should be multiple of eight bytes. Depending on the segment size L, we have number of frames $Frame_{\#} = n$. Decreasing the $vMTU$ parameter increases the number of fragment packets and the overhead, but the dependence is nonlinear. The higher is the number of fragments, the higher becomes the overhead and the lower is the efficiency of the communication.

Measurements and evaluation

Our FFTM file transfer application based on UDP transport layer mechanism has no flow management integrated, but includes segment check algorithm to detect errors on the level of segment delivery. The server module of FFTM was running on a high capacity virtual machine and the client was Ubuntu physical machine. The NIC card type of the supervisor machine and of the client was IEEE 802.3z. We downloaded binary file with $FS =$ 100 MB size from the server in each of 112 different measurement cases. At each segment chunk we used sequence number and error detection code. In this right, the real segment size becomes $L = 12 + S$.

Values of the three ortogonal parameters were: $vMTU \in \{1500, 1244, 996, 748\}$, $Bw/Gbps(\%) \in \{50, 80, 90, 95\}$, $S \in \{1k, 2k, 5k, 10k, 20k, 40k, 60k\}$. In each measurement case we collected with tcpdump application the arrival time stamp $t[i], i = 1, \ldots, N$ and size $F[i], i = 1, \ldots, N$ of every Ethernet frame at the Ubuntu client.

It was found that the transmission ratio of file bytes influences the error rate of the content delivery. Because of overhead bytes added to the protocol data unit during the fragmentation and encapsulation, congestion appears in the datalink layer channel. Congestion on the DLL channel makes the total time delivery of the file to become larger than the expected time. Detection of congestion appearance on the DLL channel we made by multiresolution analysis. Wavelets were used to detect periodic events in different time scales and moments. The found traffic patterns in time made possible to group UDP

streams in binary classes of the datalink layer for selected sampling time intervals. Recurrent neural network is created by supervised learning process to classify the DLL channel traffics.

Keywords: Big Data, fast file transfer, Transmission Control Protocol, User Datagram Protocol, wavelet, Recurrent Neural Network, Long-Short Term Memory, time series classification

References

[1] M. BAGNULO: *Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses*, in: INTERNET STANDARD RFC 6181, 2011.

[2] M. CAMELO, ET AL.: *Detection of traffic patterns in the radio spectrum for cognitive wireless network management*, IEEE Xplore (2020).

[3] N. ELGENDY, A. ELRAGAL: *Big Data Analytics: A Literature Review Paper*, in: Perner P. (eds) Advances in Data Mining. Applications and Theoretical Aspects. ICDM 2014. Lecture Notes in Computer Science, vol. 8557, Cham: Springer, 2014.

[4] A. FORD: *Architectural Guidelines for Multipath TCP Development*, in: INTERNET STANDARD RFC 6182, 2011.

[5] R. LEE, T. LUO, Y. HUAI, F. WANG, Y. HE, X. ZHANG: *Ysmart: Yet Another SQL-to-MapReduce Translator*, in: IEEE International Conference on Distributed Computing Systems (ICDCS), 2011, pp. 25–36.

[6] B. MA, B. YANG, Z. ZHANG, J. ZHANG: *Modelling Mobile Traffic Patterns Using A Generative Adversarial Neural Networks*, IEEE Xplore (2020).

[7] B. W. MEISTER, P. A. JANSON, L. SVOBODOVA: *Connection-Oriented Versus Connectionless Protocols: A Performance Study*, IEEE Transactions on Computers C34/12 (1985), pp. 1164–1173.

[8] S. THOMBRE: *Modelling of UDP throughput*, IEEE Xplore (2017).

Development of a Man-in-the-Middle Attack Device for the CAN Bus

András Gazdag[a], Csongor Ferenczi[b], Levente Buttyán[c]

[a]CrySyS Lab, BME-HIT
agazdag@crysys.hu

[b]CrySyS Lab, BME-HIT
csferenczi@crysys.hu

[c]CrySyS Lab, BME-HIT
buttyan@crysys.hu

Modern vehicles are full of embedded controllers called ECUs (Electronic Control Units). They are responsible for different functionalities involving processing information from sensors and controlling actuators. To perform their functions, ECUs also need to communicate with each other. Most vehicles use a Controller Area Network (CAN) for the communication. The CAN bus is a broadcast channel where messages with a simple format can be transmitted. Due to this architecture, a vehicle can be considered a highly distributed system where important information is sent through an internal network.

The original design of the CAN bus was focusing on safety and reliability properties. Security was not an issue because these networks were considered to be isolated systems. These assumptions were correct for a long time, but not anymore. Modern vehicles have many interfaces towards the outside world, which renders the internal network accessible to an attacker[1] [3]. Bluetooth, Wifi, wireless TPMS, or the OBD (on-board diagnostics) port are all options for attackers to either directly access the CAN network or compromise a component attached to it [4].

As the CAN bus implements a broadcast channel, any message sent over it is received by every ECU attached to the CAN. The ECUs then decide based on a CAN ID field in the message if they need to act upon it or not. However, as messages are not authenticated in any way, it is possible to inject fake messages, or potentially, to modify messages on the CAN, and hence, forcing some ECUs to act upon these fake messages, which may influence the overall behavior of the vehicle.

In an injection attack, extra messages are added to the regular traffic. The original messages and the injected messages could appear identical and the increased frequency of messages may influence the behavior of the ECUs that react on these messages. It is relatively easy both to execute and to detect an injection attack[2].

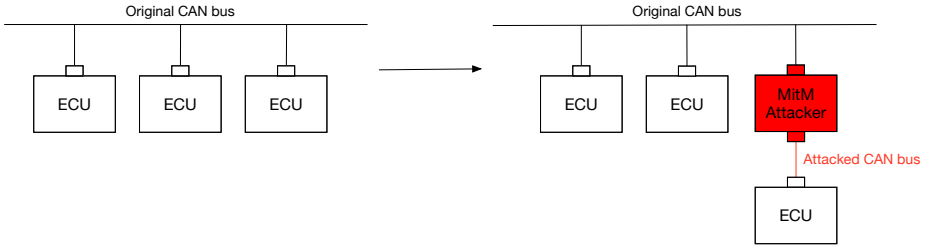


Figure 1: Network architecture change due to a Man-in-the-Middle attack.

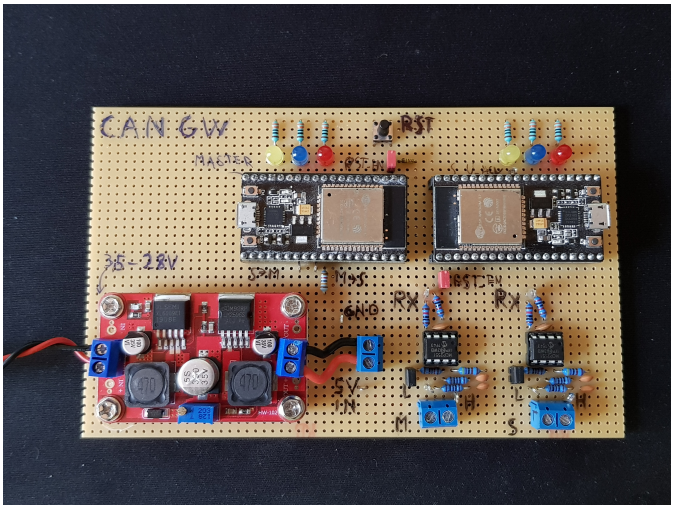


Figure 2: Proof-of-concept attacker device.

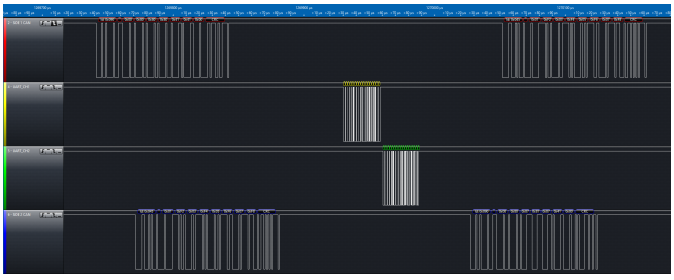


Figure 3: CAN delay measurement.

Modification attacks are more complex both to carry out and to detect. The main difficulty of modification attacks is that the sender checks whether the transmitted bits correctly appear on the bus or not due to safety concerns. The only way to circumvent this protection is to physically separate the sender and the attacked ECU on the CAN bus. This can be achieved with a physical layer Man-in-the-Middle attack. In this scenario an additional hardware component is installed in front of the attacked ECU to separate it from the original CAN bus (see Figure 1).

We built a proof-of-concept hardware device (see Figure 2) capable of modifying the CAN traffic in real-time to show that this attack is possible. It has two CAN interfaces and a microcontroller to read messages from the original CAN bus and either just forward or modify-and-forward traffic to the attacked CAN bus. We showed with measurements (see Figure 3) that we can perform a message modification attack while keeping the introduced delay, within what is allowed by the CAN specification.

Keywords: Vehicle Security CAN Man-in-the-Middle Attack

References

[1] S. CHECKOWAY, D. MCCOY, B. KANTOR, D. ANDERSON, H. SHACHAM, S. SAVAGE, K. KOSCHER, A. CZESKIS, F. ROESNER, T. KOHNO: *Comprehensive experimental analyses of automotive attack surfaces*, in: Proceedings of the 20th USENIX Conference on Security, 2011.

[2] A. GAZDAG, D. NEUBRANDT, L. BUTTYÁN, Z. SZALAY: *Detection of Injection Attacks in Compressed CAN Traffic Logs*, in: Security and Safety Interplay of Intelligent Software Systems. CSITS 2018, ISSA 2018. Ed. by SECURITY, I. 2. SAFETY INTERPLAY OF INTELLIGENT SOFTWARE SYSTEMS. CSITS 2018, 2019.

[3] K. KOSCHER, A. CZESKIS, F. ROESNER, S. PATEL, T. KOHNO, S. CHECKOWAY, D. MCCOY, B. KANTOR, D. ANDERSON, H. SNACHM, S. SAVAGE: *Experimental security analysis of a modern automobile*, in: 2010 IEEE Symposium on Security and Privacy, 2010.

[4] C. MILLER, C. VALASEK: *Adventures in Automotive Networks and Control Units*, tech. rep., IOActive Labs Research, 2013.

A Review on Latest Trends in Non-Technical Loss Detection

Khawaja MoyeezUllah Ghori[ab], Muhammad Awais[c], Akmal Saeed Khattak[d], Muhammad Imran[e], Rabeeh Ayaz Abbasi[f], László Szathmáry[g]

[a]Department of Computer Science, National University of Modern Languages, NUML, Islamabad, Pakistan
mghouri@numl.edu.pk

[b]University of Debrecen, Doctoral School of Informatics Debrecen, Hungary

[c]Department of Computer Science, Edge University, Ormskirk , United Kingdom
mawais@ieee.org

[d]Department of Computer Sciences, Quaid-i-Azam University, Islamabad, Pakistan
akhattak@qau.edu.pk

[e]College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia
dr.m.imran@ieee.org

[f]Department of Computer Sciences, Quaid-i-Azam University, Islamabad, Pakistan
rabbasi@qau.edu.pk

[g]University of Debrecen, Faculty of Informatics, Department of IT, Debrecen, Hungary
szathmary.laszlo@inf.unideb.hu

An increasing interest in digging out the consumption patterns in power and energy sector is observed globally. This includes electrical, gas and water supply industries. A reason behind analyzing the consumption patterns is the detection of fraudulent attempts which are made for the reduction of bill payments. In case of electricity, these attempts are made by reversing the meters, by-passing or slowing down the meters or inaccurate readings. The detection of theft attempts in power industry is termed as Non-Technical Loss (NTL) detection. With the increasing demand of electricity, the occurrences of NTL has been reported globally including India, Pakistan, Brazil and China etc. In this paper, we first describe an interesting characteristic of class imbalance that the dataset used in NTL detection exhibit. Then, we present a thorough review about the recent techniques used in the detection of NTL including machine learning classifiers, deep learning and hardware oriented techniques. Moreover, we introduce the synthesized and the real datasets that have been used in NTL detection. Lastly, we discuss the need for a relative comparison of classical machine learning and deep learning over a benchmark dataset for NTL detection.

Introduction

Recently, an increasing interest has been observed in recognizing the consumption patterns of the consumers of electricity, gas and water supplies [7]. One of the main objectives of this activity is to identify and forecast the potential theft attempts in order to have reduced bills. This illegal theft attempt has dented the economies of many countries causing a loss of billions of dollars. This includes China [5], Pakistan [4], India, Brazil [6], etc.

Non-Technical Loss (NTL) detection in electric power industry is a term used for the detection of faulty meters or illegal usage of electric units. Losses are bore by the electric supply companies on the account of faulty meters that record less units as compared to the consumed electricity. On the other hand, this practice can also be intentional in order to get the reduced bill. For both cases, the supplier companies look for a solution which can identify them the faulty meters or potential theft instances.

One of the important characteristics of the relevant datasets is that the dataset belongs to the class imbalance problem. It is the problem where the dataset is biased towards one class by its heavy representation while the other class is less representative. Interestingly, the problem becomes more challenging when the focus is on the true representation of the less representative class. Naturally, the number of normal electric consumption in a neighborhood is huge as compared to the number of theft attempts. This gives a clear indication that the real dataset of the consumption of electricity belongs to the class imbalance problem where the number of negative class samples is huge as compared to the number of positive class samples. The techniques used in NTL detection should be able to balance out the positive and negative class samples before the dataset is used by the machine learning algorithms [3].

One of the techniques used to identify the NTL is applying classical machine learning algorithms to the datasets pertaining to the consumption of electricity. This includes the use of Support Vector Machine (SVM), KNN, decision trees, ensemble methods and neural networks [2]. Advances in deep learning has attracted some researchers to test deep learning for NTL detection. For e.g., the authors of [1] have used deep neural networks along with long short-term memory network to identify the occurrences of NTL in a dataset pertaining to the smart meters of a utility company in Spain. However there is still a need to compare the performances of the classical machine learning algorithms with the different variants of deep learning architecture. In this paper, we focus on elaborating the importance of a comparative study of the two paradigms for NTL detection in a real dataset.

Keywords: Review, Non-Technical Loss Detection, NTL Detection, Data mining, Machine Learning, Classification Algorithms, Supervised Learning, Boosting

References

[1] M. M. BUZAU, J. TEJEDOR-AGUILERA, P. CRUZ-ROMERO, A. GOMEZ-EXPOSITO: *Hybrid deep neural networks for detection of non-technical losses in electricity smart meters*, IEEE Transactions on Power Systems 35.2 (2019), pp. 1254–1263.

[2] K. M. GHORI, R. A. ABBASI, M. AWAIS, M. IMRAN, A. ULLAH, L. SZATHMÁRY: *Performance analysis of different types of machine learning classifiers for non-technical loss detection*, IEEE Access 8 (2019), pp. 16033–16048.

[3] K. M. GHORI, A. R. AYAZ, M. AWAIS, M. IMRAN, A. ULLAH, L. SZATHMÁRY: *Impact of Feature Selection on Non-technical Loss Detection*, in: 2020 6th Conference on Data Science and Machine Learning Applications (CDMA), IEEE, 2020, pp. 19–24.

[4] K. M. GHORI, M. IMRAN, A. NAWAZ, R. A. ABBASI, A. ULLAH, L. SZATHMÁRY: *Performance analysis of machine learning classifiers for non-technical loss detection*, Journal of Ambient Intelligence and Humanized Computing (2020), pp. 1–16.

[5] W. HU, Y. YANG, J. WANG, X. HUANG, Z. CHENG: *Understanding Electricity-Theft Behavior via Multi-Source Data*, arXiv preprint arXiv:2001.07311 (2020).

[6] J. A. MEIRA, P. GLAUNER, R. STATE, P. VALTCHEV, L. DOLBERG, F. BETTINGER, D. DUARTE: *Distilling provider-independent data for general detection of non-technical losses*, in: Power and Energy Conference at Illinois (PECI), 2017 IEEE, IEEE, 2017, pp. 1–5.

[7] Q. A. AL-RADAIDEH, M. M. AL-ZOUBI: *A data mining based model for detection of fraudulent behaviour in water consumption*, in: 2018 9th International Conference on Information and Communication Systems (ICICS), IEEE, 2018, pp. 48–54.

Virtual spaces connected to the first National Theater of Hungary*

Attila Gilányi[a], Anna Rácz[b], Anna Mária Bólya[c], János Décsei[d], Katarzyna Chmielewska[e]

[a]Faculty of Informatics, University of Debrecen
gilanyi.attila@inf.unideb.hu

[b]Faculty of Informatics, University of Debrecen
racz.anna@outlook.com

[c]Inst. for Training Choreographers and Dance Pedagogues, Hungarian Dance Academy
info@bolyaannamaria.hu

[d]Faculty of Informatics, University of Debrecen
dejata@gmail.com

[e]Institute of Mathematics, Kazimierz Wielki University
katarzyna.chmielewska@ukw.edu.pl

In this talk, we present some results connected to virtual models of the first National Theater of Hungary. Our work is strongly connected to a general project at the Virtual Reality Laboratory of the Faculty of Informatics of the University of Debrecen. The aim of this project is to prepare virtual models of buildings and monuments, which are not accessible, or do not exist in their original form. A significant feature of our activity in the project is authenticity: all the important elements in our spaces are shown in the shape and form as they are (or as they were) in reality (cf., e.g., [3]).

The original building of the first National Theater of Hungary stood in Kerepesi street in Pest (now Rákóczy street in Budapest), Hungary. It was constructed in 1837. In the beginning, it was called Pest Hungarian Theater (in Hungarian, Pesti Magyar Színház), but, due to a decision of the Hungarian Parliament in 1840, it became the (first) National Theater of the country and was renamed accordingly. It played a crucial role in the cultural life of Hungary that time. Until 1884 (when the Hungarian Royal Opera House was opened), it was the venue for ballet and opera performances as well. The building does not exist today. Unfortunately, there are no detailed architectural plans for the building, therefore, the construction of its three-dimensional model is based on contemporary information (descriptions, pictures) and, in some cases, also on analogies to other similar theater buildings.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was co-financed by the Hungarian Government and the European Social Fund.
This research is connected to the research projects Aurora 1 and Aurora 2,'The Birth of Hungarian Ballet', supported by the Hungarian Academy of Arts, Research Institute of Art Theory and Methodology.
The research described in this paper has partially been performed in the Virtual Reality Laboratory of the Faculty of Informatics of the University of Debrecen, Hungary.

We developed two different models of the theater building. One of them was implemented in the platform MaxWhere (cf. `https://store.maxwhere.com`), while the other one can be used in the engine Unity (`https://unity.com/`). In our talk we point out the advantages of the applications of these models and we describe some essential differences between them (cf., also, [4], [5], [8], and [9]).

Recent investigations (cf., e.g., the papers [1], [2], [6], [7] and the references therein) show that MaxWhere can be very effectively used as an educational and presentation interface. Our virtual space developed in this system strongly uses these advantages. The space can be used as an educational, a general presentation, as well as, a collaboration room. It contains so called webtables (with other names web boards, or smart boards), which are typical components of MaxWhere spaces. They can be used to present two-dimensional information (text, pictures, videos, etc.) available on the users computer or on the internet. The most important advantage of this space is, that users can very easily (and without any special computer skills) upload the contents of these boards. Additionally, the spaces constructed in such a manner can be used on computers with weaker hardware as well. (We will present further details about this construction in our talk.)

Our model in Unity can be used with virtual reality headsets and also on a screen of a computer. Obviously, it has stronger hardware requirements, than the other version. In this space, we also created a virtual exhibition based on very recent research results on the beginning of Hungarian ballet. It mainly presents objects and documents related to the first Hungarian prime ballerina and choreographer, Emília Aranyváry.

In our talk, we will present some details about our very positive experiences in connection with the application of our spaces as presentation rooms and as educational tools connected to research of dance history and dance education in Hungary. In the future, we plan to test their possible applications in international cooperation with Macedonian, Polish and Slovakian dance higher educational institutions, as well.

Keywords: Virtual Reality; 3D Visualization; Virtual Reconstruction; Presentation of Data and Information in Virtual Spaces; MaxWhere; National Theater of Hungary.

References

[1] B. BERKI: *Better memory performance for images in MaxWhere 3D VR space than in website*, in: 2018 9th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2018, pp. 281–284.

[2] B. BERKI: *Does effective use of MaxWhere VR relate to the individual spatial memory and mental rotation skills?*, Acta Polytechnica Hungarica 16.6 (2019), pp. 41–53.

[3] A. GILÁNYI, A. RÁCZ, M. BÁLINT, K. CHMIELEWSKA: *Virtual Reconstruction of Historic Monuments*, in: 9^{th} IEEE Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2018, pp. 341–345.

[4] A. GILÁNYI, A. RÁCZ, A. M. BÓLYA, K. CHMIELEWSKA: *Early History of Hungarian Ballet in Virtual Reality*, in: 10^{th} IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2019, pp. 193–198.

[5] A. GILÁNYI, A. RÁCZ, A. M. BÓLYA, J. DÉCSEI, K. CHMIELEWSKA: *A presentation room in the virtual building of the first National Theater of Hungary*, in: 11^{th} IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2020, pp. 519–523.

[6] I. HORVÁTH, A. SUDÁR: *Factors Contributing to the Enhanced Performance of the MaxWhere 3D VR Platform in the Distribution of Digital Information*, Acta Polytechnica Hungarica 15 (2018), pp. 149–173.

[7] B. LAMPERT, A. PONGRÁCZ, J. SIPOS, A. VEHRER, I. HORVÁTH: *MaxWhere VR-learning improves effectiveness over clasiccal tools of e-learning*, Acta Polytechnica Hungarica 15 (2018), pp. 125–147.

[8] A. RÁCZ, A. GILÁNYI, A. M. BÓLYA, K. CHMIELEWSKA: *A Virtual Exhibition on the History of Hungarian Ballet*, in: 10^{th} IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2019, pp. 431–432.

[9] A. RÁCZ, A. GILÁNYI, A. M. BÓLYA, J. DÉCSEI, K. CHMIELEWSKA: *On a Model of the First National Theater of Hungary in MaxWhere*, in: 11^{th} IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2020, pp. 575–576.

Attacking the IEC 60870-5-104 protocol*

Péter György[a], **Tamás Holczer**[b]

[a]BME HIT CrySyS Lab, pgyorgy@crysys.hu

[b]BME HIT CrySyS Lab, holczer@crysys.hu

In European power systems IEC 60870-5-104 protocol is widely used for telecontrol. This protocol is known to be insecure. In this paper we show how vulnerable this protocol is.

Introduction

In European power systems IEC 60870-5-104 (IEC-104 for short) is widely used for telecontrol. The protocol doesn't specify security requirements, and is not using any technique to protect the transmitted packets.

In this paper our goal was to identify the possible pitfalls of the protocol and show the consequences of using an insecure protocol in critical infrastructure.

The remainder of this paper is organized as follows. Section is a short introduction to the packet structure of IEC-104. In Section we describes our environment used for testing and our attack scenarios. Section evaluates the attack scenarios. Finally Section summarizes our work.

IEC-104

The IEC-104 protocol is following the client/server model. It comes with predefined commands, that can be used for monitoring and controlling. In most cases the server is gathering information about its environment using sensors (for example voltage and current values at a substation). Each information has it's own unique identifier called Information Object Address (IOA). The client can send read, write or other requests to the server.

The structure of most of the packets is as follows. First there is the Application Protocol Control Information (APCI), then comes the Application Service Data Unit (ASDU). The APCI has information about the message length, and it also tracks the sequence numbers. The ASDU contains the ID of the command, the necessary identifiers and also contains command specific information.

A more detailed description and analysis of the protocol can be found in [1].

*This work was partially performed in the frame of the FIEK_16-1-2016-0007 project, implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the FIEK_16 funding scheme

Attacking the protocol

To test the security of the protocol and carry out attacks against it, we needed a test environment with a client and a server communicating using IEC-104. The client and the server was virtualized in vCenter. We choose to use the OpenMUC[1] implementation of the protocol on virtual machines. We also built a lightweight website to visualize the values of each IOA. In our test environment the client controls and monitors a small power grid and monitors the values of the IOAs. After setting up a simulated environment we can proceed to the attacks.

We designed multiple attack scenarios starting from simple Denial of Service (DoS) attacks to more complex Man in the Middle (MitM) attacks.

Unauthorized access

The protocol lacks authentication therefore an attacker can connect to a server and send commands. For example an attacker could send an interrogation command to learn the IOAs used by the server.

Tampering with IEC APCI sequence numbers

An unexpected sequence number in the APCI field of the packet results in the termination of the connection. This behaviour can be used to cause DoS. An attacker can exploit this behaviour in two ways:

- If the attacker is in MitM position, then they can change the packets that pass through.
- The attack can craft a malicious IEC packet with an unexpected sequence number and send it to one of the communicating parties.

Poison TCP stream

The communication is carried out in a single TCP stream which is constantly kept alive. If the attacker can modify or insert a packet with an incorrect TCP sequence number, or send a FIN in the name of a valid party then the communication is terminated. This behaviour can be used to cause DoS.

Packet injection

An attacker can inject packets to the communication, however simply injecting a packet will result in the termination of the connection, because it will cause a sequence number (both APCI and TCP) miss-match between the server and the client. Therefore after injecting a packet the attacker needs to patch the sequence number of every other packets. Not just the sequence number can be modified but also the values of the ASDU field. Therefore

[1] `https://www.openmuc.org/iec-60870-5-104/`

this can lead to take over the control of the power grid. An attacker needs to be in MitM position to carry out this attack.

Evaluation

The difficulty of detection and the severity of the attacks described in Section is different.

The attack described in section has a very high severity because the attacker can send arbitrary command to the server. New connections are logged by the server therefore it is easy to detect this attack.

The attacks described in section and are similar. The severity of these attack is medium because they can prevent the client from controlling the server.

The attack described in section has a critical severity because the attacker can send arbitrary command and can also stop the client from communicating with the server. No log message is generated during the course of this attack, therefore the detection is also hard.

Summary and future work

We created and carried out multiple attacks against the IEC-104 protocol and showed the possible consequences of using an insecure protocol.

There is still a lot to do, because to achieve full control the attacker also needs to know the IOA of each station in the grid. Therefore we will work on an algorithm that can make these pairings in the future.

Keywords: IEC 6087-5-104, Offensive security, Man-in-the-Middle, Power Systems

References

[1] P. MATOUŠEK: *Description and analysis of IEC 104 Protocol*, Faculty of Information Technology, Brno University of Technology, Tech. Rep (2017).

Cryptanalysis of ITRU

Hayder Raheem Hashim[a], Alexandra Molnár[a], Szabolcs Tengely[a]

[a]Institute of Mathematics, University of Debrecen
hashim.hayder.raheem@science.unideb.hu, alexandra980312@freemail.hu, tengely@science.unideb.hu

In 1996, Hoffstein, Pipher and Silverman [4] proposed a class of fast public key cryptosystems called NTRU (N^{th} degree Truncated Polynomial Ring) cryptosystem, which was published in 1998. This cryptosystem is considered as a lattice-based public key cryptosystem, and it is the first asymmetric cryptosystem based on the polynomial ring $\frac{\mathbb{Z}[X]}{(X^N-1)}$. Indeed, it has very good features comparing to other public key cryptosystems such as reasonably short, easily created keys, high speed, and low memory requirements. Its encryption and decryption procedures rely on a mixing system presented by polynomial algebra combined with a clustering principle based on elementary probability theory. From its lattice-based structure, the security of the NTRU cryptosystem is based on the hardness of solving the Closest Vector Problem (CVP), which is a computational problem on lattices closely related to Shortest Vector Problem (SVP) and considered to be NP hard (non-deterministic polynomial-time hardness) (for more details, see [5] and the references given there).

One of the known variants of NTRU cryptosystem called ITRU cryptosystem, which was presented in 2017 by Gaithuru, Salleh, and Mohamad [3]. Instead of working in a truncated polynomial ring, ITRU cryptosystem is based on the ring of integers. The parameters and the main steps of ITRU cryptosystem are as follows.

- The value of p is the small modulus (an integer).
- Random integers f, g and r are chosen such that f is invertible modulo p.
- A prime q is fixed satisfying $q > p \cdot r \cdot g + f \cdot m$, where m is the representation of the message in decimal form. The suggested conversion is based on $ASCII$ conversion tables, that is the one with $a \to 97$.
- One computes $F_p \equiv f^{-1} \pmod{p}$ and $F_q \equiv f^{-1} \pmod{q}$. These computations can be done by using the extended Euclidean algorithm.
- The public key is consisted of h and q such that $h \equiv p \cdot F_q \cdot g \pmod{q}$.
- The encryption procedure is similar to the one applied in NTRU cryptosystem [4], one generates a random integer r and computes $e \equiv r \cdot h + m \pmod{q}$.
- To get the plaintext from the ciphertext one determines $a \equiv f \cdot e \pmod{q}$.
- Recovering the message is done by computing $F_p \cdot a \pmod{p}$.

The authors claimed that ITRU has better features comparing to the classical NTRU, such as having a simple parameter selection algorithm, invertibility, and successful message decryption, and better security.

In this paper, we present an attack technique against the ITRU cryptosystem, it is mainly based on a simple frequency analysis. As a result, this techniques will recover the corresponding plaintexts immediately with no need of having the private keys. The attack is via eavesdropping on some encrypted messages. If the message is too short, then the attack may fail. Moreover, according to the index of coincidence introduced by Friedman [2] the language of the plaintext may be identified (e.g., in case of English it is about 0.0686). Therefore, once we identify the language correctly, then the frequency analysis works very well in practice. Friedman [1] claimed that 'practically every example of 25 or more characters representing monoalphabetic encipherment of a "sensible" message in English can be readily solved. In case of ITRU careful parameter selection may yield a few groups (that can be identified) for which frequency analysis can be applied.

Keywords: NTRU, ITRU

References

[1] W. F. FRIEDMAN: *Codes And Ciphers (CRYPTOLOGY)*, Encyclopaedia Britannica (1956), pp. 1–8, URL: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_535/41772109081119.pdf.

[2] W. F. FRIEDMAN: *The index of coincidence and its applications in cryptography*, Department of Ciphers. Publ 22. Geneva, Illinois, USA: Riverbank Laboratories, 1922.

[3] J. N. GAITHURU, M. SALLEH, I. MOHAMAD: *ITRU: NTRU-Based Cryptosystem Using Ring of Integers*, International Journal of Innovative Computing 7.1 (2017).

[4] J. HOFFSTEIN, J. PIPHER, J. H. SILVERMAN: *NTRU: A ring-based public key cryptosystem*, English, in: Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings, Berlin: Springer, 1998, pp. 267–288, ISBN: 3-540-64657-4.

[5] D. MICCIANCIO: *Closest Vector Problem*, in: Encyclopedia of Cryptography and Security, ed. by H. C. A. VAN TILBORG, Boston, MA: Springer US, 2005, pp. 79–80, ISBN: 978-0-387-23483-0, DOI: https://doi.org/10.1007/0-387-23483-7_66.

Digit Expansions for Efficient Group Operations*

Clemens Heuberger[a]

[a]Department of Mathematics, University of Klagenfurt, Austria
clemens.heuberger@aau.at

Elliptic curve cryptography, among others, relies on the efficient computation of scalar multiples nP of a given point P on the curve; sometimes, also linear combinations $n_1P_1 + \cdots + n_kP_k$ are of interest.

The standard approach is to compute nP by the *double-and-add method*: the binary expansion $n = \sum_{j=0}^{\ell-1} \varepsilon_j 2^j$ is used to compute nP by Horner's scheme:

$$nP = 2(2 \dots (2(2\varepsilon_{\ell-1}P + \varepsilon_{\ell-2}P) + \varepsilon_{\ell-3}P) + \cdots + \varepsilon_1 P) + \varepsilon_0 P.$$

This requires $\ell - 1$ doublings on the curve plus one addition of P for every non-zero digit ε_j for $0 \le j < \ell - 1$ as the addition of $\varepsilon_j P$ can be skipped whenever $\varepsilon_j = 0$. The number of non-zero digits is called the *Hamming weight* of the expansion.

Morain and Olivos [2] proposed to use signed digit expansions, i.e. binary expansions with digits 0 and ± 1. In general, an integer has several signed binary expansions, so the redundancy can be used to decrease the Hamming weight but keeping the length mostly fixed. This entails also adding $-P$ on the curve, which is as expensive as adding P on the curve and thus does not cause any problems.

Reitwiesner [4] showed that every integer has exactly one *non-adjacent form (NAF)*, i.e. a signed binary expansion where out of two consecutive digits, at least one is zero. He also showed that the NAF minimises the Hamming weight over all signed binary expansions of the same integer.

Several generalisations with larger digit sets have been analysed which mostly fall into the class of *sliding window methods* where at most one non-zero digit is admitted in every block of w consecutive digits (where larger w require larger digit sets); see Phillips and Burgess [3] for a rather general system. The larger digit sets come at the cost of precomputing εP for all non-zero digits ε (but out of a pair εP, $-\varepsilon P$ only one needs to be precomputed).

For linear combinations, it is advantageous to consider *joint expansions* and add precomputed linear combinations in every step, see Straus [5].

Another alternative to speed up the computations is the use of other curve endomorphisms instead of doubling. For instance, using the Frobenius endomorphism of an elliptic curve over a finite field of characteristic p (sending pairs (x, y) to (x^p, y^p)) is very efficient; this corresponds to digit expansions with complex roots. This has first been proposed by Koblitz [1].

*This research was supported by the Austrian Science Fund (FWF): P 28466-N35.

This talk will give an overview of results in the areas outlined above. We will consider questions of optimality for syntactically defined digit sets (such as the NAF) and their asymptotic analysis.

Keywords: elliptic curve cryptography, digit expansion, addition chains

References

[1] N. KOBLITZ: *CM-curves with good cryptographic properties*, in: Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991), ed. by J. FEIGENBAUM, vol. 576, Lecture Notes in Comput. Sci. Berlin: Springer, 1992, pp. 279–287,
DOI: https://doi.org/10.1007/3-540-46766-1_22.

[2] F. MORAIN, J. OLIVOS: *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. 24 (1990), pp. 531–543, ISSN: 0988-3754,
URL: http://www.numdam.org/item?id=ITA_1990__24_6_531_0.

[3] B. PHILLIPS, N. BURGESS: *Minimal Weight Digit Set Conversions*, IEEE Trans. Comput. 53 (2004), pp. 666–677,
DOI: https://doi.org/10.1109/TC.2004.14.

[4] G. W. REITWIESNER: *Binary Arithmetic*, in: Advances in Computers, Vol. 1, Academic Press, New York, 1960, pp. 231–308,
DOI: https://doi.org/10.1016/S0065-2458(08)60610-5.

[5] E. G. STRAUS: *Addition chains of vectors (Problem 5125)*, Amer. Math. Monthly 71 (1964), pp. 806–808.

The unique potential of virtual reality in enhancing the ways in which humans communicate through communications technologies

Ildikó Horváth[a]

[a]Széchenyi István University, Győr, Hungary
horvath.ildiko@sze.hu

In this paper, our goal is to show from various perspectives that virtual reality holds a unique potential in enhancing the ways in which humans communicate through communications technologies. Based on a theoretical perspective from the field of cognitive infocommunications and through specific analyses of user performance on the MaxWhere 3D VR platform, it is argued that the widespread view of VR as a technology primarily for realism and immersion is based on a misunderstanding. Rather, VR represents a breakthrough approach in using 3D spatial metaphors for communication – a language which human brains have evolved to understand at a fundamental level.

In this paper, we explore what may be missing from the common view of VR today and how we believe it may still become a breakthrough technology. Our analysis is provided based on current trends in VR-based education, and through the lens of the relatively young scientific field of cognitive infocommunications (CogInfoCom) [1, 3, 7].

Cognitive infocommunications [1, 3, 7] is a relatively young field of science established in 2010. On the one hand, the key motivation behind the field is to analyze how humans are co-evolving – and even merging together with communication technologies both at a physiological and cognitive level. At the same time, the field also aims to create (synthesize) new technologies that facilitate this co- evolution so that communication can be more effective [3].

As detailed in [1], virtual reality is a key platform for CogInfoCom by virtue of its being a 3D spatial technology. Humans are naturally accustomed to seeing the world and dealing with concepts in 3 dimensions, as a result of which VR can be not only a natural extension, but also a completely viable augmentation of current communication technologies.

Our analysis suggests that while VR has often been conceived of as primarily a platform for entertainment, the technology itself is increasingly making its way into work and education-related environments. What we are seeing is that VR is increasingly allowing users to better connect to events happening remotely, and to access more information in a shorter amount of time [2, 6]. As the practical side of VR is being discovered, the gaming technologies of the past are becoming the teaching, learning and collaborative tools of the future. In fact, a growing number of educational institutions worldwide are looking to

enhance their e-learning content through VR [4, 5, 8].

MaxWhere (http://maxwhere.com) is a 3D VR platform that runs on Windows and Mac OS. MaxWhere allows users to download 3D spaces – much like 3D apps from an application store – and to enter those spaces and manipulate and share both 2D and 3D content inside them. Although the MaxWhere store provides a wide variety of 3D spaces, they are mostly organized into the categories of "Office" spaces, "Presentation" spaces and "Education" spaces.

MaxWhere's spaces are structured like 2D web pages, only in 3D. Each space consists of a hierarchy of nodes, all of which can have a position, orientation and appearance. Further, events can be defined and handled in customizable ways for each node, so that a click of the mouse on an object, or the mouse being hovered over an object can trigger changes in the space – whether it be changes in its configuration or in its appearance.

One unique type of object in MaxWhere spaces is referred to as the smartboard. Smartboards are 2D browsers which are located in a 3D space and which are implemented through MaxWhere's Browser23 (B23) technology. B23 represents a new philosophy towards web surfing: instead of forcing users to place a limited number of tabs side by side, limiting their options in switching between them and finding the right ones at the right time, it allows browser windows to be laid out in 3D space, grouped by topic and scaled in size by importance.

More recently, the team behind MaxWhere developed the Ultra Sharing (USharing) technology, which enables users to create VR offices containing a large number of documents and even complete project workflows, and to then share those offices with a single click.

Last but not least, it is important to mention MaxWhere's unique 3D navigation technology called the Cognitive Navigation (CogiNav) technology. CogiNav introduces a context-dependent solution for navigation, allowing users to update their location and orientation in an intuitive way, even with only a very simple input device – such as an everyday 2D mouse – at their disposal.

Research shows that the combination of the B23, USharing and CogiNav technologies allow for a highly effective way to visualize, share and work on large amounts of information while maintaining a low cognitive workload – a huge asset for understanding, configuring and managing large-scale networked digital ecosystems.

In this paper, we explored what may be missing from the common view of VR today and how we believe it may still become a breakthrough technology. Our analysis is provided based on current trends in VR-based education, and through the lens of the relatively young scientific field of cognitive infocommunications. The key message of the paper is that there is much to analyze about VR when it is used in practical tasks, and findings in these analyses can in turn inspire immensely powerful new applications that would be impossible to imagine without VR.

Keywords: CogInfoCom, VR technology, human-ICT co-evolution

References

[1] P. BARANYI, Á. CSAPÓ: *Definition and synergies of cognitive infocommunications*, Acta Polytechnica Hungarica 9.1 (2012), pp. 67–83.

[2] P. BARANYI, Á. CSAPÓ: *Special issue on multimodal interfaces in cognitive infocommunication systems*, Journal on Multimodal User Interfaces 8.2 (2014), pp. 119–120.

[3] P. BARANYI, Á. CSAPÓ, G. SALLAI: *Cognitive Infocommunications (CogInfoCom)*, Springer, 2015.

[4] B. BERKI: *Desktop VR as a virtual workspace: a cognitive aspect*, Acta Polytechnica Hungarica 16.2 (2019), pp. 219–231.

[5] L. FREINA, M. OTT: *A literature review on immersive virtual reality in education: state of the art and perspectives*, in: The international scientific conference elearning and software for education, vol. 1, 133, 2015, pp. 10–1007.

[6] I. HORVÁTH, A. SUDÁR: *Factors contributing to the enhanced performance of the MaxWhere 3D vr platform in the distribution of digital information*, Acta Polytechnica Hungarica 15.3 (2018), pp. 149–173.

[7] L. I. KOMLÓSI, P. WALDBUESSER: *The cognitive entity generation: Emergent properties in social cognition*, in: 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2015, pp. 439–442.

[8] J. MARTÍN GUTIÉRREZ, E. M. CARLOS, A. D. BEATRIZ, G. M. ANTONIO: *Virtual technologies trends in education*, EURASIA Journal of Mathematics, Science and Technology Education 13.2 (2017), pp. 469–486.

A Provably Secure Authentication for Smart Homes*

Andrea Huszti[a], **Norbert Oláh**[a]

[a]Department of Computer Science, Faculty of Informatics, University of Debrecen
huszti.andrea@inf.unideb.hu
olah.norbert@inf.unideb.hu

Introduction

The number of IoT devices is constantly increasing, generating huge amount of information at the edge of the network. These sensors, devices and applications often collect our sensitive data. However, there are security problems (e.g. hacked devices, botnets, etc.). In several cases the appropriate security mechanisms are missing within the devices. Therefore, security measures have become a hot topic in the field of IoT. The most essential requirements are secure user-device authentication and confidentiality of sensitive data transferred. Only those with the appropriate access control should be able to retrieve confidential data, which increases the role of authentication. Although there are several types of authentication methods, one of the most widely used practice is still based on short secrets (like password), where the hash of the secrets are usually stored in a central database. In case of server compromise or database leakage, the secrets are vulnerable to theft.

IoT devices are often very vulnerable due to weak protection (weak or default passwords) and poor maintenance. Numerous studies have addressed the security vulnerabilities of IoT devices [5, 8]. Our goal is to reduce these security vulnerabilities. We propose a password-based multiparticipant authentication for smart homes.

By taking advantage of the distributed nature of the IoT system, in our scheme the client's secret key is shared among the smart home devices. Thus, several sensors and devices together verify the correctness of the client password. If one or more devices become compromised or broken, the protocol still provides adequate security. The password is shared among the devices, so attackers need to attack multiple devices in parallel in order to successfully impersonate the client. A smart home generates a lot of sensitive data (security cameras and sensors, smart devices such as refrigerator, washing machine, etc.), thus the confidentiality of data is ensured during the communication between the parties by generating a session key.

In the case of *key agreement*, both entities contribute to the joint secret key by providing information from which the key is derived. A key agreement protocol that provides mutual implicit key authentication is called an *authenticated key agreement* protocol (or

*This research was partially supported by the SETIT Project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme and supported by the European Union.

AK protocol). A key agreement protocol provides key confirmation between two participants where the participants make sure that the other participant possesses the secret key. A protocol that provides mutual key authentication as well as mutual key confirmation is called an *authenticated key agreement with key confirmation* protocol (or an AKC protocol).

In scientific literatures, usually centralized, one-factor [4] or two-factor identity verification protocols [2] are proposed. However, the concept of distributing authentication to multiple devices (sensors, servers, etc.) enhances the security level [7]. The advantage of distributed systems is that external attackers have to attack multiple devices simultaneously to brake the system, which increases the attack cost. Multi-factor authentication can also provide an enhanced level of assurance in higher-security scenarios so if all but one of the factors are revealed, an attacker will not be able to execute a successful attack against the system.

In this proposition [3], a multi-server authentication protocol is designed, where one-time passwords are shared among the cloud servers. A Merkle tree or a hash tree is applied for verifying the correctness of the one-time password. Mazhar Rathore et.al. [6] introduced a novel security protocol that simplifies the pairwise authentication and key exchange among smart home devices. The protocol leverages identity-based cryptography (IBC), thus alleviating the requirement for storing and managing public key certificates. It is crucial that their solution has the scalability attribute. Besides these properties, our proposition also provides a detailed security analysis. Our protocol is also provably secure.

Our protocol is designed typically for smart home environments and considers the properties of these systems like scalability, efficiency, resource constrained environment, moreover there is a central device controlling the other IoT devices. During the design, we put a great emphasis on efficiency, the session key is generated by ECDH key exchange, moreover MAC, xor operations and symmetric encryption are applied. We give necessary description of cryptographic primitives and define the secure authenticated key exchange. For our protocol, we extend the Bellare and Rogaway security model in [1] to prove that our multi-device scheme is secure according to our definition in the threshold hybrid corruption and the random oracle model.

Proof. The proposed protocol is a secure AKC protocol in the random oracle model, assuming MAC is *existentially unforgeable under an adaptive chosen-message attack* and symmetric encryption scheme is *indistinguishable under chosen plaintext attack*, moreover *ECCDH assumption holds* in the elliptic curve group. □

References

[1] S. BLAKE-WILSON, D. JOHNSON, A. MENEZES: *Key agreement protocols and their security analysis*, Proceedings of the sixth IMA International Conference on Cryptography and Coding, LNCS 1355 (1997), pp. 30–45.

[2] N. CHEN, R. JIANG: *Security Analysis and Improvement of User Authentication Framework for Cloud Computing*, Journal of Networks 9.1 (2014), pp. 198–203.

[3] A. HUSZTI, N. OLÁH: *A simple authentication scheme for clouds*, 2016 IEEE Conference on Communications and Network Security (CNS) (2016), pp. 565–569.

[4] M. S. HWANG, L. H. LI: *A new remote user authentication scheme using smart cards*, IEEE Transactions on Consumer Electronics 46.1 (2000), pp. 28–30.

[5] C. KOLIAS, G. KAMBOURAKIS, A. STAVROU, J. VOAS: *DDoS in the IoT: Mirai and other botnets*, Computer 50.7 (2017), pp. 80–84.

[6] R. M. MAZHAR, E. BENTAFAT, S. BAKIRAS: *Smart Home Security: A Distributed Identity-Based Security Protocol for Authentication and Key Exchange*, In: 2019 28th International Conference on Computer Communication and Networks (ICCCN) IEEE (2019), pp. 1–9.

[7] J. SHEN, S. CHANG, J. SHEN, Q. LIU, X. SUN: *A lightweight multi-layer authentication protocol for wireless body area networks*, Future Generation Computer Systems 78 (2018), pp. 956–963.

[8] A. TEJASVI, et AL.: *Consumer IoT: Security vulnerability case studies and solutions*, IEEE Consumer Electronics Magazine 9.2 (2020), pp. 17–25.

Simulation of traffic flow using Markov models*

Márton Ispány[a], Norbert Bátfai[a], Renátó Besenczi[a], Péter Jeszenszky[a], and Máté Szabó[a]

[a]Faculty of Informatics, University of Debrecen, Hungary
ispany.marton@inf.unideb.hu

A mathematically rigorous model is studied for modeling and simulating traffic flow in Smart Cities. The proposed methods and results are corroborated by a case study which is based on a real dataset.

Traffic flow modeling

Important tasks in the theory of intelligent transporting systems (ITS) are the modeling and simulating the movement of vehicles on the road network. By an appropriate model we can understand and handle various traffic problems, e.g., unexpected disaster events. A mathematically rigorous stochastic model that can be used for traffic analysis is proposed in [2] which is based on an interplay between graph and Markov chain theories. In this model, the road network is modeled by a directed graph, the transition probability matrix describes the traffic's dynamic while the unique stationary distribution corresponds to the distribution of the vehicles on the road network. In [1], we propose a new parametrization to this model by introducing the concept of two-dimensional stationary distribution which can handle the traffic's dynamic and the vehicles' distribution at the same time. Using the Markov model, the notion of Markov traffic is introduced on a road graph and its stationary distribution is derived explicitly. Based on trajectories data, the parameters of two-dimensional stationary distribution are estimated by the composite least squares method. An explicit formula is derived for the estimator and a few algorithms are proposed for large-scale problems.

Results

In the talk, the results of some Monte Carlo experiments and a case study are discussed in detail for simulating traffic flow on a given road network. The case study is based on the Taxi Trajectory Prediction (TTP) dataset and the road network data downloaded from the OpenStreetMap (OSM) project, both available publicly. In this real application, we have unfolded and visualized a stationary distribution on the map graph of Porto, Portugal, based on the TTP dataset.

Keywords: Road network, Traffic simulation, Discrete time Markov chain, Stationary dis-

*The publication is supported by the EFOP-3.6.1-16-2016-00022 project. The project is co-financed by the European Union and the European Social Fund.

tribution, Composite least squares estimation

References

[1] R. BESENCZI, N. BÁTFAI, P. JESZENSZKY, R. MAJOR, F. MONORI, M. ISPÁNY: *Large-scale analysis and simulation of traffic flow using Markov models*, tech. rep., arXiv:2007.02681, 2020.

[2] E. CRISOSTOMI, S. KIRKLAND, R. SHORTEN: *A Google-like model of road network dynamics and its application to regulation and control*, International Journal of Control 84.3 (2011), pp. 633–651, DOI: https://doi.org/10.1080/00207179.2011.568005.

Dealing with Uncertainty: a Rough-Set-Based Approach with the Background of Classical Logic*

Tamás Kádek[a], Tamás Mihálydeák

[a]University of Debrecen, Faculty of Informatics
tamas.kadek@inf.unideb.hu
mihalydeak@unideb.hu

Representative-based approximation space

The triple $\langle\, U, R, \mathfrak{R} \,\rangle$ is a *representative-based approximation space* if U is a nonempty set of objects, $R = \{r_1, r_2, \ldots, r_k\}$ where $k \geq 1$ is a set of representatives, and $\mathfrak{R} \subseteq R \times U$ is a relation.

Using the *extensions* of the representatives $\langle\!\langle\, r_i \,\rangle\!\rangle = \{u : r_i \mathfrak{R} u\}$ as base sets, an approximation pair $\langle\, \mathfrak{l}, \mathfrak{u} \,\rangle$ can be defined in the usual way [2]. Based on the extensions, the representative vector of each $u \in U$ is defined, so that $[\, u \,]_i$ is 1 if u belongs to the extension of r_i and 0 otherwise.

First-order language

The conventional Aristotelian semantics of a one-argument first-order language and its interpretation $\langle U, \psi \rangle$ is very widely known, hence it is not introduced here.

Definition 0.3. The ordered 4-tuple $\langle\, U, R, \mathfrak{R}, \varrho \,\rangle$ is an *approximative interpretation* of the one-argument first-order language $\langle\, LC, Var, Pred, Form \,\rangle$ if

1. $\langle\, U, R, \mathfrak{R} \,\rangle$ is a representative-based approximation space,
2. ϱ is a mapping such that $\varrho(P) = \langle\, \varrho(P)_1, \ldots, \varrho(P)_k \,\rangle$ for all $P \in Pred$, where
   (a) $\varrho(P)_i \in \{-1, 0, 1\}$;
   (b) $|\, ([\, u \,]_i \cdot \varrho(P)_i) - ([\, u \,]_\ell \cdot \varrho(P)_\ell) \,| \leq 1$ for all $u \in U$ and $i, \ell \in \{1, \ldots, k\}$;

   where k is the number of representatives, hence $R = \{r_1, \ldots, r_k\}$.

The arithmetic product $[\, u \,]_i \cdot \varrho(P)_i$ is used to express the connection between objects and the semantic value of P.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

Definition 0.4. Let $\langle\, U, R, \mathfrak{R} \,\rangle$ be a representative-based approximation space, $\mathcal{L}$ be a one-argument first-order language, and $\langle\, U, \psi \,\rangle$ be its interpretation. The

$$\varrho(P)_i = \begin{cases} 1 & \text{if } \langle\!\langle\, r_i \,\rangle\!\rangle \subseteq \psi(P), \\ -1 & \text{if } \langle\!\langle\, r_i \,\rangle\!\rangle \cap \psi(P) = \emptyset, \\ 0 & \text{otherwise;} \end{cases}$$

function is the *derived mapping* from ψ with respect to a given $\langle\, U, R, \mathfrak{R} \,\rangle$.

Corollary 0.5. *Let $\langle\, U, R, \mathfrak{R} \,\rangle$ be a representative-based approximation space, $\mathcal{L}$ be a one-argument first-order language, $\langle\, U, \psi \,\rangle$ be its interpretation, and ϱ be the derived mapping from ψ. Then $\langle\, U, R, \mathfrak{R}, \varrho \,\rangle$ is an approximative interpretation.*

The idea to use a partial three-valued system appeared in [1]. The semantic values of the zero-order connectives are defined so that they keep the truth value gap. The semantic value of a $P \in Pred$ is a $U \to \{0, 1, 2, {}^1\!/_2\}$ function, dividing U into four parts: objects related to the negativity domain of P ($formally$ $[\,u\,]_i \cdot \varrho(P)_i = -1$ for some i), objects related to the positivity domain of P, objects not related to any extensions, and others.

Definition 0.6. The semantic value of a quantified formula is the following value from the set $\{0, {}^1\!/_2, 1, 2\}$:

$$[\![\, QxA \,]\!]_v = \begin{cases} \max\limits_{u \in \mathcal{V}} \left\{ [\![\, A \,]\!]_{v\,[x\,:\,u]} \right\} & \text{if } Q = \exists \text{ and } \mathcal{V} \neq \emptyset \\ \min\limits_{u \in \mathcal{V}} \left\{ [\![\, A \,]\!]_{v\,[x\,:\,u]} \right\} & \text{if } Q = \forall \text{ and } \mathcal{V} \neq \emptyset \\ 2 & \text{otherwise;} \end{cases}$$

where $\mathcal{V} = \{u : u \in U \text{ and } [\![\, A \,]\!]_{v\,[x\,:\,u]} \neq 2\}$ and the assignment v and the modified assignment $v\,[x\!:\!u]$ are defined exactly in the same way as it was introduced in the classical first-order logic. Like in the classical case, $\exists$ and $\forall$ quantifiers are defined as the generalizations of $\vee$ and $\wedge$, respectively.

Key properties based on representatives

Theorem 0.7. *Let $I = \langle\, U, R, \mathfrak{R}, \varrho \,\rangle$ be an approximative interpretation of $\mathcal{L}$. There exists an approximative interpretation $J = \langle\, U', R, \mathfrak{R}', \varrho \,\rangle$ such that $|U'| \leq 2^k \ll |U|$ and $[\![\, A \,]\!]_v^I = [\![\, A \,]\!]_w^J$ for all $A \in Form$ where $w(x) = \tau(v(x))$ for some mapping $\tau : U \to U'$.*

Corollary 0.8. *During the evaluation process of a quantified formula it is enough to consider 2^k objects only. It can dramatically increase the speed of evaluation.*

Theorem 0.9. *The approximative interpretation generates a three-valued logic system without truth value gap if $\langle\, U, R, \mathfrak{R} \,\rangle$ is an approximation space, where the union of the extensions covers (equals to) U.*

Theorem 0.10. *Let* $\langle LC, Var, Pred, Form \rangle$ *be a one-argument first-order language and* $\langle U, R, \mathfrak{R}, \varrho \rangle$ *be its approximative interpretation relying on the representative-based covering approximation space* $\langle U, R, \mathfrak{R} \rangle$ *where* ϱ *is the derived mapping from* ψ*, and let* v *be an arbitrary assignment.*

$$\textit{If } [\![A]\!]_v^{\langle U,R,\mathfrak{R},\varrho \rangle} \in \{0,1\} \textit{ then } [\![A]\!]_v^{\langle U,R,\mathfrak{R},\varrho \rangle} = |A|_v^{\langle U,\psi \rangle}.$$

As a consequence, when the approximative interpretation provides a crisp truth value 0 or 1, then it is equal to the one provided by a much longer calculation with the help of the classical method.

Keywords: Rough set theory, approximation-based logic system

References

[1] T. MIHÁLYDEÁK: *First-Order Logic Based on Set Approximation: A Partial Three-Valued Approach*, in: 2014 IEEE 44th International Symposium on Multiple-Valued Logic, May 2014, pp. 132–137, DOI: https://doi.org/10.1109/ISMVL.2014.31.

[2] Z. PAWLAK, A. SKOWRON: *Rudiments of rough sets*, Information sciences 177.1 (2007), pp. 3–27.

FPGA-based Intelligent Solutions for Autonomous Vehicles: A Short Survey*

Ashraf Kasem[a], Ahmad Reda[a], József Vásárhelyi[a], Ahmed Bouzid[a]

[a]Institute of Automation and Infocommunication. University of Miskolc, Hungary
ashraf.kasem.94.0@gmail.com, autareda@uni-miskolc.hu
vajo@mazsola.iit.uni-miskolc.hu, qgebouzid@uni-miskolc.hu

The rapid evolution of semiconductor technology allowed the miniaturization of ICs (Integrated Circuits) which made FPGAs (Field Programmable Gate Arrays) more and more powerful allowing their use in various fields and in this case autonomous vehicles. This paper reviews the common solutions involving artificial intelligence implemented on FPGA for autonomous vehicles applications. Research, development, and current trends related to the topic are emphasized.

Introduction

Autonomous vehicles that drive us instead of us driving them will be a reality soon. Autonomous driving may increase road safety since accidents related to impaired driving could be reduced as cars cannot get drunk or be distracted by a text message. Autonomous vehicles are equipped with multiple sensors to perceive the surrounding environment. These sensors generate huge data, hence real-time processing this data requires high performance computing systems. Instead of using CPUs and GPUs for implementing AI (Artificial Intelligence), FPGAs (Field-Programmable Gate Arrays) are adopted since they feature high performance with low power consumption. This article presents the latest solutions for autonomous vehicles involving AI implemented on FPGAs.

Background

An autonomous driving system is implemented on hybrid computational technologies GPU-FPGA, where the GPU's primary job is self-driving and the FPGA's job is to perform some subtasks such as pedestrian and traffic lights detection [5].
An end-to-end solution for the design of self-driving cars based on Xilinx PYNQ-Z2 board [9]. The most important characteristic of this design is the presence of the DPU (Data Process unit) that accelerates the deep learning process. FPGA is faster than a CPU and consumes less power than the GPU when it comes to accelerate the CNN (Convolutional

*This research was supported by the European Union and the Hungarian State, co-financed by the European Regional Development Fund in the framework of the GINOP-2.3.4-15-2016-00004 project, aimed to promote the cooperation between the higher education and the industry.

Neural Networks) process [1]. The proposed architecture permits to reduce the execution time and energy consumption comparing to the CPU. The accuracy and delay of autonomous driving systems have a major impact on how the vehicle handles the surrounding environment. To make the delay that resulting from data inputs deterministic a solution is proposed in [2] considering bypassing the CPU from the input data path. The biggest challenge when implementing AI algorithms in FPGAs is the difficulty of the hardware design. H. Bingo [3] proposes a solution to this problem applying PYNQ board which allows the use of Python for its wide range libraries, especially in AI and Image processing. O. Chang-song and Y. Jong-min [8] discuss the most popular technologies to accelerate deep learning processes for autonomous cars industry. Some steps are introduced to avoid collisions in the air for UAV (Unmanned aerial vehicle) using four cameras based on FPGA SoC (System on Chip) [6]. The collision avoidance algorithm has already been implemented in GPU-based system, but the solution is not practical as it requires high energy. Road segmentation is a very important process in self-driving cars which identifies and describes the drivable parts of the roads. The problem with this process is the need of high computational resources. A model based on FPGA is suggested in [7] to perform a real-time and low power road segmentation. The authors suggest the use of LiDAR (Light Detection and Ranging) than the use of traditional cameras since they suffer from image clarity in poor lighting conditions. FPGA is used for scene perception based on CNN. It took about 16.9 ms to accomplish a CNN operation using Xilinx UltraScale XCKU115 FPGA. In self-driving cars environment, if there is more than one car starting from the same place and going to the same destination, the decision-making system will choose the same optimal path for all cars. There will be one busy road/track and other uncrowded. To solve this issue, paper [4] proposes a solution implemented on FPGA applying game theory. This solution relies on direct communication between vehicles to apply game theory instead of using the cloud.

Conclusion. In the present paper, we introduced he latest proposed hardware solutions to accelerate AI processes dedicated to autonomous vehicles. It is doubtless that reaching fully autonomous and safe cars requires overcoming many challenges, for instance real-time processing of the huge data coming from multiple sensors, taking into account the energy consumption in addition to the safety issues. Exploiting reconfigurable computational technologies significantly enhance the performance of the solutions that especially involves artificial intelligence and autonomous vehicles since they require parallel computing. Depending on the solutions discussed in the paper, we are about to witness fully autonomous and safe vehicles in the next few years.

Keywords: FPGA, AI, Autonomous Vehicles, HW Acceleration, Coprocessing

References

[1] E. ADEL, R. MAGDY, S. MOHAMED, M. MAMDOUH, E. EL MANDOUH, H. MOSTAFA: *Accelerating deep neural networks using FPGA*, in: 2018 30th International Conference on Microelectronics (ICM), IEEE, 2018, pp. 176–179,
DOI: https://doi.org/10.1109/icm.2018.8704085.

[2] J. AHMAD, A. WARREN: *FPGA based Deterministic Latency Image Acquisition and Processing System for Automated Driving Systems*, in: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2018, pp. 1–5,
DOI: https://doi.org/10.1109/iscas.2018.8351472.

[3] H. BINGO: *Development of a control target recognition for autonomous vehicle using FPGA with Python*, in: 2018 International Conference on Field-Programmable Technology (FPT), IEEE, 2018, pp. 419–420,
DOI: https://doi.org/10.1109/fpt.2018.00089.

[4] S. DU, T. HUANG, J. HOU, S. SONG, Y. SONG: *FPGA based acceleration of game theory algorithm in edge computing for autonomous driving*, Journal of Systems Architecture 93 (2019), pp. 33–39,
DOI: https://doi.org/10.1016/j.sysarc.2018.12.009.

[5] C. HAO, A. SARWARI, Z. JIN, H. ABU-HAIMED, D. SEW, Y. LI, X. LIU, B. WU, D. FU, J. GU, ET AL.: *A hybrid GPU+ FPGA system design for autonomous driving cars*, in: 2019 IEEE International Workshop on Signal Processing Systems (SiPS), IEEE, 2019, pp. 121–126,
DOI: https://doi.org/10.1109/sips47522.2019.9020540.

[6] F. KÓTA, T. ZSEDROVITS, Z. NAGY: *Sense-and-avoid system development on an FPGA*, in: 2019 International Conference on Unmanned Aircraft Systems (ICUAS), IEEE, 2019, pp. 575–579,
DOI: https://doi.org/10.1109/icuas.2019.8798265.

[7] Y. LYU, L. BAI, X. HUANG: *Real-time road segmentation using lidar data processing on an fpga*, in: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2018, pp. 1–5,
DOI: https://doi.org/10.1109/iscas.2018.8351244.

[8] C. S. OH, J. M. YOON: *Hardware acceleration technology for deep-learning in autonomous vehicles*, in: 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), IEEE, 2019, pp. 1–3,
DOI: https://doi.org/10.1109/bigcomp.2019.8679433.

[9] T. WU, W. LIU, Y. JIN: *An End-to-End solution to Autonomous Driving based on Xilinx FPGA*, in: 2019 International Conference on Field-Programmable Technology (ICFPT), IEEE, 2019, pp. 427–430,
DOI: https://doi.org/10.1109/icfpt47387.2019.00084.

Testing various numerical methods for the efficient optimization of detailed chemical reaction mechanisms*

Simret Kidane[a], Márton Kovács[b], Máté Papp[b], Tamás Turányi[b],

László Pál[c]

[a]ELTE Institute of Mathematics, Hungary
simretab1222@gmail.com

[b]ELTE Institute of Chemistry, Hungary
kmarci95@gmail.com, pappmatyi66@caesar.elte.hu, turanyi@chem.elte.hu

[c]Faculty of Economics, Socio-Human Sciences and Engineering, Sapientia - Hungarian University of Transylvania, Romania
pallaszlo@uni.sapientia.ro

Introduction

Optimization of large reaction mechanisms means that the chemical kinetic and thermodynamic parameters of these models are fitted within their uncertainty limits to better describe experimental data. These are extreme optimization tasks due to the large number of fitted parameters (typically 50-100), large number of experimental data considered (up to 25000), and the slow calculation of the simulation results. The latter is based on the solution of several thousand systems of ordinary and partial differential equations and non-linear algebraic systems. Several local and global optimization search methods were tested here using analytical test functions and a real chemical kinetics problem. This trial chemical problem is the determination of two Arrhenius parameters of a $H_2/O_2/NOx$ reaction system using 732 experimental and theoretical data points.

Testing several optimization methods on standard test functions

The most widely used optimization methods in physics and chemistry are the Levenberg-Marquardt method and the various Gauss-Newton methods. However, these methods require the calculation of the derivative of the objective function with respect to the parameters. In mechanism optimization tasks the analytical derivatives are not available and the calculation of the numerical derivatives is too expensive, provided, the number of fitted

*The authors acknowledge the financial support of the Hungarian National Research, Development and Innovation Office via NKFIH grant K132109.

parameters are large. Therefore, we started to investigate also other local methods, like the Nelder-Mead simplex method [8] (Matlab codename: fminsearch), the NEWUOA method [10], the BOBYQA method [9], and the pattern search algorithm. Also, we investigated the following evolutionary global optimization methods: genetic algorithm (GA) [11], simulated annealing (SA) [5], differential evolution (DE) , particle swarm optimization (PSO) [13], covariance matrix adaptation evolutionary strategy (CMA-ES) [2]. In all cases we tested the Matlab implementations of the algorithms. There are several test functions that are traditionally used for testing local and global optimization methods. These are the Zakharov function [3] (single global minimum), the Holder table function [7] (several local minima and four global minima points with identical objective function values), and several other test functions with several local minima and a single global minimum: the Ackley function [3], the Cross function [7] and the Rastrigin's function. In the numerical experiments, the calculations were started from 50 different random initial points and the following results were recorded: CPU time measured on a PC (Processor: AMD Phenom X4 940 3.00 GHz, RAM: 8.00 GB, Op. system: Window 7 Enterprise(2009) 64bit, Matlab version: MATLAB R2020a), average number of objective function evaluations, and the objective function value at the end of the iterations. The general conclusion was that the local methods ended up in the local minima, while in most cases the global methods found the global minimum, but consuming very different CPU time.

Testing the optimization methods on the $\mathrm{H_2/O_2/NO_x}$ system

A large amount of experimental data is available for chemical systems where hydrogen–oxygen combustion is doped with NO, $\mathrm{NO_2}$ or $\mathrm{N_2O}$. The most influential kinetic parameters were identified [6] in the Glarborg-2018 mechanism [1] using local sensitivity analysis. The Glarborg-2018 mechanism contains 149 species and 1397 reaction steps.

According to this analysis, in such systems the most important parameters are the *A* Arrhenius parameters of the following nitrogen containing elementary reactions
R1: $\mathrm{NO_2 + H = NO + OH}$
R2: $\mathrm{NO + HO_2 = NO_2 + OH}$
Therefore, in our test calculations the fitted parameters were the *A* Arrhenius parameters of reactions R1 and R2. We used a subset of the experimental and theoretical data containing 732 data-points, collected from 13 publications. These data includes 2 data-sets of ignition delay times, 27 data-sets of concentrations measured in flow reactors, 11 data-sets of direct measurements and 3 data-sets of theoretical determinations. The simulations were carried out using the Matlab version of program Optima [Varga T, Busai Á, Zsély IG. Optima: A Matlab framework code for performing combustion simulations and mechanism optimization, 2017] and the Chemkin-II simulation code [4].

The calculations were started from parameter values ln (A1)= 32.50 and ln (A2)= 28.37, which were the literature recommendations for these parameters. All optimizations gave the same optimum value (ln (A1)= 32.71 and ln (A2)= 28.51) and the same objective function value in the optimum. However, the various methods required very different CPU

time and number of objective function evaluations.

Methods	Objective function evaluation	CPU time (sec)
fmincon	41	198
fminunc	78	540
patternsearch	124	2161
fminsearch	140	323
PSO	1240	8403
[12]	2000	1793
GA	3766	43083

Table 1: Comparison of different optimization methods on the chemical kinetics problem

Conclusions

Matlab codes of several derivative-free local and global nonlinear optimization methods were collected and tested on analytical test functions and also on real experimental datasets of the $H_2/O_2/NOx$ reaction system. The general conclusion from the applications of analytical test functions is that all global methods found the same minimum, while the local methods converged to different minima. In the chemical kinetics example, all methods found the same optimum, but the CPU time requirements and the number of objective function evaluations were very different. The investigations will be continued on larger chemical kinetic systems with more parameters to be fitted.

Keywords: Nonlinear optimization, local search methods, global search methods, black box models, large chemical reaction mechanisms

References

[1] P. GLARBORG, J. A. MILLER, B. RUSCIC, S. J. KLIPPENSTEIN: *Modeling nitrogen chemistry in combustion*, Progress in Energy and Combustion Science 67 (2018), pp. 31–68, DOI: https://doi.org/10.1016/j.pecs.2018.01.002.

[2] N. HANSEN, A. OSTERMEIER: *Completely derandomized self-adaptation in evolution strategies*, Evolutionary Computation 9.2 (2001), pp. 159–195.

[3] M. JAMIL, X. S. YANG: *A literature survey of benchmark functions for global optimisation problems*, International Journal of Mathematical Modelling and Numerical Optimisation 4.2 (2013), pp. 150–194.

[4] R. J. KEE, F. M. RUPLEY, J. A. MILLER: *Chemkin-II: A Fortran chemical kinetics package for the analysis of gas-phase chemical kinetics*, tech. rep., Sandia National Labs., Livermore, CA (USA), 1989, URL: https://www.osti.gov/biblio/5681118-chemkin-ii-fortran-chemical-kinetics-package-analysis-gas-phase-chemical-kinetics.

[5] S. KIRKPATRICK, C. D. GELATT, M. P. VECCHI: *Optimization by simulated annealing*, Science 220.4598 (1983), pp. 671–680.

[6] M. KOVÁCS, M. PAPP, I. G. ZSÉLY, T. TURÁNYI: *Determination of rate parameters of key* $\mathrm{N/H/O}$ *elementary reactions based on* $\mathrm{H_2/O_2/NO_x}$ *combustion experiments*, Fuel 264 (2020), p. 116720, DOI: https://doi.org/10.1016/j.fuel.2019.116720.

[7] S. K. MISHRA: *Some new test functions for global optimization and performance of repulsive particle swarm method*, Available at SSRN 926132 (2006).

[8] J. A. NELDER, R. MEAD: *A simplex method for function minimization*, The Computer Journal 7.4 (1965), pp. 308–313.

[9] M. J. POWELL: *The BOBYQA algorithm for bound constrained optimization without derivatives*, Cambridge NA Report NA2009/06, University of Cambridge, Cambridge (2009), pp. 26–46.

[10] M. J. POWELL: *The NEWUOA software for unconstrained optimization without derivatives*, in: Large-scale nonlinear optimization, Springer, 2006, pp. 255–297.

[11] R. SALOMON: *Re-evaluating genetic algorithm performance under coordinate rotation of benchmark functions. A survey of some theoretical and practical aspects of genetic algorithms*, BioSystems 39.3 (1996), pp. 263–278.

[12] T. TURÁNYI, T. NAGY, I. G. ZSÉLY, M. CSERHÁTI, T. VARGA, B. SZABÓ, I. SEDYÓ, P. KISS, A. ZEMPLÉNI, H. CURRAN: *Determination of rate parameters based on both direct and indirect measurements*, International Journal of Chemical Kinetics 44.5 (2012), pp. 284–302.

[13] F. VAN DEN BERGH, A. P. ENGELBRECHT: *A study of particle swarm optimization particle trajectories*, Information Sciences 176.8 (2006), pp. 937–971.

A case study of using DiNA - Directed Network Analyzer*

Gergely Kocsis[a], Máté Csongor Széll[a]

[a]University of Debrecen, Faculty of Informatics,
Department of IT Systems and Networks
kocsis.gergely@inf.unideb.hu

As part of our project, we have developed a multi platform application that provides an easy-to-use alternative for structural analysis of directed graphs. At the early stage of our work we have developed the interface and the overall structure of the web application[2, 4]. Namely, we have implemented a core Java package that can contain the graph analyzer algorithms and a web interface that can automatically adapt to new algorithms added. While in that early stage our application was able to run only algorithms added by the developers, now we have extended it with the possibility of dynamically adding new algorithms by privileged users. Following a case study we present how one can test our application online, how it can be deployed on a local computer and how can it be extended with new algorithms of already existing analyzer libraries like JGraphT [3], GraphStream [1] and with self-written ones. The results of the work are continuously made available at http://dina.inf.unideb.hu

Keywords: directed graph analysis, network topology, web interface, case study

References

[1] S. BALEV., A. DUTOT., Y. PIGNÉ., G. SAVIN: *Official page of GraphStream*, 2020, URL: http://graphstream-project.org/ (visited on 10/16/2020).

[2] M. BECSEI., M. C. SZÉLL., G. KOCSIS.: *Implementing a new interface for directed graph analysis by existing and new algorithms*, in: Proceedings of the 11th International Conference on Applied Informatics - ICAI2020, CEUR-WS.org vol 2650, 2020, pp. 38–45.

[3] D. MICHAIL, J. KINABLE, B. NAVEH, J. V. SICHI: *JGraphT—A Java Library for Graph Data Structures and Algorithms*, ACM Trans. Math. Softw. 46.2 (May 2020).

[4] M. C. SZÉLL., M. BECSEI., G. KOCSIS.: *Introduction to DiNA: An Extendable Web-application for Directed Network Analysis*, in: Proceedings of the 5th International Conference on Complexity, Future Information Systems and Risk - Volume 1: COMPLEXIS, INSTICC, SciTePress, 2020, pp. 129–135, ISBN: 978-989-758-427-5,
DOI: https://doi.org/10.5220/0009577701290135.

*This work was supported by the EFOP-3.6.1-16-2016-00022 project. The project is co-financed by the European Union and the European Social Fund.

Shape of epidemic curves in spatial scale free network models

Júlia Komjáthy[a], John Lapinskas[b], Johannes Lengler[c], Ulysse Schaller[c]

[a]Eindhoven University of Technology, Department of Mathematics and Computer Science
Eindhoven, The Netherlands
j.komjathy@tue.nl

[b]University of Bristol, UK
john.lapinskas@bristol.ac.uk

[c]ETH Zürich (Swiss Federal Institute of Technology), Switzerland
johannes.lengler@inf.ethz.ch, ulysse.schaller@inf.ethz.ch

Introduction

We study the spread of information in finite and infinite inhomogeneous spatial random graphs. We model the underlying contact network of the spreading using a class of spatial scale-free network models, called (finite and infinite) Geometric Inhomogeneous Random Graphs (GIRGs) with power law degree distributions with exponent $\tau > 1$. We define GIRGs as

Definition 0.11 (Geometric Inhomogeneous Random Graph (GIRG) [1])**.** Fix $N \geq 1$ the number of nodes. Assign to each node $u \in \{1, 2, \dots, N\}$ a *fitness* $w_u > 0$, and a uniformly chosen location $x_u \in [0, \sqrt{N}]^2$ independently of the rest. Fix $\alpha > 0$. For any pair of nodes u, v with fixed w_u, w_v, x_u, x_v, connect them by an edge with probability

$$\mathbf{Prob}(u \text{ is connected to } v \mid x_u, x_v, w_u, w_v) \asymp \min\left\{\left(\frac{w_u w_v}{\|x_u - x_v\|_2^2}\right)^{\alpha}, 1\right\}. \qquad (0.1)$$

GIRGs have a natural interpretation: the fitnesses express the ability of nodes to have many connections, Φ embeds them in space, and α is the *long-range* parameter: the smaller α is, the more the model favors longer connections. The parameter space of GIRG is rich enough to model many desired features observed in real networks:

(a) extreme variability of the number of neighbours (degrees),

(b) connections present on all length-scales,

(c) small and ultra-small distances,

(d) strong clustering,

(e) local communities.

In real-life networks, an extreme variability of node degree is often observed, see [2]. Extreme node degree variability results in the presence of a few individuals with extreme influence on spreading processes, the *hubs or superspreaders* [2]. Mathematically, this extreme degree variability can be expressed using the empirical distribution of node degrees, that follows a *power-law*:

$$\mathbf{Prob}(\deg(u) \geq x) \asymp \frac{1}{x^{\tau-1}}. \tag{0.2}$$

for some $\tau > 2$. Setting a power-law fitness distribution for w_u in a GIRG yields that the degrees satisfy (0.2). The parameter α in (0.1) determines the presence of long-range connections: as α gets smaller, it is more likely that there are long-range connections, since the ratio $w_u w_v / \|x_u - x_v\|_2^2$ in (0.1) is less than 1 for most node-pairs.

We study a simple epidemic model on these networks, which is a degree-dependent SI model. We fix the network G in advance. We think of nodes in the network as individuals. Each node within the network can be in two possible states: *susceptible (S) or infected (I)*. Infected nodes stay infected forever. At time 0, we start with a single infected node located at the origin. The infection spreads on the network using random transmission delays on edges: when u becomes infected, it will transmit the disease to its neighbor v a certain time T_{uv} later. We assume that for an independent and identically distributed collection of random variables $(L_{uv}) \sim L \geq 0$,

$$T_{uv} := L_{uv}(W_u W_v)^{\mu}, \tag{0.3}$$

implying that the transmission across edges between vertices of expected degrees w_1 and w_2 are penalised by a factor of $(w_1 w_2)^{\mu}$ for some $\mu > 0$: this corresponds to a slow-down effect towards/from higher degree vertices. We then define $I(t)$ as the number of infected individuals at time t. Assume that for some $t_0 > 0$

$$\mathrm{P}(L \geq t) \asymp t^{\beta} \quad \text{ on } [0, t_0]. \tag{0.4}$$

We show that based on the parameters τ, α, β, μ from Definition 0.11 and (0.3), the growth of $I(t)$ as a function of t satisfies the following phase diagram:

$$I(t) \begin{cases} = \infty \text{ for some finite } T < \infty & \text{when } \beta < (3-\tau)/(2\mu) \\ \asymp \exp(t^{\zeta}) & \text{when } \beta \in \left(\frac{3-\tau}{2\mu}, \frac{3-\tau}{\mu}\right) \text{ or } \alpha \in (1,2), \\ \asymp t^{\eta} & \text{when } \beta \in \left(\frac{3-\tau}{\mu}, \frac{1}{d} + \frac{3-\tau}{\mu} \vee 2\frac{\alpha-\tau+1}{d(\alpha-2)}\right) \\ & \text{and } \alpha > 2 \\ \asymp t^2 & \text{when } \beta > \frac{1}{d} + \frac{3-\tau}{\mu} \vee 2\frac{\alpha-\tau+1}{d(\alpha-2)} \text{ and } \alpha > 2, \end{cases} \tag{0.5}$$

where $\zeta = \zeta(\alpha, \tau, \beta, \mu) < 1$, $\eta = \eta(\alpha, \tau, \beta, \mu) > 2$. In words, the shape of the epidemic curves moves from explosive, to stretched exponential, to polynomial, to polynomial corresponding to the dimension of the underlying model.

References

[1] K. BRINGMANN, R. KEUSCH, J. LENGLER: *Geometric inhomogeneous random graphs*, Theoretical Computer Science 760 (2019), pp. 35–54.

[2] M. NEWMAN, A. L. BARABÁSI, D. J. WATTS: *The structure and dynamics of networks*, vol. 19, Princeton University Press, 2011.

Multi-Dimensional Analysis of Sensor Communication Processes*

Mohamed Amine Korteby, Zoltán Gál, Péter Polgár

University of Debrecen, Faculty of Informatics
korteby.amine@inf.unideb.hu
gal.zoltan@inf.unideb.hu
polgarp@mailbox.unideb.hu

This paper aims to study the complexity of the Low Energy Adaptive Clustering Hierarchy (LEACH) system. It has been analyzed based on status data-sets of several hundred simulation cases. The serviceability of LEACH network and dependency properties were done with two analytic techniques which consist of the Principal Component Analysis (PCA) and the Singular Value Decomposition (SVD), the combined effect of both methods proved to be powerful in studying the behavior of the actual Wireless Sensor Network system.

Introduction

Routing protocols play a key role in sending aggregated data, which is why such tasks need to be handled intelligently. A successful model of a Wireless Sensor Network (WSN) system is one that can strike a good compromise between maximum amount of data collection and minimum amount of energy consumption. In WSN hierarchical routing mechanisms, clustering appears to be an important consideration as it provides efficient energy savings and data delivery at the network level. Hierarchical routing, which includes clustering, has been proved to be a preferred method of managing sensor communication[1] [5]. At the same time, the method increases scalability, reduces the amount of energy loss, and delay time, while providing good connectivity and load balancing with increased network life. Because the LEACH hierarchical mechanism provides significant energy savings, nodes with Cluster Head (CH) functions are randomly selected during each epoch period and then operate according to two alternating phases (*Setup* and *Steady*). The CH takes over the frames of the cluster members and, after aggregation, sends it to the Sink (SN). Because the CH function consumes extra power, this is rarely received by WSN nodes [4] [3]. A new cost-balanced routing mechanism is proposed in the paper and the high-quality behavior of it is analyzed for different sets of parameters.

*This paper was supported by the FIKP-20428-3/2018/ FEKUTSTRAT project of the University of Debrecen, Hungary and by the QoS-HPC-IoT Laboratory. This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund. The paper was supported by the QoS-HPC-IoT laboratory, too.

Cost Balance Mechanism: CB-LEACH

With the change we proposed, we endowed the basic LEACH mechanism with additional skills and intelligence. This is a Cost Balanced (CB) version of LEACH, which decides the route for transmitting frames based on complex metrics. In the case of CB-LEACH, we allow the SN to move along a given path, as well as the selection of the optimal CH for the nodes. Because nodes in the current epoch time may be closer to the moving SN than any selected CH, it is preferable for them to send their frames directly to the SN than indirectly through the selected CH [6]. To this end, we also include the SN in the set of selected CH nodes, the energy of which does not decrease over time and is the largest in the Wireless Sensor Network system. We consider not only the distance of the possible CHs from the nodes but also their energy level. To do this, a given sensor node decides which CH to connect to, based on a COST metric. We analyze and evaluate the synthetic state data sets obtained from n = 360 simulation cases of Direct Sequence (DS), Basic LEACH (BAS-LEACH) and Enhanced LEACH (ENH-LEACH). Each data set having over 600k samples are captured according to different parameters: Balance Factor (α), Ratio of the CH nodes (p), Ratio of the AN node to the total number of nodes (m), Radio frames length (L), Aggregation level (g), and Velocity (v).

Multi-Dimensional Data Set Analytical Methods

The CB-LEACH mechanism depends on a significant number of parameters. The simulation was run in 360 cases. In each case, the communication activity of a given WSN was completed during an epoch period in the order of millions. Vectorisation of the analyzed system responses is based on standardization, normalization, and concatenation methods. There is a legitimate need to identify the parameters that most significantly influence the behavior of the present network. For this, we applied two analytic techniques which consist of the Principal Component Analysis (PCA) and the Singular Value Decomposition (SVD) [2]. The combined effect of both methods proved to be powerful in studying the behavior of the actual WSN system.

Benefits of the Applied Methods

The methods used allowed the behavior analysis of the CB-LEACH wireless sensor network. CB-LEACH is an energy-efficient version of the classic LEACH, the operation of which can be influenced based on six parameters. To determine the optimal parameter tuplet, the analysis of the synthetic state data set generated by several hundred different simulation cases required the use of Big Data processing methods. To this end, based on the principal component analysis and singular value decomposition, we got the rank of the simulation matrix r = 6, which is not a coincidence due to the number of parameters *(α, p, m, L, g, v)*, but a property due to the special skills of the CB-LEACH system. The found rank value served to group the status data sets into corresponding clusters, identifying in

this way principal base vectors of the CB-LEACH routing mechanism.

Keywords: wireless sensor networks, Low Energy Adaptive Clustering Hierarchy (LEACH), switching, cluster, classification analysis.

References

[1] A. V. BALJINDER. S, M. K: *A survey on various energy-efficient routing protocols in WSN*, International Journal of Advanced Research, Ideas and Innovations in Technology 4 (2019), pp. 862–865.

[2] V. C. CRESCENZIO. G: *Feature Selection with Non Linear PCA: A Neural Network Approach*, Journal of Applied Mathematics and Physics 7 (2019), pp. 1–18.

[3] S. U. MITTAL. N, S. B: *A stable energy efficient clustering protocol for wireless sensor networks*, Wireless Networks 23 (2017), pp. 1809–1821.

[4] M. A. O: *Dynamic relocation of mobile base station in wireless sensor networks using a cluster-based harmony search algorithm*, Information Sciences 178 (2017), pp. 76–95.

[5] H. S, V. S: *Energy Efficient Clustering for Network Stability and Longevity for Heterogeneous Wireless Sensor Network*, International Journal of Engineering Science and Computing 8 (2018), pp. 18867–18872.

[6] G. Z, K. M. A: *Energy Sparing of the Leach Communication Mechanism in Heterogeneous WSN*, in: 8th International Conference on Advanced Computer Science and Information Technology, 2019, pp. 53–64.

Portfolio Solver for Verifying Binarized Neural Networks

Gergely Kovásznai[a], Krisztián Gajdár[a], Nina Narodytska[b]

[a]Eszterházy Károly University, Eger, Hungary

[b]VMware Research, Palo Alto, USA

Introduction

Deep learning is a very successful AI technology that makes impact in a variety of practical applications ranging from vision to speech recognition and natural language [2]. However, many concerns have been raised about the decision-making process behind deep learning technology, in particular, deep neural networks.

One important family of deep neural networks is the class of *Binarized Neural Networks (BNNs)* [3]. These networks have a number of useful features that are useful in resource-constrained environments, like embedded devices or mobile phones [4, 5]. They are computationally efficient as all activations are binary, which enables the use of specialized algorithms for fast binary matrix multiplication.

The goal of this work to attack the problem of verifying important properties of BNNs by applying several kinds of approaches and solvers, such as *SAT*, *SMT* and *MIP* solvers. We introduce our solver that is able to encode BNN properties for those solvers and run them in parallel, in a *portfolio setting*. In some sense, this work can be considered to be the continuation of that in [1, 6]. We focus on the important properties of neural networks *adversarial robustness* and *network equivalence*. Experimental results show that VERBINE is capable of verifying those properties of medium-sized BNNs in reasonable runtime, especially when the solvers MINICARD + Z3 are run in parallel.

Encoding of binarized neural networks

A *binarized neural network (BNN)* is a feedforward network where weights and activations are predominantly binary [3]. It is convenient to describe the structure of a BNN in terms of composition of blocks of layers rather than individual layers. Each block consists of a collection of linear and non-linear transformations. Blocks are assembled sequentially to form a BNN, as Figure 1 shows.

Internal Block. Each internal block performs a collection of transformations over a binary input vector and outputs a binary vector. A common construction of an internal block [3]) is composed of three main operations: a linear transformation (LIN), batch normalization (BN), and binarization (BIN).

Output Block. The output block produces the classification decision for a given binary

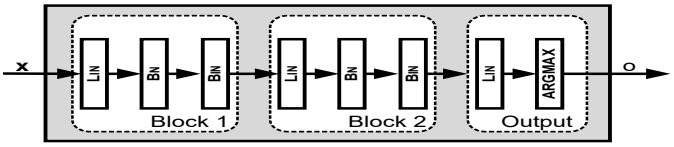


Figure 1: A schematic view of a binarized neural network.

input vector. It consists of two layers: a linear transformation that maps its input to a vector of integers, followed by an ARGMAX layer to predict the label.

We propose an encoding of BNN verification problems into *clauses* $l_1 \vee \cdots \vee l_n$ as well as *equivalences over Boolean cardinality constraints* in the form

$$l \Leftrightarrow \sum_{i=1}^{n} l_i \geq c \tag{0.1}$$

where $l, l_1, \ldots, l_n$ are Boolean literals and $c \in \mathbb{N}$ is a constant where $0 \leq c \leq n$. Depending on the approaches one wants to apply to the satisfiability checking of those constraints, they have to be encoded in different ways.

There are various existing, well-known approaches expressing Boolean cardinality constraints into Boolean logic, for example by using sequential counters, cardinality networks or modulo totalizers.

It is straightforward to encode clauses and constraints (0.1) into SMT over the quantifier-free logic of integer arithmetic (QF_LIA).

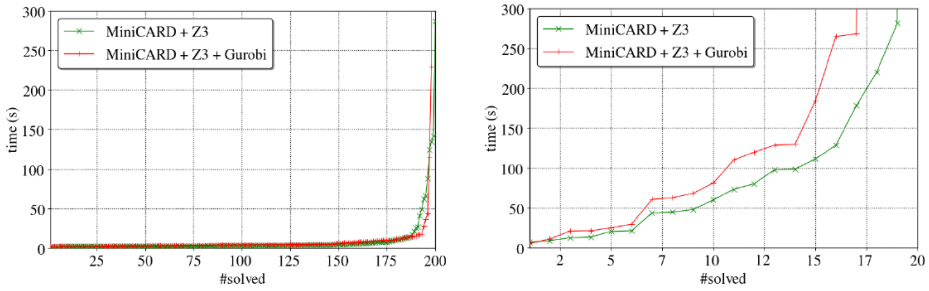
Implementation, experiments, and results

All the proposed encodings are implemented in Python, as part of our portfolio solver, which executes different kind of solvers (SAT, SMT, MIP) in parallel. Our solver can check both adversarial robustness and network equivalence.

In our experiments, the BNN architecture consists of 4 internal blocks and 1 output block. Each internal block contains a LIN layer with 200, 100, 100 and 100 neurons, respectively. We trained the network on the MNIST dataset. The accuracy of the resulting network is 93%.

We tried different combinations of solvers in our experiments, but our solver produced the best results when running MINICARD as a SAT solver and Z3 as an SMT solver in parallel.

In two sets of experiments, we focused on the problem of checking adversarial robustness and network equivalence, respectively. Figure 2 presents some of the results



(a) Checking adversarial robustness.

(b) Checking network equivalence.

Figure 2: Results on 4-BLOCK BNN on MNIST dataset.

References

[1] C. CHIH-HONG, N. GEORG, R. HARALD: *Verification of Binarized Neural Networks*, CoRR abs/1710.03107 (2017), arXiv: 1710.03107,
URL: http://arxiv.org/abs/1710.03107.

[2] I. GOODFELLOW, Y. BENGIO, A. COURVILLE: *Deep Learning*, The MIT Press, 2016, ISBN: 978-0262035613.

[3] I. HUBARA, M. COURBARIAUX, D. SOUDRY, R. EL-YANIV, Y. BENGIO: *Binarized Neural Networks*, in: Advances in Neural Information Processing Systems 29, Curran Associates, Inc., 2016, pp. 4107–4115,
URL: http://papers.nips.cc/paper/6573-binarized-neural-networks.pdf.

[4] J. KUNG, D. ZHANG, G. VAN DER WAL, S. CHAI, S. MUKHOPADHYAY: *Efficient Object Detection Using Embedded Binarized Neural Networks*, Journal of Signal Processing Systems (2017), pp. 1–14.

[5] B. MCDANEL, S. TEERAPITTAYANON, H. T. KUNG: *Embedded Binarized Neural Networks*, in: EWSN, Junction Publishing, Canada / ACM, 2017, pp. 168–173.

[6] N. NARODYTSKA, S. KASIVISWANATHAN, L. RYZHYK, M. SAGIV, T. WALSH: *Verifying Properties of Binarized Deep Neural Networks*, in: 32nd AAAI Conference on Artificial Intelligence, 2018, pp. 6615–6624.

A study on the intersections of the envelope of RE curves in skinning*

Kinga Kruppa[ab], Roland Kunkli[b], Miklós Hoffmann[bc]

[a]Doctoral School of University of Debrecen, University of Debrecen

[b]Faculty of Informatics, University of Debrecen
kruppa.kinga@inf.unideb.hu
kunkli.roland@inf.unideb.hu

[c]Institute of Mathematics and Informatics, Eszterházy Károly University
hoffmann.miklos@uni-eszterhazy.hu

Medial axis transforms have been thoroughly studied in computer graphics and image processing. Choi et al. [3] presented their mathematical foundations and introduced the so-called envelope formula, which can be used to reconstruct the boundary of a planar object. Moon showed that curves in the $\mathbb{R}^{2,1}$ Minkowski-space are very suitable to describe medial axis transforms, and he introduced the class of Minkowski Pythagorean hodograph (MPH) curves [7]. He showed that in the case of MPH curves, the envelopes and their offsets are rational. Since then, numerous studies have been published on MPH curves, and in 2016, Bizzarri et al. introduced the class of Rational Envelope (RE) curves [2] that also produce rational envelopes.

A different area of computer-aided geometric design is called skinning, by which we mean the process of creating two, at least G^1 continuous splines for a discrete sequence of circles that touch each circle only at one point. In skinning, the result can be also regarded as an envelope, but in a discrete aspect. Nowadays, there are more and more works that deal with skinning techniques [1, 5, 6].

We may observe that the boundary reconstruction using medial axis transforms and the skinning process is somehow similar, yet fundamentally different based on their problem setting. Nevertheless, based on the two fields' similarities, we started the study of applying medial axis transforms for skinning purposes. In [4], we have shown how RE curves can be employed for skinning a sequence of circles. We explored how to choose the input data for the interpolation so that the resulting envelope satisfies the conditions of skinning.

In skinning, the problems of intersecting skins are of utmost importance. In [5], we showed that we may modify the tangent vectors' lengths to resolve intersections. However, only general methods exist to detect whether the skins intersect and to determine the actual intersection points. But in the case of using RE curves, we can approach and solve these problems much more efficiently. In this work, we study the intersections of the generated envelope curves of RE curves when applied for skinning. We show how to detect the

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

intersection points and offer possible solutions to resolve the intersections.

References

[1] B. BASTL, J. KOSINKA, M. LÁVIČKA: *Simple and branched skins of systems of circles and convex shapes*, Graphical Models 78 (2015), pp. 1–9, ISSN: 15240703, DOI: https://doi.org/10.1016/j.gmod.2014.12.001.

[2] M. BIZZARRI, M. LÁVIČKA, J. KOSINKA: *Medial axis transforms yielding rational envelopes*, Computer Aided Geometric Design 46 (2016), pp. 92–102, ISSN: 01678396, DOI: https://doi.org/10.1016/j.cagd.2016.05.006.

[3] H. I. CHOI, S. W. CHOI, H. P. MOON: *Mathematical theory of medial axis transform*, Pacific Journal of Mathematics 181.1 (1997), pp. 57–88, ISSN: 0030-8730, DOI: https://doi.org/10.2140/pjm.1997.181.57.

[4] K. KRUPPA: *Applying Rational Envelope Curves For Skinning Purposes*, Frontiers of Information Technology and Electronic Engineering, DOI: https://doi.org/10.1631/FITEE.1900377.

[5] K. KRUPPA, R. KUNKLI, M. HOFFMANN: *An improved skinning algorithm for circles and spheres providing smooth transitions*, Graphical Models 101 (2019), pp. 27–37, ISSN: 15240703, DOI: https://doi.org/10.1016/j.gmod.2018.12.001.

[6] R. KUNKLI, M. HOFFMANN: *Skinning of circles and spheres*, Computer Aided Geometric Design 27.8 (2010), pp. 611–621, ISSN: 01678396, DOI: https://doi.org/10.1016/j.cagd.2010.07.003.

[7] H. P. MOON: *Minkowski Pythagorean hodographs*, Computer Aided Geometric Design 16.8 (1999), pp. 739–753, ISSN: 01678396, DOI: https://doi.org/10.1016/S0167-8396(99)00016-3.

A contribution to scheduling of cluster networks with finite-source*

Attila Kuki[a], Tamás Bérczes[a], Ádám Tóth[a], János Sztrik[a]

[a]University of Debrecen, Hungary
[kuki.attila;berczes.tamas;toth.adam;sztrik.janos]@inf.unideb.hu

Introduction

This paper deals with scheduling jobs in heterogeneous resources of networks, like the computational grid. In the literature, various job allocation algorithms have been proposed to schedule arriving jobs in computational clusters [5], [4], [1]. In addition, some algorithms have been designed to consider knowledge about the characteristics of jobs; these algorithms may be classified as either clairvoyant or as non-clairvoyant [8], [10], [9].

Apart from the effective scheduling, the energy consumption of such grid systems turns into a really crucial requirement due to the rapid increase of the size of the grid and the goal of a green network. The most common techniques of reducing energy consumption are related to the dynamic power management used at runtime. It is therefore of interest to examine algorithms which offer the greatest performance while using an amount of energy that is as low as possible.

The Model

Do introduced a generalized infinite model for the performance evaluation of scheduling compute-intensive jobs with unknown service times in computational clusters [2]. In this paper we use a finite model instead of the infinite one [7] to make the queueing model more realistic and we introduce two new scheduling policies. In addition to the existing HP policy, new policies are introduced:

- *HP (High Performance priority)*: This policy chooses the shortest queue in the system. If there is more than one queue with this property, a queue whose server has the highest performance is chosen.
- *MRT (Mean Response Time priority)*: This policy first calculates the expected mean response time for every queue and then selects a queue where this value is the minimal.
- *MRTHP (Mean Response Time with High Performance priority)*: This policy is a combination of MRT and HP. If there is an idle server, it behaves like the HP policy; if all servers are busy, it behaves like MRT.

*The research work was supported by the construction EFOP - 3.6.3 - VEKOP - 16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

To calculate the performance, mean response times and energy consumption of a server, we consider every server of the cluster to be one of a specific type (class), which can be characterized by the following parameters: C_s - the throughput of the server; $P_{\mathrm{ac},s}$ - the average active energy consumption of the server under full load; $P_{\mathrm{id},s}$ - the power consumption of the server in the idle state. These measures are applied based on the SPECpower_ssj2008 benchmark [6]. According to these parameters the modeled servers were Intel Xeon E5-2670, Intel Xeon E5-2660, and Intel Xeon E5-4650L.

We investigate these policies with respect to three schemes of buffering the arriving jobs:

- *Separate Queue*: In this scheme every server has its own queue. Jobs are scheduled to the queue of a specific server according to the chosen policy.
- *Class Queue*: In this scheme a buffer is assigned to each class. Jobs are scheduled to the queue of a specific class according to the chosen policy.
- *Common Queue*: In this scheme only a single common buffer is available for all servers. If more than one server is idle, then the local scheduler chooses the server with the highest performance.

In this paper, we present a generalized finite source model for the performance evaluation of scheduling compute-intensive jobs with unknown service times in a computational cluster which is built from servers of different types. The state space of the describing Markov chain is extremely large. Therefore, to obtain the performance measures the SimPack, a collection of C/C++ libraries and executable programs for computer simulation is used [3].

In particular, we determine various performance measures for all combinations of three scheduling policies for assigning jobs to servers with three schemes for buffering arriving jobs; furthermore, we investigate the effect of switching off idle servers, thus the energy consumption of the system under these combinations of scheduling policies and buffering schemes can be estimated.

Large number of figures were generated to illustrate the effects of scheduling algorithms and buffering schemes for the performance measures and the energy consumption. Simulation results show that the choice of the scheduling policy and of the buffering scheme plays an important role in ensuring quality of service parameters such as the waiting time and the response time experienced by arriving jobs. The energy consumption, however, is only affected by the scheduling policy and the energy saving mode, while the buffering scheme does not have significant impact.

Keywords: performance evaluation, cluster network, finite-source queueing systems, buffering scheme

References

[1] M. CANKAR, M. ARTAČ, M. ŠTERK, U. LOTRIČ, B. SLIVNIK: *Co-Allocation with Collective Requests in Grid Systems*, Journal of Universal Computer Science 19.3 (2013), pp. 282–300, DOI: https://doi.org/10.3217/jucs-019-03-0282.

[2] T. V. DO, B. T. VU, X. T. TRAN, A. P. NGUYEN: *A generalized model for investigating scheduling schemes in computational clusters*, Simulation Modelling Practice and Theory 37.0 (2013), pp. 30–42.

[3] P. A. FISHWICK: *Simpack: Getting Started With Simulation Programming In C And C++*, in: WSC '92 Proceedings of the 24th Conference on Winter Simulation, ed. by J. S. ET AL., ACM, New York, 1992, pp. 154–162.

[4] A. TCHERNYKH, J. RAMÍREZ, A. AVETISYAN, N. KUZJURIN, D. GRUSHIN, S. ZHUK: *Two level job-scheduling strategies for a computational grid*, in: Proceedings of the 6th International Conference on Parallel Processing and Applied Mathematics, 2006, pp. 774–781.

[5] G. TERZOPOULOS, H. D. KARATZA: *Performance evaluation of a real-time grid system using power-saving capable processors*, The Journal of Supercomputing 61.3 (2012), pp. 1135–1153.

[6] THE STANDARD PERFORMANCE EVALUATION CORPORATION: *SPECpower_ssj2008 Result File Fields*, Web Page: https://www.spec.org/power/docs/SPECpower_ssj2008-Result_File_Fields.html.

[7] Á. TÓTH, T. BÉRCZES, A.KUKI, B. ALMÁSI, W. SCHREINER, J. WANG, F. WANG: *Analysis of finite-source cluster networks*, Creative Mathematics and Informatics 2 (2016), pp. 223–235.

[8] S. ZIKOS, H. D. KARATZA: *A clairvoyant site allocation policy based on service demands of jobs in a computational grid*, Simulation Modelling Practice and Theory 19.6 (2011), pp. 1465–1478.

[9] S. ZIKOS, H. D. KARATZA: *Communication cost effective scheduling policies of nonclairvoyant jobs with load balancing in a grid,* Journal of Systems and Software 82.12 (2009), pp. 2103–2116.

[10] S. ZIKOS, H. D. KARATZA: *The impact of service demand variability on resource allocation strategies in a grid system*, ACM Transactions on Modeling and Computer Simulation 20.19 (2010), pp. 1–29, DOI: https://doi.org/10.1145/1842722.1842724.

Deep learning-based cell classification in case of unbalanced dataset*

Dávid Kupás[a], **Balázs Harangi**[a]

[a]University of Debrecen
david_kupass@yahoo.com
harangi.balazs@inf.unideb.hu

The so-called Papanicolaou test [6], also known as the Pap test, is a microscopic examination of cells detached from the surface of the cervix, which allows the detection of cancer-preventing conditions as well as early cervical cancer. During the Pap test, special microscopes are used to examine the cell smears that can contain up to more than 10,000 cells. When performing the test on a sick patient, only a low proportion of these cells are abnormal cells. During the study, it is the task of the cytologists to recognize the unhealthy cells on the smears, which is a significantly time-consuming and thus an expensive task [5].

After the appropriate digitalization of the aforementioned smear, based on the results of previous research [3], we performed an automatic cell segmentation method, which produced a binary mask, that identifies the groups of cells on each smear. Using the results of this algorithm as input, we ran an automated slicing algorithm that applies digital image processing algorithms in order to extract the image slices of each cell.

The available database, containing the images found on the smears was unbalanced, hence the healthy images were in vast majority. In our work, we propose a new system to solve the aforementioned problem, intending to find the abnormal cells using neural networks. With the use of a database, that was manually annotated by cytologists, we train a deep learning [4] network that aims to classify the cells into two different classes. Deriving from the initial results obtained in this way, we could assume that there was a need for a solution that increases the accuracy of the network by also balancing the available dataset. We have further developed a system for synthetic image generation which is based on an algorithm known from literature [1] that is capable of generating reliably unhealthy cell images regarding the classification, thus balancing the available dataset. With the intent of focusing on the identification of unhealthy cells, we apply modern class weighting solutions by using a custom loss function. Furthermore, we also connect a simple classification network to the output of the encoder part of our system. The concept is to train a variational autoencoder [2] with the appropriate parameters together with the classification network. In this way we have used this system, to generate images that are more appropriate regarding the classification of them into two classes. These generated images are then

*This research was supported by the ÚNKP-19-2-I-DE-345 and the ÚNKP-20-5-DE-31 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund. Moreover, the research was supported in part by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, the GINOP-2.2.1-18-2018-00012 and the EFOP-3.6.2-16-2017-00015 supported by the European Union, co-financed by the European Social Fund.

added to the original dataset, only if the classifier predicts them to be abnormal.

The resulting images were used to expand the existing data set, which was used to retrain the aforementioned deep learning based model. The retrained model produced growth in its performance. In order to thoroughly test the model, we also propose a metric that focuses on the network's ability to recognize unhealthy cells.

Keywords: Pap test, cell classification, unbalanced data, autoencoder

References

[1] R. CHALAPATHY, A. K. MENON, S. CHAWLA: *Anomaly Detection using One-Class Neural Networks*, CoRR (2018).

[2] F. CHOLLET: *Deep Learning with Python and Keras: The practical manual from the developer of the Keras library*, MITP-Verlags GmbH Co. KG, 2018.

[3] B. HARANGI, J. TÓTH, G. BOGACSOVICS, D. KUPÁS, L. KOVÁCS, A. HAJDU: *Cell detection on digitized Pap smear images using ensemble of conventional image processing and deep learning techniques*, in: 2019 11th International Symposium on Image and Signal Processing and Analysis (ISPA), 2019, pp. 38–42.

[4] F. IANDOLA, M. MOSKEWICZ, S. KARAYEV, R. GIRSHICK, T. DARRELL, K. KEUTZER: *DenseNet: Implementing Efficient ConvNet Descriptor Pyramids* (Apr. 2014).

[5] L. G. KOSS: *The Papanicolaou Test for Cervical Cancer Detection: A Triumph and a Tragedy*, JAMA 261.5 (Feb. 1989), pp. 737–743,
DOI: https://doi.org/10.1001/jama.1989.03420050087046.

[6] G. N. PAPANICOLAOU, H. F. TRAUT: *The Diagnostic Value of Vaginal Smears in Carcinoma of the Uterus*, American Journal of Obstetrics and Gynecology 42.2 (1941), pp. 193–206,
DOI: https://doi.org/10.1016/S0002-9378(16)40621-6.

Introducing w-Horn and z-Horn: A Generalization of Horn and q-Horn Formulae

Gábor Kusper[a], Csaba Biró[a], Attila Adamkó[b], Imre Baják[c]

[a]Eszterházy Károly University
kusper.gabor@uni-eszterhazy.hu, biro.csaba@uni-eszterhazy.hu

[b]University of Debrecen
adamkoa@inf.unideb.hu

[c]Budapest Business School
bajak.imre@uni-bge.hu

Introduction

Propositional Satisfiability is the problem of determining, for a formula of the propositional calculus, if there is an assignment of truth values to its variables for which that formula evaluates to true. By SAT we mean the problem of propositional satisfiability for formulae in conjunctive normal form (CNF).

SAT is the first, and one of the simplest, of the many problems which have been shown to be **NP**-complete [5]. It is dual of propositional theorem proving, and many practical **NP**-hard problems may be transformed efficiently to SAT. Thus, a good SAT solver would likely have considerable utility. It seems improbable that a polynomial time algorithm will be found for the general SAT problem but we know that there are restricted SAT problems that are solvable in polynomial time. So a "good" SAT solver should first check the input SAT instance whether it is an instance of such a restricted SAT problem.

In this paper we introduce the w-Horn SAT problem, which is solvable in polynomial time. We also introduce the z-Horn SAT problem, but we do not know yet whether it is solvable in polynomial time or not.

Horn SAT is the restriction to instances where each clause contains at most one positive literal. Horn SAT is solvable in linear time [6, 9], as are a number of generalizations such as *renamable Horn SAT* [1, 8], *extended Horn SAT* [4] and *q-Horn SAT* [2, 3].

In this paper we generalize the well-known notions of Horn and q-Horn formulae. A Horn clause, by definition, contains at most one positive literal. A Horn formula contains only Horn clauses.

We generalize these notions as follows. A clause is a w-Horn clause if and only if it contains at least one negative literal or it is a unit. A formula is a w-Horn formula if it contains only w-Horn clauses after propagating all units in it, i.e., after a BCP step. We show that the set of w-Horn formulae properly includes the set of Horn formulae.

A function $\beta(x)$ is a valuation function if $\beta(x) + \beta(\neg x) = 1$ and $\beta(x) \in \{0, 0.5, 1\}$, where x is a Boolean variable.

A formula is q-Horn if and only if each clause in it contains at most one "positive" literal (where $\beta(x) = 1$) or at most two half ones (where $\beta(x) = 0.5$).

We generalize these notions as follows. A formula is z-Horn if and only if each clause in it after a BCP step contains at least one "negative" literal or exactly two half ones.

We show that the set of z-Horn formulae properly includes the set of q-Horn formulae. We also show that the w-Horn SAT problem can be decided in polynomial time. We also show that each satisfiable formula is z-Horn.

Examples

Examples for w-Horn formulae:

1. $(\neg a \vee b \vee c)$.
2. $(\neg a \vee \neg b) \wedge (\neg a \vee b) \wedge (a \vee \neg b)$.
3. $(\neg a \vee \neg b \vee \neg c) \wedge (\neg a \vee \neg b \vee c) \wedge (\neg a \vee b \vee \neg c) \wedge (\neg a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (a \vee \neg b \vee c) \wedge (a \vee b \vee \neg c)$, this example shows the great expressiveness of w-Horn.
4. $(a) \wedge (\neg a \vee b)$, because after BCP we obtain the empty clause set.
5. $(\neg a \vee \neg b) \wedge (\neg a \neg b) \wedge (a \vee \neg b) \wedge (a \vee b \vee c) \wedge (\neg c)$, because after BCP we obtain $(\neg a \vee \neg b) \wedge (\neg a \vee b) \wedge (a \vee \neg b)$.

The following examples are not w-Horn formulae:

1. The formula $(a) \wedge (\neg a)$ is not w-Horn, because after BCP we obtain a clause set which contains the empty clause, and the empty clause is not w-Horn.
2. The formula $(a) \wedge (\neg a \vee b \vee c)$ is not w-Horn, because after BCP we obtain $(b \vee c)$, which is not a w-Horn clause.

Examples for z-Horn formulae:

1. (a $\vee$ b) and ($\neg$ a $\vee$ c), because every 2-SAT problem is a z-Horn formula.
2. ($\neg$ a $\vee$ b $\vee$ c) $\wedge$ ($\neg$ a $\vee$ $\neg$ b $\vee$ $\neg$ c), a feasible valuation is $\beta(a) = \beta(b) = \beta(c) = 0$, but it is enough to say that $\beta(a) = 0$. Note that this formula is said to be non q-Horn, see example 2.9. and 2.10. in [7], but it is actually q-Horn, because $\beta(a) = 1$, and $\beta(b) = \beta(c) = 0.5$ is a q-feasible function for it.

Properties of w-Horn and z-Horn formulae

Lemma 0.12. *The set of w-Horn formulae properly includes the set of Horn formulae.*

Lemma 0.13. *The w-Horn SAT problem is solvable in polynomial time.*

Lemma 0.14. *The set of z-Horn formulae properly includes the set of q-Horn formulae.*

Lemma 0.15. *Any satisfiable F formula is z-Horn.*

References

[1] B. ASPVALL: *Recognizing disguised NR (1) instances of the satisfiability problem*, Journal of Algorithms 1.1 (1980), pp. 97–103.

[2] E. BOROS, Y. CRAMA, P. L. HAMMER, M. SAKS: *A complexity index for satisfiability problems*, SIAM Journal on Computing 23.1 (1994), pp. 45–49.

[3] E. BOROS, P. L. HAMMER, X. SUN: *Recognition of q-Horn formulae in linear time*, Discrete Applied Mathematics 55.1 (1994), pp. 1–13.

[4] V. CHANDRU, J. N. HOOKER: *Extended Horn sets in propositional logic*, Journal of the ACM (JACM) 38.1 (1991), pp. 205–221.

[5] S. A. COOK: *The complexity of theorem-proving procedures*, in: Proceedings of the third annual ACM symposium on Theory of computing, 1971, pp. 151–158.

[6] W. F. DOWLING, J. H. GALLIER: *Linear-time algorithms for testing the satisfiability of propositional Horn formulae*, The Journal of Logic Programming 1.3 (1984), pp. 267–284.

[7] J. FRANCO: *Relative size of certain polynomial time solvable subclasses of satisfiability*, in: Satisfiability Problem: Theory and Applications (DIMACS Workshop March 11-13, 1996), vol. 35, 1997, pp. 211–223.

[8] H. R. LEWIS: *Renaming a set of clauses as a Horn set*, Journal of the ACM (JACM) 25.1 (1978), pp. 134–135.

[9] M. G. SCUTELLA: *A note on Dowling and Gallier's top-down algorithm for propositional Horn satisfiability*, The Journal of Logic Programming 8.3 (1990), pp. 265–273.

Investigation of the efficiency of an interconnected convolutional neural network by classifying medical images

Oktavian Lantang[a], György Terdik[a], András Hajdu[b], Attila Tiba[b]

[a]Doctoral School of Informatics, Section of Applied Information Technology and its Theoretical Background, University of Debrecen
oktavian_lantang@unsrat.ac.id,terdik.gyorgy@inf.unideb.hu

[b]Department of Computer Graphics and Image Processing, Facuty of Informatics, University of Debrecen
hajdu.andras@inf.unideb.hu,tiba.attila@inf.unideb.hu

Convolutional Neural Network (CNN) for medical image classification has produced satisfying work [1, 2, 6, 7]. Several pre-trained models such as VGG [9], Inception [10], and ResNet [5] are products that can be relied on to design high accuracy classification models. Our work investigates the performance of the three pre-trained models when trained together. We use two methods for comparison. First, we train the model independently. This means that each model is given input and trained separately, then the best results are determined by majority voting. In the second method, we train the three pre-trained models mutually. In other words, these three models are trained simultaneously as the Interconnected Model.

The interconnected model adopts an ensemble architecture as shown in [4]. Our design is a combination of the three sub-models previously mentioned. The first sub-model is VGG19, consisting of sixteen convolution layers, five polling layers, and three fully-connected layers. Meanwhile, Inception and Resnet50 each consist of forty-eight and fifty layers. We trained these three models with the number of parameters, respectively, 1,863,702 for VGG19, 3,297,302 for Inception, and 10,055,702 for Resnet50. We took 70% of the pictures as a training set and the rest as a validation set in the training process. Each subnet is also installed with three fully connected layers with a Relu activation function after previously passing the Flatten layer that changing each feature's dimensions. The three outputs from each subnet are concatenated before entering a multilayer perceptron with three layers. Each has two fully-connected layers using the Relu activation function and the final layer with two class Softmax activation function.

The model we suggest is examined on two datasets. The first data set is the chest x-ray dataset[1]. The data are the results of radiological photographs, which are divided into two categories. The first category is Normal, and the other is Pneumonia. The two classes in the dataset each had 3875 images for Pneumonia and 1341 Normal ones. The second dataset is thin blood smear images[2], which have been categorized into two classes, namely,

[1]https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia
[2]https://www.kaggle.com/miracle9to9/files1

Parasitized and Uninfected. These two classes proportionally distributed 13780 images for each category.

We uniform several things for simplicity, including the input size is set to 200x200 Pixels, 16 Minibatch, 50 Epochs. We also take advantage of Adam optimizers with 0.0001 learning rates and decrease 1e-6 for each subsequent epoch. From the experimental results using the chest x-ray dataset, we can report the interconnected model's accuracy[3, 8] reaching 0.95, VGG19 0.93, Inception 0.83, and Resnet50 0.74. Meanwhile, from the malaria dataset, the Interconnected model achieved an accuracy of 0.87, followed by VGG19 0.89, Inception 0.79 and 0.50 for Resnet50. At the end of the paper, we will present the comparison of the majority voting of three subnets toward the Interconnected model.

Keywords: Convolutional Neural Network, Medical Images Classification, Interconnected Model

References

[1] C. BUTT, J. GILL, D. CHUN, B. A. BABU: *Deep system to screen coronavirus disease 2019 pneumonia*, Applied Intelligence (2019),
DOI: https://doi.org/10.1007/s10489-020-01714-3.

[2] U.-O. DORJ, K.-K. LEE, J.-Y. CHOI, J.-Y. CHOI: *The Skin Cancer Classification Using Deep Convolutional Neural Network*, Multimedia Tolls and Applications 77.8 (2018), pp. 9909–9924,
DOI: https://doi.org/10.1007/s11042-018-5714-1.

[3] T. FAWCETT: *An Introduction to ROC Analysis*, Pattern Recognition Letters 27.8 (2006), pp. 861–874,
DOI: https://doi.org/10.1016/j.patrec.2005.10.010.

[4] B. HARANGI: *Skin Lesion Classification With Ensembles of Deep Convolutional Neural Networks*, Journal Of Biomedical Informatics 86 (2018), pp. 25–32.

[5] K. HE, X. ZHANG, S. REN, J. SUN: *Deep Residual Learning for Image Recognition*, in: Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA: IEEE, 2016, pp. 770–778,
DOI: https://doi.org/10.1109/CVPR.2016.90.

[6] O. LANTANG, A. TIBA, H. ANDRAS, G. TERDIK: *Convolutinal Neural Network for Predicting The Spread of Cancer*, in: Proceedings of the 2019 10th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Naples, Italy: IEEE, 2019, pp. 175–180,
DOI: https://doi.org/10.1109/CogInfoCom47531.2019.9089939.

[7] Z. LIANG, A. POWELL, I. ERSOY, M. POOSTCHI, K. SILAMUT, K. PALANIAPPAN, P. GUO, M. A. HOSSAIN, A. SAMMER, R. J. MAUDE, J. X. HUANG, S. JAEGER, G. THOMA: *CNN-Based Image Analysis for Malaria Diagnosis*, in: 2016 IEEE Conference on Bioinformatics and Biomedicine (BBIM), Shenzhen, China: IEEE, 2016, pp. 493–496,
DOI: https://doi.org/10.1109/BIBM.2016.7822567.

[8] D. M. W. POWERS: *Evaluation: From Precision, Recall and F-measure to ROC, Informedness, Markedness and Correlation*, Journal of Machine Learning Technologies 2.1 (2011), pp. 37–63,
DOI: https://doi.org/10.9735/2229-3981.

[9] K. SIMONYAN, A. ZISSERMAN: *Very Deep Convolutional Networks for Large-Scale Image Recognition*, arXiv preprint arXiv:1409.1556 60.6 (2014), pp. 1079–1105,
DOI: https://doi.org/10.1145/3065386.

[10] C. SZEGEDY, W. LIU, Y. JIA, Y. JIA, S. REED, D. ANGUELOV, D. ERHAN, V. VANHOUCKE, A. RABINOVICH: *Going Deeper with Convolutions*, in: Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA: IEEE, 2015, pp. 1–9, DOI: https://doi.org/10.1109/cvpr.2015.7298594.

Virtual Reality Games for Low Back Pain Patients with Fear of Movements

Thomas Fiskeseth Larsen[a], Ilona Heldal[b], Harald Soleim[b], Atle Geitung[b], Remy Monsen[b]

[a]Helse-Vest IKT, Bergen, Norway
thomas.fiskeseth.larsen@helse-vest-ikt.no

[b]bWestern Norway University of Applied Sciences Bergen, Norway
ilona.heldal@hvl.no, daniel.patel@hvl.no, harald.soleim@hvl.no, atle.geitung@hvl.no, remy.monsen@hvl.no

This paper explores the feasibility of Virtual Reality (VR) and Serious Games (SG) for helping low back pain patients in physiotherapy. The suggested application encourages back flexion beyond the patients' maladapted comfort zones while immersed in sensory-distracting exercise games. Data is collected via observation of the single-subject experimental study and by interviewing two health domain experts. The paper discusses the possibility of encouraging back flexion through exercise games and sensory distractions for pain avoidance. The main contribution is illustrating the possibilities of SGs and VR to treat fear of movements but only by involving domain knowledge in the evaluation process.

Introduction

Chronic low back pain is one of the leading causes of debilitating pain conditions, sick leave, and healthcare costs worldwide [4]. A subset of patients suffering from low back pain will also develop a fear of movement (kinesiophobia) that can be further exacerbating their condition, despite not having a specific pathology, prevailing injury, or danger of re-injury. Treating this condition has proven difficult, and there is currently little consensus on demonstrably effective treatment [8]. However, it is known that finding an effective treatment early reduces the impact or possible onset of chronicity and can significantly improve the patient's quality of life prospects [6]. While there are suggestions for Virtual Reality (VR) supported treatments, the majority of the papers show either the clinical (e.g., [2]) or the technical (e.g., [1]) parts of evaluations. This paper illustrates the design and explores the feasibility of affordable VR technology and Serious Games (SG) in physiotherapy based on collaboration between clinicians and technology developers. The application helps patients with non-specific chronic low back pain (NSCLBP) by encouraging back flexion (through graded exposure) beyond the patients' maladapted comfort zones, at the same time, when they are immersed in sensory-distracting games.

Study design

After investigating a list of possible HMDs and available games, the developer [5], in collaboration with a physiotherapist [7], chose Oculus Rift [3]| and identified two commercial games for the study: HoloBall and HoloDance. After discussing the necessary functions and features, a prototype game (RoBoW) was developed to complement the treatment (see Figure 1).

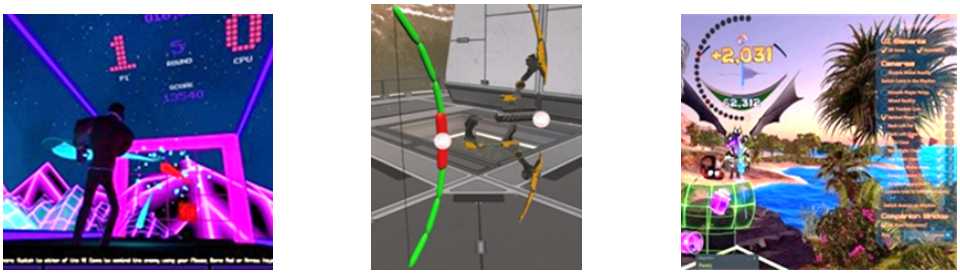


Figure 1: The three games applied, from left to right: HoloBall, RoBoW, HoloDance.

The final application was evaluated by ten patients with non-specific chronic low back pain (NSCLBP) and fear of movements [7] via observing a single-subject experimental study, followed by interviewing two health domain experts. After rigorously planned inclusion and exclusion criteria and the interventions, the patients were given information and could try VR equipment with an introductory game provided by Oculus, and answered questions before interventions. The intervention contained 7 steps, including 30 minutes of playing (10 minutes for each game), evaluations of experiences and ended with clinical evaluations. After the interventions, the patients also undergo a follow-up session with health-related data collection and assessment.

Briefly about the games

All patients were able to have a varied experience while playing HoloBall with low difficulty. They could start by pressing the trigger button to spawn a ball and hitting it at the beginning. The difficulty of the game could be increased or adjusted after the need of patients. For RoBoW, primary interactions occur for picking up arrows or batteries and firing weapons. Arrows could be either picked up from a spawner or drawn from a quiver (given by a collider and a behaviour/script) that followed the HMD, allowing the user to reload by using a grab interaction close to the shoulders—this resembles a normal movement to what one would expect if using a shoulder-strapped quiver in real life. The reaching activities, according to observations either involve stepping or performed from a stationary center encouraged to more ”use the room” and ”move freely” (see Figure 2).

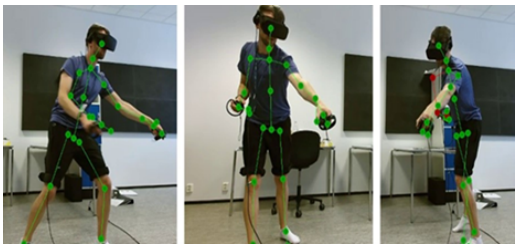


Figure 2: Arrow-bucket grab-interactions with different reaching

HoloDance was observed to elicit motions primarily with extended arms and some rotational movements and flexion. With the added challenge of incoming spheres, additional hand-eye coordination challenges were prominent.

Concluding remarks

This study shows the feasibility of developing SGs using VR technology for a patient group based on tailored interactions identified and tested by clinical personnel. The chosen applications facilitated the desired targeted movements and were customizable for each patient's capability. The application would not be successful without the knowledge and involvement of physiotherapists already in the design and the development process due to necessary adjustments of the prototypes to clinical goals. The results from observing the trials, corroborated and amended by two interviews, suggest that VR technology and appropriate experiences can be beneficial clinical treatments, since the trial games, including the prototype contribution, facilitated movements that were considered helpful for the trial objectives, so long as the games were sufficiently adjustable to a variety of cases. Clinical goals must easily translate to game settings and parameter adjustments given in therapeutic vernacular. Various interaction paradigms were examined through commercial games and experimental work. However, the clinical assessment needs to steer development considerations through developing new games. The observations and the interviews pinpoint the importance of adjusting the game- and exercise-difficulty for individual patients. Clinical guidance is also considered necessary, with an emphasized possibility for remotely monitoring progress outside clinical hours.

The prototype games designed and/or developed in the project can be expanded upon in their viable areas, gaining new insights from the project. In particular, the RoBoW game can be amended with new challenge types, better interface, and clinical tailoring towards external testing or deployment. Internal interest in maintaining a working version also motivated this. The application of commercial consumer games can be potentially useful in clinical settings or research. Developers of these tools and UX designers can likely benefit from domain-specific insights into how clinicians work to accomplish this and reflect on how the tools can deliver an experience that distracts from pain and motivates for a better quality of life.

Keywords: Virtual Reality, Serious Games, Training, Low Back Pain, Collaboration

References

[1] A. ALAZBA, H. AL-KHALIFA, H. ALSOBAYEL: *RabbitRun: An Immersive Virtual Reality Game for Promoting Physical Activities Among People with Low Back Pain*, Technologies 7.1 (Dec. 2018), p. 2.

[2] F. ALEMANNO, E. HOUDAYER, D. EMEDOLI, M. LOCATELLI, P. MORTINI, C. MANDELLI, A. RAGGI, S. IANNACCONE: *Efficacy of virtual reality to reduce chronic low back pain: Proof-of-concept of a non-pharmacological approach on pain, quality of life, neuropsychological and functional outcome*, PLOS ONE 14.5 (May 2019), ed. by J. E. ASPELL, e0216858.

[3] E. AMOS: *Oculus Rift Consumer-version1 HMD*, `https://commons.wikimedia.org/wiki/File`, [Online Avilable], 2020.

[4] D. HOY, L. MARCH, P. BROOKS, F. BLYTH, A. WOOLF, C. BAIN, G. WILLIAMS, E. SMITH, T. VOS, J. BARENDREGT, C. MURRAY, R. BURSTEIN, R. BUCHBINDER: *The global burden of low back pain: estimates from the Global Burden of Disease 2010 study*, Annals of the Rheumatic Diseases 73.6 (Mar. 2014), pp. 968–974.

[5] T. F. LARSEN: *Virtual Reality games and gamified exercises in physiotherapeutic treatment of non-specific low back pain patients with kinesiophobia.* The University of Bergen (2018).

[6] M. D. ROGERSON, R. J. GATCHEL, S. M. BIERNER: *A Cost Utility Analysis of Interdisciplinary Early Intervention Versus Treatment as Usual For High-Risk Acute Low Back Pain Patients*, Pain Practice 10.5 (Aug. 2010), pp. 382–395.

[7] M. SIGERSETH: *Virtual Reality training for patients with non-specific persistent low back pain and pain-related fear of movement: A single-subject experimental study*, The University of Bergen (2018).

[8] A. P. VERHAGEN, A. DOWNIE, N. POPAL, C. MAHER, B. W. KOES: *Red flags presented in current low back pain guidelines: a review*, European Spine Journal 25.9 (July 2016), pp. 2788–2802.

On an approach for clustering social media data

Zhanna Lopuliak[a], Hanna Livinska[a]

[a]Taras Shevchenko National University of Kyiv, Ukraine
zhanna.lopuliak@gmail.com, livinskaav@gmail.com

Introduction

In today's growing internet marketing access to customer information is almost a crucial success factor and the better the information is gathered, the better a company can meet its customers' needs [2]. To reasons for businesses to use personalization belong: more sales less unsubscribes; better conversion; better customer experience; fewer follow-up emails, due to sending just highly relevant; saving money and time [5]. As an example, the successful campaigns of Amazon, Cadbury's, and Netflix, where personalization usage contributed to their success, can be pointed out.

The increasing influence of social media and the enormous participation of users proceed with new opportunities to found out some emotional and behaviouristic similarities among various people in a social network, as well as to use these similarities for creating certain marketing efforts. Every internet user's click can potentially be a part of marketing information. Approaches with clustering social media data are needed as well to directly support the companies' teams in understanding, monitoring, and motivation the evolution of user's reactions in social media.

Therefore, one of the up-to-date problems for marketing strategies building is to distinguish different groups of internet users to send them correspondent responses or promotions. For instance, users with a highly positive reaction with a large number of subscribers can be chosen for more active promotions of additional bonuses, loyalty programs, etc. Such a problem can be solved based on some interpretation of social media logs, discussions, amounts of reactions, comments.

Last decade, many works were devoted to the discovery of clusters or communities. A similar approach is analyzed id [3]. Different approaches are summarized in [1].

In our work we propose a model for users clusterization based on their social media activity with an accent on their emotional behavior and leadership features using the k-mean clustering technique.

Model description

For our model data from one social network were collected. We scraped the user's post where four different airlines were mentioned, assigned a numeric sentiment score to each, and clustered data based on this and some other characteristics. For each sample object following features were included: text of a post, number of user followers, number of "favorite", number of reposts, and number of lists, to which user was added.

To access data from selected social media, special credentials are required. A developer account was created to get them.

Firstly, collected data was cleaned (posts, where a lot of users or hashtags were mentioned, were deleted). To measure the emotions of the writer, dictionary 'VADER' was used, which is a lexicon and rule-based sentiment analysis tool. We form a compound assessment of the post and use it for further clustering. This assessment yields quite precise measuring of post sentiments. Among different clustering methods we choose k-means, it fits well for our purpose [4]. In order to have equally-weighted features, as needed for k-means clustering, feature range was normalized.

Secondly, to reduce model dimension, PCA (principal components analysis) was applied. Figure 1 (dimensions - Polarity, Followers count, Favorite count) and Figure 2 show data points before and after applying PCA.

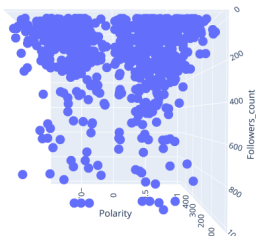


Figure 3: Data points before applying PCA

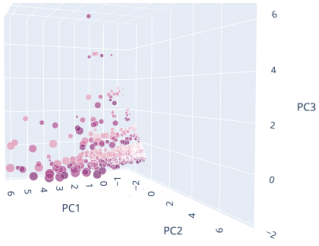


Figure 4: Data points after applying PCA

To determine the number of clusters the Elbow method and the Silhouette method were used. Figure 5 shows that the optimal number of clusters for our dataset is k = 4.

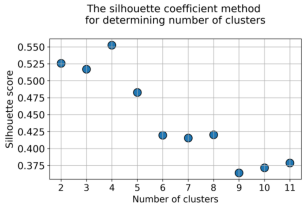


Figure 5: Silhouette coefficient values

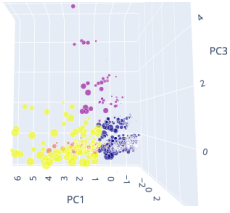


Figure 6: Data points after clustering

The program is written in execution environment Jupyter Notebook, the programming language is Python, main packages used for scrapping data, creating visualizations, and performing computations are `'tweepy'`, `'plotly'`, `'nltk'` and `'scikit-learn'`.

Results and future research

After applying k-means clustering on the prepared dataset, we got 4 clusters, which could nearly be described as groups with good/bad attitude towards the company and larger/fewer number of followers. Data points, divided into clusters, are shown in Figure

4. In the real business model, a company would have a different approach to potential clients from each cluster.

Future work on this topic should focus on clearly identifying the specific causes of customer satisfaction and dissatisfaction, that would reveal the most common problems and advantages. The analysis of user loyalty to brands could also be expanded by using more features, e.g. date after the launch of a new product or geodata to analyze reviews from a particular area.

Keywords: personalization, clustering, social network analysis, market segmentation

References

[1] N. ALNAJRAN, K. A. CROCKETT, D. MCLEAN, A. LATHAM: *Cluster Analysis of Twitter Data: A Review of Algorithms*, in: ICAART, 2017.

[2] M. R. BROWN, R. MUCHIRA: *Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior*, J. Electron. Commer. Res. 5 (2004), pp. 62–70.

[3] V. FRIEDEMANN: *Clustering a Customer Base Using Twitter Data*, in: 2015.

[4] U. KAUR, S. GURU: *Comparison Between K-Mean and Hierarchical Algorithm Using Query Redirection*, in: Computer Science, 2013.

[5] N. SAHNI, S. WHEELER, P. CHINTAGUNTA: *Personalization in Email Marketing: The Role of Noninformative Advertising Content*, Mark. Sci. 37 (2018), pp. 236–258.

Motor Imagery EEG Classification using Feedforward Neural Network*

Tamás Majoros[a], Stefan Oniga[a], Yu Xie[a]

[a]Intelligent Embedded Systems Research Laboratory, Faculty of Informatics, University of Debrecen
majoros.tamas@inf.unideb.hu, oniga.istvan@inf.unideb.hu, 741910908@qq.com

Electroencephalography (EEG) is a complex voltage signal of the brain and its correct interpretation requires years of training. Modern machine-learning methods help us to extract information from EEG recordings and therefore several brain-computer interface (BCI) systems use them in clinical applications [4]. These system allow persons with disabilities or paralysis to communicate [3] and to control robots [5]. Accurate classification of motor-imagery based EEG is inevitable in developing such BCI applications.

By processing the publicly available PhysioNet EEG dataset [2], we extracted information that can be used to train feedforward neural network to classify three types of activities performed by 109 volunteers. While volunteers were performing different activities, a BCI2000 system was recording their EEG signals from 64 electrodes. In our work we used that kind of motor imagery runs where a target appeared on either the top or the bottom of a screen. The subject had been instructed to imagine opening and closing either both fists (if the target is on top) or both feet (if the target is on the bottom) until the target disappears.

We used the EEGLAB Matlab toolbox [1] for EEG signal processing and applied several feature extraction techniques. Then we instantiated feedforward, multi-layer perceptron (MLP) networks with different structures (number of layers, number of neurons) and evaluated their classification performance. 70% of the data was used for training, 30% for testing, accuracy for test data was 71.5%.

Keywords: neural network, multilayer perceptron, classification, EEG, BCI

References

[1] A. DELORME, S. MAKEIG: *EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics including independent component analysis*, Journal of Neuroscience Methods 134.1 (2004), pp. 9–21, DOI: https://doi.org/10.1016/j.jneumeth.2003.10.009.

[2] A. L. GOLDBERGER, L. A. AMARAL, L. GLASS, J. M. HAUSDORFF, P. C. IVANOV, R. G. MARK, J. E. MIETUS, G. B. MOODY, C. K. PENG, H. E. STANLEY: *PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals*, Circulation 101.23 (2000), pp. 215–220,
DOI: https://doi.org/10.1161/01.CIR.101.23.e215.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

[3] F. NIJBOER, E.W.SELLERS, J.MELLINGER, M.A.JORDAN, T.MATUZ, A.FURDEA, S.HALDER, U.MOCHTY, D.J.KRUSIENSKI, T.M.VAUGHAN, J.R.WOLPAW, N.BIRBAUMER, A.KÜBLER: *A P300-based brain–computer interface for people with amyotrophic lateral sclerosis*, Clinical Neurophysiology 119.8 (2008), pp. 1909–1916,
DOI: https://doi.org/10.1016/j.clinph.2008.03.034.

[4] R. T. SCHIRRMEISTER, J. T. SPRINGENBERG, L. D. J. FIEDERER, M. GLASSTETTER, K. EGGENSPERGER, M. TANGERMANN, F. HUTTER, W. BURGARD, T. BALL: *Deep learning with convolutional neural networks for EEG decoding and visualization*, Human Brain Mapping 38.11 (2017), pp. 5391–5420,
DOI: https://doi.org/10.1002/hbm.23730.

[5] L. TONIN, T. CARLSON, R. LEEB, J. DEL R MILLÁN: *Brain-controlled telepresence robot by motor-disabled people*, Annual International Conference of the IEEE Engineering in Medicine and Biology Society (2011), pp. 4227–4230,
DOI: https://doi.org/10.1109/iembs.2011.6091049.

Comparison of Similarity-based Rough Sets and Covering Approximation Spaces on Real Data*

Dávid Nagy[a], Tamás Mihálydeák

[a]University of Debrecen, Faculty of Informatics
nagy.david@inf.unideb.hu
mihalydeak@unideb.hu

Nowadays the amount of data is growing exponentially. However, this data is often incomplete or inconsistent. There can be many reasons why a value is missing. For example, it can be unknown, unassigned, or even inapplicable. Inconsistency occurs when the data is contradictory. These issues can cause some undesirable events (bad prediction, inappropriate decision making, etc). In computer science, there are numerous ways to handle these kinds of inaccuracies. Rough set theory can be considered as a rather new field in computer science. Its fundamentals were proposed by Zdislaw Pawlak in the 80's [3–5]. The Pawlakian systems handle the uncertainty among the data with a relation that is based on the indiscernibility of objects. In many cases, based on the available knowledge, two objects cannot be distinguished from each other. Two arbitrary objects can be treated as indiscernible if all of their known properties are the same. This indiscernibility can be modeled by an equivalence relation that represents our background knowledge or its limits. It can affect the membership relation by making the judgment on this relation uncertain. It makes a set vague because a decision about a certain object has an effect on the decisions about all the objects that are indiscernible from the given object. In this case, if we would like to check, whether an object is in a set, then the following three possibilities appear:

- the object is surely in the set if all the objects that are indiscernible from the given object, are in the set;
- the object may be in the set if there are some objects that are in the set and are indiscernible from the given object;
- it is sure that the object is not in the set if all the objects that are indiscernible from the given object, are not in the set.

The equivalence relation (representing indiscernibility) defines a partition of a given set of objects (often called the universe). The equivalence classes are called base sets and they contain those objects that are indiscernible from each other. So the system of base sets represent the background knowledge or sometimes its limit.

A rough set can be defined as a pair of sets such that the first is a subset of the second. If a rough set represents a set, then the lower approximation is the first member and the upper approximation is the second one. The lower approximation contains objects that

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

surely belong to the set, and the upper approximation contains objects that possibly belong to the set. Their difference is called the boundary region. If the boundary region of a set is non-empty, then the given set is rough. So, a rough set does not have a "clear" boundary. A rough set can also be characterized numerically by the accuracy of the approximation which is the fraction of the cardinalities of the lower and upper approximation.

In practical applications not only the indiscernible objects must be handled in the same way but also those that are similar to each other based on some property. Over the years, some new approximation spaces have been developed (they are generalizations of the original Pawlakian space). The main difference between these spaces (with a Pawlakian approximation pair) lies in the definition of the system of base sets. Covering-based approximation spaces generated by tolerance relations [6] generalize Pawlakian approximation spaces in the following points:

- The equivalence relation representing indiscernibility is replaced with a tolerance relation representing similarity.
- Every base set has a generator object. The members of the given base set are the objects that are similar to the generator object.

Therefore, a base set contains objects that are similar to a distinguished member. This means that the similarity to a given element is considered not the similarity in general. The number of base sets is not more than the number of members of the universe, so there are too many base sets for practical applications.

Correlation clustering [1] is a clustering technique that is based on a tolerance relation. Its result is a partition. The gained clusters contain objects that are mostly similar to each other. In the authors' previous work, it was shown that the partition can be understood as a system of base sets. As a result, a new approximation space appears, called similarity-based rough sets [2]. It uses the same tolerance relation as the aforementioned covering spaces and it has the following good properties:

- the similarity among objects is taken into account not the similarity to a given object;
- the base sets are pairwise disjoint sets;
- only the necessary number of base sets appears;
- the size of base sets is not too small, or too big.

In this work, we use some widely-used data sets to compare the developed approximation space to the tolerance relation-based covering space. We use several accuracy measures to test how well the methods can approximate different sets, and we also compare the execution time of the approximation processes. The similarity-based rough sets space provided a much faster and a more precise result which is inevitable in practical applications.

Keywords: rough set theory, correlation clustering, set approximation

References

[1] N. BANSAL, A. BLUM, S. CHAWLA: *Correlation clustering*, Machine Learning 56.1-3 (2004), pp. 89–113,
DOI: http://dx.doi.org/10.1023/B:MACH.0000033116.57574.95.

[2] D. NAGY, T. MIHÁLYDEÁK, L. ASZALÓS: *Similarity Based Rough Sets*, in: Rough Sets: International Joint Conference, IJCRS 2017, Olsztyn, Poland, July 3–7, 2017, Proceedings, Part II, ed. by L. POLKOWSKI, Y. YAO, P. ARTIEMJEW, D. CIUCCI, D. LIU, D. ŚLĘZAK, B. ZIELOSKO, Cham: Springer International Publishing, 2017, pp. 94–107, ISBN: 978-3-319-60840-2,
DOI: https://doi.org/10.1007/978-3-319-60840-2_7.

[3] Z. PAWLAK ET AL.: *Rough sets: Theoretical aspects of reasoning about data*, Systern Theory, Knowledge Engineering and Problem Solving, Kluwer Academic Publishers, Dordrecht, 199l 9 (1991).

[4] Z. PAWLAK: *Rough sets*, International Journal of Parallel Programming 11.5 (1982), pp. 341–356.

[5] Z. PAWLAK, A. SKOWRON: *Rudiments of rough sets*, Information sciences 177.1 (2007), pp. 3–27.

[6] A. SKOWRON, J. STEPANIUK: *Tolerance approximation spaces*, Fundamenta Informaticae 27.2 (1996), pp. 245–253.

The impact of server reliability on the characteristics of cognitive radio systems*

Hamza Nemouchi[a], Mohamed Hedi Zeghouani[b], János Sztrik[c]

[ab] Doctoral School of Informatics, University of Debrecen

[a] nemouchih@gmail.com

[b] zeghouani.hedi@gmail.com

[c] Faculty of Informatics, University of Debrecen
sztrik.janos@inf.unideb.hu

The present paper deals with a finite-source retrial queuing system, which has two service channels that use the cognitive technology. For more details on the system model, see [1], [6], [8], [7], [4].

In this paper, finite-source retrial queueing cognitive radio system is analyzed with the following assumptions. Consider two interconnected subsystems, where the licensed requests are generated by finite number of sources N_1. These sources generate primary calls corresponding to an exponentially distributed time with an average value of $1/\lambda_1$ which are sent to the primary service unit. If the server is idle, the service starts immediately. If the server is busy, the call joins a preemtive priority queue. The primary service time is supposed to be exponentially distributed random variable with a mean $1/\mu_1$. For the secondary part, the number of sources is denoted by N_2. Each source generates low priority calls according to an exponentially distributed time with mean value of $1/\lambda_2$. The secondary service time is exponentially distributed with a parameter μ_2. We assume that the secondary service unit is non-reliable, which means that the server is subject to random failures depending on whether it is busy or idle. The secondary service unit may fail after a time, which is generally distributed with a rate θ_2 when it is idle, and γ_2 when it is busy. The operating time (or inter-failure time) during busy or idle state is supposed to be hyper-exponential, hypo-exponential, gamma, lognormal and Pareto distributed random variables. Similarly, the same holds for repair times with rate σ_2. The retrial time of the secondary customers is supposed to be exponentially distributed random variable with a parameter ν.

In [2], [5], [3], the authors applied a tool-supported approach to determine the most important operating characteristics of the system. They examined several scenarios of server unreliability in a system as complex as this, which allows an exponential distribution of operation and repair time.

The aim of this paper is to investigate the impact of the various distributions on the performance measures of the secondary part of the system. Using stochastic simulation,

*The work of János Sztrik is supported by the EFOP-3.6.1-16-2016-00022 project. The project is co-financed by the European Union and the European Social Fund. The work of Mohamed Hedi Zaghouani is supported by the Stipendium Hungaricum scholarship.

several scenarios of the servers unreliability are treated.

Keywords: finite-source retrial queueing systems, cognitive radio networks, non-reliable servers, performance and reliability analysis, simulation modeling.

References

[1] B. ALMÁSI, T. BÉRCZES, A. KUKI, J. SZTRIK, J. WANG: *Performance Modeling of Finite-Source Cognitive Radio Networks*, Acta Cybernetica 22.3 (2016), pp. 617–631, DOI: https://doi.org/10.14232/actacyb.22.3.2016.5.

[2] B. ALMÁSI, J. ROSZIK, J. SZTRIK: *Homogeneous Finite-Source Retrial Queues with Server Subject to Breakdowns and Repairs*, Mathematical and Computer Modelling 42 (2005), pp. 673–682, DOI: https://doi.org/10.1016/j.mcm.2004.02.046.

[3] A. KUKI, T. BÉRCZES, B. ALMÁSI, J. SZTRIK: *A queueing model to study the effect of network service breakdown in a CogInfoCom system*, Proceedings of the 2013 IEEE 4th International Conference on Cognitive Infocommunications (CogInfoCom) (2013), pp. 205–210, DOI: https://doi.org/10.1109/CogInfoCom.2013.6719242.

[4] A. M. LAW, W. D. KELTON: *Simulation Modeling and Analysis*, second edition, McGraw-Hill College, 1991.

[5] J. SZTRIK, B. ALMÁSI, J. ROSZIK: *Heterogeneous finite-source retrial queues with server subject to breakdowns and repairs*, Journal of Mathematical Sciences 132 (2006), pp. 677–685, DOI: https://doi.org/10.1007/s10958-006-0014-0.

[6] J. SZTRIK, T. BÉRCZES, H. NEMOUCHI, A. Z. MELIKOV: *Performance modeling of finite-source cognitive radio networks using simulation*, Communications in Computer and Information Science. Springer 678 (2016), pp. 64–73, DOI: https://doi.org/10.1007/978-3-319-51917-3_7.

[7] Y. XIAO, F. HU: *Cognitive Radio Networks*, CRC Press, 2008.

[8] Y. ZHANG, J. ZHEND, H. CHEN: *Cognitive Radio Networks: Architectures, Protocols, and Standards*, CRC Press, 2016.

Classifying Raman spectroscopy data using machine learning algorithms for diagnosing infection with SARS-COV-2

Róbert István Oniga

oniga.robi@gmail.com

The rapid development of the corona crisis requires novel methods and approaches that could help flatten the curve. For this reason a new detection method is investigated in order to diagnose in a faster and more reliable manner the disease and help prevent the spread. Raman spectroscopy on blood serum is a potential candidate for this issue and thus, research was done towards this direction.

Introduction

In December 2019, a novel virus has emerged and in a brief period it has reached all the corners of the world. This virus is called the corona virus and it has affected all people. Due to the continuous rise in the number of infected and deceased persons, a new approach must be taken in order to deal with this situation. Since the measures taken to isolate infected individuals had no significant result, perhaps the development of a new detection method that is more precise and rapid could prevent the further spread of the virus [1]. A possible detection method that could satisfy the requirements is Raman spectroscopy.

Used method

Raman spectroscopy is a method that relies on a nonionizing laser that can excite a molecule if the energy of the incident photon matches the energy gap between the ground state and the excited state of said molecule. The phenomena of fluorescence will occur when the molecule relaxes and generates emission of photons in both the visible and near-infrared spectral ranges. The emission can happen either by means of a elastic scattering which has no relevant information, or plastic scattering which means that a part of the energy was absorbed and only a fraction of that was released back into the medium. That difference in terms of energy is studied in order to obtain relevant information that may be used for bio-medical applications but not only [2].

In many bio-medical applications that include the use of Raman spectroscopy, the probe being analyzed is blood serum. Many important features can be observed that prove to be relevant in diagnosis. Knowingly, the use of Raman spectroscopy on blood serum is proposed to be used as a novel detection method of infection with the SARS-COV-2 virus. For this, a database containing the Raman spectra of healthy and infected people

was used in order to create a machine learning algorithm capable of extracting discriminatory features that can be used to detect infected individuals. The applied method was a supervised-learning algorithm called linear discriminant analysis (LDA). Additionally, leave-one-out cross-validation was applied in order to obtain a more accurate result. The overall accuracy, sensitivity and specificity were taken into consideration in order to assess the performance of the created model for this task (Table 1).

Accuracy	93.55%
Sensitivity	83.33%
Specificity	90.38%

Table 1: Performance of the classifier

Results

The dataset was composed of a total of 309 individuals of which 150 were healthy and 159 were infected with the corona virus [3]. The dataset was divided into a training and test set (70% training and 30% test). The created model had an accuracy of 93.5%. To be more accurate when talking about the rate of success of the model the exact percentages are discussed: the percentage of correctly identified healthy individuals was 100% and the percentage of correctly identified infected individuals 86.7% while the rest of 13.3% were labeled as healthy (Figure 1). The predominant features in terms of wave-number were in the following ranges: [400-591]cm^{-1}, [647-673]cm^{-1}, [721-798]cm^{-1}, [820-896]cm^{-1}, and [1003-1241]cm^{-1}. This means that the features that best prove the presence of the virus in the blood serum scatter photons in these ranges of wave-numbers and energies, respectively.

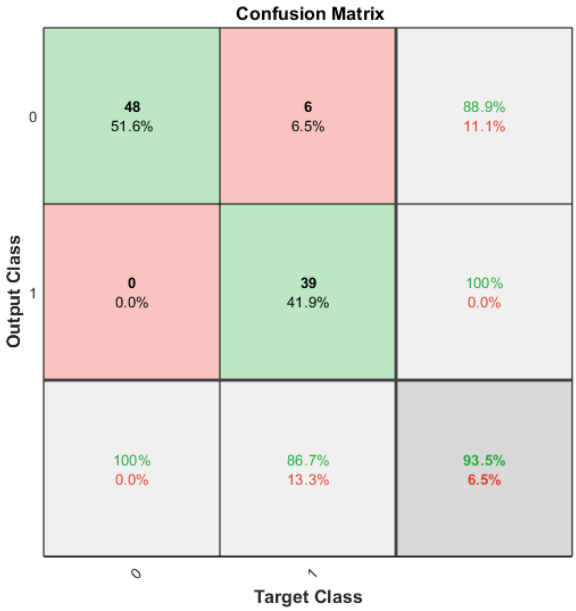


Figure 1: Confusion matrix

Keywords: SARS-COV-2, LDA, Raman spectroscopy, data processing.

References

[1] S. Ludwig, A. Zarbock: *Coronaviruses and SARS-CoV-2: A Brief Overview*, Anesthesia & Analgesia 131.1 (2020), pp. 93–96,
DOI: https://doi.org/doi:10.1213/ane.0000000000004845.

[2] Q. Tu, C. Chang: *Diagnostic applications of Raman spectroscopy*, Nanomedicine: Nanotechnology, Biology and Medicine 8.5 (2012), pp. 545–558,
DOI: https://doi.org/doi:10.1016/j.nano.2011.09.013.

[3] G. Yin, L. Li, S. Lu, Y. Yin, Y. Su, Y. Zeng, et al.: *Data and code on serum Raman spectroscopy as an efficient primary screening of coronavirus disease in 2019 (COVID-19)*, Nanomedicine: Nanotechnology, Biology and Medicine (2020),
DOI: https://doi.org/10.6084/m9.figshare.12159924.v1.

Adding Cardinality Constraint Support to CryptoMiniSat

Krisztián Palanek[a], **Gergely Kovásznai**[a]

[a]Eszterházy Károly University, Eger, Hungary

Introduction

Recently, reasoning over Boolean Cardinality Constraints (BCCs) gains in importance by the advent of deep learning approaches, or more precisely, by the formal verification of Binarized Neural Networks (BNNs) [3]. Another recent example of problems that can be encoded as BCCs is the optimization of Wireless Sensor Networks (WSNs) [1]. The encoding of such practical problems typically generates a large amount of BCCs.

There exist approaches that can naturally reason over BCCs such as integer linear programming, Satisfiability Modulo Theories (SMT), pseudo-Boolean solving approaches etc., but in most of the cases those are not efficient enough when solving large amount of BCCs, compared to SAT approaches. On the other hand, SAT approaches force BCCs to be converted to CNF, causing blowup in the encoding.

There exists, however a SAT solver called MiniCARD [2] that provides native support for BCCs on the level of Conflict-Driven Clause Learning (CDCL). For large amount of BCCs, MiniCARD typically outperforms [1] any of the aforementioned solvers, despite the fact that MiniCARD is considered to be an outdated solver and its source code did not get any update in the last 5 years. In this work, we add native support for BCCs to a state-of-the-art full-fledged SAT solver called CryptoMiniSat [5], in a similar way as it was done in MiniCARD, that is, on the CDCL-level, including the generalization of the clause datastructure and the watched literals scheme, Boolean constraint propagation, conflict analysis and clause learning. CryptoMiniSat is recently used as the underlying SAT solver inside the approximate model counter ApproxMC [4], due to CryptoMiniSat's native support for XOR clauses. Our work could make it feasible to count models over BNNs, which could be useful in the comparative analysis of BNNs.

Native support for Boolean Cardinality Constraints

A Boolean Cardinality Constraint (BCC) is a constraint on the number of literals which are true among a given set of literals. There are two kinds of BCCs:

$$\text{Atmost: } \sum_{i=1}^{n} l_i \leq c \tag{0.1}$$

$$\text{Atleast: } \sum_{i=1}^{n} l_i \geq c \tag{0.2}$$

where $l_1, \ldots, l_n$ are Boolean literals and $c \in \mathbb{N}$ is a constant where $0 \leq c \leq n$. Atmost (0.1) determines the maximum number of variables that are allowed to be true, on the other hand, Atleast (0.2) determines the minimum number of variables to be true.

The key fact is that BCC generalizes the definition of a clause, which comes from the fact that a clause $l_1 \vee \cdots \vee l_n$ can be interpreted as an Atleast BCC $\sum_{i=1}^{n} l_i \geq 1$. This allows us to extend any CDCL SAT solver into a Cardinality solver using the following techniques.

First, we extend the clause data structure with two additional fields. One of them is a flag indicating whether the clause is an Atmost constraint or a regular clause. The other one is for the bound, or more precisely, the number of literals to be watched, which can be calculated from the bound.

Then, we generalize the 2-watched-literal scheme, which is basic technique in CDCL SAT solvers, into an m-watched literal scheme, where

$$m = n - c + 1, \tag{0.3}$$

n is the number of literals and c is the bound. This formula is specifically for Atmost BCCs. Note that any Atleast constraint $\sum_{i=1}^{n} l_i \geq c$ can always be translated to an Atmost constraint $\sum_{i=1}^{n} \neg l_i \ \leq n - c$, therefore the solver implementation only needs to support Atmost BCCs.

Using these techniques, any CDCL SAT solver can be extended into a Cardinality solver without requiring any extensive modification to conflict detection, clause learning and other higher functionalities.

Implementation and validation

We extended CryptoMiniSat with the techniques mentioned above. The solver is now able to receive Cardinality Constraints as input, parse them and handle them accordingly.

We also extended the solvers verification module (fuzzer). The module uses a third party solver to verify whether the solvers output is correct based on the input.

Our preliminary experiments were run with promising resutls, however there are still some inaccurate results coming from the solver. In the future we hope to fix these issues and run more extensive experiments, then use the solver with ApproxMC to count models over Binarized Neural Networks.

References

[1] G. KOVÁSZNAI, K. GAJDÁR, L. KOVÁCS: *Portfolio SAT and SMT Solving of Cardinality Constraints in Sensor Network Optimization*, in: 21st International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2019, pp. 85–91,
DOI: https://doi.org/10.1109/SYNASC49474.2019.00021.

[2] M. H. LIFFITON, J. C. MAGLALANG: *A Cardinality Solver: More Expressive Constraints for Free*, in: Theory and Applications of Satisfiability Testing – SAT 2012, vol. 7317, Lecture Notes in Computer Science, Springer, 2012, pp. 485–486, ISBN: 978-3-642-31612-8, DOI: https://doi.org/10.1007/978-3-642-31612-8_47.

[3] N. NARODYTSKA, S. KASIVISWANATHAN, L. RYZHYK, M. SAGIV, T. WALSH: *Verifying Properties of Binarized Deep Neural Networks*, in: 32nd AAAI Conference on Artificial Intelligence, 2018, pp. 6615–6624.

[4] M. SOOS, S. GOCHT, K. S. MEEL: *Tinted, Detached, and Lazy CNF-XOR Solving and Its Applications to Counting and Sampling*, in: Computer Aided Verification, ed. by S. K. LAHIRI, C. WANG, Cham: Springer International Publishing, 2020, pp. 463–484, ISBN: 978-3-030-53288-8.

[5] M. SOOS, K. NOHL, C. CASTELLUCCIA: *Extending SAT Solvers to Cryptographic Problems*, in: Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings, ed. by O. KULLMANN, vol. 5584, Lecture Notes in Computer Science, Springer, 2009, pp. 244–257, DOI: https://doi.org/10.1007/978-3-642-02777-2_24.

A continuous-time random graph model*

Bettina Porvázsnyik[a]

[a]University of Debrecen, Debrecen, Hungary
porvazsnyik.bettina@inf.unideb.hu

Network theory is one of the most actively studied area of both theoretical and applied probability. Random graphs are frequently used to model complex networks. In the last few decades a large number of evolving random graph models were introduced to describe real-life networks. For an overview see e.g. [2–4, 6, 7].

Empirical results show that large networks have several common features. It is known that many real-world networks (e.g. the world wide web (WWW), social or biological networks) are scale-free that is their asymptotic degree distributions follow power-laws. One of the most studied discrete time models is the preferential attachment model which was introduced by Barabási and Albert (see [3]) to describe the scale-free nature of real-world networks. On the other hand, the continuous-time models seem to be more appropriate to model real-world networks. For an overview and introduction see [1, 2, 4, 7, 8].

In our paper we define and study a continuous-time evolving random graph model. The examined model is a generalization of the model introduced by Móri and Rokob in [9]. An extension of Móri and Rokob's model describing the interactions of 3 vertices was examined by Fazekas, Barta, Noszály and Porvázsnyik in [5]. The results of our paper are also valid for the 3 vertices model.

The main units of our model are complete graphs on N vertices (N-cliques) where $N \geq 3$ is a fixed integer. During their lifetime, each individual (N-clique) reproduce according to independent Poisson processes with rate 1. At the initial time $t = 0$ we are starting with a single complete graph on N-vertices. At each birth event one new vertex is added to the graph which is connected to its ancestor N-clique with random but bounded number of edges. In this way new complete graphs on N vertices (offsprings) can be created. After their birth, the offspring N-cliques can also start producing offsprings, and so on. We remark that

The asymptotic behaviour of the number of vertices and the asymptotic behaviour of the number of m-cliques ($2 \leq m \leq N$) are studied. The proofs are based on general results of the theory of branching processes.

References

[1] K. B. ATHREYA, A. P. GHOSH, S. SETHURAMAN: *Growth of preferential attachment random graphs via continuous-time branching processes*, Proc. Indian Acad. Sci. Math. Sci. 118.3 (2008), pp. 473–494, DOI: https://doi.org/10.1007/s12044-008-0036-2.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

[2] K. B. ATHREYA, P. E. NEY: *Branching Processes*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer, Berlin, Heidelberg, 1972,
DOI: https://doi.org/10.1007/978-3-642-65371-1.

[3] A. L. BARABÁSI, R. ALBERT: *Emergence of scaling in random networks*, Science 286.5439 (1999), pp. 509–512.

[4] B. BOLLOBÁS, O. RIORDAN: *Random Graphs and Branching Processes*, in: Handbook of Large-Scale Random Networks, Bolyai Society Mathematical Studies, ed. by B. BOLLOBÁS, R. KOZMA, D. MIKLÓS, vol. 18, Springer, Berlin, Heidelberg, 2008,
DOI: https://doi.org/10.1007/978-3-540-69395-6_1.

[5] I. FAZEKAS, A. BARTA, C. NOSZÁLY, B. PORVÁZSNYIK: *A continuous-time evolution model describing 3-interactions*, preprint (2020), submitted for publication.

[6] P. HACCOU, P. JAGERS, V. A. VATUTIN: *Branching Processes: Variation, Growth and Extinction of Populations*, Cambridge University Press, 2005.

[7] R. VAN DER HOFSTAD: *Random Graphs and Complex Networks. Vol. 1.* Cambridge Series in Statistical and Probabilistic Mathematics, 2017.

[8] P. JAGERS: *Branching Processes with Biological Applications*, Wiley, London, 1975.

[9] T. F. MÓRI, S. ROKOB: *A random graph model driven by time-dependent branching dynamics*, Annales Univ. Sci. Budapest., Sect. Comp. 46 (2017), pp. 191–213.

Compositional Trend Filtering*

Christopher Rieser[a], Peter Filzmoser[a]

[a] Institute of Statistics and Mathematical Methods in Economics, Computational Statistics.
christopher.rieser@tuwien.ac.at
p.filzmoser@tuwien.ac.at

Introduction

We consider trend filtering for multivariate time series in a compositional data context. Filtering trends, e.g. piecewise linear functions, of a univariate time series has been extensively investigated and many good methods exist, see [2] or [3]. To the best of our knowledge, so far none of these methods have been extended to compositional data. However, since [1] it has been made clear that a compositional view can be advantageous when the relative rather than the absolute information is of interest. Consider, for example, the case where we compare the number of healthy individuals to infected ones in the whole population. In such a setting, not the absolute number of infections but rather the relative number to the whole population might be more meaningful. This perspective is relevant in many other contexts, e.g. comparing the performance of different stocks, and it explains the success of compositional data analysis methods in various applications. The method we propose guarantees to find an estimator of piecewise (compositional) linear trends, naturally being strictly positive and summing up to a given total. This is a necessity when we want to use further compositional data analysis tools like log-ratios, pivot-coordinates, etc. for the estimated trends.

Compositional trend filtering

In the following, consider a vector $\boldsymbol{x} \in \mathbb{R}^D$ with D strictly positive entries which sum up to 1. This leads to the definition of compositional data as observations from the D part simplex $\mathcal{S}^D$,

$$\mathcal{S}^D := \left\{ \boldsymbol{x} = (x_1, ..., x_D)' \in \mathbb{R}^D_+, \sum_{i=1}^{D} x_i = 1 \right\}.$$

The constraint of sum equal to 1 can always be achieved by rescaling, and rescaling will not change the analyses later on, because they are all based on log-ratio information between the compositional parts. The simplex can be equipped with an addition, multiplication with a scalar, an inner product and a norm, which leads to the so-called Aitchison geometry on the simplex [1]:

*This research was supported by the Austrian Science Fund(FWF) under the grant number P 32819 Einzelprojekte.

- For $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{S}^D$, perturbation is defined as $\boldsymbol{x} \oplus \boldsymbol{y} := (x_1 y_1, ..., x_D y_D)'$.
- For $\boldsymbol{x} \in \mathcal{S}^D$ and $\alpha \in \mathbb{R}$, powering is defined as $\alpha \odot \boldsymbol{x} := (x_1^\alpha, ..., x_D^\alpha)'$.
- For $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{S}^D$, the inner product is defined as

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_A := \frac{1}{2D} \sum_{i=1}^{D} \sum_{j=1}^{D} \log\left(\frac{x_i}{x_j}\right) \log\left(\frac{y_i}{y_j}\right).$$

- The Aitchison norm is defined as $\|\boldsymbol{x}\|_A = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle_A}$.

Given a compositional time series, i.e. a time series $\boldsymbol{x}_t$ with elements in the D part simplex $\mathcal{S}^D$, we then define the trend filtering estimator of the compositional time series $\boldsymbol{x}_t$ as:

$$(\hat{\boldsymbol{a}}_1, ..., \hat{\boldsymbol{a}}_T)' := \underset{\boldsymbol{a}_t \in \mathcal{S}^D}{\arg\min} \ \frac{1}{2} \sum_{t=1}^{T} \|\boldsymbol{x}_t \ominus \boldsymbol{a}_t\|_A^2 + \frac{\lambda}{2} \sum_{t=3}^{T} \left\|\Delta^2 \boldsymbol{a}_t\right\|_A, \tag{0.1}$$

where $\Delta^2 \boldsymbol{a}_t$ denotes $\boldsymbol{a}_t \ominus 2\boldsymbol{a}_{t-1} \oplus \boldsymbol{a}_{t-2}$, for a fixed $\lambda > 0$. This means that we fit T vectors $\hat{\boldsymbol{a}}_1, ..., \hat{\boldsymbol{a}}_T \in \mathcal{S}^D$ to the observed data $\boldsymbol{x}_1, ..., \boldsymbol{x}_T$, taking into account a given level of smoothness controlled by the penalty term. When λ goes to infinity we get $\Delta^2 \boldsymbol{a}_t = 0$ which can be shown to be equal to $\boldsymbol{a}_t = \boldsymbol{a} \oplus (t \odot \boldsymbol{b})$, for all t, for some $\boldsymbol{a}$ and $\boldsymbol{b}$ in $\mathcal{S}^D$; i.e. $\boldsymbol{a}_t$ is a linear function in the compositional sense. We show how to solve efficiently Problem (0.1), and that for a range of different λ values, the estimated $\boldsymbol{a}_t$ describes a compositional piecewise linear multivariate time series.

Results

To illustrate the utility of the method we look at the number of Corona infections, per 100,000 inhabitants, in 9 different countries between 2020-03-01 and 2020-07-31. This data is publicly available at `https://ourworldindata.org/coronavirus-testing`. Figure 1 displays the estimated $\hat{\boldsymbol{a}}_t$ in log-ratio coordinates comparing Austria to 8 other European countries: each plot shows the log-ratio for a pair of countries, i.e. $\log\left(\frac{(\hat{\boldsymbol{a}}_t)_i}{(\hat{\boldsymbol{a}}_t)_j}\right)$ where i resp j denotes the i-th resp j-th entry in $\hat{\boldsymbol{a}}_t$ corresponding to a certain country. We can see from the log-ratio between Austria and Germany that Austria since July has had increasingly more cases than Germany. This upward trend has already started at the beginning of May when Austria still had less positive cases. At the same time the trend for the log-ratio between Austria and Italy started to change. This means that the positive cases per 100,000 inhabitants in Austria had been growing at a faster pace compared to each, Germany and Italy, since beginning of July. Finland has had since May, increasingly less numbers of infections than Austria.

Keywords: Compositional Data, Trend Filtering

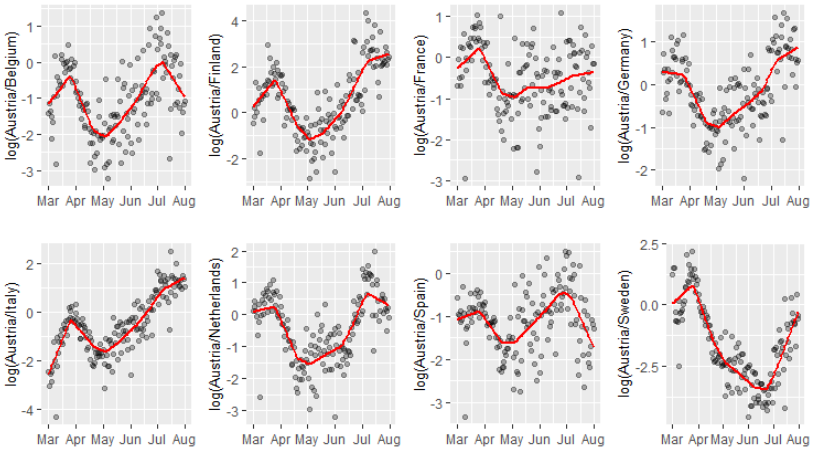


Figure 1: Log-ratios of Austria and all other countries of the considered composition. The black points are the observations and in red we display the trends.

References

[1] J. AITCHISON: *The statistical analysis of compositional data*, Journal of the Royal Statistical Society: Series B (Methodological) 44.2 (1982), pp. 139–160.

[2] S. J. KIM, K. KOH, S. BOYD, D. GORINEVSKY: l_1 *Trend Filtering*, SIAM Review 51.2 (2009), pp. 339–360.

[3] R. J. TIBSHIRANI: *Adaptive Piecewise Polynomial Estimation via Trend Filtering*, The Annals of Statistics 42.1 (2014), pp. 285–323.

Cybersecurity in virtual reality: a service for developing and deepening students' cyber responsibility*

Tibor Roskó[a], Gyöngyi Bujdosó[b], Cornelia Mihaela Novac[c]

[a]Doctoral School of Faculty of Informatics, University of Debrecen, Hungary
rosko.tibor@inf.unideb.hu

[b]Faculty of Informatics, University of Debrecen, Debrecen, Hungary
bujdoso.gyongyi@inf.unideb.hu

[c]Faculty of Electrical Engineering and Information Technology University of Oradea, Oradea, Romania
mnovac@uoradea.ro

In the 20th century, the decisive importance and impact of the Internet are indisputable. There are more and more online services that need (or just ask) personal data from the users wishing to register. This practice has resulted that people do not think about the necessity of the required data, as well as, in most cases people do not read the texts that belong to the "Accept all cookies" buttons – they answer and click without considering the risk of their decisions/actions. Even if there are many incidents published – for example, released medical data [3], e-mail data [6], personal data [13] and bank account sensitive data, e.g. passwords [9] – Internet users do not pay enough attention on those risk factors that they can meet during their online activities.

The main goal of the program that we started at our universities is to make the students more conscious and responsible Internet users.

We started to design and develop a learning environment that the students can access and use if they would like to know more about this field. For finding out which field would need more strength in the content, we had a survey on the students' password usage habits. Based on our previous experiences in teaching this field and on the results of the survey, we designed an environment.

We chose the Virtual Reality (VR) for displaying the information and for developing an interactive environment for learning about the chosen topics. VR has a deep impact of information displayed in its 3D interactive environment on those learners and other audiences who enter them. It has been demonstrated in some important researches, see, e.g., [7, 10–12], because 3D environments have special influences on the educational processes [**Falah**, **Bujdoso1**, **Hu**]. It was shown in many cases that the VR environments can improve the effectiveness of learning [2, 5] and – in addition – the users' various skills [4, 8, 14].

*Supported partly by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

We built our environment in the MaxWhere 3D online collaborative system [1] because of its many benefits: it has many 3D spaces and we can choose one for our specific topic, students can download and use it for free, it provides an easy to use interface for navigation and creating a personalized environment (see Figure 1).

Figure 1: A view of the Cybersecurity MaxWhere space designed and prepared for students

In this paper we present the results of our research, and the design of the environment that we developed for improving the students' confident and safe Internet usage.

Keywords: Cybersecurity, virtual reality, VR, cyber responsibility, protecting sensitive data, higher education

References

[1] P. BARANYI, Á. CSAPÓ: *Definition and synergies of cognitive infocommunications*, Acta Polytechnica Hungarica 9 (1 2012), pp. 67–83.

[2] B. BERKI: *Better memory performance for images in MaxWhere 3D VR space than in website*, in: Proc. 9th IEEE International Conference on Cognitive Infocommunications, CogInfoCom 2018, ed. by P. BARANYI, IEEE Computer Society, 2018, pp. 281–284.

[3] B. FREED: *Tennessee health data breach exposes information on thousands of HIV patients*, StateScoop, July 13, 2018,
URL: `https://statescoop.com/tennessee-health-data-breach-exposes-information-about-thousands-of-hiv-patients/` (visited on 10/27/2020).

[4] A. GILÁNYI, E. HIDASI: *Virtual reality systems in the rehabilitation of Parkinson's disease*, in: Proceedings of 7th IEEE Conference on Cognitive Infocommunications, ed. by P. BARANYI, IEEE Computer Society, 2017, pp. 301–305.

[5] I. HORVÁTH: *Innovative engineering education in the cooperative VR environment*, in: Proc. IEEE 7th International Conference on Cognitive Infocommunications (CogInfoCom 2016), IEEE Computer Society, 2016, pp. 359–364.

[6] T. HUNT: *The 773 Million Record "Collection #1" Data Breach*, Jan. 17, 2019,
URL: `https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/` (visited on 10/27/2019).

[7] S. JANG, J. M. VITALE, R. W. JYUNG, J. B. BLACK: *Direct manipulation is better than passive viewing for learning anatomy in a three-dimensional virtual reality environment*, Computers & Education (2017), pp. 150–165.

[8] L. KISS, B. HAMORNIK, M. KOLES, P. BARANYI, P. GALAMBOS, G. PERSA: *Training of business skills in virtual reality*, in: Proc. 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom 2015), ed. by P. BARANYI, IEEE Computer Society, 2015, pp. 215–216.

[9] J. KOLOUCH: *Evolution of Phishing and Business Email Compromise Campaigns in the CzechRepublic*, AARMS 17 (3 2018), pp. 83–100.

[10] A. D. KOVACS, Z. KVASZNICZA: *Use of 3D VR environment for educational administration efficiency purposes*, in: IEEE – 9th International Conference on Cognitive Infocommunications: CoginfoCom 2018 Proceedings, ed. by P. BARANYI, IEEE Computational Intelligence Society, 2018, pp. 361–366.

[11] V. KÖVECSES-GŐSI: *Cooperative learning in VR environment*, Acta Polytechnica Hungarica 15 (3 2018), pp. 205–224.

[12] B. LAMPERT, A. PONGRÁCZ, J. SIPOS, A. VEHRER, I. HORVÁTH: *MaxWhere VR-learning improves effectiveness over clasiccal tools of e-learning*, Acta Polytechnica Hungarica 15 (3 2018), pp. 125–147.

[13] P. LESKIN: *Here's how to check if you were one of the 500 million customers affected by the Marriott hack*, Business Insider, Nov. 30, 2018,
URL: https://www.businessinsider.com/marriott-starwood-hotel-hack-data-breach-how-to-check-if-you-were-affected-2018-11 (visited on 09/07/2019).

[14] A. TARABASZ, M. SELAKOVIĆ, C. ABRAHAM: *The classroom of the future: disrupting the concept of contemporary business education*, Entrepreneurial Business and Economics Review 6 (4 2018), pp. 231–245.

Exploiting the structure of communication in actor systems

Krisztián Schäffer[a], **Csaba István Sidló**[b]

[a]Monotic Mo. Kft., Budapest, Hungary
krisztian.schaffer@monotic.com

[b]Institute for Computer Science and Control (SZTAKI), Budapest, Hungary
sidlo@sztaki.hu

We propose a novel solution to the data-locality problem, gaining performance advantage for multi-threaded and distributed actor systems by dynamically adapting to the structure of actor communication. We provide an implementation in Circo, an open source actor system, and show promising experimental results.

Introduction and related work

Actor-based concurrency models [1] have been used for decades for scalable distributed applications [4]: Actors - the primitives of concurrency - communicate through messages, and form arbitrary topological relations. Various industrial-strength frameworks permit actor-style programming, including Akka and Orleans as popular ones [6], or Pony for high performance [3].

We assume that actors are significantly more numerous than threads, and that actor communication is structured: Only a small, slowly changing portion of possible actor connections is used. As networks are slower than shared-memory communication, which is slower than in-thread data passing, frequently communicating actors are to be moved to a common, or at least nearby location - e.g. to the same NUMA (Non-Uniform Memory Access) location, computer or data center.

We introduce the decentralized "Infoton optimization" algorithm, which can be applied both to multi-threaded environments and multi-node scenarios to explore and exploit communication structure to co-locate actors.

Infoton optimization

We assume that communication cost between schedulers - threads executing actor code - is fixed. Computational load with actors can however be moved between schedulers, affecting communication cost.

Actors and schedulers are mapped to 3D Euclidean space. The main idea is that distance approximates communication cost, and actors move towards their communication partners to minimize communication cost. Euclidean space is chosen on purpose as the

model of the physical universe, where communication cost often depends on the physical distance. Other spaces might also be investigated.

Infoton optimization is essentially a decentralized, scalable version of force-directed graph drawing - a physical system of bodies with cohesive forces, where the energy of the system is to be minimized [5]:

1. A so-called infoton, a force-carrying particle is attached to every message passed between actors. It is a small structure that holds the position of the source actor and a scalar value ("energy").
2. When the message arrives at its destination actor, the infoton that is attached to it acts on that actor, pulling it towards the source of the message.

Another force spreads actors in the segment of the space near schedulers, avoiding all concentrating around a single point:

1. Schedulers are embedded in a way that their distance represents communication overhead - either by static positioning, or by using network coordinates.
2. Actors are migrated to the nearest scheduler.
3. When a message arrives, the scheduler that executes the target actor creates a new "scheduler infoton", with itself as source.
4. Scheduler infotons either pull or push actors toward or away from the scheduler, depending on the load of the scheduler.

Implementation and experiments

We have added an experimental implementation to the Circo [2] actor system (where the main author and maintainer is the main author of this paper).

Figure 1 (also added to the Circo website [2] by the authors) illustrates an actor-based balanced binary tree (left; orange lines represent inter-scheduler communication) and a linked list (right), when optimization reached a stable layout after many operations. Starting from a random layout, where - in case of six schedulers - only one sixth of the communication happens between actors on the same scheduler, when optimized, respectively 80% and 95% of the messages are dispatched in-scheduler.

The cost of optimization grows linearly with the number of messages.

Future work

In addition to the details not discussed here, there is ongoing work clarifying the solution. For example, convergence criteria of infoton optimization and optimality of the results are studied. Detailed benchmark experiments are also being performed, comparing common actor systems with Circo.

We believe that incorporating sparsity into deep learning using actor systems like Circo has great potential towards artificial general intelligence.

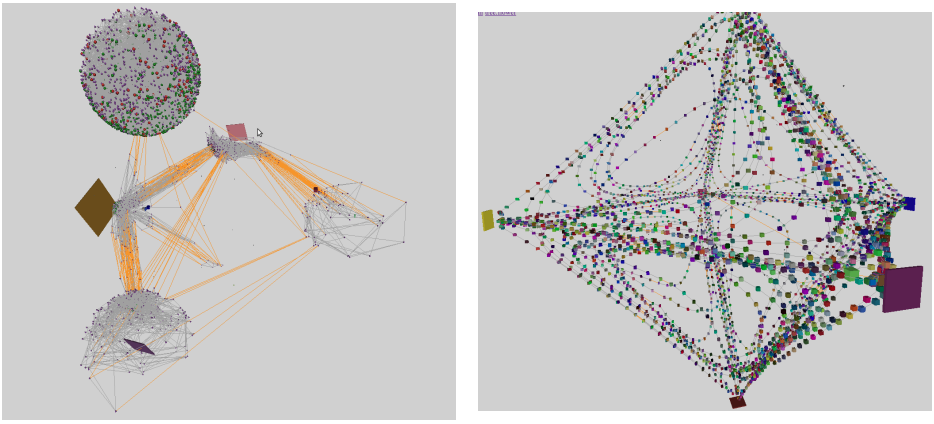


Figure 1: Optimized layouts of 4000 actors and 6 schedulers

References

[1] G. AGHA: *Actors: A Model of Concurrent Computation in Distributed Systems*, Cambridge, MA, USA: MIT Press, 1986, ISBN: 0262010925.

[2] *Circo: A fast, scalable and extensible actor system.* `https://github.com/Circo-dev/Circo`, [Accessed: 25 October 2020].

[3] S. CLEBSCH, S. DROSSOPOULOU, S. BLESSING, A. MCNEIL: *Deny Capabilities for Safe, Fast Actors*, in: AGERE 2015, Association for Computing Machinery, 2015, pp. 1–12, DOI: `https://doi.org/10.1145/2824815.2824816`.

[4] J. DE KOSTER, T. VAN CUTSEM, W. DE MEUTER: *43 years of actors: a taxonomy of actor models and their key properties*, in: Oct. 2016, pp. 31–40, DOI: `https://doi.org/10.1145/3001886.3001890`.

[5] T. M. FRUCHTERMAN, E. M. REINGOLD: *Graph drawing by force-directed placement*, Software: Practice and experience 21.11 (1991), pp. 1129–1164.

[6] D. WYATT: *Akka Concurrency*, Sunnyvale, CA, USA: Artima Incorporation, 2013, ISBN: 0981531660.

Simulating differential distributions in Beta-Poisson models, in particular for single-cell RNA sequencing data*

Roman Schefzik[ab]

[a]German Cancer Research Center (DKFZ)

[b]Current affiliation: Medical Faculty Mannheim, Heidelberg University

Roman.Schefzik@medma.uni-heidelberg.de

Introduction

Beta-Poisson (BP) models employ Poisson distributions, where the corresponding rate parameter itself is a Beta-distributed random variable [2]. The BP distribution has been used in various theoretical and practical applications, in particular to model single-cell RNA sequencing (scRNA-seq) data in biology [3]. Providing gene expression distributions over multiple cells, scRNA-seq is highly relevant and offers new fundamental insights into various biological fields [4], and there is an ever increasing amount of produced scRNA-seq data. The BP distribution has been shown to model scRNA-seq data appropriately and take account of their specific nature, where there are different procedures for model fitting and parameter estimation [1, 3].

To evaluate novel statistical methods in scRNA-seq analysis, simulations play a very important role, as typically no ground truth is available for real data. For instance, to adequately test and validate differential gene expression methods for scRNA-seq data [1], it is important to simulate differential distributions (DDs) in a reliable way. We here focus on a specific procedure to generate DDs in the scRNA-seq context using BP models. In particular, we create different types of DDs, mirroring various sources or origins of a difference, and different degrees of DDs, from weak to strong.

Despite the focus is on the application field of scRNA-seq data, the introduced procedures can principally be applied also to settings in other research areas, for both theoretical and practical considerations. The methods are implemented in the R package `SimBPDD`, which is publicly available at `https://github.com/RomanSchefzik/SimBPDD`.

Methods

A BP model $\mathrm{Poi}(x|\lambda_1 \,\mathrm{Beta}(\alpha, \beta))$ covers a mixture of Poisson distributions $\mathrm{Poi}(\lambda_1 u)$ with mean $\lambda_1 u$, where $\lambda_1 \in (0, \infty)$ denotes a scaling parameter and $u \sim \mathrm{Beta}(\alpha, \beta)$ has a Beta distribution with shape parameter $\alpha \in (0, \infty)$ and scale parameter $\beta \in (0, \infty)$. In the

*The work was funded by project VH-NG-1010 of the HGF.

scRNA-seq context, a large α may indicate a high transcriptional burst frequency, reflecting among others the proportion of zero expression, and a large β may indicate a high burst size, mirroring the magnitude of the non-zero expression values [3]. More specifically, we here consider the five-parameter BP (BP_5) model in [3], using an additional parameter $\lambda_2 \in (0, \infty)$ to model non-negative real-valued data (i.e., normalized scRNA-seq data) and a further parameter $p_0 \in [0, 1]$ to explicitly capture the proportion of cells with zero expression:

$\mathrm{BP}_5(x) := p_0 \mathbb{1}_{\{x=0\}} + (1 - p_0)\lambda_2 \,\mathrm{Poi}(x|\lambda_1 \,\mathrm{Beta}(\alpha, \beta))\mathbb{1}_{\{x>0\}}$.

To simulate DDs for the BP_5 model, we start with a pre-processed, normalized real-experiment scRNA-seq data set in form of a $(G \times C)$ expression matrix based on G genes and C cells. We first fit a BP_5 model to the expression data for each gene separately using the R package `BPSC` [3] and obtain corresponding parameter estimates $\alpha, \beta, \lambda_1, \lambda_2$ and p_0. Further, we test for each gene whether its distribution is indeed fitted well by the corresponding BP_5 model and only keep those cases (genes) that show a good fit as controls.

We then simulate DDs and construct differential proportions of zero expression (DPZ) for each control separately by manipulating the corresponding parameter estimates α, β, $\lambda := \lambda_1$ and p_0. To this end, we consider five specific cases of DDs that vary regarding the origin of the difference, see Table 1. We also incorporate different degrees of DD ranging from weak to strong differences.

case	changed parameter(s)	same location	same size	same shape
DLambda	λ_1	no	no	yes
DAlpha	α	no	no	no
DBeta	β	no	no	no
DAlphaBeta	α, β	yes	no	no
DPZ	p_0	no	no	no

Table 1: Settings for the DD simulations based on BP models

Results from a validation study

We apply our DD simulation procedure in a study starting with a real-experiment scRNA-seq data set, based on which we implement the DD simulation cases from Table 1 and additionally different degrees of DD. As representatives of the so-obtained control and manipulated BP_5 models, for each instance, we draw a sample from each model, with the sample size being equivalent to the number of cells in the scRNA-seq setting.

For each instance separately, to validate the soundness of our simulation procedures, we calculate the corresponding 2-Wasserstein distance between the samples from the control and manipulated models. In particular, a decomposition of the 2-Wasserstein distance helps to judge whether overall differences between two BP models are mainly due to differences with respect to location (mean), size (standard deviation) and/or shape. To explicitly

test for DPZ, we use the classical Fisher's exact test.

In general, for all cases, detection powers meaningfully increase with larger numbers of cells and strength of the difference between the distributions. This intuitively makes sense and confirms in particular that the implementation of the varying degrees of DD from weak to strong in our simulation procedure is valid. DPZ can mainly be detected when the parameters α or p_0 are changed. In contrast, DPZ typically plays only a minor role when the parameters λ or β are changed. Moreover, the decomposition patterns of the 2-Wasserstein distance meaningfully become more and more obvious the larger the number of cells is and the stronger the degree of DD is. In particular, the shape and location component in the cases DLambda and DAlphaBeta (Table 1), respectively, are minor to negligible. Further, the shape component is more pronounced when the shape parameter α is changed.

In a nutshell, the results confirm the soundness of our simulation procedures, in that these are able to reflect what is to be expected from the underlying theory (Table 1). In particular, we can provide some guidance on how to generate DDs between two BP models when the difference shall be of a specific type.

References

[1] M. DELMANS, M. HEMBERG: *Discrete distributional differential expression (D^3E) – a tool for gene expression analysis of single-cell RNA-seq data*, BMC Bioinformatics 17 (2016), p. 110.

[2] J. GURLAND: *A generalized class of contagious distributions*, Biometrics 14 (1958), pp. 229–249.

[3] T. N. VU, Q. F. WILLS, K. R. KALARI, N. NIU, L. WANG, M. RANTALAINEN, Y. PAWITAN: *Beta-Poisson model for single-cell RNA seq data analyses*, Bioinformatics 32 (2016), pp. 2128–2135.

[4] Y. WANG, N. E. NEVIN: *Advances and applications of single-cell sequencing technologies*, Molecular Cell 58 (2015), pp. 598–609.

Single Stranded Architectures for Computing*

Shinnosuke Seki[a]

[a]Department of Computer and Network Engineering, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 1828585, Japan
s.seki@uec.ac.jp

A single-stranded RNA sequence is a chain of ribonucleotides of four kinds (denoted respectively by the letters A, C, G, U). While being synthesized sequentially from its template double-stranded DNA (transcription), it folds upon itself into intricate higher-dimensional structures in such a way that the free energy is minimized, that is, the more hydrogen bonds between ribonucletoides or larger entropy a structure has, the more likely it is chosen, and furthermore the minimization is done locally.

This phenomenon called cotranscriptional folding (CF) has turned out to play significant roles in *in-vivo* computation throughout experiments and furthermore it has recently proven even programmable artificially so as to self-assemble a specific RNA rectangular tile structure *in vitro* [1].

The next step is to program a computation onto DNA in such a way that the computation can be "called" by cotranscriptional folding. In this novel paradigm of computation, what programmers could do is only twofold: designing a template DNA and setting environmental parameters. Oritatami is an introductory "toy" model to this paradigm of computation. This model allows programmers also to employ an arbitrarily large finite alphabet as well as an arbitrarily complex rule set for binding.

We shall present known architectures of computing in oritatami from a simple half-adder to Turing machine [2] along with several programming techniques of use, with hope that they will inspire *in-vivo* architectures of CF-driven self-assemblable computers, which could be even heritable.

References

[1] C. GEARY, P. W. K. ROTHEMUND, E. S. ANDERSEN: *A Single-Stranded Architecture for Cotranscriptional Folding of RNA Nanostructures*, Science 345.6198 (2014), pp. 799–804.

[2] D. PCHELINA, N. SCHABANEL, S. SEKI, Y. UBUKATA: *Simple Intrinsic Simulation of Cellular Automata in Oritatami Molecular Folding Model*, in: Proceedings of the 14th Latin American Theoretical Informatics Symposium, LNCS, Springer, 2020.

*Supported in part by the JST Program to Disseminate Tenure Tracking System, MEXT, Japan, No. 6F36 and JSPS KAKENHI Grant-in-Aid for Challenging Research (Exploratory) No. 18K19779.

Proposing a complex cognitive desktop virtual reality test*

Anna Sudár[a], Borbála Berki[a]

[a]Széchenyi István University, Győr, Hungary
{sudar.anna,berki.borbala}@sze.hu

In daily life, people perform thousands of complex actions, for which is essential that our brain properly organize the information, behavioral responses, and coordinate these processes according to a purpose. This complex function involves the cognitive processes that form the basis of goal-oriented behavior and can be primarily linked to the prefrontal cortex [6, 7, 9]. These so-called executive functions play a behavior organizing role and build up from three main components: shifting, inhibition, and working memory. However numerous studies discuss the aforementioned components separately in different virtual reality scenarios, there is a growing need for more complex approaches. MaxWhere is a desktop virtual reality platform that capable of displaying both 2D and 3D content and becoming in the focus of several studies in the past years [1–3, 5, 8]. The proposed study takes place in a virtual city, where the center of a small town is displayed with a suburb and a business district. The experiment begins in an outdoor pavilion where the first task is presented. The user has to classify different objects from three categories and sort them by pressing one of the three corresponding buttons. When an object appears on a smartboard the participants have to decide which category it belongs to. Two unique items are defined in the beginning of the experiment. When the first unique item appears the user has to go to another specific building in the virtual space where a Stroop task [10] will be presented. After the Stroop task, the participant goes back to the pavilion and continue the categorization task. When the second unique element appears, the user needs to go again to the other building, where the participants have to complete the final test of the experiment which is a virtual mental rotation test [4].

Keywords: virtual reality, cognitive test, executive functions, Stroop task, mental rotation

References

[1] B. BERKI: *Experiencing the Sense of Presence within an Educational Desktop Virtual Reality*, Acta Polytechnica Hungarica 17.2 (2020), pp. 255–265,
DOI: https://doi.org/10.12700/aph.17.2.2020.2.14.

[2] I. K. BODA, E. TÓTH: *English language learning in virtual 3D space by visualizing the library content of ancient texts*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 305–311.

*The project was supported by EFOP-3.6.1-16-2016-00003 founds, Consolidate long-term R and D and I processes at the University of Dunaujvaros.

[3] G. BUJDOSÓ, K. BOROS, C. M. NOVAC, O. C. NOVAC: *Developing cognitive processes as a major goal in designing e-health information provider VR environment in information science education*, in: Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications: CogInfoCom 2019, ed. by P. BARANYI, IEEE, 2019, pp. 187–192,
DOI: https://doi.org/10.1109/CogInfoCom47531.2019.9089958.

[4] A. F. CSINCSÁK: *A new VR paradigm to measure mental rotation*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 581–586.

[5] I. HORVÁTH, A. SUDÁR: *Factors Contributing to the Enhanced Performance of the MaxWhere 3D VR Platform in the Distribution of Digital Information*, Acta Polytechnica Hungarica 15.3 (Mar. 2018), pp. 149–173,
DOI: https://doi.org/10.12700/APH.15.3.2018.3.9.

[6] A. R. LURIA: *The frontal lobes and the regulation of behavior*, in: Psychophysiology of the frontal lobes, Elsevier, 1973, pp. 3–26.

[7] E. OLSON, M. LUCIANA: *The development of prefrontal cortex functions in adolescence: theoretical models and a possible dissociation of dorsal versus ventral subregions*, English, in: The Handbook of Developmental Cognitive Neuroscience, ed. by C. NELSON, M. LUCIANA, 2nd, MIT Press, 2008.

[8] A. RÁCZ, A. GILÁNYI, A. M. BÓLYA, J. DÉCSEI, K. CHMIELEWSKA: *On a Model of the First National Theater of Hungary in MaxWhere*, in: Proceedings of the 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), ed. by P. BARANYI, IEEE, 2020, pp. 575–576.

[9] A. P. SHIMAMURA: *The role of the prefrontal cortex in dynamic filtering*, Psychobiology 28.2 (2000), pp. 207–218.

[10] J. R. STROOP: *Studies of interference in serial verbal reactions.* Journal of experimental psychology 18.6 (1935), p. 643.

Machine Learning on Android with Oracle Tribuo, SMILE and Weka*

Máté Szabó[a]

[a]University of Debrecen, Faculty of Informatics
szabo.mate@inf.unideb.hu

Machine learning has been reached nearly all programming languages and most kind of devices. While the most popular language for developing machine learning application is Python, it has its own limits, for example the partial compatibility with Android devices. When a mobile application needs to train a model, it is easier to achieve this with the device's native language like Java or Kotlin. There are many machine learning libraries for Java, but most of them lacks Android support.

Introduction

In September 2020, Oracle announced Tribuo, their open source Java machine learning library under Apache 2.0 license. It features many commonly used algorithms like random forest, SVM, lasso, K-means, so it can solve prediction, classification, regression, clustering and anomaly detection problems. SMILE, the Statistical Machine Intelligence and Learning Engine is another machine learning library for Java. Its main advantage is the performance compared to other libraries and algorithm support. Weka is a general purpose open source machine learning software with Java API, which is easy to use and has its own graphical interface. The common thing in these libraries is that they can be used with Java or Kotlin and there are many algorithms that all of them support. Because of this, their performance can be compared in the same environment, which will be an Android device with a mobile processor in it. Although these are not native Android libraries, they can work on these systems and their performance can be compared. In this paper, we present the Android machine learning ecosystem, the libraries, the challenge of porting machine learning libraries, and the results.

With the evolution of mobile devices and applications, it was inevitable to use machine learning techniques for more personal user experience. Most applications use pre-trained models to recognize voice, to take better pictures or to swap faces. There are many disadvantages of training models on mobile, for example the energy consumption [3]. Beside that, there are many use cases of models trained on mobiles like comparison of machine learning capability of processors [1], detecting potholes [2] or malware [4].

*The work is supported by the EFOP-3.6.1-16-2016-00022 project. The project is co-financed by the European Union and the European Social Fund.

Application

The aim of the Android application is to measure properties of machine learning libraries like memory usage or runtime. The libraries involved are the newly open sourced Oracle Tribuo, the SMILE and Weka. The application runs the same test with each library, which means it trains models like SVM, Decision tree on multiple datasets with different sizes. The test uses the same algorithms and parameters for all libraries. The results and other runtime properties are logged by the application.

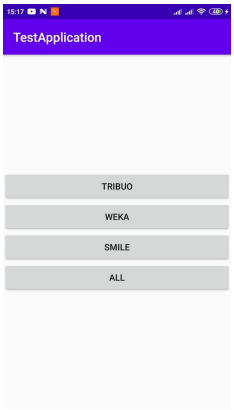


Figure 1: First screen of the measuring application. The user can decide to run tests for a specific library or all available libraries.

Keywords: Android, machine learning, Tribuo, SMILE, mobile

References

[1] A. IGNATOV, R. TIMOFTE, W. CHOU, K. WANG, M. WU, T. HARTLEY, L. VAN GOOL: *AI Benchmark: Running Deep Neural Networks on Android Smartphones*, in: Proceedings of the European Conference on Computer Vision (ECCV) Workshops, Sept. 2018, DOI: https://doi.org/10.1007/978-3-030-11021-5_19.

[2] A. KULKARNI, N. MHALGI, S. GURNANI, N. GIRI: *Pothole detection system using machine learning on Android*, International Journal of Emerging Technology and Advanced Engineering 4.7 (2014), pp. 360–364.

[3] A. MCINTOSH, A. HINDLE, S. HASSAN: *What can Android mobile app developers do about the energy consumption of machine learning?*, Empirical Software Engineering 24.1 (2019), pp. 562–601, DOI: https://doi.org/10.1007/s10664-018-9629-2.

[4] J. SAHS, L. KHAN: *A Machine Learning Approach to Android Malware Detection*, in: 2012 European Intelligence and Security Informatics Conference, 2012, pp. 141–147, DOI: https://doi.org/10.1109/EISIC.2012.34.

Throughput Performance Measurement of the MPT-GRE Multipath Technology in Emulated WAN Environment*

Szabolcs Szilágyi[a], Imre Bordán[a]

[a]University of Debrecen, Faculty of Informatics
szilagyi.szabolcs@inf.unideb.hu
bordanimre@gmail.com

Internet architecture enables only a single data path between two communication endpoints within a communication session. On the other hand decent communication equipment (laptops, tablets, phones) are equipped at the factory with several network interfaces (Ethernet, Wi-Fi, 3G, 4G). It does not worth not to use these hardware-given possibilities, which could increase the performance of the communication between two devices, using two or more communication paths. In this paper we presented a possible solution by implementing the MPT-GRE software library [4]. This software was developed under Linux and is based on a totally new architecture, in comparison with the classical TCP/IP model, providing an easy-to-use extension of the current TCP protocol stack. In our previous papers we investigated its performance in various laboratory measurement environments (see, e.g. [1–3, 5–9]). In this paper we tried to do it in a much more realistic environment, using the Dummynet WAN emulation software. The measurement results confirmed that the MPT-GRE multipath solution is able to efficiently aggregate the performance of physical connections in the emulated WAN environment as well.

Keywords: MPT-GRE, multipath communication, Dummynet, throughput, WAN Emulator.

References

[1] B. ALMÁSI, G. LENCSE, S. SZILÁGYI: *Investigating the Multipath Extension of the GRE in UDP Technology*, Computer Communications 103 (2017), pp. 29–38,
DOI: https://doi.org/10.1016/j.comcom.2017.02.002.

[2] B. ALMÁSI, S. SZILÁGYI: *Investigating the Throughput Performance of the MPT Multipath Communication Library in IPv4 and IPv6*, International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems 5.1 (2016), pp. 53–60,
DOI: https://doi.org/10.11601/ijates.v5i1.148.

[3] B. ALMÁSI, S. SZILÁGYI: *Throughput Performance Analysis of the Multipath Communication Library MPT*, in: TSP 2013 – The 36th International Conference on Telecommunications and Signal Processing, Rome, Italy, 2013, pp. 86–90,
DOI: https://doi.org/10.1109/TSP.2013.6613897.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

[4] G. LENCSE, S. SZILÁGYI, F. FEJES, M. GEORGESCU: *MPT Network Layer Multipath Library - Internet Draft v6*, 2020,
URL: https://tools.ietf.org/html/draft-lencse-tsvwg-mpt-06 (visited on 10/10/2020).

[5] S. SZILÁGYI, I. BORDÁN: *The Effects of Different Congestion Control Algorithms over Multipath Fast Ethernet IPv4/IPv6 Environments*, in: Proceedings of the 11th International Conference on Applied Informatics (ICAI 2020), vol. 2650, Eger, Hungary, 2020, pp. 341–349,
URL: http://ceur-ws.org/Vol-2650/paper35.pdf.

[6] S. SZILÁGYI, I. BORDÁN, L. HARANGI, B. KISS: *MPT-GRE: A Novel Multipath Communication Technology for the Cloud*, in: 9th IEEE International Conference on Cognitive Infocommunications : CogInfoCom 2018 Proceedings, Piscataway (NJ), USA, 2018, pp. 81–86,
DOI: https://doi.org/10.1109/CogInfoCom.2018.8639941.

[7] S. SZILÁGYI, I. BORDÁN, L. HARANGI, B. KISS: *Throughput Performance Analysis of the Multipath Communication Technologies for the Cloud*, Journal of Electrical and Electronics Engineering 12.2 (2019), pp. 69–72,
DOI: https://doi.org/10.26636/jtit.2018.122817.

[8] S. SZILÁGYI, I. BORDÁN, L. HARANGI, B. KISS: *Throughput Performance Comparison of MPT-GRE and MPTCP in the Gigabit Ethernet IPv4/IPv6 Environment*, Journal of Electrical and Electronics Engineering 12.1 (2019), pp. 57–60,
DOI: https://doi.org/10.26636/jtit.2018.122817.

[9] S. SZILÁGYI, F. FEJES, R. KATONA: *Throughput Performance Comparison of MPT-GRE and MPTCP in the Fast Ethernet IPv4/IPv6 Environment*, Journal of Telecommunications and Information Technology 3.2 (2018), pp. 53–59,
DOI: https://doi.org/10.26636/jtit.2018.122817.

A Survey of Recent Results in Finite-Source Retrial Queues with Collisions and Impatient Customers in the Orbit*

János Sztrik[a], Ádám Tóth[a]

[a] University of Debrecen, Faculty of Informatics
sztrik.janos@inf.unideb.hu, toth.adam@inf.unideb.hu

The goal of the paper is to study a finite-source retrial queuing system with collisions and customers' impatient behavior in the orbit. The server is not reliable, breakdown can happen either in busy or in idle states. The situation when an incoming customer from the orbit or from the source finds the server busy causes a collision and both requests are directed toward the orbit (including the customer under service, too). It is assumed that every request in the source is eligible to generate customers whenever the server is not working but these requests immediately get into the orbit. A customer after some waiting for the server to be served can depart from the orbit without fulfilling its service requirement these are the so-called impatient customers. In that case it goes back to the source. The source, service, retrial, impatience, operation and repair times are supposed to be independent of each other.

The novelty of the investigation is to carry out a sensitivity analysis comparing various distributions of impatient time of customers on the performance measures such as mean number of customers in the orbit, mean waiting time of an arbitrary customer, mean waiting time of customers who leave the system without service, probability of abandonment, server utilization, etc.

The aim of the present paper is to give a review of recent results on single server finite-source retrial queuing systems with impatient customers in the orbit. There are investigations when the server is reliable and there are models when the server is subject to random breakdowns and repairs depending on whether it is idle or busy. Tool supported, numerical, simulation and asymptotic methods are considered under the condition of unlimited growing number of sources. Several cases and examples are treated and the results of different approaches are compared to each other showing the advantages and disadvantages of the given method. In general we could prove that the steady-state distribution of the number of customers in the service facility can be approximated by a normal distribution with given mean and variance. Using asymptotic methods under certain conditions in steady-state the distribution of the sojourn time in the orbit and in the system can be approximated by a generalized exponential one. Furthermore, we guess that the distribution of the number of retrials until the successful service in the limit is geometrically distributed. By the help of stochastic simulation several systems are analyzed showing

*The research of both authors was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

directions for further analytic investigations. Tables and Figures are collected to illustrate some special features of these systems.

Queueing systems with impatient customers can be found for example, in [1–3], [7]. Our recent results are in [4–6], [8, 9].

Keywords: finite-source queuing system, retrial queues, collisions, server breakdowns and repairs, impatient customers.

References

[1] J. R. ARTALEJO, V. PLA: *On the impact of customer balking, impatience and retrials in telecommunication systems*, Computers & Mathematics with Applications 57.2 (2009), pp. 217–229.

[2] F. A. HAIGHT: *Queueing with reneging*, Metrika 2.1 (1959), pp. 186–197.

[3] J. S. KIM: *Retrial queueing system with collision and impatience*, Communications of the Korean Mathematical Society 25.4 (2010), pp. 647–653.

[4] A. KUKI, T. BÉRCZES, Á. TÓTH, J. SZTRIK: *Numerical analysis of finite source Markov retrial system with non-reliable server, collision, and impatient customers*, in: Annales Mathematicae et Informaticae, vol. 51, Liceum University Press, 2020, pp. 53–63.

[5] A. NAZAROV, J. SZTRIK, A. KVACH: *A survey of recent results in finite-source retrial queues with collisions*, in: Information Technologies and Mathematical Modelling. Queueing Theory and Applications, Springer, 2018, pp. 1–15.

[6] W. SCHREINER, J. SZTRIK: *On the Probabilistic Model Checking of a Retrial Queueing System with Unreliable Server, Collision, and Constant Time Impatience*, tech. rep. 19–11, Johannes Kepler University, Linz, Austria: Research Institute for Symbolic Computations, 2019.

[7] P. SUGANTHI, S. P. MADHESWARI: *Retrial Queueing System with customer Impatience*, Global Journal of Pure and Applied Mathematics 11.5 (2015), pp. 3177–3188.

[8] Á. TÓTH, J. SZTRIK: *Simulation of Finite-Source Retrial Queuing Systems With Collisions, Non-Reliable Server and Impatient Customers in the Orbit*, Proceedings of 11th International Conference on Applied Informatics, Eger, Hungary (2020), CEUR Workshop Proceedings (CEUR-WS.org) 2650 (2020), pp. 408–419,
URL: http://ceur-ws.org/Vol-2650/.

[9] M. H. ZAGHOUANI, J. SZTRIK: *Performance evaluation of finite-source Cognitive Radio Networks with impatient customers*, in: Annales Mathematicae et Informaticae, vol. 51, Liceum University Press, 2020, pp. 89–99.

Tuning of Category Hierarchy Enhanced Classification-based Indoor Positioning

Judit Tamás[a], **Zsolt Tóth**[a]

[a]Eszterházy Károly University
tamas.judit@uni-eszterhazy.hu
toth.zsolt@uni-eszterhazy.hu

The tuning of classification refinement using hierarchical grouping of categories is presented in this paper. The classification refinement [9] uses a classifier, a threshold and a dendrogram as parameters. The dendrogram can be predefined by a linkage matrix, or it can be generated by using linkage method and distance method on the topology information. The refinement can improve the accuracy of classifiers in the case of low confidence level.

For the examination, the k–NN [1] and the Naive Bayes [4] classifiers are used. These classifiers are based on instances, and they do not require retraining in case of new instances. The data set for the classification is part of the Miskolc IIS (Institute of Information Science) Hybrid IPS (Indoor Positioning System) Data set [6, 12, 13] recorded with the ILONA (Indoor Localization and Navigation) [11] System.. The data set had been recorded in the Miskolc IIS Building of University of Miskolc. The data set contains information about the location both as symbolic and absolute position, metadata of the measurement, and the measured values of WiFi, Bluetooth, and Magnetometer. The environment is selected to be the second floor of the Miskolc IIS Building, hence 431 measurement is used for the test. The threshold is an element of the $\{0.6, 0.7, 0.8, 0.9, 1\}$ set. The topology of the environment is described by IndoorGML (Indoor Geographic Markup Language) [7] document [2, 3]. IndoorGML is a standard defined by the Open Geospatial Consortium (OGC) [5], and it represents the indoor spaces as non-overlapping closed objects. The indoor spaces are bounded by physical or fictional boundaries. For each indoor space, the identifier is chosen to be derived from the corresponding space of Miskolc IIS Hybrid Data set. The dendrograms are generated by using average, complete, single and weighted linkage methods and the distance is calculated as the dissimilarity value of gravitational force-based approach [3, 8, 10].

Three properties are examined of a setup, namely hitRate, confidence and abstraction. Each property is calculated to have a maximization goal. However, when the increment of the hitRate is focused on, the method can return all of the rooms as the result, producing a low abstraction level. In addition, when higher confidence values are aimed at increased threshold, the abstraction level can decrease. Therefore, the goal of the method can not be based on only one of these properties. Tuning is required to find the balance of these properties to improve the enhancement of the classification-based indoor positioning.

A fitness function is introduced using these properties for the purpose of tuning. The introduced fitness function assigns a weight to each property, and it needs to be maximized. In this paper, the different weight tuples are examined in the given test environment. The

goal of the paper is to find a weight tuple, which can balance the hitRate, confidence, and abstraction level features for indoor positioning purposes.

Keywords: classification, hierarchical clustering

References

[1] P. CUNNINGHAM, S. J. DELANY: *k-Nearest neighbour classifiers*, Multiple Classifier Systems 34 (2007), pp. 1–17.

[2] K. ILKU, J. TAMÁS: *IndoorGML Modeling: A Case Study*, in: Carpathian Control Conference (ICCC), 2018 19th International, IEEE, 2018, pp. 633–638.

[3] K. ILKU, J. TAMÁS: *Topology-based Classification Error Calculation based on IndoorGML Document*, in: THE 11TH CONFERENCE OF PHD STUDENTS IN COMPUTER SCIENCE, Institute of Informatics of the University of Szeged, 2018, pp. 101–105.

[4] G. H. JOHN, P. LANGLEY: *Estimating Continuous Distributions in Bayesian Classifiers*, in: Eleventh Conference on Uncertainty in Artificial Intelligence, San Mateo: Morgan Kaufmann, 1995, pp. 338–345.

[5] J. LEE, K. J. LI, S. ZLATANOVA, T. H. KOLBE, C. NAGEL, T. BECKER: *OGC® indoorgml*, Open Geospatial Consortium standard (2014).

[6] *Miskolc IIS Hybrid IPS Data Set*, `http://archive.ics.uci.edu/ml/datasets/Miskolc+IIS+Hybrid+IPS`, [Online; Date donated 04-July-2016].

[7] *OGC IndoorGML-with Corrigendum*, http://docs.opengeospatial.org/is/14-005r4/14-005r4.html, [Online; Accessed 13-October-2017].

[8] J. TAMÁS, Z. TÓTH: *Topology-based Evaluation for Symbolic Indoor Positioning Algorithms*, IEEE Transactions on Industry Applications (2019), pp. 1–1, ISSN: 0093-9994, DOI: `https://doi.org/10.1109/TIA.2019.2928489`.

[9] J. TAMÁS, Z. TÓTH: *Classification Refinement with Category Hierarchy*, in: The 11th International Conference on Applied Informatics (ICAI 2020), vol. 2650, published at `http://ceur-ws.org`, 2020, pp. 358–369.

[10] J. TAMÁS, Z. TÓTH: *Topology-based Classification Error Calculation for Symbolic Indoor Positioning*, in: Carpathian Control Conference (ICCC), 2018 19th International, IEEE, 2018, pp. 643–648.

[11] Z. TÓTH: *ILONA: indoor localization and navigation system*, Journal of Location Based Services 10.4 (2016), pp. 285–302, DOI: `https://doi.org/10.1080/17489725.2017.1283453`.

[12] Z. TÓTH, P. MAGNUCZ, R. NÉMETH, J. TAMÁS: *Data model for hybrid indoor positioning systems*, Production Systems and Information Engineering 7.1 (2015), pp. 67–80.

[13] Z. TÓTH, J. TAMÁS: *Miskolc IIS hybrid IPS: Dataset for hybrid indoor positioning*, in: 2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, Kosice, Slovakia, 2016, pp. 408–412.

Compute Shader in Image Processing Development*

Robert Tornai[a], Péter Fürjes-Benke[a]

[a]University of Debrecen, Faculty of Informatics
tornai.robert@inf.unideb.hu
furjes.peter99@gmail.com

This paper will present the BlackRoom which is an image processing program. Beside Vulkan fragment shader and OpenGL fragment shader, the software implements OpenGL compute shader as another GPU-based processing path. In order to support wider range of devices with different amount of memory, users can utilize tile rendering and the program can be run in browsers thanks to the WebAssembly format. BlackRoom has been capable of rendering images by CPU with the support of multi-threading and SIMD. Besides that, in order to take advantage of computing potential of the graphics card, we used OpenGL fragment shader. OpenGL compute shader was implemented to further improve the rendering with GPU. Moreover, BlackRoom has Vulkan support, as well.

Thanks to our program's built-in benchmark system, the performance differences between the implemented CPU- and GPU-based executing branches can be easily determined. We made a comprehensive comparison among the rendering performance of our CPU, OpenGL's compute shader and fragment shader and Vulkan fragment shader branches.

Introduction

BlackRoom is an image processing application developed in Qt 5.15 version. The goal was to use the most modern techniques, so we implemented the algorithms using compute shader also beyond fragment shader of OpenGL and Vulkan fragment shader. This paper will cover the results of these implementations.

The Blackroom's structure is based on the standard skeleton which is introduced in GPU Gems [2]. Similarly to the framework of Seiller et al., each processing paths is implemented in a separate class to follow the basic principles of object-oriented programming [4]. During the research we have studied some of the existing accelerated image processing libraries. Although the progressive GPUCV library was found to be one of the best, it has not been developed since 2010 [1].

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.

Performance comparisons

Our test system contains an AMD Ryzen 5 3600 processor @ 4.35 GHz and an Nvidia GTX 960 graphics card with 4 GB memory. The following effects were used in order to compare the performance of the different executing branches: basic modifications, edge detection, Gauss filter, infrared and grayscale effects. As for basic modifications, we are talking about exposure value and brightness. To obtain the execution times we used the `QElapsedTimer` class, which measures the elapsed time in nanoseconds. Because the magnitude of the running time of our algorithms is millisecond, after readout the timer variable is divided by 1 000 000 in order to yield values of milliseconds.

Context-free algorithms

As context-free effects the basic – exposure value and brightness – modifications', the infrared and the grayscale effect's performance was measured. According to the results, rendering by GPU is approximately twice as fast as rendering by CPU on a single core. Utilizing multi-threading and SIMD decreases the gap but raises another problem. The memory bandwidth is limiting the all core performance of the CPU. Furthermore, thread management also increases the execution time. Nevertheless, taking into consideration the basic, infrared, and grayscale effects we can see almost 20% decrement in execution time compared to the single thread performance. The multi-core performance is more consistent because of the smaller gap between the extreme values.

Looking at the comparison of different execution branches of the GPU rendering we can see a little performance advantage in favor of OpenGL fragment shader with grayscale effect. Talking about basic and infrared effects' execution time the Vulkan fragment shader is the best. Inconsistency is its worst drawback since the difference between the extreme values is here the biggest among the execution branches. The OpenGL compute shader is behind the two other GPU rendering branches in terms of execution time. Meanwhile, it provides really consistent performance.

Context-sensitive algorithms

The context-sensitive algorithms were represented by edge detection and Gauss filter effects during the benchmarks. These effects calculate each pixel based on its neighbors. The benchmark tests show that there is quite a big difference between these two effects in terms of performance. As an example, rendering Gauss filter can profit from the extra threads of the CPU. Its execution time is almost eight times faster on multiple threads than on a single thread. On the other hand, the edge detection's runtime is slower by utilizing multi-threading. The reason of this is the simplicity of the edge detection compared to Gauss filter.

The variance between the three GPU-based execution branches is greater compared to the results with context-free algorithms. The OpenGL compute shader falls behind both OpenGL fragment shader and Vulkan fragment shader. OpenGL fragment shader provides the second best overall performance in edge detection and in Gauss filtering. The Vulkan execution branch is a little bit faster.

Benefits of OpenGL compute shader

Previously BlackRoom used only OpenGL fragment shader for computing the effects on GPU. However, the access of the neighborhood was not really effective, it has improved by introducing rectangle textures that enabled the usage of integer indices instead of float values. Secondly, the histogram generation may be even slower than computing it on the CPU [3]. Finally, the implementation of the OpenGL fragment shader is a little bit more complex compared to our needs.

So, we started to implement our algorithms in OpenGL compute shader because of the above reasons. For this executing branch the program uses OpenGL fragment shader only for the onscreen rendering, the effect chain calculation is done completely by OpenGL compute shaders. The code for histogram generation is more elegant than by OpenGL fragment shader.

Keywords: image processing, benchmark, CPU, shaders, Vulkan.

References

[1] J.-P. FARRUGIA, P. HORAIN, E. GUEHENNEUX, Y. ALUSSE: *GPUCV: A framework for image processing acceleration with graphics processors*, in: IEEE International Conference on Multimedia and Expo, Toronto, July 2006, pp. 585–588,
DOI: https://doi.org/10.1109/ICME.2006.262476.

[2] F. JARGSTORFF: *A Framework for Image Processing*, in: GPU Gems, ed. by R. FERNANDO, 1th, Boston: Addison-Wesley Professional, Apr. 2004, chap. 27, pp. 445–467.

[3] A. KUBIAS, F. DEINZER, M. KREISER, D. PAULUS: *Efficient computation of histograms on the GPU*, in: SCCG '07: Proceedings of the 23rd Spring Conference on Computer Graphics, Apr. 2007, pp. 207–212,
DOI: https://doi.org/10.1145/2614348.2614377.

[4] N. SEILLER, N. SINGHAL, I. K. PARK: *Object oriented framework for real-time image processing on GPU*, in: Proceedings of 2010 IEEE 17th International Conference on Image Processing, Hong Kong, Sept. 2010, pp. 4477–4480,
DOI: https://doi.org/10.1109/ICIP.2010.5651682.

CRC Check in a High-Speed Connectionless File Transfer System*

Robert Tornai[a], Dalma Kiss-Imre[b], Zoltán Gál[c]

University of Debrecen, Faculty of Informatics
[a]tornai.robert@inf.unideb.hu
[b]imre.dalma99@gmail.com
[c]zgal@unideb.hu

This paper describes the usage of CRC checking in an application named FMFT (Fast Manager of File Transfer) that is based on Xinan Liu's Reliable File Transfer Protocol. The system consists of a server and a client C++ program utilizing UDP connection. The aim is to transfer big files quickly by this program on busy network connections. The $Java$-based minimum viable product relying on Xinan Liu's solution was rewritten in C++ and enhanced by adding control over chunk size. To make this program available for as many platforms as possible, WebAssembly programming language was used. This article introduces the performance results of the utilization of CRC checking of sent and received packages. Finally, it will be discussed that thanks to an advanced scheduling, our application can utilize the network more efficiently.

Introduction

Transferring a huge amount of data between workstations and supercomputer nodes for processing introduces new problems: not only the upload process is slow, but the result can be huge also to download. Even gigabit connections can slow down to a few megabit range in a busy network in real-life use cases having even packet loss [6] or damage, as we experienced this at file transfers forth and back with a server hosted in the Gyires supercomputer's data center [3]. This paper will focus on the integrity of the transferred packages and the performance hit caused by the handling algorithm. Furthermore, the scheduling of packages will be discussed too.

Developing environment

For the platform independent development the Qt 5.15.1 stable version was chosen. This part of the work was carried out on a Debian 10.5 workstation. The server is designed to

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund. This paper was supported by the FIKP-20428-3/2018/FEKUTSTRAT project of the University of Debrecen, Hungary and by the QoS-HPC-IoT Laboratory.

run in headless mode. The client is built for the necessary target system natively having a GUI. The initial approach in our software was to have a UDP data channel with a TCP control channel similar to SABUL [2] which lived on as UDT until it was abandoned in 2013 [7]. Solutions based on UDP, especially by adopting rate-based algorithms, give better performance than other alternatives according to Cosimo Anglano et al. work [1]. Later this led us to the conclusion to refine our software to use a UDP channel for the control messages also [5]. On lost of either the data packet or the acknowledge packet, a resend is needed. It is also true, if the integrity of the package is damaged. For the data transfer we used `QNetworkDatagram` and `QUdpSocket` classes. We could measure that the CPU utilization of the C++ code was less than our original $Java$ implementation's [4].

CRC checking

The testing was carried over with a 100 MB test file, its data was transferred from the desktop workstation to the test server residing in the Gyires supercomputer's server room. It can be observed that without computing CRC-16 for data packets, the transfer rate stabilizes over 800 Mbps from chunk size of 1100 bytes up to 4000 bytes.

By computing CRC-16 for data packets, the transfer rate cross the 800 Mbps boundary with 824 Mbps just at chunk size of 2400 bytes. The curve of results of transfer rates with computing CRC-16 values stays almost entirely under the curve of raw transfer of packages. This was consistent over various sized test data with the difference being around 5% with higher than 2400 bytes chunk sizes. For small chunk sizes as 900 bytes the difference can be as high as 37%. During our test runs we have not encountered any package to fail the CRC-16 check. The reason for this was maybe the fact that the packages had to travel a relatively few hops. For longer data transfer paths having more hops it is potential to start having failing packages at CRC-16 checking.

Scheduling of packages

The first solution was to send packages continuously from the client to the server. The best packet transmission success rate for tests was 92.6% in the $Java$ based minimum viable product. The reimplemented C++ pair of software decreased the packet transmission success rate to 83.3% what is explained by the twofold increase in efficiency to stress both the CPU and the network stack. By introducing a transfer rate cap at software side the packet transmission success rate was increased over 90.0% again. The scheduling was based on one second length bursts of packages. It means that after sending out enough number of packages of a preset chunk size for the predetermined transfer rate, there was a pause in sending until the next one second time slot. It gives network buffers an unnecessarily heavy load at regular intervals. The next iteration was to fine tune the time interval to one millisecond. Final solution was to use a nanosecond timer for scheduling. At each timer event we check one second history of sent packages. If it is showing that the actual transfer rate is under the desired target, the missing number of packages needed of the given chunk

size to achieve the predetermined transfer rate is sent out. The predetermined transfer rate is approximated accurately at very low margin this way.

Keywords: CRC checking, high-speed networking, high-performance computing, Internet, parallel communication.

References

[1] C. ANGLANO, M. CANONICO: *A Comparative Evaluation of High-Performance File Transfer Systems for Data-intensive Grid Applications*, 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (June 2004), pp. 283–288.

[2] Y. GU, R. GROSSMAN: *SABUL: A Transport Protocol for Grid Computing*, Journal of Grid Computing 1.4 (Dec. 2003), pp. 377–386, ISSN: 1572-9184,
DOI: https://doi.org/10.1023/B:GRID.0000037553.18581.3b.

[3] *Gyires supercomputer*, May 8, 2020,
URL: https://hpc.unideb.hu/hu/node/219.

[4] *Java performance*, The page was last edited on 7 November 2019,
URL: https://en.wikipedia.org/wiki/Java_performance#cite_note-43.

[5] X. LIU: *ReliableFileTransferProtocol*, October 30, 2015,
URL: https://github.com/xinan/ReliableFileTransferProtocol/tree/master/src.

[6] H. SAWASHIMA, Y. HORI, H. SUNAHARA: *Characteristics of UDP Packet Loss: Effect of TCP Traffic*, in: Proceeding of the 7th Annual Conference of the Internet Society, Kuala Lumpur, Malaysia, June 1997,
URL: https://web.archive.org/web/20160103125117/https:/www.isoc.org/inet97/proceedings/F3/F3_1.HTM.

[7] *UDP-based Data Transfer Protocol (UDT)*, September 9, 2020,
URL: https://udt.sourceforge.io/.

Encryption in a High-Speed Connectionless File Transfer System*

Robert Tornai[a], Dalma Kiss-Imre[b], Zoltán Gál[c]

University of Debrecen, Faculty of Informatics
[a]tornai.robert@inf.unideb.hu
[b]imre.dalma99@gmail.com
[c]zgal@unideb.hu

This paper describes the usage of encryption in FMFT (Fast Manager of File Transfer) program that is based on Xinan Liu's Reliable File Transfer Protocol. The system consists of a server and a client software pair utilizing UDP connection. The aim is to protect big data transfers by utilizing encryption maintaining the high transfer rates. Relying on Xinan Liu's solution a $Java$-based minimum viable product was developed and further enhanced later, which was even more improved by rewriting it in C++. By adding a graphical user interface to the client, it is more user friendly now. Furthermore, by using WebAssembly, the program is available for many platforms now. After presenting the performance hit of the usage of encryption on data packets, finally, it will be discussed that thanks to multithreading, our application can utilize the CPU in a better way.

Introduction

We experienced at file transfers forth and back with a server hosted in the Gyires supercomputer's data center, that even gigabit connections can slow down to a few megabit range on a busy network in real-life use cases having even packet loss or damage [7]. This paper will focus on the encryption of the transferred packets and the performance hit introduced by the handling algorithm. Furthermore, the introduction of multithreading into the software will be discussed too.

A User Datagram Protocol (UDP) based software handles big data transfers a way better than Transmission Control Protocol (TCP) based solutions. There are UDP based systems as UFTP and UFTPD software pair that mostly accomplish our needed features [8], but they are not available in browsers, which is a basic requirement in our project. Because of this, we decided to write an own implementation designed for WebAssembly from scratch. Furthermore, the Stream Control Transmission Protocol (SCTP [4]) was implemented in our server-client pair.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund. This paper was supported by the FIKP-20428-3/2018/FEKUTSTRAT project of the University of Debrecen, Hungary and by the QoS-HPC-IoT Laboratory.

Developing environment

For the platform independent development the Qt 5.15.1 stable version was chosen. This part of the work was carried out on a Ubuntu 18.04.5 LTS desktop workstation. The performance of the TCP based FTP transfer and our SCTP and UDP based file transfer implementations need more investigation [6].

For testing purposes we used a gigabit network. Similar to SABUL [3], the initial approach in our software was to have a UDP data channel with a TCP control channel. SABUL lived on as UDT until it was abandoned in 2013 [10]. Solutions based on UDP, especially by adopting rate-based algorithms, give better performance than other alternatives according to Cosimo Anglano et al. work [1]. Later this led us to the conclusion to refine our software to use a UDP channel for the control messages also based on Xinan Liu's Reliable File Transfer Protocol [5].

Encryption

For encryption Datagram Transport Layer Security (DTLS) was taken into consideration [2]. Due to its complexity, for the first attempt to secure the packages, Qt's SimpleCrypt sample program was used [9]. A 100 MB test file was used to carry out the measurements. By encrypting the data packets, the transfer rate cross the 800 Mbps boundary with 811 Mbps just at chunk size of 1100 bytes. The curve of results of transfer rates with encryption stays almost entirely under the curve of raw transfer of packages. Exception to this is chunk size of 2200 bytes where encrypted transfer rate of 836 Mbps was better by 1 Mbps over raw transfer rate of 835 Mbps. The difference is mostly under 1.5% at 900 bytes chunk size or higher. For small chunk sizes as 600 bytes the difference can be as high as almost 20%.

Multithreading

Multithreading was introduced into the client software first, because at long workload the graphical user interface became unresponsible. Separating the GUI from the work thread, the GUI elements as progress bar or buttons started to give appropriate feedback. This could be achieved by using the signal-slot system of Qt. The next essential change was to separate the connection setup from the data transfer. This was done for the server also. Having a distinct thread for the data transfers was a huge boost especially for the server program, because one thread has a practical physical limit for the number of the clients to be served. Modern servers are massively multithreaded nowadays, thus the number of served clients can be raised this way.

Keywords: encryption, high-speed networking, high-performance computing, Internet, parallel communication.

References

[1] C. ANGLANO, M. CANONICO: *A Comparative Evaluation of High-Performance File Transfer Systems for Data-intensive Grid Applications*, 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (June 2004), pp. 283–288.

[2] *Datagram Transport Layer Security*, September 9, 2020, URL: https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security.

[3] Y. GU, R. GROSSMAN: *SABUL: A Transport Protocol for Grid Computing*, Journal of Grid Computing 1.4 (Dec. 2003), pp. 377–386, ISSN: 1572-9184, DOI: https://doi.org/10.1023/B:GRID.0000037553.18581.3b.

[4] S. KHATRI: *SCTP Performance Improvement Based on: Adaptive Retransmission Time-Out Adjustment*, Paperback, LAP LAMBERT Academic Publishing, 2012.

[5] X. LIU: *ReliableFileTransferProtocol*, October 30, 2015, URL: https://github.com/xinan/ReliableFileTransferProtocol/tree/master/src.

[6] D. MADHURI, P. C. REDDY: *Performance comparison of TCP, UDP and SCTP in a wired network*, in: 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, Oct. 2016, pp. 1–6, ISBN: 978-1-5090-1066-0, DOI: https://doi.org/10.1109/CESYS.2016.7889934.

[7] H. SAWASHIMA, Y. HORI, H. SUNAHARA: *Characteristics of UDP Packet Loss: Effect of TCP Traffic*, in: Proceeding of the 7th Annual Conference of the Internet Society, Kuala Lumpur, Malaysia, June 1997, URL: https://web.archive.org/web/20160103125117/https:/www.isoc.org/inet97/proceedings/F3/F3_1.HTM.

[8] B. SCHULLER, T. POHLMANN: *UFTP: High-Performance Data Transfer for UNICORE*, in: 7th UNICORE Summit 2011 Proceedings, ed. by M. ROMBERG, P. BAŁA, R. MÜLLER-PFEFFERKORN, D. MALLMANN, vol. IAS Series 9, Toruń, Poland: Forschungszentrum Jülich GmbH, July 2011, pp. 135–142, URL: https://core.ac.uk/download/pdf/34995345.pdf#page=144.

[9] *SimpleCrypt algorithm details*, September 9, 2020, URL: https://wiki.qt.io/SimpleCrypt_algorithm_details.

[10] *UDP-based Data Transfer Protocol (UDT)*, September 9, 2020, URL: https://udt.sourceforge.io/.

Performance analysis of two-way communication retrial queueing systems with non-reliable server and impatient customers in the orbit*

Ádám Tóth[a], János Sztrik[a]

[a]Faculty of Informatics, University of Debrecen, Debrecen, Hungary
toth.adam@inf.unideb.hu, sztrik.janos@inf.unideb.hu

Many models of two-way communication queueing systems have been studied in recent years, they can be utilized in many fields of life like in [2], [6], [7]. Customers have always been characterized by the phenomena of impatience due to the long wait for being served ([1], [3], [4], [5]). In this paper, we consider two-way communication systems with a non-reliable server where primary customers may decide to leave the system after spending a considerable amount of time in the system before getting its proper service. The service unit can break down during its operation or in an idle state, too. Whenever the server becomes idle it may generate requests towards the customers residing in an infinite source. These requests the so-called secondary customers can enter the system after a random time if the service unit is available and functional upon their arrivals. Otherwise, they return to the source without coming into the system. Every primary customer has a property of impatience meaning that an arbitrary request has the ability to quit the system after some time while its demand remains unsatisfied. During server failure, every individual may generate requests but these will be forwarded immediately towards the orbit. The source, service, retrial, impatience, operation, and repair times are supposed to be independent of each other.

The novelty of the present paper is to achieve a sensitivity analysis using various distributions of impatient time of customers on the performance measures like the mean response time of a primary customer, the utilization of the service unit occupying just primary or secondary customers, the probability of abandonment, etc. To compare the effect of the different distributions on distinct metrics a stochastic simulation program is developed based on SimPack. The obtained results demonstrate the importance of utilized distribution under different parameter settings represented by numerous figures and highlight some interesting specialties of these types of systems.

Keywords: queueing, impatience, two-way communication system, finite-source, abandonment, stochastic simulation, sensitivity analysis

*The research work of Ádám Tóth, János Sztrik was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund

References

[1] J. R. ARTALEJO, V. PLA: *On the impact of customer balking, impatience and retrials in telecommunication systems*, Computers & Mathematics with Applications 57.2 (2009), pp. 217–229.

[2] V. DRAGIEVA, T. PHUNG-DUC: *Two-Way Communication $M/M/1//N$ Retrial Queue*, in: International Conference on Analytical and Stochastic Modeling Techniques and Applications, Springer, 2017, pp. 81–94.

[3] C. KIM, S. DUDIN, A. DUDIN, K. SAMOUYLOV: *Analysis of a Semi-Open Queuing Network with a State Dependent Marked Markovian Arrival Process, Customers Retrials and Impatience*, Mathematics 7.8 (2019), pp. 715–734,
DOI: https://doi.org/10.3390/math7080715.

[4] L. KLEINROCK: *Creating a mathematical theory of computer networks*, Operations research 50.1 (2002), pp. 125–131.

[5] K. RAKESH, S. SAPANA: *Transient performance analysis of a single server queuing model with retention of reneging customers*, Yugoslav Journal of Operations Research 28.3 (2018), pp. 315–331,
DOI: https://doi.org/10.2298/YJOR170415007K.

[6] J. SZTRIK, Á. TÓTH, Á. PINTÉR, Z. BÁCS: *Simulation of Finite-Source Retrial Queues with Two-Way Communications to the Orbit*, in: Information Technologies and Mathematical Modelling. Queueing Theory and Applications, ed. by A. DUDIN, A. NAZAROV, A. MOISEEV, Cham: Springer International Publishing, 2019, pp. 270–284, ISBN: 978-3-030-33388-1.

[7] Á. TÓTH, J. SZTRIK: *Simulation of Finite-Source Retrial Queuing Systems With Collisions, Non-Reliable Server and Impatient Customers in the Orbit*, in: Proceedings of 11th International Conference on Applied Informatics, CEUR-WS, pp. 408–419,
URL: http://ceur-ws.org/Vol-2650/#paper42.

Error detection and analysis of P4 programs*

Gabriella Tóth[a], Máté Tejfel[a]

[a]Eötvös Loránd University
kistoth@inf.elte.hu, matej@inf.elte.hu

In this paper, we introduce a solution for error detection and analysis of P4 programs. Our solution does not only contain error cases but suspicious ones, which can cause errors. These can be caused by the usage of invalid headers or uninitialized fields, incorrect reading or writing of metadata, or improper usage of the drop flag. The analysis of the program is based only on the P4 source and separates the handling of the ingress and egress pipeline. A prototype of the error detector and analyzer is created with which we checked the possible error cases in many P4 programs, and monitor the different way for packet processing, which results will be shown in this paper.

P4 [1, 3] is a domain-specific programming language to develop the processing of network packets in network devices. In the code, we can define what kind of header information we would like to handle. The programs have three main parts: $parser$, $modifier$ and $deparser$. The $parser$ defines the way how the program gets the header information from the input packet, the $modifier$ describes how it changes the header information, and after the modification, the $deparser$ contains that how it creates the new output packet from the new header information.

P4 creates a more flexible way to develop network devices, although this makes it easier to develop inconsistent and incorrect programs. Therefore, different approaches have already been created to verify and analyze P4 programs. There are some tools – for example P4V [5] and Assert-P4 [4] – which expect annotated programs to check the given properties. With these solutions, the developers can get more specific analysis but need to do more work to learn the language of the annotations and how to create them. We would like to give a solution, which only uses the simple source of the program for the checking. There are similar approaches for this too - for example, Vera [6] - where they use symbolic execution. A new area in our result is to check the correctness of the programs based on the PSA, which is a new approach with static analysis.

The base of this research was written in our previous publication [7], where we showed the theoretical part of the idea to detect specific errors in P4 programs. In this paper, we supplement this idea with new case analysis, detection, and the practical part, as a prototype of the analyzer tool.

The checking is based only on the P4 source from which the specification of the program is created: it gets the precondition from the $parser$, the post-condition from the $deparser$, and the description of the functional part of the program from the $modifier$. The method checks if the execution of the program, starting from any initial state (where the precondition is true), will reach one of the final states (where the post-condition is

*This work has been supported by the European Union, co-financed by the European Social Fund (EFOP-3.6.3-VEKOP-16-2017-00002)

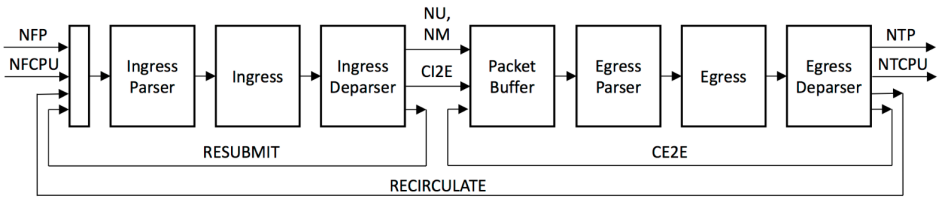


Figure 1: Packet processing paths [2]

true). During the checking, it stores the validity of the used header information and checks the correct usage of them in all possible execution paths.

Besides the validity checking, the solution was extended to handle the ingress and egress pipeline separately. In Figure 1 we can see the different paths of the packet processing. If we only see the most simple path, then first the ingress pipeline gets the input packet and processes it, and based on this result, the egress pipeline continues the processing.

Although, the path of packet processing can be more complicated. It depends on the definition of the target architecture. We work with the latest, official one, the Portable Switch Architecture (PSA) [2]. As it can be seen in Figure 1, there are three ways for the more complex paths: the $resubmit$, in which after the ingress deparser, the packet goes back to the ingress parser; the $CE2E$, when a clone of the packet goes through the egress again; and the $recirculate$, in which after the execution of the egress deparser, it continues with the beginning, i.e. ingress parser.

The way, how the packet goes, is defined by the specification of the PSA. We can check if the P4 program is correct for the PSA by simulating all of the possible packet paths to give further information for the developer about the execution. During this calculation, we can extend our solution to work with the metadata too, besides the header information.

In both of the ingress and egress pipelines, there are limitations of the usage of certain metadata – among others in $standard\_metadata$, there is a field $egress\_spec$, which can be written only in the ingress pipeline, and $ingress\_port$ is only readable. The improper usage of these types of data can be easily checked and reported to the developer.

The drop of the packet can be controlled too. Possible drop paths and suspicious drop usages – for example drop the packet twice in a path or undo the drop of the packet – can be reported.

Our goal is to create a tool for P4 developers to make their work easier by giving a report about their P4 code. These reports contain error and warning detection while giving some useful results of the analysis, and all of it calculated only from the P4 code.

References

[1] $P4_{16}$ *Language Specification*, `https://p4.org/p4-spec/docs/P4-16-v1.1.0-spec.pdf`, 2020.

[2] $P4_{16}$ *Portable Switch Architecture (PSA)*, `https://p4.org/p4-spec/docs/PSA.html`, 2020.

[3] M. BUDIU, C. DODD: *The $P4_{16}$ Programming Language*, SIGOPS Oper. Syst. Rev. 51.1 (Sept. 2017), pp. 5–14, ISSN: 0163-5980,
DOI: http://dx.doi.org/10.1145/3139645.3139648.

[4] L. FREIRE, M. NEVES, L. LEAL, K. LEVCHENKO, A. SCHAEFFER-FILHO, M. BARCELLOS: *Uncovering Bugs in P4 Programs with Assertion-based Verification*, in: Proceedings of the Symposium on SDN Research, SOSR '18, Los Angeles, CA, USA: ACM, 2018, 4:1–4:7, ISBN: 978-1-4503-5664-0,
DOI: http://dx.doi.org/10.1145/3185467.3185499.

[5] J. LIU, W. HALLAHAN, C. SCHLESINGER, M. SHARIF, J. LEE, R. SOULÉ, H. WANG, C. CAŞCAVAL, N. MCKEOWN, N. FOSTER: *P4V: Practical Verification for Programmable Data Planes*, in: Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication, SIGCOMM '18, Budapest, Hungary: ACM, 2018, pp. 490–503, ISBN: 978-1-4503-5567-4,
DOI: http://dx.doi.org/10.1145/3230543.3230582.

[6] R. STOENESCU, D. DUMITRESCU, M. POPOVICI, L. NEGREANU, C. RAICIU: *Debugging P4 Programs with Vera*, in: Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication, SIGCOMM '18, Budapest, Hungary: ACM, 2018, pp. 518–532, ISBN: 978-1-4503-5567-4,
URL: http://dx.doi.org/10.1145/3230543.3230548.

[7] G. TÓTH, M. TEJFEL: *A formal method to detect possible P4 specific errors*, in: Position Papers of the 2019 Federated Conference on Computer Science and Information Systems, vol. 19, Annals of Computer Science and Information Systems, PTI, 2019, pp. 49–56,
DOI: http://dx.doi.org/10.15439/2019F355.

A possible optimisation procedure for US and MRI tongue contours*

Réka Trencsényi[a], **László Czap**[b]

[a]University of Debrecen, Department of Electrical and Electronic Engineering
trencsenyi.reka@science.unideb.hu

[b]University of Miskolc, Institute of Automation and Infocommunication
czap@uni-miskolc.hu

One of the fundamental tools of the study of speech production is the analysis of dynamic records of human speakers, made by ultrasound (US) [2] and magnetic resonance imaging (MRI) [5] techniques. Investigating and processing these two-dimensional records created in the so-called sagittal plane resulting in a side view of the human body, relevant qualitative and quantitative information can be gained about the main features of articulation. Qualitative statements mainly refer to the relative position of the tongue and palate in the case of different speech sounds and sound transitions, while quantitative descriptions focus on the recognition and connection of the geometric parameters which have high importance in the understanding of the relationships between the acoustic and articulatory characteristics of speech. Quantitative analyses can be performed in several ways with a wide variety [1, 3, 4]. The starting points of the investigations of our present study are tongue contours fitted to the frames of US [7] and MRI [6] records by automatic algorithms. The used US and MRI sources differ from each other in many details, such as the gender and nationality of the speakers, the geometry, resolution, and scale of the images, and the visually evaluable anatomic segments of the vocal tract. The aim of our research work is to match the US and MRI sources by elaborating and applying the proper geometric transformations between the US and MRI tongue contours in a biunique way.

When writing the exact mathematical form of the transformation, we relied on the special geometry of the available US records. Namely, the imaging US head scans such a radial region of the oral cavity which is seen at an angle of 90° measured from a fixed centre C. Consequently, it is obvious to treat the US images and the points of the belonging tongue contours in such a polar coordinate system of C origin where the position of each pixel is given by radius r measured from point C and the signed angle φ measured from the central vertical axis of the image unambiguously. The aim of the transformation is to embed the radial geometry of the US frames to the rectangular geometry of the MRI records described by the two-dimensional Cartesian coordinates so that the US and MRI tongue contours assigned to the same sound should overlap with each other as much as possible. The transformation of the US tongue contours can include three basic operations: the scaling of the radial range, the scaling of the angular range, and the rotation of the

*We would like to thank the Lingual Articulation Research Group (Hungarian Academy of Sciences), for providing the recordings with the SonoSpeech system.

angular range. The three operations can be realised mathematically by the formulas

$$r' = r \cdot R, \quad \varphi' = FI \cdot \varphi, \quad \varphi'_0 = \varphi_0 + FI_0, \tag{1}$$

where the scale factors R and FI allow the normalisation of the radial and angular range, and the term FI_0 performs the translation of the initial angle of the angular range. Thus, the relationships (1) fit the US tongue contour to the corresponding MRI frame. Applying the inverse of the transformations (1), however, also the reverse conversion can be executed, i.e., by dint of the inverse operations

$$r = \frac{r'}{R}, \quad \varphi = \frac{\varphi'}{FI}, \quad \varphi_0 = \varphi'_0 - FI_0, \tag{2}$$

the MRI tongue contour can be projected onto the corresponding US frame. The parameter set $\{R, FI, FI_0\}$ of the transformations performed in the directions US-MRI and MRI-US must necessarily be the same since, thereby, the maintaining of the relative scale ratio of the US and MRI environment can be ensured independently of the direction of the conversion. During the investigations, we fixed the value of factor FI by $FI = 1$, which means that the transformation is conformal.

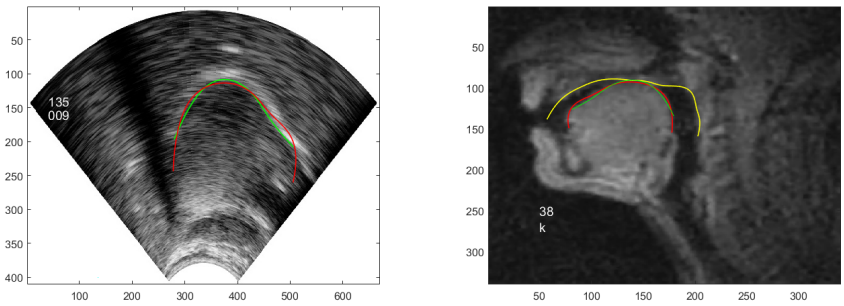


Figure 1: The results of the optimisation in the case of sound *k* by presenting the US (green) and MRI (red) tongue contours simultaneously. The contour of the palate is indicated by the yellow curve in the MRI frame.

The transformations (1) and (2) become valid by the numerical determination of parameters R and FI_0, to which the optimisation of the values of the parameters offers a possible way. During the optimisation procedure, using an algorithm elaborated by us, we find the parameter set, in the case of that the distance between the transformed US tongue contour and the MRI tongue contour serving as a reference curve is minimal. To the successful transformation, however, not only the exact values of parameters R and FI_0 are needed but also centre C' designated in the MRI frame must be known, which is the transform of centre C of the US record. Beyond these, during the construction of the optimisation algorithm, the peak of the epiglottis G can serve as a good reference point. Therefore, we created the optimisation algorithm via such mathematical formulas which enable the simultaneous optimisation of parameters $\{R, FI_0, C', G\}$. We fulfilled the optimisation of the parameters $\{R, FI_0, C', G\}$ for two speech sounds, which were *k* and

t, but for the verification, we also checked the projection of the tongue contours of other sounds. The optimisation of the tongue contours is exemplified by Figure 1.

References

[1] S. G. DANNER, A. V. BARBOSA, L. GOLDSTEIN: *Quantitative analysis of multimodal speech data*, Journal of Phonetics 71 (2018), pp. 268–283,
DOI: https://doi.org/10.1016/j.wocn.2018.09.007.

[2] B. DENBY, M. STONE: *Speech synthesis from real time ultrasound images of the tongue*, in: 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 1, 2004, pp. I–685,
DOI: https://doi.org/10.1109/ICASSP.2004.1326078.

[3] L. FULCHER, A. LODERMEYER, G. KAHLER, S. BECKER, S. KNIESBURGES: *Geometry of the vocal tract and properties of phonation near threshold: calculations and measurements*, Applied Sciences 9.13 (2019), p. 2755,
DOI: https://doi.org/10.3390/app9132755.

[4] A. OJALAMMI, J. MALINEN: *Automated segmentation of upper airways from MRI-vocal tract geometry extraction*, International Conference on Bioimaging 3 (2017), pp. 77–84,
DOI: https://doi.org/10.5220/0006138300770084.

[5] A. D. SCOTT, M. WYLEZINSKA, M. J. BIRCH, M. E. MIQUEL: *Speech MRI: morphology and function*, Physica Medica 30.6 (2014), pp. 604–618,
DOI: https://doi.org/10.1016/j.ejmp.2014.05.001.

[6] SPAN | SPEECH PRODUCTION AND ARTICULATION KNOWLEDGE GROUP: *the rtMRI IPA chart (John Esling)*, Accessed in 2020 May 9th,
URL: https://sail.usc.edu/span/rtmri_ipa/je_2015.html.

[7] K. XU, T. G. CSAPÓ, P. ROUSSEL, B. DENBY: *A comparative study on the contour tracking algorithms in ultrasound tongue images with automatic re-initialization*, Journal of the Acoustical Society of America 139.5 (2016), EL154–EL160,
DOI: https://doi.org/10.1121/1.4951024.

Neuron network model in the study of Smart City ideas

Mátyás Varga[a], Bence Soltész[a], Norbert Fiedler[a], Anikó Apró[a], Balázs Borsos[a], Gábor Kiss[b], Zoltán A. Godó[a]

[a]Information Technology, Faculty of Informatics, University of Debrecen, Hungary
godo.zoltan@inf.unideb.hu

[b]Institute of Machine Design and Safety Engineering, University of Óbuda, Budapest, Hungary

Problem statement

In today's most popular personal computers, which are based on the von Neumann architecture, true parallelism is not yet implemented. Despite modern processors having multiple cores, the concept of per-core task execution points beyond the complexity of current personal computer architectures. The basic advantage of multicore processors is that they are capable of running multiple threads in parallel at the same time. With multiple cores built into a single processor, the overall performance is multiplied, thanks to calculations running parallel to each other. However, processors that are capable of processing parallel instructions are called superscalar processors.

Typically, the real world can be characterized by data traffic that consists of unprocessably many, parallel signals. This is further complicated by the fact that everything around us is analog. However, traditional computer processing works with quantized numbers, which are digitized with a high degree of loss, and move in a discrete range of values.

However, the nervous system is typically an analog, massively parallel neuron system [4]. While neural networks are software emulated parallel systems on a oneflow, von Neumann architecture machine, the goal of networks is to achieve true, full, hardware architecture based parallel task execution. Neural networks already provide some amazing results, for example with learning algorithms or different levels of artificial intelligence. Therefore, we can expect even more exciting results from neuron networks, which are much closer to the structure of the natural nervous system.

Levels of parallelism

With the system that we developed, we would like to model Smart City dataflow [6], [1], the propagation of information and the city traffic as well. Due to its universal structure, any other field can be modelled with it, with the change of the processor's program. For example, an obvious use case would be neuro-informational application, due to the similarities with the nervous system. In this case we would connect the system with a living nervous system and implement two-way communication. In our current research, 216 high

performance processors are available, which makes it possible to build a 6 x 6 x 6 sized, massively parallel neuron system cube. Taking use of modern technological opportunities, nodes are represented by complete microcontrollers. This way, each node in the neuron network contains a combined processor, memory, and I/O unit.

Analogue implementation

Our system under construction is capable of performing tasks of any complexity due to intelligent nodes. The program uploaded to the nodes is suitable for controlling the data flow, which is realized by the connections of the I / O PINs of the node microcontrollers. Because the nodes are separate processing units, it is possible to implement analog data traffic in addition to or instead of digital.

Analog stream processing adds new possibilities to the system. Because signals from the natural environment are typically analog, the architecture of our neural network system is also closer to the nature of the data to be processed. If we analyze Smart City problems, a number of analog signals need to be processed. Analog communication is typically represented by voltage levels in similar systems.

Software levels

Node microcontrollers require multi-level program execution [3]. The most basic program is the bootloader, which is responsible for uploading and running the running main program. We can upload our own main program to the nodes running below this. However, the running main program is an interpreter that will process the data stream. The stream contains special control information that gives instructions on how to process the stream [5]. This allows for extremely complex processing and wide applicability.

We need to use so-called cascade programming because we can't upload program one by one. The point is that the first processor receives the new master program, and then the modified bootloader passes the master program to the next program via an I / O PIN. This, programming takes place automatically in a cascade system. Each node has its own ID. This allows the main program to adapt to the physical location of the node. This, the interpreter program processing the data stream can be developed at any time after the neural network has been assembled. The scripting language that controls the interpreter can also be developed and expanded.

The main program then becomes capable of receiving and sending data streams to neighboring nodes via dedicated I / O PINs. The instructions placed in the data stream are interpreted and executed by the main program as an interpreter.

Summary

A stream-driven, massively parallel neural network with such a structure, with both analog and digital features, with such a large number of intelligent processors, running an intelligent interpreter, is unique in the scientific world. It is completed with serious and

very thoughtful planning. However, its presentation and expected results may be of great interest to the scientific world. Its universal analog-to-digital architecture and data stream interpreter control open up exciting modeling opportunities in Smart City modeling [2].

Keywords: smartcity, neuron-network, parallel system, multiprocessoral

References

[1] N. CHEN, Y. CHEN: *Smart city surveillance at the network edge in the era of IoT:opportunities and challenges*, in: Smart Cities, Netherlands: Springer, Berlin, 2018, pp. 153–176.

[2] S. FURBER, S. TEMPLE, A. BROWN: *On-chip and inter-chip networks for modelling large-scale neural systems*, in: Procedural International Symposium on Circuits and Systems, Kos, Greece: ISCAS-2006, 2006.

[3] A. GAUR, B. SCOTNEY, G. PARR, S. MCCLEAN: *Smart city architecture and its applications based on IoT*, in: Procedia Computer Science. 52, 2015, pp. 1089–1094.

[4] K. GAUTAM, V. PURI, J. G. TROMP, N. G. NGUYEN, C. V. LE: *Internet of Things (IoT) and Deep NeuralNetwork-Based Intelligent and Conceptual Model for Smart City*, in.

[5] J. JIN, J. GUBBI, S. MARUSIC, M. PALANISWAMI: *An information framework for creating a smart city through internet of things.* In: IEEE Internet Things Journal 1(2), 2014, pp. 112–121.

[6] S. LATRE, P. LEROUX, T. COENEN, B. BRAEM, P. BALLON, P. DEMEESTER: *City of things: An integrated and multi-technology testbed for iot smart city experiments*, in: Smart Cities Conference (ISC2) 2016, IEEE International, 2016, pp. 1–8.

A secure electronic exam system using Identity-based Cryptography*

Ádám Vécsi[a] **and Attila Pethő**[a]

[a]Department of Computer Science, Faculty of Informatics, University of Debrecen
vecsi.adam@inf.unideb.hu
petho.attila@inf.unideb.hu

The rapid emergence of the digital technologies and the World Wide Web gave rise to e-learning systems built on top of these foundations. Although such systems already made a huge impact on education, their importance is further amplified by the social distancing measures induced by the COVID-19 pandemic. This widespread deployment, however, presents both existing and new challenges in even greater scale. Security-wise, the most challenging building block of an e-learning system is the e-exam management. In comparation with other parts of an e-learning system, such as educational material management, that mostly rely on authorization and data encryption, the examination and assessment process require authenticity, anonymity, and even accountability. Here, anonymity is a crucial aspect of the system as it ensures unbiased grading. This is an obligatory requirement, since in many cases, assessment results have a great influence of examinees' lives. For example, train drivers, Chinese officials, etc. are required to perform exams regularly, which if they fail, may result in losing their job.

The work of Huszti and Pethő [2] satisfies many important security requirements and the core idea of the construction is excellent, although contains some defects. The main defect is that the teachers, whose responsibility is to check the tests and give a grade for the students, are not accountable for their actions. As a result of the strong anonymity guarantees in the system, their identity cannot be found out unless revealed by themselves. This property could lead to fraudulent behavior from the teachers-side, without any consequence.

A particular advantage of this system is the reusable anonymous return channel, which is built on the protocol of Golle and Jakobsson [1]. This protocol consists of three parties: a message sender, a mixnet, delivering the message, and a message receiver. The system proposed by Huszti and Pethő uses this protocol to make anonymous conversation between students and teachers possible.

Our protocol follows the idea of the Huszti-Pethő system but is based on Identity-based Cryptography (IBC), which is a branch of public-key cryptography. The original concept behind IBC was coined by Adi Shamir [3]. The uniqueness of IBC lies in the fact that the

*This research was partially supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund, and was partially supported by the 2018-1.2.1-NKP-2018-00004 *Security Enhancing Technologies for the Internet of Things* project.

public key is a string that identifies an entity in a particular domain. One may think about an email address, a username, or a phone number.

The importance of this kind of public key is in direct connection with the core idea of the IBC, which was to simplify the certificate management and eliminate the need for certification authorities. In the public key infrastructure scenario, public keys and user identities are bound together with certificates. With IBC, however, there is no need for such certificates since the public key corresponds directly to the user identity.

Another feature of IBC is that the public key may contain more information than just the identity of the user, for example, dates, coordinates and so on. This extension of the public key with domain-specific data enables a wide spectrum of advanced use cases.

We think that IBC fits naturally into the system proposed by Huszti and Pethő because the data embedded into the public keys could result in a faster authentication process. Furthermore, the architecture of IBC is well-aligned with the anonymity requirements of an e-exam system. As the private key pairs of the public keys are generated by a trusted third party, called public key generator (PKG), this entity seems to be an obvious candidate to assume the role of exam authority (EA), which issues pseudonyms for the eligible participants and manages the whole exam process.

The EA is the only participant, who knows the real identities of actors. Teachers and students create pseudonyms with unrestricted warranty. Finishing the exam students are interested to uncover their identity because they want to get their grades. Teachers, however, have no interest in revealing themselves. If students protest against the teacher's opinion and grade the exam authority has to prove and decide. If a teacher committed fraudulent behavior, then he/she has to get a penalty. This is only possible after recovering the real identity from the pseudonym. In the IBC scenario, this is an easy task for the PKG who is at the same time the exam authority.

Another benefit of IBC is the absence of certificates, which reduces the friction of communication between the parties as the public key certificates of mix servers do not have to be distributed among users.

We show that our protocol satisfies the same properties as the Huszti-Pethő protocol did, moreover it can recover teachers' real identities from their pseudonyms.

References

[1] P. GOLLE, M. JAKOBSSON: *Reusable anonymous return channels*, in: Proceeding of the 2003 ACM workshop on Privacy in the electronic society - WPES '03, ACM Press, 2003, pp. 94–100.

[2] A. HUSZTI, A. PETHŐ: *A secure electronic exam system*, Publicationes Mathematicae Debrecen 77 (2010), pp. 299–312.

[3] A. SHAMIR: *Identity-based Cryptosystems and Signature Schemes*, in: Proceedings of CRYPTO 84 on Advances in Cryptology, Santa Barbara, California, USA: Springer-Verlag New York, Inc., 1985, pp. 47–53, ISBN: 0-387-15658-5.

Platform-independent microbenchmarking in C

György Vereb[a], **Attila Bagossy**[b]

[a]University of Debrecen, Faculty of Informatics
verebgeorge@gmail.com

[b]Chree
attila.bagossy@chree.io

Software benchmarking is the practice of estimating the relative performance of a software by running several tests against it. Performance has always been critical in computing, and benchmarking provides a way to compare, or keep track of performance. At first, it was the processors to be benchmarked by code. There are two widespread approaches for processor benchmarking: Whetstone and Dhrystone, the former is for floating-point operations (FLOPS), the latter is for integer arithmetic operations (MIPS)[5]. Processor benchmarking laid a foundation for benchmarking in software engineering: assessing the performance of critical business functionality. There is a type of benchmarking, which targets the critical aspects of the software at the code level, running the benchmarks against functions like unit tests. This approach, called microbenchmarking, provides an easy and fast way to measure and compare the performance of different implementations or code optimizations.

The best-known market standard benchmarking tool is Google Benchmark [1], which is a microbenchmarking library written in C++. It is capable of handling and defining custom timers and counters, benchmarking multithreaded code, and even calculating asymptotic complexity. Despite its heavy use of C++ templates and a large array of features, Google Benchmark maintains a moderate learning curve, making it approachable even for beginners. While these characteristics make the library attractive, having access to such features comes with a trade-off. It is heavy in terms of dependencies, therefore not easy to apply to any project, and since it requires C++11 to be built, it is hard for pure C developers to use. It is not platform-independent and uses dynamic memory allocation, which makes it impossible to be used in an embedded environment. We are not the first to notice these inconveniences, as there are benchmark libraries that were created specifically to satisfy some of the previously mentioned. Two of those are, for example, Picobench [2], which is for C++ only, and Ubench [3], which is capable of benchmarking code built with any mainstream C compiler (GCC, MSVC, Clang). However, they are still not platform-independent, nor deployable in an embedded environment.

Our goal was to design a library targeting the widest possible spectrum of platforms, ranging from embedded to desktop, with support for various operating systems and even WebAssembly [4]. The library we created, Sokutei, was designed with the greatest common denominator of these platforms in mind. In order to achieve support for a greater variety of platforms, we had to give up some capabilities, or in some cases, implement them in the library to use them. Although C compilers are available for virtually every

platform, the standard libraries may not be available everywhere, so we can not depend on them. Also, as many platforms like WebAssembly and microcontrollers do not have platform-level support for dynamic memory allocation, we had to resort to static memory allocation altogether. These sacrifices made for platform independence, however, do not limit our library's capabilities of making and handling custom counters and timers. In favor of the platform-independency goal, we had to implement key functionalities like string copying and comparing in a naive design, which, by default, cannot be optimized by the compiler. To get the greatest possible support, we made these functions default, but optional, and easy to replace. Input and output handling is also a platform-dependent functionality, and in our case, it is responsible for exporting benchmark results and possible error messages, therefore it was a crucial factor to make it customizable. The library can generate reports in JSON and CSV formats. We provide default settings for the most popular platforms, but every platform-dependent functionality was made pluggable, so they are easily modifiable to meet the requirements of other platforms.

Keywords: benchmark, platform-independence, performance, webassembly, embedded devices

References

[1] *Google Benchmark - A microbenchmark support library*, 2020,
URL: `https://github.com/google/benchmark` (visited on 10/24/2020).

[2] *Picobench - A microbenchmark support library for C++*, 2020,
URL: `https://github.com/iboB/picobench` (visited on 10/24/2020).

[3] *Ubench - A microbenchmark support library for C*, 2020,
URL: `https://github.com/sheredom/ubench.h` (visited on 10/24/2020).

[4] *WebAssembly - A binary instruction format for a stack-based virtual machine*, 2020,
URL: `https://webassembly.org/` (visited on 10/24/2020).

[5] R. P. WEICKER: *An overview of common benchmarks*, Computer 23.12 (1990), pp. 65–75.

Open Data, FAIR Data, Aspects of Research Data Management

Márta Virágos[a]

[a]University of Debrecen, Faculty of Informatics
viragos.marta@inf.unideb.hu

Abstract

Over the last 10 years, there has been a growing recognition that research data are of significant value. The importance of transparency, reuse, and verifiability of research data is often emphasised. Many funders encourage or demand researchers to critically plan their Research Data Management (RDM) at the start of a project, and to retain and possibly publish datasets once the research has been completed (e.g., European Commission, Welcome Trust, National Science Fund). Publishers, too, are showing awareness of the value of data, asking or sometimes requiring authors to share the datasets underlying their publications (e.g., PLOS, 2017). Researchers also recognise the value of RDM, since it brings benefits of various kinds, such as efficiency of research, more societal impact, and increased chances of getting funding.

"The Open Data Directive" or "the Directive" of the European Commission takes positive steps to enhance the way that publicly funded research data is made available, accessed, shared and re-used [8]. Member States are required to develop national policies for open access to research data resulting from public funding, following the principle of 'open by default'. Furthermore, new harmonised rules on re-usability are applied to all publicly funded research data which is already made accessible via open repositories. Access to research data follows the principle of "as open as possible, as closed as necessary", according to the FAIR principles : **Findable**: data and supplementary materials have sufficiently rich metadata and a unique and persistent identifier; **Accessible**: metadata and data are understandable to humans and machines and deposited in a trusted repository; **Interoperable**: metadata use a formal, accessible, shared, and broadly applicable language for knowledge representation; **Reusable**: data and collections have a clear usage licenses and provide accurate information on provenance, accessible, interoperable, reusable). The realisation of FAIR data relies on, at minimum, the following essential components: policies, Data Management Plans, identifiers, standards and repositories. Registries need to catalogue each component of the ecosystem, and the automated workflows between them. The presentation will briefly discuss all elements, highlighting the most important features and presenting a model for FAIR Digital Objects. To ensure that institutions meet the above-discussed requirements, and that their research data assets are safely guarded and fully exploited, more and more universities are implementing research data management policies. While data policies have been most prolific in the UK and Australia [6], they have been also established at North American and European universities, respectively [2,

7]. Where policies are not yet in place, they are often planned, or already in the process of being established. Overviews of implemented data policies are provided and maintained by the Digital Curation Centre (DCC) for the UK [4], the Australian National Data Service (ANDS) for Australia, and the National Coordination Point Research Data Management (LCRDM) for the Netherlands (LCRDM, 2017). Research Data Management (RDM) involves services, tools and infrastructure that support the management of research data across the lifecycle [1, 3, 5]. The paper will examine the various aspects of RDM, how they are often distributed across different support services and academic departments (e.g. Research Office, IT Services, Library). Case studies demonstrate that researchers need support in numerous areas across the entire research lifecycle: planning, organizing, security, documenting and sharing, preparing datasets for deposit and long-term preservation, as well as issues related to copyright, licensing, and intellectual property more generally.

The paper also looks at the four elements of Research data Infrastructure (research data itself, data management, data management tools and technical components staffing), and presents some relevant examples.

Keywords: open research data, data management

References

[1] K. G. AKERS: *Going beyond data management planning: Comprehensive research data services*, College and Research Libraries News 8.75 (2014), pp. 435–436,
URL: http://crln.acrl.org/content/75/8/435.full.pdf+html.

[2] K. BRINEY, A. GOBEN, L. ZILINSKI: *Do you have an institutional data policy? A review of the current landscape of library data services and institutional data policies*, Journal of Librarianship and Scholarly Communication 3 (2015), pp. 1–25,
DOI: https://doi.org/10.7710/2162-3309.1232.

[3] R. HIGMAN, S. PINFIELD: *Research data management and openness: The role of data sharing in developing institutional policies and practices*, Program 4.49 (2015), pp. 364–381,
DOI: https://doi.org/10.1108/PROG-01-2015-0005.

[4] L. HORTON, DCC: *Overview of UK institution RDM policies*, 2016,
URL: http://www.dcc.ac.uk/resources/policy-and-legal/institutional-data-policies.

[5] S. JONES, G. PRYOR, A. WHYTE: *'How to Develop Research Data Management Services - a guide for HEIs'. DCC How-to Guides*, Edinburgh: Digital Curation Centre, 2013,
URL: http://www.dcc.ac.uk/resources/how-guides.

[6] K. SHEARER: *Comprehensive brief on research data management policies*, 2015,
URL: https://portagenetwork.ca/wp-content/uploads/2016/03/%20Comprehensive-Brief-on-Research-Data-Management-Policies-2015.pdf.

[7] C. TENOPIR, S. TALJA, W. HORSTMANN, E. LATE, D. HUGHES, D. POLLOCK, S. ALLARD: *Research data services in European academic research libraries*, LIBER Quarterly 1.27 (2017), pp. 23–44,
DOI: https://doi.org/10.18352/lq.10180.

[8] M. D. WILKINSON, M. DUMONTIER, I. J. AALBERSBERG, G. APPLETON: *The FAIR Guiding Principles for scientific data management and stewardship*, Scientific Data 3.160018 (2016),
DOI: https://doi.org/10.1038/sdata.2016.18.

Comparison of EEG data processing using feedforward and convolutional neural network

Yu Xie[a], Stefan Oniga[b]

[a]IT Systems and Networks Faculty of Informatics University of Debrecen
yu.xie@inf.unideb.hu

[b]Faculty of Informatics University of Debrecen, Techical University of Cluj-Napoca, North University Centre of Baia Mare
oniga.istvan@inf.unideb.hu

Brain-Computer Interface (BCI) is a communication control system established between the brain and external devices (computers or other electronic devices) through signals generated during brain activity [2]. The aim of BCI is to create a communication link between human brain and computer. It provides a way to transform brainwaves into physical effects without using muscles [3]. In the decades since the birth of BCI technology, the research on electroencephalogram (EEG) signal classification methods has always been the driving force for the continuous development of BCI technology. EEG is a non-invasive acquisition method in the BCI system [1]. It detects weak EEG signals by placing electrodes on the scalp and records changes in electrical signals during brain nerve activity. However, since EEG will be greatly weakened when it travels from the cerebral cortex to the scalp, the signal-to-noise ratio of the extracted signal is extremely low, which increases the difficulty of subsequent feature extraction and classification. It is difficult for traditional classification methods to find well distinguished and representative features to design a classification model with excellent performance. In recent years, however, the deep learning methods such as layer-by-layer automatic learning of data features, step-by-step abstraction, and good generalization capabilities have made itself a great success in the field of image and speech.

This study created a convolution neural network that can recognize and automatically extract the features of EEG signals and compare the accuracy of traditional methods of feature extraction and classification. We used PhysioNet EEG data for this project, which are composed of over 1500 one- and two-minute EEG recordings, received from 109 subjects. The goal of our work is to explore Fast Fourier Transform (FFT) signal analysis techniques for distinction between two states, eyes open (EO) and eyes closed (EC), through the detection of EEG activity obtained from eight scalp channels.

Our results demonstrated that the determination of the activity from the EEG signal is possible with high classification accuracy. We obtained a 96% recognition rate using MLP and 91% using CNN. Our result showed a higher accuracy rate and shorter training time of using MLP instead of CNN for this purpose. Compared with MLP, however, CNN combines signal preprocessing, feature extraction and classification. It avoids the blindness and cumbersomeness of EEG signal processing, and it also has a good accuracy rate. It is necessary to design a classification model with strong robustness and high accuracy

for EEG signals.

References

[1] F. CARPI, D. DE ROSSI, C. MENON: *Non invasive brain-machine interfaces*, ESA Ariadna Study 5 (2006), p. 6402.

[2] J. J. SHIH, D. J. KRUSIENSKI, J. R. WOLPAW: *Brain-computer interfaces in medicine*, in: Mayo Clinic Proceedings, vol. 87, 3, Elsevier, 2012, pp. 268–279.

[3] J. SUTO, S. ONIGA: *Music stimuli recognition in electroencephalogram signal*, Elektronika ir Elektrotechnika 24.4 (2018), pp. 68–71.

Automatic Text Summarization for Hungarian

Zijian Győző Yang[abc], Ádám Agócs[a], Gábor Kusper[a], Tamás Váradi[c]

[a]Eszterházy Károly University, Faculty of Informatics
agadam98@gmail.com,{kusper.gabor,yang.zijian.gyozo}@uni-eszterhazy.hu

[b]MTA-PPKE Hungarian Language Technology Research Group
yang.zijian.gyozo@itk.ppke.hu

[c]Research Institute for Linguistics
varadi.tamas@nytud.hu

In our research, we have created a text summarization software tool for Hungarian using multilingual and Hungarian BERT-based models. Two types of text summarization method exists: abstractive and extractive. The abstractive summarization is more like human generated summarization. Target summaries may include phrases that the original text does not necessarily contain. This method generates the summarized text by applying keywords that were extracted from the original text. The extractive method summarizes the text using the most important extracted phrases or sentences from the original text.

We have built extractive and abstractive summarization models for Hungarian. We have carried out experiments to compare the different kinds of BERT-based models. Our experiments were conducted using the following models:

- BERT Base Multilingual Cased (multi-BERT)
- huBERT [5] Base: Wiki (huBERT wiki) and Web (huBERT web)
- Hungarian ELECTRA Base: Wiki (ELECTRA wiki) and Large (ELECTRA large)

The 'BERT Base Multilingual Cased'model [2] was pretrained in 104 languages with the biggest the largest Wikipedia. The system was pretrained using two tasks i.e. Masked language modeling (MLM) and Next sentence prediction (NSP).

The huBERT system is a Hungarian BERT model trained on Webcorpus 2.0 [5] and a snapshot of the Hungarian Wikipedia. There are two different kinds of huBERT model: huBERT cased, and huBERT lowercased. All models outperform the multilingual BERT model in masked LM, NER and NP chunking tasks and the full huBERT outperforms the Wikipedia models by 0.5%.

ELECTRA [1] is a new method for self-supervised language representation learning. It can be used to pre-train transformer networks using relatively little compute. ELECTRA models are trained to distinguish "real" input tokens vs "fake" input tokens generated by another neural network, similar to the discriminator of a GAN. At small scale, ELECTRA achieves strong results even when trained on a single GPU.

We have trained two ELECTRA models for Hungarian: ELECTRA wiki and ELECTRA large.

- ELECTRA wiki: Hungarian wikipedia: 13,098,809 segments; 131,976,236 tokens
- ELECTRA large: Hungarian large (include wikipedia): 283,099,534 segments; 3,993,873,992 tokens

For creating summarization corpora for fine-tunning, we used the articles taken from the online weekly magazine hvg.hu, as well as the related leads. The main characteristics of the hvg corpus are as follows:

- Online article database (daily newspaper): 2012-2020;
- 480,660 articles; 129,833,741 tokens; 5.133.030 type
- The articles cover the following topics: economy, politics, science, sports, culture, psychology, blog
- Training corpus: 472,660 articles; Test corpus: 3,000 articles; Validation corpus: 5,000 articles
- Source text (articles) average paragraph length: 246,27 words; 12.43 sentences
- Target text (lead) average paragraph length: 23,74 words; 1.46 sentences

For building extractive and abstractive models, we used the PreSumm [4] tool. Table 1 and 2, we can see the ROUGE [3] recall results of our abstractive and extractive experiments.

	ROUGE-1	ROUGE-2	ROUGE-L
multi-BERT	47.02	19.72	39.29
huBERT wiki	49.49	21.62	41.46
huBERT web	**51.47**	**23.27**	**43.82**

Table 1: ROUGE recall results of abstractive summarization

	ROUGE-1	ROUGE-2	ROUGE-L
multi-BERT	48.58	20.12	39.42
huBERT wiki	48.63	20.32	39.44
huBERT web	48.82	20.34	39.54
ELECTRA wiki	48.83	20.37	39.53
ELECTRA large	**48.84**	**20.38**	**39.61**

Table 2: ROUGE recall results of extractive summarization

In the case of abstract summarization (see Table 1), the integration of Hungarian models could gain higher performance than the multilingual model. In the case of extractive summarization (see Table 2), all Hungarian models have achived higher performance than the multi-BERT and our ELECTRA models, which were trained with less computational demand, could achieve the best results for Hungarian.

In conclusion, we have created an automatic text summarization tool for the Hungarian language. This is the first automatic abstractive and extractive text summarization tool for Hungarian that is based on neural network technology.

Keywords: text summarization, extractive summarization, abstractive summarization, BERT, ELECTRA

References

[1] K. CLARK, M.-T. LUONG, Q. V. LE, C. D. MANNING: *ELECTRA: Pre-training Text Encoders as Discriminators Rather Than Generators*, in: International Conference on Learning Representations, 2020.

[2] J. DEVLIN, M.-W. CHANG, K. LEE, K. TOUTANOVA: *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, in: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers), Minneapolis, Minnesota: Association for Computational Linguistics, June 2019, pp. 4171–4186.

[3] C.-Y. LIN: *ROUGE: A Package for Automatic Evaluation of Summaries*, in: Text Summarization Branches Out, Barcelona, Spain: Association for Computational Linguistics, July 2004, pp. 74–81.

[4] Y. LIU, M. LAPATA: *Text Summarization with Pretrained Encoders*, in: Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, Hong Kong, China: Association for Computational Linguistics, 2019, pp. 3730–3740.

[5] D. M. NEMESKEY: *Natural Language Processing Methods for Language Modeling*, PhD thesis, Eötvös Loránd University, 2020.

N-bit per Volt ADC implemented on FPGA and FPAA: Design of the Front End*

Salam Zayer[a], Marwah Muneer Al-bayati[a], György Györök[b], Ahmed Bouzid[a]

[a]Institute of Automation and Infocommunication. University of Miskolc, Hungary
salaamzayer@gmail.com, marwamoner11@gmail.com,
qgebouzid@uni-miskolc.hu

[b]Alba Regia Technical Faculty Obuda University
gyorok.gyorgy@amk.uni-obuda.hu

Reconfigurability has made it possible, among other benefits, to replace traditional discrete components with chips, whose internal components can be programmed in this case FPAAs (Field Programmable Analog Arrays). This paper presents a design and implementation of FPAA of the analog front end dedicated to a new ADC architecture called "N bit per Volt". After validation of the algorithm in simulation, the experimentation results show that the obtained reconfigurable circuit can replace the traditional discrete components based circuits.

Introduction and Background

Alongside the development of the semiconductor technologies, manufacturers developed approaches to refresh their products with extra highlights on existing hardware. Programmable equipment whose sub-framework designs can be changed even after manufacture, falls under the classification of Reconfigurable System [6][3]. Field-programmable analog array (FPAA) is coordinated circuits with an assortment of simple structure blocks associated through a wire and change texture to accomplish reconfigurability like the FPGAs of the advanced space [1]. In [4] is discussed an application of combining FPGA and FPAA reconfiguration capabilities for IEEE 1451.5 for compliant smart sensor applications. In [5], the authors discussed the Compact Intelligent Bioelectric Signals Acquisition System with an Adaptive fronted interface Implemented Using FPGA and FPAA. Classical voltage dividers were often used for interfacing analog sensors with ADCs having low input ranges. For instance the 7-series Xilinx devices cannot handle voltages exceeding 1 V_{p-p}. This article addresses this issue by proposing a new ADC architecture.

*This research was supported by the European Union and the Hungarian State, co-financed by the European Regional Development Fund in the framework of the GINOP-2.3.4-15-2016-00004 project, aimed to promote the cooperation between the higher education and the industry.

Implementation and results

This paper presents an implementation and experimentation of the front end of a new ADC (presented in [2]) named N bit per Volt ADC exploiting FPAA and FPGA hybridization. Figure 1 illustrates the circuit design implemented using Anadigm Software. The working principle is as follows: The FPAA1 computes the voltage range of the input, then passes the information to the FPGA in 3 bits. The FPAA2 shifts the input voltage into three different values and passes all of them to the FPGA as well. The circuit mainly contains three comparators, they compare the input to respectively 3 V, 2 V and 1 V. Mainly, FPAA2 contains three subtractors, each one shifts down the signal by a specific voltage. For better accuracy, an additional gain stage was needed before the subtractors. Figure 2 shows the results of the first configuration, while the yellow, green, blue and magenta traces correspond to the input, the output of the comparator 1, 2, and 3 respectively.

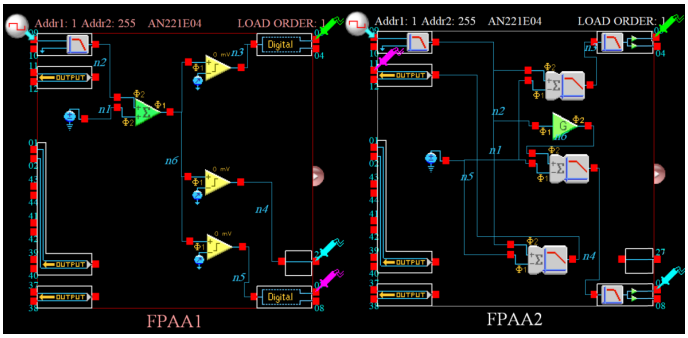


Figure 1: Circuit of the reconfigurable analog front end implemented on FPAA

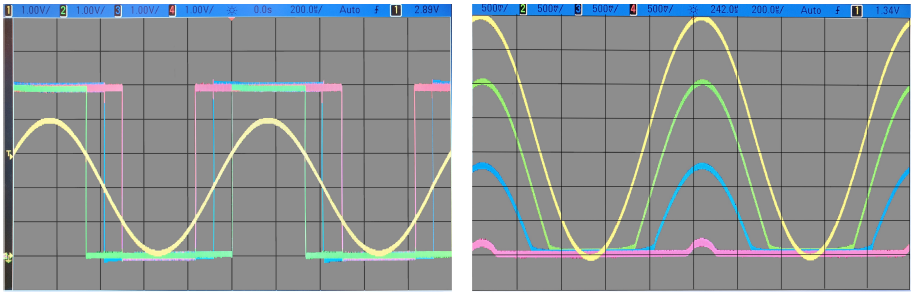


Figure 2: Input and outputs of the FPAAs after configuration (FPAA1 on the left and FPAA2 on the right)

Conclusion. Parameterization of FPAAs is not a straightforward matter since their behavior is not as deterministic as expected from simulation, a calibration phase is required.

Initially, the whole reconfigurable analog part of the design was performed in a single FPAA chip, but a single net caused overconsumption of the resources. The next step will be to optimize the design in order to fit the configuration in a single FPAA chip. In the close future, the FPAA will be connected to the previously configured FPGA in order to test the whole ADC.

Keywords: ADC, FPAA, FPGA

References

[1] I. F. BASKAYA: *Physical design automation for large scale field programmable analog arrays*, PhD thesis, Georgia Institute of Technology, 2009.

[2] A. BOUZID, J. VÁSÁRHELYI: *High Resolution Large Scale ADC. Case study of an N bit per Volt ADC Implemented using FPAA and FPGA Applied for Precision Altimetery*, in: 21st International Carpathian Control Conference. Proceedings. IEEE, 2020.

[3] G. ESTRIN: *Reconfigurable computer origins: the UCLA fixed-plus-variable (F+ V) structure computer*, IEEE Annals of the History of Computing 24.4 (2002), pp. 3–9.

[4] D. P. MORALES, A. GARCIA, A. J. PALMA, A. MARTINEZ-OLMOS: *Merging FPGA and FPAA reconfiguration capabilities for IEEE 1451.4 compliant smart sensor applications*, in: 2007 3rd Southern Conference on Programmable Logic, IEEE, 2007, pp. 217–220.

[5] P. A. MOU, C. H. CHEN, S. H. PUN, P. U. MAK, M. I. VAI: *Portable intelligent bioelectric signals acquisition system with an adaptive frontend implemented using fpga and fpaa*, in: World Congress on Medical Physics and Biomedical Engineering, September 7-12, 2009, Munich, Germany, Springer, 2009, pp. 348–351.

[6] J. ZHU, M. DEXHEIMER, H. CHENG: *Reconfigurable systems for multifunctional electronics*, npj Flexible Electronics 1.1 (2017), pp. 1–13.

Examination of viability and utilization of eye tracking in mobile VR applications, analysis of mobile VR trends*

Gergő Zilizi[a], Anett Rácz[a]

[a]Faculty of Informatics
University of Debrecen
Debrecen, Hungary
zilizigergo@gmail.com
racz.anett@inf.unideb.hu

Introduction

In our earlier studies we developed high performance desktop VR applications for architecture and tourism. Later we explored the potential of the mobile VR platform, tested our applications on it, and established guidelines for development of such high performance portable Virtual Reality experiences.

We intended to augment this field of VR technology with eye tracking and try to solve the main issues of the platform. Previous methods only worked in very specific scenarios and conditions, with very specific hardware. We wanted to come up with an easily generalizable eye tracking solution for mobile VR. Although we could not realize our final goal, our research and development shed light on important limitations and pitfalls of this field.

In this paper we also present our findings regarding the future of mobile VR platform, current sales and popularity trends, and the impact of mobile VR on Virtual Reality as a medium.

Introduction to mobile VR

Mobile VR is an excellent way to deliver virtual reality experiences to a wide range of users. Nowadays even a midrange smartphone can handle a mobile VR application, and a basic mobile VR headset like the Google Cardboard viewer does not cost more than a few dollars.

Despite these advantages, the development of high-fidelity mobile VR applications that give a great, comfortable experience is a very difficult task. In one of our previous papers "Challenges of developing mobile versions for high performance desktop VR applications" [4] we discuss the challenges of mobile virtual reality development in detail.

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was co-financed by the Hungarian Government and the European Social Fund.

Examination of the main problems of mobile VR

Mobile VR experiences are not that polished and stable, and with some users this can induce motion sickness [3] while using them.

The severity of motion sickness in mobile VR originates from three main technical factors: insufficient performance, absence of intuitive input device and inferior depth of immersion.

Considering the factors above, mobile VR gives lower fidelity compared to more premium standalone or desktop VR headsets.

Eye tracking as a potential solution

After further examination we found that well implemented eye tracking could solve almost all of the previously mentioned problems, mitigate motion sickness, and increase the quality and immersion of the users' experience in Virtual Reality.

In this paper we investigate the possibilities of eye tracking for mobile VR and how it can solve the three main problems.

Why widely applicable, generalized eye tracking is currently not feasible for mobile VR

Theoretically eye tracking would be a very good augmentation for mobile VR, but along the development of our generalized and more widely applicable solution we discovered many factors that prevent this approach from achieving acceptable stability and consistency for everyday use.

Previous solutions exist, but they require very specific phone-headset combinations [1], and in some cases modification of the headset [2]. These solutions only work in best case scenarios, they exhibit many usability problems, and have significant limitations.

In the full paper we explain the difficulties that make the implementation of more generalized eye tracking solutions almost impossible.

Mobile VR market trends

At the end of our paper we write about the future of mobile VR as a platform. We analyze current sales and popularity trends, and describe the impact of mobile VR on Virtual Reality as a medium.

Keywords: Virtual Reality; Mobile VR; Eye tracking

References

[1] P. DRAKOPOULOS, G. A. KOULIERIS, K. MANIA: *Front Camera Eye Tracking For Mobile VR*, in: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), 2020, pp. 642–643,
DOI: https://doi.org/10.1109/VRW50115.2020.00172.

[2] S. W. GREENWALD, L. LORETI, M. FUNK, R. ZILBERMAN, P. MAES: *Eye Gaze Tracking with Google Cardboard Using Purkinje Images*, in: Proceedings of the 22nd ACM Conference on Virtual Reality Software and Technology, VRST '16, Munich, Germany: Association for Computing Machinery, 2016, pp. 19–22, ISBN: 9781450344913,
DOI: https://doi.org/10.1145/2993369.2993407.

[3] L. J. HETTINGER, G. E. RICCIO: *Visually Induced Motion Sickness in Virtual Environments*, Presence: Teleoperators and Virtual Environments 1 (1992), pp. 306–310,
DOI: https://doi.org/10.1162/pres.1992.1.3.306.

[4] G. ZILIZI, A. RÁCZ: *Challenges of developing mobile versions for high performance desktop VR applications*, in: 2019 15th International Conference on Engineering of Modern Electric Systems (EMES), 2019, pp. 45–48,
DOI: https://doi.org/10.1109/EMES.2019.8795204.

TEE-Based Protection of Cryptographic Keys on Embedded IoT Devices

Máté Zombor[a], Dorottya Papp[a], Levente Buttyán[a]

[a]Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Budapest University of Technology and Economics
www.crysys.hu

The Internet of Things (or IoT for short) consists in billions of embedded devices connected to the Internet. This new phenomenon is the basis for today's smart applications in the domains of manufacturing (Industry 4.0), transportation (Cooperative Intelligent Transportation Systems), and healthcare (personalized e-Health), as well as in everyday life (smart cities, smart homes). However, in almost all application areas of IoT, we face security and privacy issues, which require solutions developed for or adapted to the special characteristics of IoT systems. In particular, security and privacy mechanisms should take into account the resource limitations of embedded devices and they should not rely on special hardware that would significantly increase the development cost of IoT applications. This leads to interesting challenges for managing cryptographic keys on IoT devices.

In many applications, IoT devices are managed remotely by system operators. Such remote management requires secure remote access to the devices, which in turn, requires the devices to store and use long-term cryptographic keys. For instance, the operator usually needs to authenticate the device before uploading configuration data or software updates on it, which may require the device to use a long-term, devices specific private key. However, as IoT devices are connected to the Internet, they may be compromised by malicious actors (aka attackers). If an attacker can obtain the long-term key of a compromised device, (s)he can impersonate and clone that device, which is undesirable. Hence, there is a need to protect long-term cryptographic keys on IoT devices such that a key remains inaccessible to the attacker even if the device itself is compromised.

A possible solution to the problem above would be to store cryptographic keys on IoT devices in secure co-processors, such as a TPM chip[1], that would never output a key, but only use it internally in cryptographic operations. However, requiring an additional co-processor on every IoT device would be too expensive in most cases.

In this work, we propose a more cost efficient approach: we ensure protection of cryptographic keys by using a Trusted Execution Environment (TEE), which is mostly based on software with some minimal hardware support, and which is supported on many embedded platforms used in IoT applications. For instance, many embedded devices use ARM processors that feature the ARM TrustZone technology[2], which enables the establishment

[1]https://trustedcomputinggroup.org/resource/tpm-library-specification/ (last accessed: October 3, 2020)

[2]https://developer.arm.com/ip-products/security-ip/trustzone (last accessed: October 3, 2020)

of a software based TEE and provides some hardware based protection mechanisms to it. TEEs usually implement a persistent secure storage service (see, e.g., the TEE specifications[3] of GlobalPlatform, a non-profit industry association aiming at enabling digital services and devices to be trusted and securely managed throughout their lifecycle), which can be used to store long-term cryptographic keys. Moreover, operations with those keys can be performed by trusted applications running within the TEE, hence, the keys would never leave the protected environment of the TEE.

Our approach provides similar protection to keys as a secure co-processor, but does not actually require another processor on the device: the same processor runs a normal execution environment and a TEE, and also implements the required hardware mechanisms that isolate these two execution environments. This isolation ensures that even if the normal execution environment is compromised, the attacker would not be able to obtain the keys stored and used within the TEE.

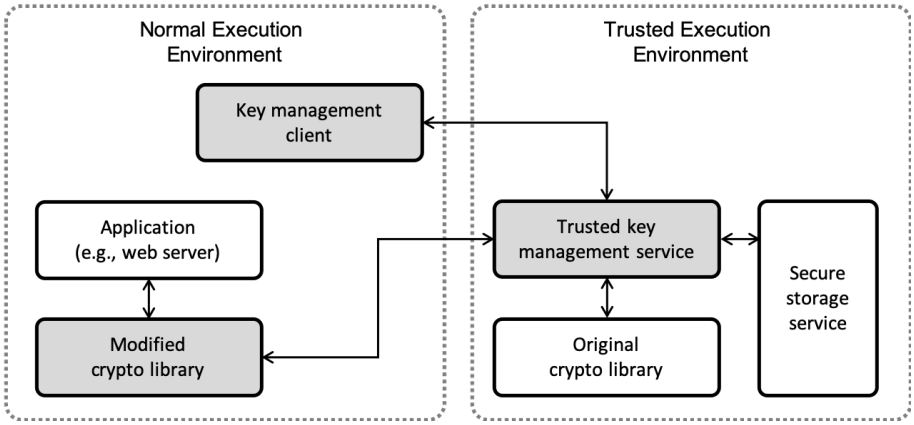


Figure 1: Architecture of our TEE-based key management solution. Grey boxes represent components that we developed or modified.

The architecture of our solution is illustrated in Figure 1. The basic idea is that any application (e.g., a web server that provides a remote configuration possibility for the operator of the device) that runs in the normal execution environment can be compiled with a cryptographic library that we modified such that private key cryptographic operations are delegated to a trusted key management service running in the TEE. The trusted key management service is compiled with the original cryptographic library, and it calls this library to execute the requested operation. The private key is stored in the secure storage of the TEE. This key could be generated by the operator off-line and loaded in the secure storage in a controlled way with the help of a key management client, or the key can actually be generated and stored in secure storage by the trusted key management service itself, in which case it would output the corresponding public key to the key management client such that it can be made available to applications running outside of the TEE. In

[3] `https://globalplatform.org/specs-library/?filter-committee=tee` (last accessed: October 3, 2020)

both cases, a handle to the private key would be output from the trusted key management service that can be used by applications in the normal execution environment to refer to the private key when calling operations with it in the cryptographic library. The handle is passed to the trusted key management service when the operation is delegated, and it is used to retrieve the key from the secure storage. The key is then passed to the cryptographic library that actually performs the requested cryptographic operation. Finally, the trusted key management service passes the result of the operation back to the calling application.

In the full paper, we explain in more details our proposed architecture and the way it supports delegating private key cryptographic operations to the trusted key management service running in the TEE. In particular, we describe the API provided by the trusted key management service through which keys can be loaded or generated in the TEE, and signing and decryption operations can be delegated from the normal execution environment. We also provide a security analysis of our solution, and we report about its prototype implementation using mbedTLS[4] as the cryptographic library and OP-TEE[5] as the TEE implementation.

Acknowledgements. The presented work was carried out within the SETIT Project (2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

[4] `https://tls.mbed.org/` (last accessed: October 3, 2020)
[5] `https://www.op-tee.org/` (last accessed: October 3, 2020)