Vilnius University

The International Doctoral Consortium on Informatics Education and Educational Software Engineering Research

Organisers:
Prof. Dr. Valentina Dagienė
Dr. Gabrielė Stupurienė

December 2–6, 2019,
Druskininkai, Lithuania

Contents

Improving the Efficiency of Methods for Calculating Elementary Functions in Floating-Point Arithmetic

Oleh Horyachyy

Third year of postgraduate studies
Lviv Polytechnic National University, Ukraine
12 Bandera str.
Lviv, 79013, Ukraine
oleh.y.horiachyi@lpnu.ua

Biography

I received my MSc degrees in Applied Computer Science from Ivan Franko National University of Lviv in 2013 (*Thesis:* Solution of integro-differential equations by the projection-iterative method) and in Information and Communication Systems Security from Lviv Polytechnic National University in 2017 (*Thesis:* Communication technologies used for low-power, low-bandwidth Internet of Things networks). In 2014, I worked as an ASP.NET/C# software developer. In 2017, I participated in the Erasmus+ international student exchange program in Sweden for one semester. Currently, I am a PhD student in Cybersecurity at Lviv Polytechnic National University and an engineer at the Department of Information Technologies Security. My supervisor is Prof. Leonid Moroz. My teaching experience includes working as a teaching assistant (*Subjects:* Algorithmic fundamentals of Cryptology, Applied Cryptology, Security of Information and Communication Systems, Public Key Infrastructure, Computer methods for analysis and design of electronic circuits) in the same department. My research interests include iterative methods, biometric identification systems, security of communication technologies, cryptography, public key infrastructure, and secure multiparty computations.

Publications

1. Horyachyy, O., Boretskyy, T., & Horiachyi, I. (2019). Improving the Methods of Protection and Hacking of Modern Wi-Fi Networks. In *Materials of 7th International Scientific and Technical Conference on Information Protection and Information Systems Security* (pp. 60-61). Lviv, Ukraine: Publishing House of Lviv Polytechnic National University.
2. Hrynchyshyn, A., Horyachyy, O., Tymoshenko, O., & Moroz, L. (2018). An Efficient Algorithm for Fast Inverse Square Root. In J. Rysiński, & S. Zawiślak (Eds.), *Processing, transmission and security of information, vol. 2* (pp. 105-114). Bielsko-Biała, Poland: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej.
3. Moroz, L., Samotyy, V., & Horyachyy, O. (2018). An Effective Floating-Point Reciprocal. In *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)* (pp. 137-141). Lviv, Ukraine: IEEE.
4. Moroz, L., Samotyy, V., Horyachyy, O., & Dzelendzyak, U. (2019) Algorithms for calculating the square root and inverse square root based on the second-order Householder's method. In *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1* (pp. 436-442). Metz, France: IEEE.

Research area description

- The main problem and its relevance

Floating-point arithmetic is a common way to represent real numbers in computers. This representation of the number in the form of three separate parts of a fixed size – a sign, an exponent, and a significant – have some drawbacks. However, it allows us to store approximate values in a wide range of real numbers with good

accuracy in the limited memory of computers. The peculiarity of this representation is that it has a fixed relative error for all normalized numbers and their absolute error varies depending on the magnitude of the exponent. Floating-point numbers and operations on them are defined in the IEEE 754-2008 standard.

The implementation of mathematical operations with floating-point numbers and corresponding functions can be either hardware or software on different platforms. On modern computer systems, basic operations and functions defined by the standard, such as square root and fused multiply-add (FMA), are usually implemented in hardware and are fast enough. They can have integrated or separate FPU (Floating-Point Unit) in order to increase the speed of floating-point computations. Other functions are emulated by software library and therefore have much worse performance (exp, cos, log, etc.). For example, the C++ compiler has cmath library with built-in functions sqrt(x) and fma(x, y, z) for float, double and long double types, available on almost any device. FPUs of Intel Core i-7 and ARM Cortex A-53 processors have fast SQRT and FMA instructions of full accuracy both in single and in double precision. For some applications where full accuracy is not required, but speed is critical, approximate instructions are given on modern computers for the reciprocal (RCP) and reciprocal square root (RSQRT) functions. Such hardware instructions, if available, are platform-dependent and vary in accuracy and performance (for example, on Intel there are no RSQRT instruction for double). Also, SIMD (Single Instruction, Multiple Data) versions of these instructions can be provided for pipelined calculations. However, on simpler and cheaper devices, e.g. microcontrollers, similar fast hardware instructions are missing. Also, compared to other basic arithmetic operations, division is more complex and expensive. That is why on some devices, for example, in the ESP-WROOM-32 microcontroller, this operation is not implemented in hardware. In addition, sometimes hardware engineers and developers should implement these elementary functions on other devices, such as field-programmable gate arrays (FPGA) and application-specific integrated circuits (ASIC).

In our research, we have limited ourselves to calculating such common elementary functions in floating-point arithmetic as the reciprocal, division, inverse square root, and square root. We mainly study the software implementation of these functions in C++, however, we also consider the possibility of their further hardware implementation, for example on FPGA. These functions are frequently used in computer graphics (e.g. for computer vision, object detection, and lighting tasks), digital signal processing, and in science (e.g. in mathematics, statistics, and physics). An example of where these algorithms are greatly used and where the accuracy of computations is important is linear algebra. All these functions are used in various decomposition and inverse matrix algorithms. Sometimes bugs and errors of floating-point arithmetic can have serious consequences. We can recall a bug in division operation of some Intel Pentium processors (Coe, 1995), which was discovered in 1994 and caused Intel's losses in the amount of 475 million dollars; after the scandal, the company was forced to replace all defective processors. Such errors can be critical in space and military industries when launching rockets or missile guidance. Other applications such as lighting and shading for 3D graphics do not require much accuracy, but computational performance is quite important.

- The aim of research

This scientific research aims to develop such simple and effective algorithms for calculating the elementary functions of the reciprocal, division, inverse square root, and square root in floating-point arithmetic, which will allow us to get a better compromise between the required accuracy and speed of calculations.

Other basic requirements for the algorithms are:

a. support for floating-point numbers in the IEEE 754 format of various precision (single, double, quadruple, etc.);

b. use only simple and fast integer and floating-point operations, which are most often available in hardware; it means avoiding the expensive division operation;
c. cross-platform, the ability to use both on personal computers and on simple microcontrollers that do not have specialized hardware instructions; the possibility of hardware implementation on FPGAs and ASICs;
d. avoiding cumbersome lookup tables (LUTs);
e. reduction of the maximum relative error of the algorithms.

- Current knowledge of the problem domain

Currently, for calculation of elementary functions, many algorithms can be used both in hardware and software. Such algorithms can be divided into several main classes: digit recurrence, iterative, polynomial, table-based methods, and their combinations. Nowadays, the SRT (Sweeney, Robertson, Tocher) digit recurrence algorithm is commonly used for the division operation in modern microprocessors. It also uses lookup tables (LUTs). In computer systems having fast hardware multiplication instructions, such elementary functions as reciprocal and inverse square root are implemented using iterative methods, which have much better convergence. The most commonly used methods are Newton-Raphson and Goldschmidt's, which double the number of correct bits of the result after each iteration. There are also methods that have a higher convergence order, but they have more operations. Iterative methods need an initial value, the accuracy of which greatly affects the number of required iterations and the convergence of the method. The state-of-the-art solution to obtain the initial value in modern CPUs and FPGAs includes lookup tables. For example, RCP and RSQRT hardware instructions, which can be used for this purpose, are based on this approach. A significant drawback of this method is the large use of the device's memory for LUT storage, which grows exponentially with the necessary accuracy. That is why Intel RCP and RSQRT instructions have 11 correct bits of the result for single-precision numbers; in ARM Cortex-A processors, such instructions have 8 correct bits for single and double precision.

Given all the above, we decided to use the fast inverse square root algorithm (FISR) as the basis for our algorithms. The most popular version of the algorithm was implemented in the computer game Quake III Arena (Id Software, 1999), released in December 1999. This algorithm is widely used for both software and hardware implementations in many applied applications, in particular in scientific research. It uses Newton-Raphson iterations and a clever bit trick, also known as the magic constant method, for relatively fast and accurate calculation of the inverse square root initial value. Here, the initial approximation is obtained using only simple and fast arithmetic operations in integer and floating-point arithmetic, and the so-called magic constant is used to reduce the relative error. Our idea is to use simple modifications of this algorithm to calculate the reciprocal, division, inverse square root, and square root functions, minimizing the maximum relative error of calculations for floating-point numbers of different IEEE 754 data types. In this case, division can be obtained by calculating the reciprocal of the divisor and multiplying the result by the dividend. To get the square root function, you can multiply the result of calculating the inverse square root by the value of the argument. The advantage of the Newton-Raphson formulas for the reciprocal function and the inverse square root is the lack of a division operation and their fast convergence.

As far as we know, the first study of the theory of the FISR algorithm was done by Chris Lomont (Lomont, 2003), who defined an improved magic constant 0x5F375A86 for the classic algorithm. This algorithm provides nearly 18 bits of accuracy for two Newton-Raphson iterations in single precision (float). The analytical theory of the algorithm was also investigated by (Moroz, Walczyk, et al., 2018), and, as a result, an improved algorithm was

proposed in (Walczyk et al., 2018). Their algorithm uses another magic constant, 0x5F376908, and modified Newton-Raphson iterations. The accuracy of the algorithm is 20 bits for type float. The algorithm proposed by (Lemaitre et al., 2017) gives approximately the same accuracy. It uses Householder's method and Lomont's magic constant 0x5F375A86 for single precision, 0x5fe6eb50c7b537a9 from (Robertson, 2012) for double-precision numbers. Also, it is worth mentioning that in (Kadlec, 2010), a practical optimization method was used to search for such parameters of the algorithm that minimize the errors of the FISR for one iteration. In this case, single-precision numbers were considered. This method allowed to slightly increase the accuracy of the basic algorithm after the first iteration (up to 10.5 bits).

Similarly, algorithms for calculating the reciprocal and division using the magic constant and the Newton-Raphson method for numbers of type float were studied in (Moroz et al., 2015, 2016). The most accurate division algorithm from (Moroz et al., 2016), which uses the magic constant 0x7EB504F3 and the first modified iteration, has an accuracy of 23 bits after two iterations. On the other hand, Huang and Chen (2015) suggest using Goldschmidt's algorithm and modified magic constants (0x7EF4FB9D in single precision and 0x7FDE9F73AABB2400 in double precision) for initial approximation. This algorithm is faster but has worse accuracy. In particular, for accuracy of about 22 bits for type float, three iterations must be performed.

As you can see, there is still a need to develop accurate, fast, and universal algorithms for calculating these functions for both software and hardware implementations, which can be effectively used for any floating-point data type.

A presentation of any preliminary ideas, the proposed approach and achieved results

- My contribution and research plan

Our main recommendations for developing advanced algorithms: use the magic constant method or fast hardware instructions RCP and RSQRT (if available) for the initial approximation; to refine the results, use a combination of modified Newton-Raphson and/or Householder's methods of small orders; calculate Newton-Raphson and Householder's methods in a specific form (Schulte et al., 1997), especially at the last iteration (at the accuracy boundary), to reduce calculation error; if available, use fast hardware FMA instructions in calculations, especially at the last iteration, to reduce rounding errors; reduce the evaluation latency, reduce the number of multiplications; determine such values of the magic constant (integer) and other coefficients of the modified iterations (floating point) that minimize the maximum relative error of the algorithm (at the theoretical and practical level).

In accordance with the research plan, the following main tasks can be distinguished:

1. The choice of direction and research methods, setting goals and objectives. [Done]
2. Literature review. [In progress]
3. Justification of the relevance and novelty of the research. Definition of the main research questions. [In progress]
4. Research and analysis of existing methods for calculating elementary functions. [In progress]
5. Analysis of the features of floating-point arithmetic (IEEE 754 standard). [Done]
6. Studying the theory of the FISR algorithm and its generalization to calculate other functions (reciprocal, square root, inverse cube root, etc.): [Done]
    a. magic constant method;
    b. iterative methods (Newton-Raphson, Householder's, Goldschmidt's, and Heron's methods).
7. Development of research methodology:
    a. evaluation of absolute and relative errors, the accuracy of algorithms; [Done]
    b. measuring performance (latency and throughput) of algorithms; [Done]
    c. development of a mathematical model of algorithms; [Done]

   d. determination of the best uniform approximation for relative error (theoretical method); [In progress]
   e. method of numerical multidimensional optimization of the algorithm parameters, which minimizes the maximum relative error (practical method). [Done]
8. Design and research of advanced algorithms for calculating elementary functions:
   a. improved reciprocal algorithm for single- and double-precision numbers with modified coefficients; [Published in (Moroz, Samotyy, & Horyachyy, 2018)]
   b. a simple modification of the FISR algorithm for single-precision numbers (float); [Published in (Hrynchyshyn et al., 2018)]
   c. improved modified FISR-based algorithms for single- and double-precision numbers, using additional magic constant instead of a single multiplication; [In review]
   d. square root and inverse square root algorithms based on a modified second-order Householder's method (for float and double); [Published in (Moroz et al., 2019)]
   e. algorithms for calculating the inverse square root and square root for single and double precision using the method of switching magic constants; [In review]
   f. inverse square root algorithms based on fast hardware ARM RSQRT instructions (for float and double). [In progress]
9. Practical implementation of algorithms and their testing:
   a. in software on Intel i-7, Raspberry Pi (ARM Cortex A-53), ESP-WROOM-32 (Xtensa), STM32F4 (ARM Cortex M-4), etc.; [In progress]
   b. in software using SIMD instructions of AVX2 and NEON technologies; [To do]
   c. in hardware on Intel Cyclone 10 GX FPGA. [To do]
10. Practical application of the proposed algorithms on the example: matrix decomposition problem (Cholesky, QR-, and LU-decomposition). [To do]
11. Analysis of the results. Comparison of improved algorithms with standard methods. [In progress]
12. Writing a dissertation and its abstract. [To do]

- Applied research methodology

To determine the accuracy of the algorithms, we go over all possible values (for float) of the input argument from some interval and calculate the maximum error of the result. Further, using a mathematical formula, we evaluate the accuracy of the algorithm. To determine the performance, we measure the latency of the algorithms based on averaged results using the chrono library. The C++ programming language is used to implement algorithms and test them. For theoretical optimization of algorithms, a method similar to the Remez algorithm is mainly used. We can further refine the coefficients using a numerical method based on multidimensional optimization, brute-force search, and randomness function. More information on the research methodology used can be found in (Moroz, Samotyy, & Horyachyy, 2018).

- Achieved results and expectations

Our results show that the proposed algorithms have much better accuracy than the basic FISR algorithm and in some cases reduce the number of required iterations. The proposed algorithms are designed for microcontrollers supporting the floating-point computations but which do not have hardware-implemented FPUs for these functions. For microcontrollers, such as ESP-WROOM-32, and Raspberry Pi, they are also usually much faster than using sqrtf(x) function for single-precision numbers, although they do not provide correct rounding of the result. Our single-precision reciprocal function on ESP-WROOM-32 is also faster than the division operation. For double-precision numbers, the gain in performance is not always so obvious. The proposed methods work only with normalized floating-point numbers. For further research, we plan to implement our improved algorithms on FPGA and show their application for solving a real practical problem.

Bibliographic References

1. Coe, T. (1995). Inside the Pentium FDIV bug. *Dr. Dobb's Journal of Software Tools, 20*(4), 129-135.
2. Hrynchyshyn, A., Horyachyy, O., Tymoshenko, O., & Moroz, L. (2018). An Efficient Algorithm for Fast Inverse Square Root. In J. Rysiński, & S. Zawiślak (Eds.), *Processing, transmission and security of information, vol. 2* (pp. 105-114). Bielsko-Biała, Poland: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej.
3. Huang, K., & Chen, Y. (2015). Improving Performance of Floating Point Division on GPU and MIC. In *Proceedings of the 15th International Conference on Algorithms and Architectures for Parallel Processing* (pp. 691-703). Zhangjiajie, China: Springer, Cham. doi: 10.1007/978-3-319-27122-4_48
4. Id Software. (1999). Quake III Arena. https://github.com/id-Software/Quake-III-Arena/blob/master/code/game/q_math.c
5. Kadlec, J. (2010). Improving the fast inverse square root. http://rrrola.wz.cz/inv_sqrt.html
6. Lemaitre, F., Couturier, B., & Lacassagne, L. (2017). Cholesky factorization on SIMD multi-core architectures. *Journal of Systems Architecture, 79*, 1-15.
7. Lomont, C. (2003). Fast inverse square root. Technical report. http://www.lomont.org/Math/Papers/2003/InvSqrt.pdf
8. Moroz, L., & Hrynchyshyn, A. (2015). A fast calculation of function y=1/x with the use of magic constant. *Bulletin of Lviv Polytechnic National University: Automation, Measurement and Control*, *821*, 23-29 [in Ukrainian].
9. Moroz, L., Hrynchyshyn, A., & Miretska, Y. (2016). Simple floating point division algorithms. *Bulletin of Lviv Polytechnic National University: Automation, Measurement and Control*, *852*, 35-38 [in Ukrainian].
10. Moroz, L., Samotyy, V., & Horyachyy, O. (2018). An Effective Floating-Point Reciprocal. In *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)* (pp. 137-141). Lviv, Ukraine: IEEE. doi: 10.1109/IDAACS-SWS.2018.8525803
11. Moroz, L., Samotyy, V., Horyachyy, O., & Dzelendzyak, U. (2019) Algorithms for calculating the square root and inverse square root based on the second-order Householder's method. In *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1* (pp. 436-442). Metz, France: IEEE.
12. Moroz, L., Walczyk, C., Hrynchyshyn, A., Holimath, V., & Cieśliński, J. (2018). Fast calculation of inverse square root with the use of magic constant – analytical approach. *Applied Mathematics and Computation, 316*, 245-255.
13. Robertson, M. (2012). A brief history of invsqrt (Bachelor's thesis). University of New Brunswick, New Brunswick, Canada. https://cs.uwaterloo.ca/~m32rober/rsqrt.pdf
14. Schulte, M., Stine, J., & Wires, K. (1997). High-speed reciprocal approximations. *In Conference Record of the Thirty-First Asilomar Conference on Signals, Systems and Computers, vol. 2* (pp. 1183-1187). IEEE.
15. Walczyk, C., Moroz, L., & Cieśliński, J. (2018). Improving the accuracy of the fast inverse square root algorithm. *ArXiv preprint arXiv*, 1802.06302, 1-21.

Expectations and motivation to attend Doctoral Consortium

Participation in International Doctoral Consortium, is a great opportunity to gain new experience, improve my research skills and rethink my dissertation work thanks to valuable comments and feedback from senior researchers and other PhD students who work in a similar area of research. It will be helpful to get some suggestions and guidance on using research methods. I hope this discussion will help me to find some drawbacks and focus on those aspects of my research that need improvement. In addition, I would like to share my ideas with other participants, to hear different opinions and get acquainted with their research.

Inquiry-Based learning robotics

Patrik Klofáč
Year of my doctoral studies: 2
University of South Bohemia České Budějovice
Address Line 1
České Budějovice, Czech Republic, Jeronýmova 10, 371 15 České Budějovice
pklofac@pf.jcu.cz

What is inquiry-based learning - learning in the 20th century focused on reading, writing and arithmetic. In the 21st century, we have to focus more on building logical thinking at an early age, in which research plays a big role. The concept of research has a long history, one of the first definition of the term appears at the beginning of the 20th century. Since then it is included in many subjects, especially science and mathematics. These items have been long struggling with inadequate teaching methods. Also, a new approach to science should be based on learning theory, conceptual thinking and pedagogical principles and not on imitation, memorization and interaction with the computer. Response to this situation is very inquiry-based learning, teaching method, in which the use of the pupils' knowledge system generated asked questions and solutions to problems. In accordance with constructivist theories of learning is an active student, solve problems, gain experience and is led to the creation of models of cognitive phenomena observed. Active and creative position of the student in the classroom is crucial for successful learning. It is a necessary condition.

There are several kinds of division, sufficiently accurate in these four stages.

- confirmation inquiry - the question of procedure is provided to students, the results are known, the thing is to check their own practice
- structured inquiry -the teacher tells the question of a possible procedure; students formulate explanations based on the studied phenomenon
- guided inquiry - the teacher gives the research question, students create a methodology and implement it
- open Inquiry - students wonder rethinking process, conduct research and formulate results

In computer science lately, there is a trend developing informatics thinking. I can say that it is the ability to think like computer science to solve problems. Informatics to clarify whatever solves identifies the essential features of the problem systematically considering the available options and tools, looking for an effective procedure. Never mind that the situation should be a new beginning and confused, rather the contrary. Striving for efficiency leads to the fact that they often use a computer (because they know what a computer is able) and seek algorithmic solutions. Informatics is a thinking problem-solving process.

If we want children and their parents to take, it is necessary to use an area that is motivating, interesting and attractive. That means that requirement robotics, among other things, develops informatics thinking. Robotics is a field that deals with the study, design and programming of robots and similar devices. Robots can be found all around us, in all sectors and it is difficult to find an area where they do not enter. The application area is so wide that appeals to girls, boys and adults.

My Brief Biography

Education
Since October 2018 University of South Bohemia in České Budějovice
Faculty: Faculty of Pedagogy
Study programme: Specialization in Pedagogy (Doctoral Study)
Field of study: Information and Communication Technologies in Education

2016 - 2018 University of South Bohemia in České Budějovice
Faculty: Faculty of Pedagogy
Study programme: Elementary School Teaching (Master degree Study)
Field of study: Teaching Informatics and Physics for Elementary School

2013 - 2016 University of South Bohemia in České Budějovice
Faculty: Faculty of Pedagogy
Study programme: Specialization in Pedagogy (Bachelor Study)
Field of study: Information technology and e-learning

Employment history:

Since October 2018 - University of South Bohemia in České Budějovice, Faculty of Pedagogy
Position: Computer Science Teacher

Since September 2018 Elementary School Dobrá Voda u Českých Budějovic
Position: Teacher of Informatics and Physics

Properties and interests
I am friendly, accommodating, physically fit, reliable, happy to work with people and not afraid of new challenges. I'm interested in news from the world of informatics and physics for self-education. I watch and play football and I like to spend my free time with friends.

Publications

ŠIMANDL, V., KLOFÁČ, P. Využití Wi-Fi sítí na základních školách. In Journal of Technology and Information Education. 2017, 9(1), s. 213-222. ISSN 1803-537X. http://doi.org/10.5507/jtie.2017.017

Research area description

- My driving force is the concept of improving science education (informatics) in primary schools, because pupils in the future, will be need it. It is wrong to just repeat after the teacher. But students develop skills to solve problems. Lesh and Zavojewská, recognized experts reported that a highly developed ability to solve problematic situations facilitate the training, successful participation in society, and it is also necessary for many personal activities. Teachers of informatics often do not have sufficient approbation and this work would provide a new perspective on teaching science. It is proven that teachers are not competent enough to inquiry-based teaching and fear of failure if they would do something new.
- Main objectives: By what and how extent does IBL contribute to pupil´s development. Discover, clarify IBL in robotics.
- An outline of the current knowledge of the problem domain (What is the state-of-the-art in relation to existing solutions to the problem)

- In the current state of inquiry-based learning is used in science subjects such as biology, physics, mathematics etc., but not in informatics (robotics) or I have not found anything about it yet
- I'm still at the beginning, but I am looking for and creating IBL assignments in robotics, studying literature, making pupils familiar with robotic kits

A presentation of any preliminary ideas, the proposed approach and achieved results

- Currently I teach pupils in a classical way with robotic kits and make records about the course. Along with that I create the first IBL robotics tasks.
- Methods of exploration. The work will use qualitative research. My plan is to involve two primary schools, which will use about 20-30 pupils. Applying active observation of students and teachers and then I will lead them deep (structured, semi-structured) interviews. I'm thinking also about the method of design research, but for now I can not closer to her familiar, so I will do, I will decide whether I use it or not.

Bibliographic References

1. PAPÁČEK, Miroslav. Limity a šance zavádění badatelsky orientovaného vyučování přírodopisu a biologie v České republice. In: *Didaktika biologie v České republice 2010 a badatelsky orientované vyučování. DiBi 2010: sborník příspěvků semináře, 25. a 26. března 2010*. Editor Miroslav Papáček. Jihočeská univerzita v Českých Budějovicích, 2010, 165 s.
2. *Science Education in Europe: National Practices, Policies and Research.* Brussels: EuropeanCommission, 2011, 166 s. ISBN 978-92-9201-218-2.
3. STUCHLÍKOVÁ, Iva. O badatelsky orientovaném vyučování. In: *Didaktika biologie v České republice 2010 a badatelsky orientované vyučování. DiBi 2010: sborník příspěvků semináře, 25. a 26. března 2010*. Editor Miroslav Papáček. Jihočeská univerzita v Českých Budějovicích, 2010, 165 s. s. 129135. ISBN 978-80-7394-210-6.
4. TRNA, Josef. Taxonomy of Physics Experiments in Inquiry-Based Science Education. In: *WCPE-TheWord Conference on Physics Education*. 2012.
5. DOSTÁL, Jiří. (a) Experiment jako součást badatelsky orientované výuky. In *Trends in Education*. Olomouc: Univerzita Palackého v Olomouci, 2013, s. 9–19.
6. DOSTÁL, Jiří. (b) Badatelsky orientovaná výuka jako trend soudobého vzdělávání. *e-Pedagogium.*2013, č. 3, s. 81–93.
7. DOSTÁL, Jiří. (c). Experiment jako součást badatelsky orientované výuky. *Trends in Education*. 2013, č. 1, s. 9–19. ISSN 1805-8949.
8. *National Professional Standards for Teachers in Pakistan*. Islamabad: Policy and Planning Wing, Ministry of Education, Government of Pakistan, February 2009, 25 s. Dostupné z: http://unesco.org.pk/ education/teachereducation/files/National%20Professional%20 Standards%20for%20Teachers.pdf.
9. ZHANG, Baohui, Joseph S. KRAJCIK, Leeann M. SUTHERLAND, Lei WANG, Junming WU a Yangyi QIAN. Opportunities and cha- llenges of China?s inquiry-based education reform in middle and high schools: Perspectives of science teachers and teacher educators. *International Journal of Science and Mathematics Education*. 2005, roč. 1, č. 4, s. 477–503.

Expectations and motivation to attend Doctoral Consortium

I like meeting new people and places, so i expect a great, friendly team that will help me move my dissertation a little further.

A Reference Framework for Smart Learning Infrastructure in Computer Science Education

Maia Lust

Year of your doctoral studies: 1st year
Your Affiliation: Tallinn University School of Digital Technologies
Address Line 1: Peterburi tee 20-39
City, State, Postcode, Country: Tallinn, Harjumaa, 11411, Estonia
Email address: maia.lust@tlu.ee

In order to maintain the development potential of Estonian society in line with Smart Specialization Strategy and to meet the needs of the labour market, it is important to create conditions for each primary and secondary school student to learn not just basic digital skills, but also get acquainted with computing as a cross-disciplinary domain. The concept of Informatics (also known as computing or computer science) has developed significantly over the past 50 years. While natural sciences are defined with reference to the world in which we live, Informatics as a scientific discipline is harder to define; and it is far from just being a compilation of engineering principles and technology (Vahrenhold et al., 2017).

Vahrenhold et al., (2017) underline that the ambiguity of IT in education is a fundamental problem. Computer Science, Computing, Computational Thinking, Digital Literacy, Digital Skills, Informatics, Instructional Technology, and ICT. Harel, (1987) in his book "Algorithmics: The Spirit of Computing", describes the discipline as covering three complexities: computational complexity; behavioural complexity; cognitive complexity. Denning and Rosenbloom (2009) describe computing as a 4-th major area of science alongside the physical, life and social sciences.

The current national curriculum for Estonian schools does not include informatics as a subject based on academic discipline of computer science. This situation is about to change with the emergence of the new national curriculum for informatics on upper-secondary level (GINF) that has been developed by an expert group at HITSA and is already being piloted in ten Estonian schools. The GINF curriculum consists of two phases: 5 elective courses for 10th grade students and collaborative software development project in grade 11. Participation in the software development project requires that each participant has successfully passed 1-2 elective courses a year before, in accordance with their role in the project team (developer, analyst, tester, project manager) (HITSA, 2017). Due to the lack of qualified informatics teachers in Estonian schools, the elective courses and their online learning environment is designed to support self-directed and collaborative learning.

The existing prototypical online learning environment designed for GINF consists of three- layered components (HITSAa, 2017)

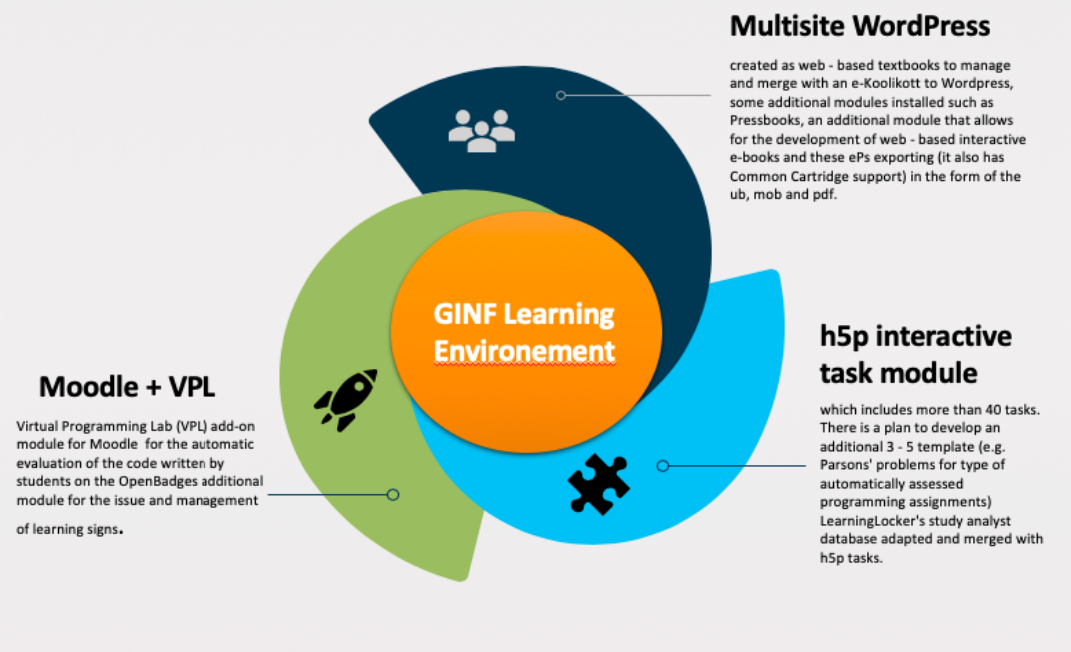

Figure 1. GINF infrastructure

To support schools in delivering GINF curriculum, the platform should be able to take over some of the functions of teachers such as guiding through learning materials, supporting students learning process by providing instant personalized feedback on completed tasks etc., leaving to teacher a role of coach or facilitator who guides students through collaborative problem-solving process. At the moment GINF platform includes a few elements of learning analytics support but there is missing a path for using collected data for instant improvements and guidance, also a bridge that connects collected data and predicts student learning outcomes and behaviour in concrete cases: completion of different tasks, reading additional information etc. In the future, the platform should enhance the support to innovative learning approaches such as personalised and collaborative learning or peer learning. Learning analytics and learner modeling should provide an overview of each and every student individual contribution to common work to ensure that learning outcomes listed in curriculum was obtained by all students. The similar aims of innovating the learning infrastructure for Computer Science Education (CSE) seem to resonate among CSE researches around the world. In 2017, a group of CSE researchers initiated a SPLICE research community with the ultimate goal to develop and disseminate infrastructure that facilitates three aspects of CSE research: (1) development and broader re-use of innovative learning content that is instrumented for rich data collection, (2) formats and tools for analysis of learner data, and (3) best practices to make large collections of learner data and associated analytics available to researchers in CSE, data science, or learning science (SPLICE, 2017). Recently the SPLICE community has been working on topics such as identifying learner communities in blended learning in CSE (Gitinabard et al., 2017); writing reusable code feedback at scale (Head et al., 2017); interactive exploratory learning analytics in CSE (Mahzoon et al., 2018). The efforts of SPLICE community for improvement of CSE learning infrastructure are also focusing on how to make learning environments more adaptive, supportive and smart by using contemporary methods

of learning such as problem-solving tasks, programming, collaborative work etc., and by making learner interface in learning environments for CSE more visual and responsive to learner level on knowledge.

Your Brief Biography

Education

21.08.2019–... Infosociety Technologies PhD studies
21.08.2015–14.06.2018 Educational Technology masters study
28.12.1999–07.01.2002 Estonian and Finno-Ugric linguistics
28.08.1995–18.06.1999 Teacher of Estonian language in Russian Speaking Schools

Institutions and positions

01.09.2012–... Tallinna Pae Upper Secondary School, Educational Technologist
01.09.2004–31.08.2012 Tallinn Mahtra Secondary School, Teacher
01.09.1999–31.08.2004 Kohtla- Järve Slaavi Upper Secondary School, Teacher
1997–31.08.1999 Ahtme Upper Secondary School, Teacher

Academic degrees

Maia Lust, Phd student, (sup) Mart Laanpere, A Reference Framework for Smart Learning Infrastructure in Computer Science Education, Tallinn University, School of Digital Technologies, Centre for Educational Technology.

Field of research

ETIS CLASSIFICATION: 4. Natural Sciences and Engineering; 4.6. Computer Sciences;
CERCS CLASSIFICATION: P170 Computer science, numerical analysis, systems, control

ETIS CLASSIFICATION: 4. Natural Sciences and Engineering; 4.6. Computer Sciences;
CERCS CLASSIFICATION: T120 Systems engineering, computer technology

Dissertations under supervision

Jelena Reisi, Master's student, (sup) Maia Lust; Mart Laanpere, Ida-Virumaa üldhariduskoolide võimalused süvendatud IT-õppe läbiviimiseks., Tallinn University, School of Digital Technologies.

Maria Brusnevskaja, Master's student, (sup) Maia Lust, Inglise keele ja Lego Education metodoloogia lõimitud õpiobjekt 3.-6. laste algoritmilise mõtlemise arengu toetamiseks. (English language and Lego Education methodology integration for algorithmic thinking development of children ages 3.-6.), Tallinn University, School of Digital Technologies.

Research area description

- The main problem you are trying to tackle and its relevance:

Research problem: How to model Pedagogy-driven design of smart learning infrastructure to support learner modelling and learning analytics in CSE.

Relevance: The current national curriculum for Estonian schools does not include informatics as a subject based on academic discipline of computer science. This situation is about to change with the emergence of the new national curriculum for informatics on upper-secondary level (GINF) that has been developed by an expert group at HITSA and is already being piloted in ten Estonian schools. The GINF curriculum consists of two phases:

5 elective courses for 10th grade students and collaborative software development project in grade 11. Participation in the software development project requires that each participant has successfully passed 1-2 elective courses a year before, in accordance with their role in the project team (developer, analyst, tester, project manager) (HITSA, 2017). Due to the lack of qualified informatics teachers in Estonian schools, the elective courses and their online learning environment is designed to support self-directed and collaborative learning.

The aim of research: To develop and validate empirically a reference framework for Smart Learning Infrastructure for Computing Education (SLICE)

- An outline of the current knowledge of the problem domain (What is the state-of-the-art in relation to existing solutions to the problem)

The term 'learning environment' expresses that learning is dependent on various environmental factors, which are created to various degrees by external factors. A learning environment is made up of an arrangement of teaching strategies and methods, learning materials, and media. The learning environment represents the current temporal, spatial, and social learning situation and also includes the relevant cultural context. The basis for concrete measures to create learning environments provides a fundamental concept for teaching and learning (Mandl & Reinmann-Rothmeier, 2001).

A variety of interpretations of the concept of learning environment can be found in the literature. In some of these, the focus is on the role of information and communication technology (ICT), as in the "innovative learning environment" (Kirschner, 2005), which should have the necessary technological, social and educational affordances to provide opportunities to learn. Similar is the "collaborative learning environment" which responds to societal trends by increasing the focus on open-ended problem-solving tasks via heterogeneous, distributed teams using Computer Supported Collaborative Learning (CSCL) technology (Beers et al, 2005). Some concepts are more encompassing, like "powerful learning environment" (Könings et al., 2005) that take the intended learning processes and learning goals into account (Zitter & Hoeve, 2012).

Problem-based learning is a widely used learning methodology in the field of technological disciplines, especially in distance education environments. In these environments, the most used tools, which provide learning scenarios, are remote and virtual laboratories. Additionally, recent developments in the field of smart embedded devices have allowed users to have a wide variety of physical objects (or "things") integrated into smaller and smaller units, to capture and control the environment by wireless communications (Tobarra et al., 2019).

Computer Science Education (CSEd) heavily uses online educational tools like Integrated Development Environments (IDEs), Learning Management Systems (LMS), eTextbooks, interactive programming environments, and other smart content. Learning technologies themselves offer promise in remediating these difficulties (Järvelä & Hadwin, 2013; Morris et al., 2010). The past two decades have witnessed an explosion of

computer supported collaborative learning (CSCL) technologies supporting shared knowledge construction and productive interactions (Resnick, Levine, & Teasley, 1991; Roschelle & Teasley, 1995) as well as individual and collective outcomes (Salomon, Perkins, & Globerson, 1991). While CSCL tools often target productive interaction or functional coordination in the aim of domain knowledge construction, their capacity to support regulation has been largely overlooked (Järvelä & Hadwin, 2013). During past few years several online learning environments and platforms were developed in order to enhance online and blended learning for CSE, such as for example ProTus (the programming tutoring system), which initially was developed to provide various interactive courses in learning complex problem-solving skills (Ivanović et al., 2012) ProTuS is an adaptive and learning platform that provides personalization and adaptation to support the learning process (Klašnja-Milicević et al., 2018) Teaching students to write code with good style is important but difficult: detailed feedback currently requires a teacher. To resolve this issue AutoStyle program was developed, a style tutor that scales, offers adaptive, real-time holistic style feedback and hints as students improve their code. (Wiese, 2017)

CS Education (CSEd) researchers increasingly make use of learning analytics (Hundhausen et al., 2017; Fernandez-Delgado et al., 2014;) However, students, instructors and researchers all face barriers that slow progress: Educational tools do not integrate well. Information about computer science learning process and outcome data generated by one system is not compatible with that from other systems. Computer science problem solving and learning (e.g., open-ended coding solutions to complex problems) is quite different from the type of data (e.g., discrete answers to questions or verbal responses) that current educational data mining focuses on. CSEd infrastructure should support broader re-use of innovative learning content that is instrumented for rich data collection, formats and tools for analysis of learner data, and development of best practices to make collections of learner data available to researchers. (SPLICE, 2018)

The distributed and flexible nature of the learning process in blended and online learning environments, has created various new challenges for teachers, as it becomes much harder to observe, control, and adjust the learning experiences (Vozniuk et al. 2013). However, this does not imply that the control should be reinstated back to the teachers. It just conveys the idea that learning is distributed; thus contemporary learning systems should create engaging and efficient learning experiences to empower self-regulation and support learners towards autonomous learning (Hwang 2014).

Smart learning is a form of technology-enhanced learning that not only supports information-transfer and control of resource use, but also actively provides the necessary learning guidance, supportive tools, and help-seeking behavior at the right time and in the right form (Hwang 2014).

Numerous methods and techniques have been proposed to increase the quality of teaching and tooffer more engaging learning experiences to students. According to (Vesin, et al., 2018) the most commonly used are: adaptation of the learning environment and teaching material, personalization, learning analytics, and open learning models.

Several educational platforms have already introduced learning analytics components and data-driven learning activities in their systems, creating more adaptive and personalized learning experiences (Mangaroska, Giannakos, 2018).

Learning analytics integrates the analysis of user interaction logs, learning resources, teaching goals, and also the activities of scholars from completely different sources, so as to enhance the creation of prognostic models, recommendations, and reflections (Santos et al. 2012) Numerous examples of visualized LA (e.g.dashboards) exist, that visualize the various aspects of the training method (Bodily et al., 2018) Examples embody learners' artifacts, time spent on tasks, social interaction, usage of resources, assignments and check results (Santos et al. 2012; Lin et al. 2016; Bull and Kay 2016; Charleer et al. 2016; Verbert et al. 2013). The authors suggested that data should be accessible to students (e.g., giving insight into the learning path to support reflection, peer comparison and self-regulated learning) and how to visualize it.

One of the basic requirements for implementing learning analytics in the Smart Learning Environment (that might be distributed between various platforms and services) is the need for standardising the way we describe the learner, his/her background, capacity, results, aims, social contexts etc in a machine-readable manner. This is where learner profiling standards will come into play, such as IEEE PAPI. The Public and Private Information (PAPI) for Learners is a standard that represents the learner information in six categories (Farrance, 2000): contact, relations, security, preference, performance, portfolio. There exist other, similar and competing standards for learner profiling. For instance, the Chinese E-Learning Technology Standards (CELTS-11) is a specification for Learner Model that includes seven categories (Wang, et al., 2012), where in comparison with PAPI the category of relations is divided to two: academic affiliation and social relationships. Robson and Barr (2013) identified five types of learner information to be included in the Learner Model that includes (in addition to PAPI categories) data on learner's affective and motivational dimension. Affective characteristics such as motivation, engagement, interest, joy, surprise, boredom and frustration have a huge impact on decision making, managing learning activities, timing, and reflection on learning (Sandanayake & Madurapperuma, 2013). A number of adaptive learning systems have incorporated an Affective Learner Model (Ghergulescu & Muntean, 2010, 2016).

Various researchers have been researching a common format for systematic representation of learner models, called Open Learner Models or OLMs (Barria-Pineda, Brusilovski, 2018; Conaty, et al., 2018; Guerra et al., 2018; Dmitrova, Brna 2016, Kump et al.,2012). These are standardised student models that allow users to access their content with varying levels of interactivity (Bull & Kay, 2016). Traditionally, OLMs have been designed for students as users of Intelligent Tutoring Systems (ITS), with two main purposes: one, pedagogical in nature, is to encourage effective learning skills such as self-assessment and reflection; the second is to improve model accuracy by enabling students to adjust the model's predictions or even its underlying representation when such are deemed inaccurate by the students. Clearly, even OLMs that are merely scrutable require having an underlying representation that is interpretable at some level, so that the model's assessment can be visualised

for and understood by its users. However, the more interactive the OLM, the more interpretable and explainable the underlying representations may need to be, because of the increased control that the user has over the access to the different aspects of the model.

- Advances beyond the state-of-the-art in terms of your specific contribution and research plan (A description of the Ph.D. project's contribution to the problem solution)

To sum up the discussion above, the goal of my PhD research is to conceptualise the Smart Learning Infrastructure for Computer Science education (SLICE), that facilitates:

- contemporary pedagogy (flipped, blended, collaborative, active learning, self-directed)
- design and presentation of CSE-specific learning resources and learning environment (both physical and virtual)
- personalised learning through Learning analytics and Learner Modeling.

A presentation of any preliminary ideas, the proposed approach and achieved results

- Current status of the research plan

By the end of the first year Literature review should be completed and also design research iteration I resulting with conference paper for ISSEP 2020

- A sketch of the applied research methodology (data collection and analyzing methods)

Research design

Research design will follow the design-based approach (McKenney and Reeves, 2004), a genre of research in which the iterative and rigorous development of solutions to complex educational problems provides the setting for scientific inquiry. The solutions that results from educational design research can be educational product, process, program or policy (ibid.). In my PhD research, the solution that will result from iterative design-based research is a reference framework for SLICE. According to van den Akker et al., (2006) design based research incorporates a cyclic (or iterative) approach of design, evaluation and revision of a solution. Then, the research typically consists of a constructive part that builds an artefact and a part that evaluates the designed artefact (March, Smith, 1995). My PhD research will start with the definition of basic design requirements for SLICE informed by literature review and participatory design that will engage both typical users and experts. Based on this assessment and the reviewed literature, a reference framework will be constructed and, eventually, validated empirically.

During **the first iteration,** the primary data collection will be conducted through 2-3 participatory design sessions engaging a sample of 6-8 persons. The purposive sampling is informed by personas the stereotypical user profiles of GINF platform. The design sessions focus on usage scenarios and various aspects of existing prototypes for Smart Learning Infrastructure for Computing Education (SLICE), resulting with a conceptual model of SLICE in a form of concept map and ontology. Additional (quantitative and qualitative) data will be collected from GINF

platform in form of learning outcomes, learning analytics data from GINF exercises, feedback questionnaire at the end of each GINF course.

The second iteration will focus on defining the design requirements reference framework for SLICE and implementing these requirements to improve the GINF platform. The learner modelling and learning analytics support will be added to the platform, to support the primary data collection. The secondary data will be collected through an online survey (the sample includes all students and teachers who participated in GINF that year) and also through interviews with teachers and experts.

The third iteration will be dedicated to the improvement and validation of the reference model. The primary data will be collected through focus group interviews using Nominal Group Technique (Gallagher et al, 1993). According to Delbecq & van de Ven (1971) NGT is a structured brainstorm procedure to facilitate effective group decision-making in research and evaluation. NGT protocol consists of five phases (Potter et al, 2004):

1. Introduction and explanation of the purpose and procedure of the meeting
2. Silent generation of ideas about SLICE framework
3. Sharing ideas about the requirements for and potential improvement of SLICE framework
4. Moderated group discussion: synthesizing collected ideas about SLICE framework
5. Voting and ranking: prioritizing collected thoughts and ideas about the requirements and improvement recommendations for SLICE framework trough voting and ranking processes

NGT session will result with the validation requirements for SLICE and recommendations for improvement. The purposive sample for the NGT will be based on the same personas as in the first iteration. The final validation will be conducted in a form of heuristic evaluation by the panel of experts.

Expectations and motivation to attend Doctoral Consortium

I would like to attend Doctoral Consortium in order to get to know practices from other students, supervisors, to get research related information and insights. To make contact to field research community. To get knoweledge about PhD studies and some thoughts about how to write dissertation. I'd like to finish my PhD studies during nominal time of studies, so i'm very motivated to get to know more about field of research in general.

Title: Adaptive Student Modeling in Intelligent Learning Environments

Davaasuren Nyamjav
Informatics Faculty, Eötvös Loránd University, Hungary
Lágymányosi ELTE Campus - Southern Block, Pázmány Péter stny. 1/C.,
Budapest, 1117, Hungary
Davaa.mgl@gmail.com

Research summary:

During history, the most advanced technologies of its time such as radio, TV, internet, computers, mobile device, and tablets were used in the educational sector to increase learning outcomes. In the field of Technology Enhanced Learning (TEL), the effectiveness of learning outcomes increased by using the Learning Management System (LMS) among the faculty of the Higher Education Institute (HEI). However, the LMS system has lacked adaptability and interactivity to learners' needs and measuring, analyzing, and reporting data on the learning process. The student modeling is to develop data-driven student modeling methods using data mining and machine learning techniques that accurately model and assess students learning process and individualize the learning path. The dataset of Open University, UK, 30 000 students and over 1 million learning activities, will be used for Leaning Analysis. Effectiveness and usability of the purposed student modeling in Intelligent Learning Environment will be studied, evaluated and concluded.

Brief Biography

I'm currently doctoral student in ELTE, Eötvös Loránd University. I enrolled the doctoral program September 2018. I'm a native Mongolian, and I have my bachelor degree in Math and Informatics at Mongolian National University of Education. From 2000 until 2004, I worked as teaching assistant in Mongolian National University.

I earned my master degree in Computer Science at Pacific States University in 2008 in Los Angeles, California, USA. I worked in The Holmangroup, behavioral health care company based in Los Angeles, as web and report developer between 2008 and 2014.

After returning to my home country, I worked as lecturer in Mongolian National University of Education for IT courses.

Research area description

The one of the main problems in the Intelligent Learning Management System is tracking student activities and personalizing the learing. Student modeling must include following features: adapting to the learner's state of knowledge, track their learning and problem-solving behaviors, and providing feedback when they are unable to progress in their learning and problem-solving tasks.

- The aim of research
    - The aim of the student modeling is to develop data-driven student modeling methods using data mining and machine learning techniques that accurately model and assess students learning process and individualize the learning path.

Expectations and motivation to attend Doctoral Consortium

The expectation from this doctoral consortium is networking with many people who had experiences in many research areas and who are doing research in the area of my research field. I hope I'll learn a lof from the doctoral dissertation and research study.

Teaching Algorithmic Programming Using Discovery Learning

László Nikházy

2nd year PhD student
Eötvös Loránd University, Faculty of Informatics
Pázmány Péter sétány 1/C
Budapest, 1117, Hungary
laszlo.nikhazy@gmail.com

Brief Biography

Starting from my childhood I enjoyed thinking about puzzles, brainteasers and later mathematics problems. During high school I was involved in a lot of extracurricular math talent education programs, in which I loved to participate. I also entered maths and computer programming contests, I had a lot of good results, but in computer programming there was nothing like the talent education in mathematics in Hungary. My parents being teachers, I was always interested in education.

At university I studied software engineering, but I also earned a degree as a teacher. I had plans to improve the situation of computer science education in Hungary. After university I worked as a software engineer at Google in Munich and NNG (navigation software) in Budapest.

About 3 years ago I left the industry and started focusing on education, first giving extra classes and private lessons to gifted teenagers. I became involved in the commitee of Hungarian national programming contests and now I am a coach of the Hungarian teams at some international competitions (CEOI, ACM, RMI, Innopolis Open, maybe IOI next year). I entered academia in September 2018 for a PhD program with the goal of establishing a talent education system for computer science, based on research, similar to what we have in mathematics in Hungary.

Studies

- 2018 – present PHD. COMPUTER SCIENCE EDUCATION
  Eötvös Loránd University (ELTE), Hungary
- 2010 – 2013 MSC. COMPUTER SCIENCE AND MATHEMATICS TEACHER
  Eötvös Loránd University (ELTE), Hungary
- 2010 – 2012 MSC. COMPUTER SCIENCE
  Budapest University of Technology and Economics (BME)
- 2006 – 2010 BSC. COMPUTER SCIENCE
  Budapest University of Technology and Economics (BME)

Work experience

- 2015 – 2016 SOFTWARE ENGINEER AT NNG, BUDAPEST
  Developing navigation software
- 2013 – 2015 SOFTWARE ENGINEER AT GOOGLE MUNICH
  Developing a planet-scale distributed file system
- 2014 – present TEACHING MATHEMATICS AT THE JOY OF THINKING FOUNDATION, HUNGARY
  Conducting math camps for talented teenagers

Interests

- Algorithms and data structures

- Programming contests (coaching for ACM, IOI, CEOI, Innopolis Open, Romanian Master, etc.)
- Teaching programming
- Sports, music, and travel ☺

Publications

- To be published: L. Nikházy: *A Problem-based Curriculum for Algorithmic Programming.* (CEJ-NeTREP (2020)
- L. Nikházy: *Algoritmusok tanítása problémaközpontú módszerrel.* (In Hungarian.) Tavaszi Szél Konferenciakötet (2019).
- L. Nikházy, G. Horváth, Á. Horváth, V. Müller: *Computer-Aided Detection of COPD Using Digital Chest Radiographs*. IFMBE Proceedings Volume 29. (2010)

Research area description

There is a unique system for mathematics talent education in Hungary, led by mathematician Lajos Pósa and his students. The core element of this system is the series of camps in which gifted pupils have the opportunity to explore mathematics with inquiry-based learning [1]. It is my goal to establish a similar initiative in the field of computer programming. There are a lot of excellent resources available online which promote learning algorithmic programming on an advanced level, for example Halim's book [2], and the massive problem base of past Codeforces contests [3]. However, to use them for our educational goals, we need to organize these materials and exercises in such a way that enables learning through series of problem solving. In this discovery learning scenario, we would like create situations in which there are students facing a problem, and they have already seen the key ideas leading to the desired algorithm, while solving different tasks previously.

Educational goals, discovery learning in computer science

As for the mathematics talent education program, Juhász [4] says "*children should be taught how to think, rather than making them learn theorems and formulas by heart or giving them ready-made methods to solve problems*". In accordance with this principle, our main focus is teaching algorithmic thinking and problem solving. Another important objective is to show the joy in thinking about interesting problems and creating working programs to solve them. With this, we would like to open up the world of competitive programming for the children.

The emphasis is not on competition, but these contests are aimed to test the algorithmic thinking and problem-solving skills of the participants with "nice" tasks. The community of qualified programmers are preparing the problems of these competitions and they make them so that other people would enjoy thinking on them. There is a certain beauty in problems that is hard to describe, and it is much celebrated within the community. This beauty can come from an interesting question, an elegant solution, application of a method in an unexpected situation, a nice idea, connection between different topics, etc. So, the world of competitive programming is partly self-serving, it provides fun for people doing it, very much like how Lajos Pósa describes the world of mathematics [5].

Computer programming is a bit different from math, though. There are a lot of standard algorithms and data structures that are almost ready-made methods that you have to customize, combine, and apply in numerous different scenarios. We try to teach them through series of problems, having the students discover them mostly on their own, if possible. However, we put more emphasis on the applications of these methods in different problems. Therefore, we consider our approach a problem-based pedagogy. The problems have similar dependencies and connections between each other as the ones in Pósa's mathematics camps. We create problem threads for the algorithms and data structures we teach, and try to connect them, thus forming

our own web of problems. Fortunately, the tasks at programming contests usually have some funny story to cover the underlying problem, so it is not obvious at first sight to which thread they belong.

According to Bibergall [6], guided discovery learning is characterized by convergent thinking. "*The educator devises a series of statements or questions that guide the learner step by step, making a series of discoveries that leads to a predetermined goal"*. In our math camps, the learner is guided through exercises which have strong interconnection under the surface. Katona and Szűcs [7] describe this as a web of problem threads, which is the most valuable resource of that initiative. I started developing such a problemset for my future computer science camps.

Achievements and plans

I wrote a paper about a suggested curriculum for a computer science talent education program, titled *A Problem-based Curriculum for Algorithmic Programming* [8], it will be published soon. The key to the success of this teaching method is an excellently engineered network of problems that guide students through discovering the world of algorithms and data structures. In this paper I attempt to design a network of problems selected specifically for discovery learning of algorithms and data structures from beginner to advanced level, targeted for secondary and high school talented students. This could serve as the curriculum for extra classes or camps conducted with the problem-based teaching method I describe.

I plan to conduct computer science camps starting next year, using the described guided discovery learning paradigm and problem-based learning. I am going to report about the planning and execution of these camps, furthermore attempt to measure their impact using structured feedback of students (questionnaires) and occasional tests of their progress.

Bibliographic References

1. J. Győri, P. Juhász: *An extra-curricular gifted support programme in Hungary for exceptional students in mathematics.* Teaching Gifted Learners in Stem Subjects. Routledge, London (2017) 89–106. DOI: 10.4324/9781315697147-7
2. S. Halim: *Competitive Programming 3.* Lulu Independent Publish (2013)
3. *Problemset, Codeforces*. (2019) https://codeforces.com/problemset
4. P. Juhász: *Hungary: Search for Mathematical Talent*. The De Morgan Journal. Vol 2(2) (2012) 47–52.
5. L. Pósa: *Matematika táboraim*. Természet Világa. Vol. 132, N°3. (In Hungarian.) http://www.termeszetvilaga.hu/tv2001/tv0103/posa.html
6. J. A. Bibergall: *Learning by discovery: Its relation to science teaching*. Educational Review. Vol. 18(3) (1966) 222–231. DOI: 10.1080/0013191660180307
7. D. Katona, G. Szűcs: *Pósa-Method and Cubic-Geometry – A Sample of a Problem Thread for Discovery Learning of Mathematics*. Differences in Pedagogical Theory and Practice. (2017) DOI: 10.18427/iri-2017-0079
8. L. Nikházy: *A Problem-based Curriculum for Algorithmic Programming.* To be published in the next issue Central-European Journal of New Technologies in Research, Education and Practice (CEJ-NeTREP). Author's version is available at this link.

Expectations and motivation to attend Doctoral Consortium

I would like to receive feedback about my research and my teaching methods, also get some ideas from fellow PhD students and professors. I hope to make new friends, build some valuable international connections. Last, but not least, I would like to meet Valentina, about whom I heard a lot from my colleagues. ☺

Honey Encryption applied to private data protection

Mariia Oliynyk

First year of doctoral studies
National University of Kyiv-Mohyla Academy
Faculty of computer sciences, 2 Skovorody vul., Kyiv 04070, Ukraine
m.oliynyk@ukma.edu.ua

One of the areas of applied mathematics is research related to information security, namely the mathematical component of information security - cryptography. In addition to the mathematical bases on which cryptosystem designs are based, cryptography also uses mathematical arguments to evaluate the stability of cryptographic schemes, introduces mathematical formalization of certain cryptographic protocols, mathematical substantiation of the correctness of cryptographic schemes. I plan to dedicate my dissertation to mathematical research and their application in cryptography.
The stability of cryptosystems depends on a large extent on the security of protection of the secret keys used in them. In particular, the key generation procedure should give a variety of keys so that they cannot be picked up by a brute-force attack.

The concept of honey encryption was introduced in 2014 by Ari Juels and Thomas Ristenpart [1]. Honey encryption is used as an additional barrier to protect secret keys of cryptosystems, credit card numbers, passwords (quite often, users choose weak passwords) against a brute-force attack. The idea of honey encryption turned out to be successful and has been researched by many authors [2-5]. It is that by accidentally selecting a password and the key generated, an attacker can recover a message that looks plausible but is unlikely to match the original message. Thus, the attacker "sticks" to the false data (hence the name of the scheme) and this significantly slows down the attack of a complete search.

Different honey encryption schemes are considered depending on what additional protection is intended for. The need for additional protection of secret keys arises in remote access systems, when providing access to information to authorized users.

The syntax and semantics of honey encryption are similar to symmetric cryptosystems. The encryption algorithm that generates ciphertext with a key and plaintext is random. Decryption recovers plaintext from crypto text. The difference from the usual symmetric cryptosystem is how honey encryption behaves during decryption, when someone tries to decrypt ciphertext using the wrong key. Instead of making some noise or error, the decryption will produce plain text that looks plausible.

Today, there is a well-known honey encryption scheme for additional security of RSA cryptos [1], which, as shown in my thesis, can easily be transferred to the Rabin cryptosystem. Today, however, there are no honey encryption schemes for other, most commonly used cryptosystems on elliptic curves.

In my dissertation, I plan to consider the following tasks related to honey encryption:

1) Construction of a honey encryption scheme for the digital signature of the Schnor signature.
2) Construction of honey encryption scheme for cryptosystems on elliptic curves.
3) Construction of a honey encryption scheme for the digital signature of the Schnor signature on elliptic curves.

For all these tasks it is planned to build an algorithm, prove the correctness of the algorithm and conduct a study on the reliability of the introduced schemes.

Another topical area of research in cryptography is its use in machine learning. Machine learning uses lots of data, the so-called datasets, that often contain personal information. In this context, the task of depersonalizing such data arises in such a way as to preserve the privacy of the party who owns the data and, on the other, to confirm that the data is real. For this mathematical schemes, which are called proof without disclosure, are using. It is planned to explore the existing schemes and find their usage in problems that use machine learning.

Biography
Education

National University of Kyiv-Mohyla Academy
2019 –
PhD student, Kyiv-Mohyla Academy Doctoral School

National University of Kyiv-Mohyla Academy
2017 – 2019
Master of Applied Mathematics, Faculty of Computer Sciences, Graduate (2019)

Taras Shevchenko National University of Kyiv
2013 - 2017
Bachelor, Department of Mechanics and Mathematics, Graduate (2017)

Professional Experience

National University of Kyiv-Mohyla Academy 2019 –
Instructor
Wine Bureau 2018 - 2019
Junior analyst: sales analysis; sales forecast

Extracurricular and Volunteer Experience

- Participated in 8th All-Ukrainian Scientific Conference for young mathematicians and physicists (2019)
- Assisted in All-Ukrainian Olympiad in mathematics (2014)
- Assisted in International Conference dedicated to the centenary of Professor L.A. Kaluzhnin (2014)
- Have helped other students by explaining the material after classes in case they had not understood something during a lecture

Research Experience

- Abstract: *Honey Encryption applied to Rabin cryptosystem*
  2017
  11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 3--7, 2017
- Paper preparation on: *Honey Encryption applied to private data protection*

Interests: Mathematical methods of cryptography, Honey encryption, Algorithms

Research area description

- The main problem of my research is the need for additional protection of private data.
- The aim of research is to create an additional barrier to protect secret keys of cryptosystems.
- Currently only basic approaches to protect privacy are developed. They include encryption, authentication and access control.
- The target of my PhD research is twofold: the first direction is to construct an additional protection to secret cryptographic keys; the second direction is to apply additional capabilities to ciphertext in order to process data in encrypted form without decryption.

A presentation of any preliminary ideas, the proposed approach and achieved results

- In order to protect cryptographic keys different methods of honey encryption will be applied
- In order to process data in encrypted form without decryption homomorphic encryption will be aplied

Bibliographic References

1. Ari Juels, Thomas Ristenpart. Honey Encryption: Security Beyond the Brute-Force Bound. In: Nguyen P.Q., Oswald E. (eds) Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science, vol 8441. Springer, Berlin, Heidelberg
2. Joo-Im Kim, Ji Won Yoon. Honey chatting: a novel instant messanging system robust to eavedropping over communication. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)
3. Joseph Jaeger, Thomas Ristenpart, Qiang Tang. Honey Encryption Beyond Recovery Security. Advances in Cryptology – EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I (pp.758-788)
4. Ji Won Yoon, Hyoungshick Kim, Hyun-Ju Jo, Hyelim Lee, Kwangsu Lee. Visual Honey encryption: Application to Steganography. In IH and MMSec 2015 - Proceedings of the 2015 ACM Workshop on Information Hiding and Multimedia Security (pp. 65-74).
5. Marc Beunardeau, Houda Ferradi, Remi Geraud, Gavid Naccache. Honey encryption for language. Cryptology ePrint Archive: Report 2017/031

Expectations and motivation to attend Doctoral Consortium

As a PhD-student I am actively looking for mathematical conferences as International Doctoral Consortium on Informatics and Informatics Engineering Education Research is.

I think that math knowledge is necessary for any research, therefore, I chose it as my major. At the same time, I always loved to apply my theoretical expertise in practical problems, so I become interested in Cryptography. The main purpose of my research is to explore algebraic and statistical methods of private data protection.

For the last two years I have participated in such conferences as 8th All-Ukrainian Scientific Conference for young mathematicians and physicists and 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko. It was an outstanding experience for me, but it would be much more interesting and helpful to attend an international event where there is possibility to communicate with another doctoral student in my particular field and exchange experience about our research problems.

The mobility program gives a possibility to study and compare educational methods and lecture topics in different universities. It is a great opportunity to share my work with students in a similar situation.

Algorithmic properties of Sylow 2-subgroups of alternating and symmetric groups.

Vita Olshevska

The 3-d year of study at PhD program.
National University of Kyiv-Mohyla Academy
2 Skovorody st.
Kyiv, 04070, Ukraine
Email address: v.olshevska@ukma.edu.ua

Biography

Education:

- 2017-present – Assistant, Department of Mathematics, National University of Kyiv-Mohyla Academy.
- 2019 (06.24-28) – Simons Semester Geometric and Analytic Group Theory. Rigidity. Warsaw, Poland.
- 2017-present – PhD- degree, National University of Kyiv-Mohyla Academy, Faculty of Informatics, Department of Mathematics.
- 2015-2017 – Master's Degree, Taras Shevchenko National University of Kyiv, Faculty of Mechanics and Mathematics, the Department of Algebra.
- 2011-2015 – Bachelor degree, Taras Shevchenko National University of Kyiv, Faculty of Mechanics and Mathematics, the Department of Algebra.
- 2008-2011 – Ukrainian Physics and Mathematics Lyceum of Taras Shevchenko National University of Kyiv.

Publications:

- 2018 – Article «Algorithm for calculation in Sylow 2-subgroups of alternating groups using the computer algebra system GAP» (Journal of National University of Kyiv-Mohyla Academy, p.30-34).
- Abstracts:
    - 2018 – «Representations of permutations by rooted trees»
      (International conference on modern problems of mechanics and mathematics).
    - 2017 – «Algorithms for computations in Sylow 2-subgroups of symmetric and alternating groups»
      (11^{th} International Algebraic Conference in Ukraine dedicated to the 75^{th} anniversary of V.V. Kirichenko).
    - 2017 – «Using GAP for calculation in Sylow 2-subgroups of the alternating groups»
      (XV National Scientific-Practical Conference «Theoretical and practical problems of physics, mathematics and computer science»).
    - 2017 – «Commutators of Sylow 2-subgroups of the alternating groups»
      (VI National conference of young scientists in mathematics and physics).
    - 2017 – «Sylow 2-subgroups of the alternating group A8»
      (XV International Scientific-Practical Conference «Shevchenkivska Vesna 2017»).
    - 2016 – «Systems of generators of Sylow 2-subgroups of the alternating groups»
      (International mathematical conference «Groups and Actions: Geometry and Dynamics», dedicated to the memory of professor Vitaly Sushchanskyy).

Interests:

- Computer Algebra

- Computational complexity theory
- Graph Theory
- Group Theory
- Mathematical logic
- Programming languages: GAP, Sage, C++, MatLab, LaTeX.

Research area description

- *The main problem you are trying to tackle and its relevance*
  The term Sylow 2-subgroup of symmetric group refers to a group that occurs as the Sylow 2-subgroup of a symmetric group on finite set, i.e., a symmetric group on a set of finite size. Previously, this concept was described by Leo Kaluzhnin [1]. He presented the elements of these groups as a table, i.e. the ordered sets of polynomials of a certain form. Such groups and their generalizations have been widely studied by many authors (V. Sushchanskii, Yu. Dmytruk, A. Slupik and other mathematicians) [2-4]. However, the Sylow 2-subgroups of alternating groups are still largely out of sight. The case $p = 2$ is unique when the Sylow p-subgroup of the alternating group is the proper subgroup of the corresponding symmetric. That is why its structure and properties require a separate study. The basic step, that provides my research, is the representation of group elements in the form of marked binary rooted trees.
- *The aim of research is:*
  - To study representation of Sylow 2-subgroups of alternating and symmetric groups by binary rooted trees;
  - to study new connection between graphs and groups;
  - to build algorithms for calculations in Sylow 2-subgroups of permutation groups;
  - to investigate the algorithmic properties of the group Sylow 2-subgroups of permutation groups;
- *An outline of the current knowledge of the problem domain (What is the state-of-the-art in relation to existing solutions to the problem)*
  In paper [2] Yu. Dmitruk and V.Sushchanskii describe the structure of the Sylow 2-subgroups Q_n of the alternating groups A_n of arbitrary degree by using the tableau representation of such groups for $n = 2^k, k > 1$. This concept was described by Leo Kaluzhnin [1]. In addition, the normalizers of a Sylow p-subgroup of the symmetric group S_n in S_n and of the subgroup Q_n in S_n and A_n are characterized in terms of tableau representations. The method of tableau representations gives a unified approach to the description of the normalizers in all these cases.
- *Advances beyond the state-of-the-art in terms of your specific contribution and research plan (A description of the Ph.D. project's contribution to the problem solution)*
  Areas of research that establish new connections between mathematical objects have always been and will be interesting for Mathematics. In my research, I build representations of Sylow p-subgroups of alternating groups by binary rooted trees, create an algorithm of the corresponding representation, prove its correctness and evaluate its complexity.

A presentation of any preliminary ideas, the proposed approach and achieved results

- *Current status of the research plan.*
  Currently the following results have been obtained:
  - Presentation of elements of the group $Syl_2(A_{2^n})$ using marked binary rooted trees $T_{2,n}$.
  - An example of an irreducible system of generators for groups of this type.
  - Commutator for partial cases A_8 andA_{16}. This result allowed to check whether the proposed system of generators irreducible and minimal in these cases.

- The algorithm and its implementation for the computer algebra system GAP. The main task of the program is to check whether some set S can be a system of generators. In addition, this program finds the commutator and the factor group of these groups and checks whether it Abelian.
- Basic calculation algorithms using binary rooted trees and binary strings:
  - an algorithm for constructing permutations from binary string;
  - an algorithm for constructing binary string from permutations;
  - permutation parity check algorithm;
  - algorithm for finding the inverted tree;
  - algorithm of multiplication of two trees.

  All algorithms are unified and can be applied in the case of a symmetric group.
  In addition, it was successfully programmed in the C ++ programming language.
- Separately, the set of marked binary rooted trees were investigated as a group. All the necessary algorithms are built regardless of the permutation properties. The correctness of the necessity of such a group is described.
- An isomorphism between Sylow 2-subgroups of alternating (and symmetric) groups and a group of marked binary rooted trees is established.

- *Methods and tools:*
  - The methods of combinatorial group theory, graph theory, algorithm theory and discrete mathematics are applied.
  - The computer algebra system GAP and the programming language C ++ are used for the calculations.
- *Expected achievements and possible evaluation metrics to establish the level of success of your results.*
  I have to write three math articles for successful graduate PhD degree. At least one of them should be in the journal, which is included in the scientific databases of Scopus or Web of Science. Also I have to produce a text for the dissertation.

Bibliographic References

1. L. A. Kaluzhnin. Selected Chapters of Group Theory (Калужнин Л. А. Избранные главы теории групп). / L. A. Kaluzhnin. // Kyiv: Taras Shevchenko National University of Kyiv. – 1979. — P. 52.
2. Yu. V. Dmitruk and V. I. Sushchanskii. Structure of Sylow 2-subgroups of the alternating groups and normalizers of Sylow subgroups in the symmetric and alternating groups. / Yu. V. Dmitruk and V. I. Sushchanskii// Ukrainian Mathematical Journal 33 (1981), no. 3, P. 235-241.
3. Bartlomiej P. The action of sylow 2-subgroups of symmetric groups on the set of bases and the problem of isomorphism of their cayley graphs / P. Bartlomiej, V. I. Sushchansky // Algebra and Descrete Mathematics. — 2016. — Vol. 21, no. 2. — P. 264–281.
4. Slupik A. J. Minimal generating set and cayley graphs of sylow p-subgroups of finite symmetric groups / A. J. Slupik, V. I. Sushchansky // Algebra and Discrete Mathematics. — 2009. — No. 4. — P. 167–184.

Expectations and motivation to attend Doctoral Consortium

Participation in such program allows me to fix my research at current stage, find related areas to my topic and get an independent, comprehensive evaluation from colleagues. Potentially, I hope to meet scientists who are working in the same direction. Moreover, I can get new ideas from other speakers and their research. Finally, it will bring me great experience as a researcher and as a participant in such events.

Modeling of surface plasmon polariton (SPP) waves propagation in multilayered structures.

Vitalii Polovyi

Third year of PhD
Lviv Polytechnic National University
Mytropolyta Andreia, 5, room 213,
Lviv, 79016, Ukraine
vitalii.y.polovyi@lpnu.ua

Biography

Received bachelor's degree in Applied Mathematics in July 2015 and master's degree in Applied Mathematics in May 2017 both from Lviv Polytechnic National University. From September 2017 a PhD student in Applied Mathematics, Lviv Polytechnic National University (expected 2021).

My bachelor's thesis concerned a problem of Lithium atom movement through porous media (material with many little voids). The aim was to study how voids walls affect the electron on the second orbital that is less tightly bound to an atom nucleus than the electron on the first orbital and to understand if walls can influence this electron in a way that it will leave the atom. For my master's thesis and later PhD study, my supervisor and I decided to change the subject of study to surface plasmon polaritons (SPPs) propagation [1] in a stratified media (especially dielectric/metal/dielectric structures). Here we want to make a mathematical model that will not only take into account thickness of a metal layer but also the Coulomb interaction [2], electroneutrality condition [2], electrons density fluctuations [3] etc. at a dielectric/metal interface. The final goal is to calculate how all these effects will change the behaviour of SPPs frequency spectrum and propagation length.

Selected publications and conferences proceedings on my research subject:

- Kostrobij P. P., Pavlysh V. A., Nevinskyi D. V., Polovyi V. Y. (2018). SPP waves in "dielectric–metal–dielectric" structures: influence of exchange correlations, *Math. Model. Comput.* Vol. 5, No. 2, pp. 184-192. doi: 10.23939/mmc2019.01.109.
- Kostrobij P. P., Polovyi V. Y. (2019). Influence of the thickness of a metal nanofilm on the spectrum of surface plasmons, *15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*. doi: 10.1109/CADSM.2019.8779260.
- Kostrobij P. P., Polovyi V. Y. (2019). Surface plasmon polaritons in dielectric/metal/dielectric structures: metal layer thickness influence, *Math. Model. Comput.* Vol. 6, No. 1, pp. 109-115. doi: 10.23939/mmc2019.01.109.
- Kostrobij P. P., Polovyi V. Y. (2019). The behaviour of the surface plasmon spectrum in heterogeneous structures depending on the thickness of the metal layer, *Nanotechnology and nanomaterials (NANO-2019): international research and practice conference*, 27–30 August 2019, Lviv, Ukraine: book of abstracts. p. 533.

Research area description

The main problem is to choose what effects (for example spacial and frequency dispersion or Coulomb interaction) that occurring at a dielectric/metal interface are the most relevant and have the greatest impact on the characteristics of SPPs waves. In the same time the correct identification is only one part

of the work because we should describe these effects in a way that will allow us to solve Maxwell's equations and to obtain from them analytical expression for dispersion relation. Most models that exists now either neglecting the spatial properties of the system [1] or provide mostly experimental data with just a little theory [3] or taking into account just some of effects [4, 5].

Currently one of the most widely used model is Drude model of electrical conduction [1] which reseanobly well describing SPPs behaviour for relatively thick metal layers for which spatial dispersion and quantum sized effects can be neglected. Skjørlstrup, Søndergaard and lately Pedersen [3,6] proposed a model that describes the so called quantum spill-out effects using Density-Functional Theory (DFT) but their model of dielectric permittivity tensor/function still using of Drude model. Another model is Random Phase Approximation (RPA) [7] that describing the weak screened Coulomb interaction in the same time RPA cannot accurately describe the plasmon dispersion because of the assumption of the infnite relaxationtime of electrons and the effect of many-body interactions.

For now, we have succeeded in the following tasks:

- applied a model of 2D electron gas in a rectangular asymmetric potential well of a finite depth for describing a dielectric permittivity tensor [8].
- calculated SPPs frequency spectrum taking into account the spatial dispersion [1].
- studied how the electroneutrality condition and oscillation of the Fermi wave vector influence SPPs frequency spectrum.

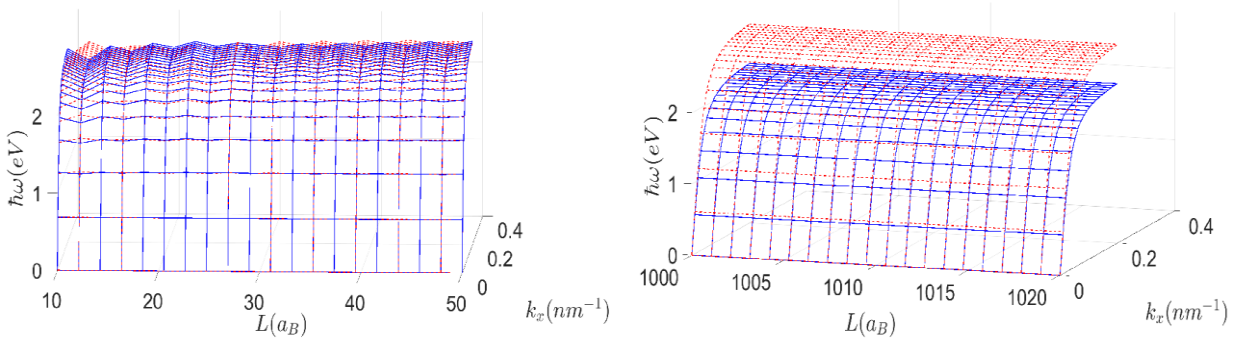

Figure 1. Influence of the electroneutrality condition on SPPs frequency spectrum (blue lines) for Vacuum/Ag/Al_2O_3 structure. On the left chart compared with similar model but without taking into account the electroneutrality condition; on the right chart with Drude model (both red lines).

In the nearest feature we want calculate the influence of Coloumb interaction on the chemical potential [2] or in other words the Fermi wave vector. After that, we want to apply DFT to calculating electron density in dielectric permittivity tensor [8].

In order to verify obtained results we compared them with experimental data [4,5] (see the second publication). Unfortunately often in articles not all the necessary paraments of used materials are present so most of the time we can only speak about a rough similarity of a simulation and an experimental model.

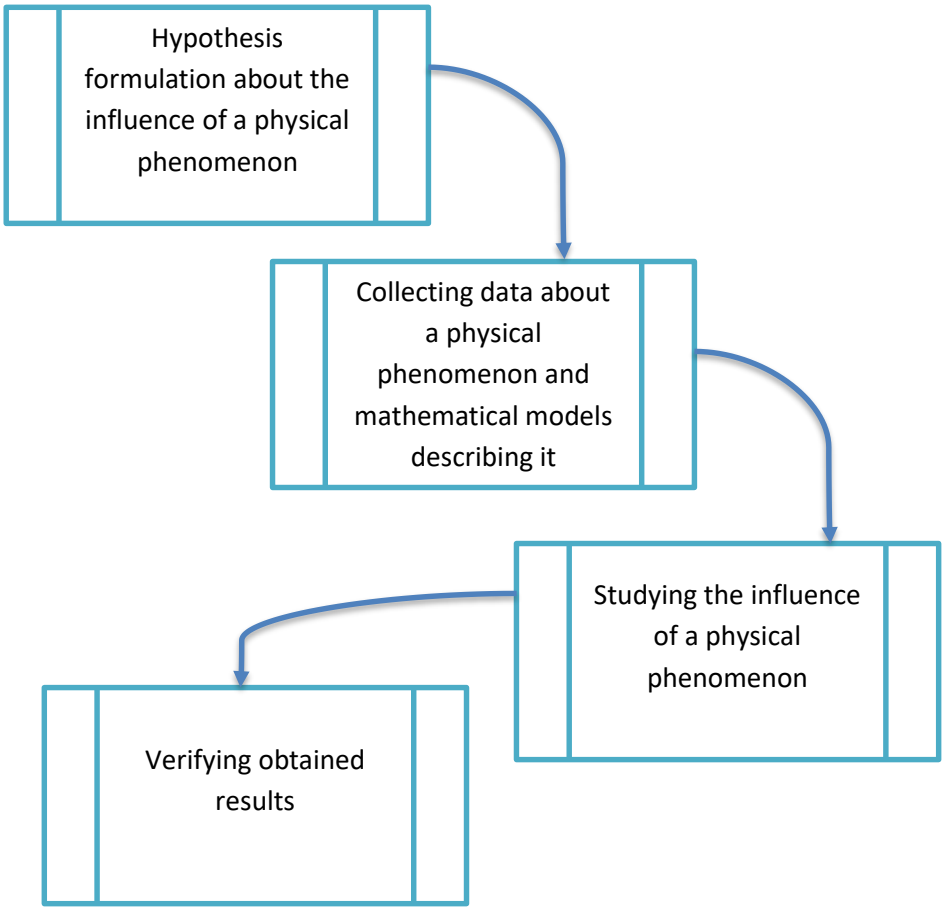

Figure 2. Research methodology.

Bibliographic References

1. Maier S. A. (2007). Plasmonics: Fundamentals and Application. *Springer - Verlag*.
2. Kostrobij, Petro. & Markovych, Bogdan. (2017). Effect of Coulomb interaction on chemical potential of metal film. *Philosophical Magazine*. doi: 10.1080/14786435.2018.1459056.
3. Enok J. H. Skjølstrup, Thomas Søndergaard, Thomas G. Pedersen (2019). Quantum spill-out in nanometer-thin gold slabs: Effect on plasmon mode index and plasmonic absorption, *Phys. Rev. B* 99, 155427. doi: 10.1103/PhysRevB.99.155427
4. M. Abd El-Fattah, Zakaria & Mkhitaryan, Vahagn Brede, et al. (2019). Plasmonics in atomically-thin crystalline silver films, *ACS Nano* 2019 13 (7), 7771-7779. doi: 10.1021/acsnano.9b01651.
5. A. Rodriguez Echarri, Joel D. Cox, F. Javier Garcia de Abajo (2019). Quantum Effects in the Acoustic Plasmons of Atomically-Thin Heterostructures, *Optica, Vol.* 6, Iss. 5, p. 798. doi: 10.1364/OPTICA.6.000630.
6. Alireza Taghizadeh, Thomas G. Pedersen. (2019). Plasmons in ultra-thin gold slabs with quantum spill-out: Fourier modal method, perturbative approach, and analytical model. *arXiv:1910.09220*.
7. M.V.Vavrukh, S.B.Slobodyan. (2019). Electron-plasmon model in the electron liquid theory, Condensed Matter Physics, 2005, Vol. 8, No. 3(43), pp. 453–472. doi: 10.5488/CMP.8.3.453.
8. V. P. Kurbatsky. (2017). Dielectric tensor of low-dimensional metal systems. *J. Exp. Theor. Phys*. 125 (1), 148–158. doi: 10.1134/S1063776117060012.

I believe that the presentation of my research for PhD students from other institutions and countries many of which will be new to my topic will arise many interesting questions I did not encounter before and also it will give me a great opportunity to discuss the way I described the mathematical model of the specific physical process and, probably, to detect some problems I might overlook.

Mathematical modeling and software development of medical data processing systems using fractal operators.

Ivan Sokolovskyy

2-nd year of my doctoral studies
Lviv Polytechnic National University
12 Stepan Bandera street
Lviv, Lviv, 79013, Ukraine
coffice@lpnu.ua

Your Brief Biography
Including information about your studies:

From 2018 till now – postgraduate of the Artificial Intelligent Systems Department, Institute of Computer Science and Information Technologies, Lviv Polytechnic National University;

2016 - 2018 – Full Higher education, Master of of Applied Mathematics, Ivan Franko National University of Lviv (together with double degree program – Intermaths - between University of Lviv and University of L'Aquila (Italy)).

2012 - 2016 – Basic Higher education, Bachelor of of Applied Mathematics, Ivan Franko National University of Lviv.

Interests: Programming, sport and travelling.

Publications: Below in Bibliographic References.

Research area description

- The main problem you are trying to tackle and its relevance: Construction of mathematical models and software for processing of medical data using fractal operators;
- The aim of research: developing of statistical methods and programming tools for processing medical data using fractal operators; analysis of mathematical models of medical data processing; development of statistical algorithms for parallel implementation of mathematical models and validation of results; construction of models of non-stationary fractal series for medical data analysis;
- An outline of the current knowledge of the problem domain (What is the state-of-the-art in relation to existing solutions to the problem): the modern approach for solving the declared scientifically applied problem is using of fractal analysis methods and apparatus of integro-differentiation on the basis of fractional order derivatives, this expand the implementation of mathematical models and methods for processing medical data;
- Advances beyond the state-of-the-art in terms of your specific contribution and research plan (A description of the Ph.D. project's contribution to the problem solution): using of fractal analysis methods and fractional-order intero-differentiation apparatus will allow to develop new methods for statistical analysis of non-stationary time series and estimation of model parameters for medical data processing.

A presentation of any preliminary ideas, the proposed approach and achieved results

- Current status of the research plan: there are investigated the processes of heat transfer in complex anisotropic media with a fractal structure which are characterized by non-locality in time (memory

effect) and non-locality by coordinate (the effect of spatial correlations). The explicit and implicit difference schemes for a nonlocal heat transfer equation using a fractional differentiation apparatus in coordinate in the sense of Riesz are developed. The difference approximations of the fractional derivative in the time interval is obtained on the basis of the Riemann-Liouville formula. The algorithmic aspects are presented for realization of the obtained difference equations using the predictor-correction method. The influence of different values of fractional parameters on the processes of heat transfer, depending on the change of coordinates and time, is investigated for given initial conditions and thermophysical characteristics of anisotropic fractal medium.

- A sketch of the applied research methodology (data collection and analyzing methods): necessary data will be taken from medical institutions; open data from google analytic will be used; statistical methods analyzing of time series; methods of integro-differential of fractional order; methods of theory of random processes;
- Expected achievements and possible evaluation metrics to establish the level of success of your results : mathematical model of non-stationary fractal series for processing medical data; modification of method of statistical tests for identification of parameters of model; numerical algorithms of fractional order for realization mothod of statistical tests; to establish the level of success of the research, it will be tested on the basis of real medical data; established statistical estimates should confirm the practical significance of the studied regalarities.

Bibliographic References

1. Ivan Sokolovskyy, Maryana Levkovych, Olha Mokrytska. Numerical Modeling and Analysis of Physical Properties in Biomaterials with Fractal Structure. // CEUR Workshop Proceedings 2255. p. 180-192.
2. Ivan Sokolovskyy, Natalia Shakhovska. Numerical Modeling of Thermophysical Processes in the Media with Fractal Structure. // 2019 9th International Conference on Advanced Computer Information Technologies (ACIT' 2019). SCOPUS.
3. Ivan Sokolovskyy, Natalia Shakhovska. Statistical Modeling of Diffusion Processes with a Fractal Structure. // CEUR Workshop Proceedings 2488. p. 145-154.
4. Ivan Sokolovskyy. Mathematical models of visco-elastic deformation in environments with fractal structure. // Master thesis: Ivan Franko National University of Lviv (Ukraine) and University of L'Aquila (Italy) 2018. 73 pages.

Expectations and motivation to attend Doctoral Consortium

The main expectations and motivation to attend Doctoral Consortium are:

- presentation and discussing about results of mine scientific research;
- to get acquaintance with colleagues from another countries and discussing about their results of researches;
- to make better knowledge and skills in spoken English;
- to get acquainted with history and culture Lithuania.

Modeling of system for interactive tasks development

Tomas Šiaulys

First year doctoral studies
Vilnius University, Institute of Data Science and Digital Technologies
Vilnius, Lithuania
siaulys.tomas@gmail.com

Brief Biography

I have a masters in Mathematics and a qualification for teaching mathematics and informatics. For the last 8 years I have been teaching in different schools in Vilnius - Vilnius Lyceum, IB Diploma programme, Waldorf-Steiner school, Vilnius Jesuit Gymnasium - all focusing on different pedagogical approaches. I'm interested in different philosophies in education, especially computer science and mathematics. For my doctoral studies, though, I would like to focus more on practical tools for learning.

Research area description

The main problem addressed is that the systems for creating interactive exercises are usually either too complex or not complex enough. So the aim of this research is to propose a model for creating a system powerful enough, but no too challenging for the user in the context of teaching computational thinking. Model would be based on existing platform *Bebras Lodge,* which already has some simplifications for designing interactive exercises, but the existing tools are not coherent with pedagogical models for tasks development.

A presentation of any preliminary ideas, the proposed approach and achieved results

The research is in its very first stage - starting the literature review, examining the existing interactive exercises for computational thinking. Once done I am planning to form a model with clear categories of what types of tools could be needed for creating any interactive exercise in the field of computational thinking.

Expectations and motivation to attend Doctoral Consortium

Since I am very new to the academic field of informatics engineering, any input from the experienced researchers would be valuable. I hope to bring more clarity to my research by this consortium and it could be a useful kick-off for my work.

Application of Web Programming in Programming Education

Márton Visnovitz

2nd year PhD student
Eötvös Loránd University, Faculty of Informatics
Pázmány Péter sétány 1/C
Budapest, 1117, Hungary
visnovitz.marton@inf.elte.hu

Brief Biography

Studies

2017	MA degree in Teacher Education (informatics, environmental science) Eötvös Loránd University, Budapest, Hungary
2014	BSc degree in Computer Science Eötvös Loránd University, Budapest, Hungary

About

I am PhD student and an assistant lecturer at Eötvös Loránd University. While I mostly teach at university level, I have some experience in both secondary school and high school education. My passion has always been the teaching of programming and web technologies. In my PhD studies I am working on combining the two and try to successfully integrate web technologies into high school and university programming curricula.

Interests

- Web programming, Progressive Web Apps
- Canvas-based web programming education
- Simulations and basic games in programming education
- Design systems
- Markdown-based documents

Research goals

The goal the PhD research is to prepare solutions to various problems in teaching programming in public education. The research has two focus points:

1. Empirical evidence shows that there is a hard transition between visual programming - be it block-based (e.g. Scratch) or program-generated graphics (e.g. Logo) - and the code-based, "classical" programming that is required at the Final Exams;
2. Various teaching strategies are appropriate for different age groups, and various technologies are used to support these teaching strategies for each age group.

During my research I would like to create a methodology that provides means to solve or at least mitigate these problems.

Research questions

1. **What programming languages, programming environments are currently being used in public education? Why?** The survey should include data from both standard and specialized (increased CS classes) groups, also curricular and extracurricular (e.g. competitions) activities.
2. **How could web programming support the introductory, code-based programming?** To answer this RQ the following problems should be addressed:
    - What problems 13-16 y/o students face when they start to learn code-based programming?
    - What properties does an ideal education-focused programming language possess?
    - Compared to that, what properties do web-based programming languages (e.g. JavaScript) and environments (e.g. browsers) have?
3. **How could we make the transition between visual and code-based programming easier?**
    - What programming activities could web programming support that could provide an easier transition?
    - How do programming activities in the browser compare to current frameworks?
4. **Would JavaScript (or some dialect of it) be suitable to teach all things that we currently teach in public education?** To answer this question a thorough analysis of the current and the upcoming National Curriculum is required. In addition to that we must examine the Final Exam requirements and some other extra contents (e.g. competitions) as well.

Hypotheses

The core idea behind my hypotheses is that web programming (more specifically JavaScript) could be an effective tool to teach programming in public education and it could solve many of the problems of the current system. I believe that the browser as a programming platform and the JavaScript programming language provide many opportunities that would enable us to introduce various programming paradigms and technologies to the pupil to broaden their view of the technological world. These technologies include computer graphics, event-driven programming, mobile technology, robotics, sensor system, smart devices. Because all these technologies require only one programming language (JS) it could be an answer to the problem of having little time to use. I believe that in addition to provide a good tool to the curricular activities JavaScript could support more advanced use-cases as well during extracurricular classes and competitions as well.

Based on these core ideas I formulated the following hypotheses:

1. JavaScript is suitable to teach the current programming curricula in Hungarian public education.
2. Using the browser and JavaScript it is possible to create a programming environment and educational assets that support an easy transition between visual and code-based programming at the age of 13-16 years.
3. Web programming is suitable to introduce and teach various programming paradigms and technologies in the age of 13-18 years.

4. JavaScript is suitable for competitive programming, compared to other languages it is easy to use and it is adequately fast for competitions.

Research methods

Method: *design-based research*

Research focus: The curriculum, the student, the learning process

Design goals:

- To create methodology using web programming that supports teaching various programming concepts and technologies in the age of 13-18.
- To develop tools, learning and coding environments, learning materials that provide additional benefits to the technology and the platform.

Qualitative measurements

- Interviews with teachers about the methods they use, programming languages and programming environments. (RQ 1, 2)
- Student interviews about their difficulties in the transitional period between visual and code-based programming and the possible reasons for those problems (RQ 2, 3)
- Analysis and evaluation the current and the upcoming National Curriculum, syllabi and Final Exam requirements. (RQ 4) – Pending because of the currently changing Curriculum

Quantitative measurements

- Evaluation of the effectiveness of the proposed programming language (JavaScript) in competitive tasks (OKTV, CEOI, IOI) (RQ 4) – In progress

Experimental measurements

- Testing and evaluating the proposed methodology in various environments (summer camps, extracurricular activities, school classes) (RQ 2, 3) – Some preliminary results

Publications

1. Visnovitz, M. (2018). Nevezetes felsorolók funkcionálisan [Notable Enumerators with Functional Programming]. In Proceedings: INFODIDACT 2018, Zamárdi, Hungary
2. Horváth, Gy., Visnovitz, M. (2018). Tesztelési módszerek webes tárgyak tanításában [Testing Methods in Teaching Web Technologies]. In Proceedings: INFODIDACT 2018, Zamárdi, Hungary
3. Visnovitz, M. (2017). Programozási tételek funkcionálisan [Fundamental Algorithms with Functional Programming]. In Proceedings: INFODIDACT 2017, Zamárdi, Hungary
4. Horváth, Gy., Visnovitz, M. (2017). Egy bevezető webfejlesztési kurzus módszertani megfontolásai [Methodological Considerations of an Introductory Web Development Course].
In Proceedings: Informatika a felsőoktatásban 2017 [Informatics in Higher Education 2017], Debrecen, Hungary, University of Debrecen, Faculty of Informatics. p. 265- 274.

Relevant Conferences

1. INFODIDACT 2018, Zamárdi, Hungary. Presentation: Nevezetes felsorolók funkcionálisan [Notable Enumerators with Functional Programming]
2. CONSTRUCTIONISM 2018, Vilnius, Lithuania. Poster: The Web – A Platform for Creation
3. INFODIDACT 2017, Zamárdi, Hungary. Presentation: Programozási tételek funkcionálisan [Fundamental Algorithms with Functional Programming]
4. DAMSS 2016, Druskininkai, Lithuania. Presentation: Aspects for Choosing Textual Programming Languages for High School Education

Bibliographic References

1. Horváth, Gy., Menyhárt, L. (2014). Teaching introductory programming with JavaScript in higher education. In Proceedings: *Proceedings of the 9th International Conference on Applied Informatics*, Eger, Hungary. p. 339-350.
2. Horváth, Gy., Menyhárt, L., Zsakó, L. (2016). Viewpoints of programming didactics at a web game implementation. In Proceedings: *Proceedings of the XXIX. DidMatTech 2016 Conference,* Budapest, Hungary. Eötvös Loránd University, Faculty of Informatics.
3. Mahmoud, Q. H., Dobosiewicz, W., Swayne D. (2004). Redesigning Introductory Computer Programming with HTML, JavaScript, and Java. In Proceedings: *SIGCSE '04 Proceedings of the 35th SIGCSE technical symposium on Computer science education,* Norfolk, Virginia, USA, ACM SIGCSE Bulletin. p. 120-124.
4. Kruglyk, V., Lvov M. (2012). Choosing the First Educational Programming Language. In Proceedings: *Proceedings of the 8th Integration, Harmonization and International Conference on ICT in Education*, Kherson, Ukraine, p. 188-198.
5. Weintrop D., Holbert N., Wilensky U., Horn M. (2012). Redefining Constructionist Video Games: Marrying Constructionism and Video Game Design. In Proceedings of Constructionism 2012, Athens. pp. 645-649.
6. Resnick, M. (2014). *Give P's a Chance: Projects, Peers, Passion, Play*. Constructionism and Creativity conference, opening keynote. Vienna
7. Bernát, P., Zsakó, L. (2017). *Methods of Teaching Programming – Strategy.* In Proceedings of XXX. DidMatTech 2017, Travana.
8. Tisue S., Wilensky U. (2004). *NetLogo: A Simple Environment for Modeling Complexity*. In Proceedings of International conference on complex systems. Boston. pp. 16-21.

Expectations and motivation to attend Doctoral Consortium

I wish to discuss my ideas with fellow PhD students and experts of the field of informatics and programming education. I'd like to get some ideas on what aspects of the field is worth delving into and what aspects do others feel important. My previous experience from the Consortium was very positive. Back then I was just a master's student and the Consortium inspired me to pursue the field of educational research. I hope that this year I will get further inspiration and ideas for my PhD topic.