Joint Estonian-Latvian Theory Days 2022

Riga, May 6–8

Program & abstracts

Contents

Friday

14:00 **Igors Stepanovs** (page 5)

14:40 **Michał Zając** (page 5)

15:10 **Nikita Snetkov and Jelizaveta Vakarjuk** (page 5)

15:40 **Coffee break**

16:10 **Jevgēnijs Vihrovs** (page 6)

16:40 **Andris Locāns** (page 6)

17:10 **Martins Kokainis** (page 6)

17:40 **Aleksandrs Belovs** (page 7)

Saturday

9:00 **Tarmo Uustalu** (page 7)

9:30 **Silvio Capobianco** (page 7)

10:00 **Niels Voorneveld** (page 8)

10:30 **Artjoms Šinkarovs** (page 8)

11:00 **Coffee break**

11:30 **Māris Ozols** (page 8)

12:10 **Maksims Dimitrijevs** (page 9)

12:30 **Sergejs Kozlovičs** (page 9)

13:00 **Lunch break**

14:30 **Vitaly Skachek** (page 9)

15:00 **Ago-Erik Riet** (page 10)

15:30 **Coffee break**

16:00 **Junming Ke** (page 10)

16:30 **Gatis Melkus** (page 11)

17:00 **Excursion and dinner**

Sunday

9:30 **Sander Mikelsaar** (page 11)

10:00 **Martin Puškin** (page 11)

10:30 **Urmas Luhaäär** (page 12)

11:00 **Henk D.L. Hollmann** (page 12)

11:30 **Coffee break**

12:00 **Hsuan-Yin Lin** (page 12)

12:30 **Peeter Laud** (page 13)

13:00 **Härmel Nestra** (page 13)

13:30 **Lunch break**

15:00 **Cheng-Syuan Wan** (page 13)

15:30 **Niccolò Veltri** (page 14)

16:00 **Coffee break**

Joint Estonian-Latvian Theory Days 2022

Estonian Computer Science Theory Days started in 2002 and have been organized many times since then. In Latvia, a similar event, Computer Science Days, has been organized several times since 2011. The first joint Estonian-Latvian Theory Days were held in 2010. This year, we (the Faculty of Computing, University of Latvia, with the help of our Estonian colleagues) are organizing the eighth such event. The main goal of the Theory Days is to let the theoretical computer scientists of our two countries to get acquainted with the work of each other. However, people from other countries are welcome to participate as well. The main audience is intended to be the graduate students in the roles of both listeners and presenters.

Program / Organising Comittee

Andris Ambainis
Jānis Iraids
Mārtiņš Kālis
Martins Kokainis
Peeter Laud
Helger Lipmaa
Aleksandrs Rivošs
Vitaly Skachek
Juris Smotrovs
Tarmo Uustalu
Jevgēnijs Vihrovs

Abstracts of talks

Igors Stepanovs

Four Attacks and a Proof for Telegram

We study the use of symmetric cryptography in the MTProto 2.0 protocol, Telegram's equivalent of the TLS record protocol. We give positive and negative results. On the positive side, we formally and in detail model a slight variant of Telegram's "record protocol" and prove that it achieves security in a suitable secure channel model, albeit under unstudied assumptions. This talk will focus on the negative results. First, we motivate our modelling deviation from MTProto by giving two attacks – one of practical, one of theoretical interest – against MTProto without our modifications. We then also give a third attack exploiting timing side channels, of varying strength, in three official Telegram clients. On its own this attack is thwarted by the secrecy of salt and id fields that are established by Telegram's key exchange protocol. To recover these, we chain the third attack with a fourth one against the implementation of the key exchange protocol on Telegram's servers. Our results provide the first comprehensive study of MTProto's use of symmetric cryptography.

Michał Zając

What Makes Fiat–Shamir zkSNARKs (Updatable SRS) Simulation Extractable?

We show that three popular universal zero-knowledge SNARKs (Plonk, Sonic, and Marlin) are updatable SRS simulation extractable NIZKs and signatures of knowledge (SoK) out-of-the-box avoiding any compilation overhead. Towards this we generalize results for the Fiat–Shamir (FS) transformation, which turns interactive protocols into signature schemes, non-interactive proof systems, or SoK in the random oracle model (ROM). The security of the transformation relies on rewinding to extract the secret key or the witness, even in the presence of signing queries for signatures and simulation queries for proof systems and SoK, respectively. We build on this line of work and analyze multi-round FS for arguments with a structured reference string (SRS). The combination of ROM and SRS, while redundant in theory, is the model of choice for the most efficient practical systems to date. We also consider the case where the SRS is updatable and define a strong simulation extractability notion that allows for simulated proofs with respect to an SRS to which the adversary can contribute updates. We define three properties (trapdoor-less zero-knowledge, rewinding-based knowledge soundness, and a unique response property) that are sufficient for argument systems based on multi-round FS to be also simulation extractable in this strong sense. We show that Plonk, Sonic, and Marlin satisfy these properties, and conjecture that many other argument systems such as Lunar, Basilisk, and transparent variants of Plonk fall within the reach of our main theorem.

Nikita Snetkov and Jelizaveta Vakarjuk

Analysis of Russian Federal Remote E-voting Scheme of 2021

We will present the details of one of the two cryptographic remote e-voting protocols used in the Russian parliamentary elections of 2021. We will present an initial security analysis of the protocol, identifying the potential weaknesses under the assumptions of corruption of the relevant key components.

Jevgēnijs Vihrovs

Quantum algorithms for Treewidth

In this paper, we study quantum algorithms for computing the exact value of the treewidth of a graph. Our algorithms are based on the classical algorithm by Fomin and Villanger (Combinatorica 32, 2012) that uses $O(2.616^n)$ time and polynomial space. We show three quantum algorithms with the following complexity, using QRAM in both exponential space algorithms:

- $O(1.618^n)$ time and polynomial space;
- $O(1.554^n)$ time and $O(1.452^n)$ space;
- $O(1.538^n)$ time and space.

In contrast, the fastest known classical algorithm for treewidth uses $O(1.755^n)$ time and space. The first two speed-ups are obtained in a fairly straightforward way. The first version uses additionally only Grover's search and provides a quadratic speedup. The second speedup is more time-efficient and uses both Grover's search and the quantum exponential dynamic programming by Ambainis et al. (SODA '19). The third version uses the specific properties of the classical algorithm and treewidth, with a modified version of the quantum dynamic programming on the hypercube. As a small side result, we give a new classical time-space tradeoff for computing treewidth in $O^*(2^n)$ time and $O^*(\sqrt{2^n})$ space.
Joint work with Vladislavs Kļevickis and Krišjānis Prūsis.

Andris Locāns

Quantum speedup for track reconstruction in particle accelerators

In High Energy Physics particles are collided at a high speed and afterwards particle tracking is used to reconstruct the collision. Since the amount of data related to this task is growing, it is important to look for ways to speed up particle tracking.
In this article we provide a time complexity analysis of typical routines currently used in particle tracking and also develop several quantum routines with lower complexities than the classical ones.

Martins Kokainis

Random walk-based benchmarking of single-electron circuits

Single-electron circuits, already used as electric-current quantum standards and prototypes of quantum computers, offer the possibility of greater control over elementary quantum systems. However, as these miniaturized circuits are governed by the laws of quantum mechanics, there are intrinsic limits on the fidelity of such devices. Furthermore, validation of error models and quantification of the fidelity is impeded by the fundamental uncertainties and noise. To address this issue, we identify and experimentally validate the statistical laws that describe the inevitable (albeit very rare) errors in accounting of individual quantum particles. The fidelity is modeled as a random walk of an error syndrome, detected by an accumulating probe. The proposed methodology allows to estimate the error rate of the circuit and the impact of the correlated noise due to the environment, contributing towards a rigorous metrology of quantum circuits.
Joint work with A. Ambainis, V. Kashcheyevs (University of Latvia) and D. Reifert, N. Ubbelohde (PTB, Germany).

Aleksandrs Belovs

Tight Quantum Lower Bounds for Approximate Counting with Quantum States

Counting is one of the basic computational tasks. Not surprisingly, quantum complexity of approximately counting the number of elements in a set was settled down early on in the history of quantum computation. It was done assuming the standard membership oracle access to the set. However, the membership oracle is not the only way how to encode the input set. Another, quite natural possibility is to encode the set using a uniform quantum superposition over its elements. The problem of quantum counting in this settings was first raised by Aaronson et al, who gave some initial results. We completely resolve this problem for different ways of accessing the uniform superposition.
Joint work with Ansis Rosmanis.

Tarmo Uustalu

List monads

We tend to speak of the (possibly empty) list monad and the nonempty list monad, meaning the free monoid monad and the free semigroup monad, as if those were the only monad structures on the list and nonempty list endofunctors (on Set). But they are not! It may at first seem hard to construct other list and nonempty list monads, but at a closer look it turns out that examples abound. There are infinitely many list monads with the singleton function as the unit that admit a presentation with one nullary and one binary operation, and infinitely many nonempty list monads with singleton as the unit and a presentation with one binary operation; some multiplications not only delete, but even duplicate and permute elements. There are list and nonempty list monads with singleton as the unit that have no finite presentation. There are nonempty list monads whose unit is the doubleton function. You cannot tell if a nonempty list monad presented to you as a blackbox is the free semigroup monad by testing the unit and multiplication on finitely many inputs. Etc. We are far from having classified all list monads or all nonempty list monads, but these are cool combinatorial problems.
Joint work with Dylan McDermott, Maciej Piróg, published in PPDP 2020.

Silvio Capobianco

Additive cellular automata monadically

In JAC 2010 we showed that cellular automata over a fixed grid are a comonadic notion of computation, in that they can be analyzed as coKleisli maps of a comonad and, in fact, also of a graded comonad. Additive cellular automata are a special case of cellular automata whose global rule is a additive. We observe that such cellular automata are also Kleisli maps of a graded monad and discuss some corollaries of the presence of both the comonadic and the monadic perspectives in this case.
Joint work with Tarmo Uustalu.

Niels Voorneveld

Stateful relators for algebraic effects

We consider programs that can raise algebraic effect operations, which act as questions from the program to its environment. Depending on the internal state of the environment, the question is answered and the internal state may change. A variety of effectful situations can be modelled this way, using stateful nondeterministic runners. Note however that different programs invoking different operations may still behave similarly when observed externally. This idea is captured by behavioural equivalence of programs, and can be formulated using relators which tell us how to translate relations on return values to relations on programs which can produce such values.
In this talk, we look at how to formulate relators using stateful nondeterministic runners, and look at some examples of effects they can model, which include; input, output, global store, cost, nondeterminism, and interleaving concurrency. We will investigate the stateful aspects of such relators, and see how behavioural equivalence can depend on the state of the environment. Moreover, we will look at how this can be extended to programs with general recursion, and how one may attempt to formalise such relators using inductive and coinductive predicate liftings. Includes joint work with Niccolò Veltri.

Artjoms Šinkarovs

Rank-Polymorphic Arrays in Dependently-Typed Languages

A large number of high-performance numerical problems use multi-dimensional arrays as a key data structure. Arrays naturally abstract spaces with regular structure; and computations on arrays can be efficiently implemented on conventional (parallel) architectures. Array languages such as APL demonstrate that many algorithms can be expressed as a composition of array combinators. The key property of such combinators is rank polymorphism — the ability to operate on arrays of arbitrary rank. Typed versions of such combinators that can guarantee lack of out-of-bound indexing requires a type system supporting dependent types.
In this talk I will demonstrate how to define rank-polymorphic array combinators in Agda. At the example of parallel prefix sums I will demonstrate how rank polymorphism can be used to organise recursive traversal over canonical sub-arrays. I will relate the proposed treatment of arrays to some of the well-known type-theoretical constructions.

Māris Ozols

Quantum Majority Vote

Majority vote is a basic method for amplifying correct outcomes that is widely used in computer science and beyond. We consider an extension of majority vote to quantum inputs and quantum outputs: given a product state of the form $|\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \ldots \otimes |\varphi_n\rangle$, where each qubit $|\varphi_k\rangle$ is in one of two orthogonal states $|\psi_0\rangle$ or $|\psi_1\rangle$, output the majority state. Importantly, the algorithm does not know the basis $\{|\psi_0\rangle, |\psi_1\rangle\}$ and should work for any choice.
We provide an optimal algorithm for this problem that achieves worst-case fidelity of $1/2 + \Theta(1/\sqrt{n})$. Under the promise that at least $2/3$ of the qubits are in the majority state, the fidelity increases to $1 - \Theta(1/n)$ and approaches one in the limit.
More generally, we initiate the study of quantum algorithms for covariant and symmetric Boolean functions $f : \{0,1\}^n \to \{0,1\}$ with quantum inputs and quantum outputs. We provide a simple linear program of size roughly $n/2$ for computing the optimal worst-case fidelity and show that a generalization of our quantum majority vote algorithm is optimal for computing any such f.

Maksims Dimitrijevs

Implementation of a quantum walk on a tree and DAG size estimation algorithms for real quantum computers

In this research, we focus on the implementation of quantum algorithms to investigate their behavior. First, we implement an algorithm for a quantum walk on a tree proposed by Ashley Montanaro, that allows to improve the search on a tree that is generated by backtracking algorithm. Next, we implement an algorithm for DAG size estimation by Andris Ambainis and Martins Kokainis. For both algorithms we investigate the capacity of currently available quantum computers and limitations of local simulators (running experiment on a local computer). We also analyze the outputs of algorithms and conclude that in some cases output of algorithm can reveal additional information on the structure of the solution for problem.
During the talk, we will show and explain some details of implementation of algorithms and discuss the outcomes of our experiments.
Algorithms that we implemented are described in the following papers: https://arxiv.org/abs/1509.02374, https://arxiv.org/abs/1704.06774v2.

Sergejs Kozlovičs

Towards the Post-Quantum Era: Quantum Entropy via a Quantum-Resistant Network

It is considered that the only true high-entropy sources of randomness are quantum random number generators (QRNG-s). We address the problem of sharing a hardware QRNG among multiple users connected to it via the classical network. In particular, we show how to secure the communication channel between the remote QRNG and its clients by applying quantum-safe algorithms. We also outline several challenges of applying post-quantum cryptography (PQC) to key generation, key exchange, and signature validation. Besides, we discuss the importance of hybrid algorithms (RSA/ECC + PQC) on the way to the post-quantum world.

Vitaly Skachek

Some results related to synchronization of data in distributed storage systems

In this talk, we present several results related to a set reconciliation problem in the distributed systems. Thus, we consider a task of function computation on the reconciled data, which generalizes a set reconciliation problem in the literature. Assume a distributed data storage system with two users A and B. The users possess a collection of binary vectors S_A and S_B, respectively. They are interested in computing a function ϕ of the reconciled data $S_A \cup S_B$. We show that any deterministic protocol, which computes a sum and a product of reconciled sets of binary vectors represented as nonnegative integers, has to communicate at least $2^n + n - 1$ and $2^n + n - 2$ bits in the worst-case scenario, respectively, where n is the length of the binary vectors. Connections to other problems in computer science are established, yielding a variety of additional upper and lower bounds on the communication complexity.
Invertible Bloom Filter (IBF) is a data structure, which employs a small set of hash functions. IBFs are employed in very efficient set reconciliation protocols. An IBF allows for an efficient insertion and, with high probability, for an efficient extraction of the data. However, the success probability of the extraction depends on the storage overhead of an IBF and the amount of the data stored. The extraction might succeed only partially, by recovering only part of the stored data. We analyze the probability of success for a partial extraction of data from an IBF, and show that partial extraction could be useful in applications, such as set reconciliation.

Ago-Erik Riet

Coding for storage and networks with subspaces.

In the case of classical error-correcting codes, redundancy is added to data before sending it over a channel introducing random errors, and then the receiver tries to recover the original data. A linear code is defined as a k-dimensional subspace C of the vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$, and a linear encoder for it is given by a full-rank k-by-n "generator matrix" G with row span C, taking a row vector of data symbols $a \in \mathbb{F}_q^k$ to the row vector of coded symbols $c = aG \in \mathbb{F}_q^n$. In that scenario, the coded vectors corresponding to data vectors carry the information.
In certain other scenarios, information is carried by subspaces without a specified basis. In the random linear network coding approach initiated by Kötter and Kschischang [4], only the span of a set of input vectors carries the information, as each vector should be viewed as replaced by a random linear combination of vectors in this set. Similarly, in the codes for distributed storage systems model studied by Hollmann and Poh [3] a storage node stores a subspace that may be given by various bases.
These kind of examples have motivated the study of subspace codes and rank-metric codes. The projective space $\mathrm{PG}(n-1,q)$ is equivalently the vector space $\mathbb{F}_q^n$ together with all its subspaces. A subspace code is a subset $C \subseteq \mathrm{PG}(n-1,q)$ that is "well-separated", often in the sense that the "subspace distance" $\dim U + \dim V - 2\dim U \cap V \geq d$ for any distinct $U, V \in C$, for some given "minimum distance" d. In a similar spirit, a rank-metric code is a "well-separated" subset $C \subseteq \mathbb{F}_q^{m\times n}$ such that the rank of the matrix $M - N$ is at least d for distinct matrices $M, N \in C$.
A subspace code is constant dimension if all codewords have the same dimension, and equidistant if the subspace distance of every two codewords is the same. Constant dimension codes were applied for random linear network coding in [4]. I will cover some structural and cardinality results about equidistant constant dimension subspace codes and give a flavor of the proof methods, based on [1, 2] and work in progress.

[1] Daniele Bartoli, Ago-Erik Riet, Leo Storme, and Peter Vandendriessche. Improvement to the sunflower bound for a class of equidistant constant dimension subspace codes. *Journal of Geometry*, 112(1):1–9, 2021.

[2] Jozefien D'haeseleer, Giovanni Longobardi, Ago-Erik Riet, and Leo Storme. Maximal sets of k-spaces pairwise intersecting in at least a $(k-2)$-space. *Electronic Journal of Combinatorics*, 29(1), 2022.

[3] Henk D.L. Hollmann and Wencin Poh. Characterizations and construction methods for linear functional-repair storage codes. In *2013 IEEE International Symposium on Information Theory*, pages 336–340, 2013.

[4] Ralf Koetter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

Junming Ke

Constructing Update-Efficient Storage Codes via Finite Projective Planes

With the increasing size of datasets nowadays, modern distributed storage systems prefer to keep data with redundancy to prevent data loss. A widely used approach is erasure coding, where the distributed system takes the data as input and generates additional redundant symbols. Any update of a single data symbol will cause the update of several redundant symbols. If data symbols and parity symbols are stored in different racks, this will lead to a number of data transmissions between racks. Therefore the update performance of storage codes is becoming a common concern in modern distributed storage systems. In this talk, we will introduce a construction of update-efficient storage codes via finite projective planes.

Gatis Melkus

Functional significance of topology in chromatin interaction networks

Inside eukaryotic cells (such as plant or animal cells), the DNA composing an organism's genome is generally not found by itself, but is instead tightly wound and packaged with a variety of proteins in a complex called chromatin. A noteworthy characteristic of chromatin is its dynamic nature, as it is not only chemically variable and significant in the regulation of individual gene function, but also carries additional significance depending on its spatial organization, where regions of chromatin in close proximity inside the cell can regulate one another and therefore determine the functioning of their attached DNA. A method capable of capturing some of this spatial organization is chromatin conformation capture (3C) and its derived methods (such as Hi-C or capture Hi-C), which allows us to tabulate the individual contacts between chromatin regions and develop a basic understanding of the interactions that may be occurring between them.
Using publicly available capture Hi-C datasets, we have constructed chromatin interaction graphs for several dozen cell types in an effort to study the topology of these interactions and understand what distinct topological features may be mapped to known functional chromatin features such as enhancers, Polycomb-mediated repressive complexes and heterochromatin. In addition, we investigate the possibility of using topological metrics to discern between cell types and the preservation of particular topological features in closely related cell types.

Sander Mikelsaar

NB LDPC and GLDPC Codes for Future Communication Standards

Low-density parity-check (LDPC) codes are a class of codes widely used in modern communication standards such as Digital Video Broadcasting (DVB-S2), WiMAX and 3GPP standards (including 5G NR) due to their nearly channel-capacity-reaching performance. Non-binary (NB) and generalized LDPC (GLDPC) codes are two competing extensions of LDPC codes which offer improved error-rate performance at the cost of increased computational complexity of decoding.
We are working on improving methods of construction for both NB LDPC and GLDPC codes, as well as simplifying decoding to provide solutions for potential practical applications.

Martin Puškin

Unequal-Data-Demand PIR codes: bounds and constructions

A t-PIR code allows the recovery of an encoded data symbol from each of t disjoint collections of code word symbols. We consider a generalization where some data symbols are in higher demand than other data symbols. We refer to such codes as $(t_1, ..., t_k)$-UDD PIR codes, where now the i-th data symbol can be recovered from each of t_i disjoint collections of code word symbols, for $i = 1, \ldots, k$.
In my talk I will present a Griesmer-like lower bound for the minimum length of a binary $(t_1, ..., t_k)$-UDD PIR code, generalizing a similar bound for binary t-PIR codes, and I will discuss two different proofs of this bound. I will also present some constructions that show this bound to be optimal for $k \leq 3$.

Urmas Luhaäär

Optimal possibly nonlinear 3-PIR codes of small size

A t-PIR code stores a data record in encoded form on a collection of servers in such a way that every position in the data record can be recovered t times by decoding the bit-values stored by t disjoint groups of servers. First, we present a generalization of the minimum-distance bound for PIR codes. Then we show that no encoder (linear or nonlinear) for the binary r-th order Hamming code produces a 3-PIR code except when $r = 2$. We use this result to determine the smallest length of a binary (possibly nonlinear) 3-PIR code of combinatorial dimension up to 6. A binary nonlinear 3-PIR code of dimension 7 and length 11 is necessarily nonlinear; the existence of such a code is an open problem.

Henk D.L. Hollmann

Permutation automorphisms of cyclic codes

Every cyclic code has certain "obvious" permutation automorphisms that can be derived directly from the generator polynomial of the code, and usually there are no others. But occasionally, a cyclic code possess "extra", non-standard permutation automorphisms; we will refer to such cyclic codes as *non-standard* (NS). Of special interest are non-standard irreducible cyclic codes or *NSIC-codes* such as the Golay codes, binary simplex codes, and the duals of certain repetition codes, and we would like to classify them. In our talk we introduce the problem and its background, and we indicate some unexpected connections with other problems.

Hsuan-Yin Lin

Improved Private Information Retrieval Rate for Noncolluding Coded Distributed Storage

Private Information Retrieval (PIR) is one of the significant privacy-preserving technologies to ensure the privacy of users in today's modern age of information. In the last years, the problem of information-theoretic PIR (i.e., assuming unbounded computational capability of the servers) has received renewed attention in the information-theory society. We consider PIR for distributed storage systems with non-colluding servers where data is stored using an arbitrary linear code. The main objective is to design a PIR protocol that achieves the maximum download rate among all possible PIR protocols. In this talk, we first propose a heuristic algorithm to decompose a storage code into punctured subcodes and then present a PIR protocol based on these punctured subcodes. The code decomposition is guided by the generalized Hamming weights of the storage code. We show that the proposed PIR protocol can achieve a larger download rate than that of all existing PIR protocols.

Peeter Laud

Efficient oblivious permutations for privacy-preserving computations

Oblivious permutations are used in privacy-preserving computations, including secure multiparty computation (MPC) and zero-knowledge proofs, to emulate operations that cause data-dependent memory accesses in computations in the clear. In this talk, we present a more efficient oblivious permutation for zero-knowledge protocols built according to the MPC-in-the-head paradigm, without making use of checking the equality of polynomials. Also, by using such equality checks, we present another oblivious permutation protocol for actively secure MPC, which is compatible with the widely used SPDZ construction. The complexity of both of our constructions is linear in the length of permuted vector.

Härmel Nestra

ZK-SecreC: a Domain-Specific Language for Zero-Knowledge Proofs

Zero-knowledge proof (ZKP) is an act of communication between two parties — Prover and Verifier — that enables Prover to convince Verifier that Prover knows the right answer to some question without revealing any information about the answer to Verifier. For example, Prover may convince Verifier that Prover knows a non-trivial factor of a large integer in such a way that Verifier will not be able to find the factor faster than before.

Our research group in Cybernetica AS is developing ZK-SecreC — a high-level programming language that enables to specify ZKPs in a form similar to usual imperative computer programs. While writing ZKPs like programs is not a new idea, ZK-SecreC seems to be unique in the static strong type and effect system that provides the necessary security guarantees. A ZK-SecreC program is compiled into an arithmetic circuit that is an environment for computations that both parties trust.

In the talk, I will introduce ZK-SecreC on examples, discuss its type and effect system, and define the essence of compilation of ZK-SecreC programs to arithmetic circuits.

Cheng-Syuan Wan

Proof theory of skew non-commutative MILL

Monoidal closed categories are models of non-commutative multiplicative intuitionistic linear logic (NMILL). Skew monoidal closed categories are weak variants of monoidal closed categories. In the skew cases, three natural isomorphisms λ, ρ, and α are merely natural transformations with a specific orientation. In previous works by Uustalu et al., proof theoretical analysis on skew monoidal categories and skew closed categories are investigated. In particular, the sequent calculus systems modelled by skew monoidal and skew closed categories are respectively constructed. Moreover, proof theoretical semantics of each system is provided according to Jean-Marc Andreoli's focusing technique. Following the results above, a question arises: is it possible to construct a sequent calculus system naturally modelled by skew monoidal closed categories? We answer the question positively by constructing a cut-free system NMILLs, a skew version of NMILL. Furthermore, we study the proof theoretical semantics of NMILLs. The inspiration also originates from focusing, but we peculiarly employ tag annotations to keep tracking new formulae occurring in antecedent and reducing non-deterministic choices in bottom-up proof search. Focusing solves the coherence problem of skew monoidal closed categories by providing a decision procedure to determine equality of maps in the free skew monoidal closed category.

This is joint work with Tarmo Uustalu (Reykjavik University) and Niccolò Veltri (Tallinn University of Technology).

Niccolò Veltri

Finitary Functors and Final Semantics in Type Theory

Coalgebras for a functor F are a versatile tool for representing a large variety of transition systems, such as NFAs or process calculi like Milner's CCS. The functor F specifies the kind of allowed transitions and it holds information about the collection of reachable states, e.g., is the system deterministic, or are reachable states organized in an ordered list or in an unordered set? The behaviour of a transition system starting from an initial state x is obtained by iteratively running the coalgebra modelling the system on x. The collection of such behaviours is the final coalgebra for the functor F. The theory investigating such objects is called universal coalgebra, and has been intensively studied during the past 30 years, but mostly using set-theoretic foundations based of classical logic. This work concerns the development of universal coalgebra in the type-theoretic foundations underlying proof assistants such as Agda and Coq. In particular, we tackle the problem of constructing final coalgebras in the case when F is a finitary set functor, such as the one delivering the finite subsets and finite multisubsets of a type.
This is joint work with Philipp Joram (Tallinn University of Technology)

Participant list

Oluwandabira Alawode
Tallinn University of Technology

Andris Ambainis
University of Latvia

Aleksandrs Belovs
University of Latvia

Silvio Capobianco
Tallinn University of Technology

Maksims Dimitrijevs
University of Latvia

Andis Draguns
Institute of Mathematics and Computer Science, University of Latvia

Valeh Farzaliyev
University of Tartu & Cybernetica AS

Denis Firsov
Tallinn University of Technology, Institute of Cybernetics

Francisco Javier Gil Vidal
University of Tartu, Institute of Computer Science, Algorithms & Theory Dept.

Henk D.L. Hollmann
University of Tartu

Jānis Iraids
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Philipp Joram
Tallinn University of Technology, Logic and Semantics Group

Mārtiņš Kālis
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Junming Ke
University of Tartu

Johanna Maria Kirss
Cybernetica AS

Martins Kokainis
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Sergejs Kozlovičs
Institute of Mathematics and Computer Science, University of Latvia

Dmitrijs Kravčenko
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Dāvis Jānis Lāriņš
Institute of Mathematics and Computer Science, University of Latvia

Peeter Laud
Cybernetica AS

Hsuan-Yin Lin
Simula UiB, Norway

Helger Lipmaa
Simula UiB, Norway

Andris Locāns
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Urmas Luhaäär
University of Tartu

Gatis Melkus
Institute of Mathematics and Computer Science, University of Latvia

Sander Mikelsaar
University of Tartu, Institute of Computer Science

Nikolajs Nahimovs
University of Latvia

Härmel Nestra
Cybernetica AS

Māris Ozols
University of Amsterdam & QuSoft

Raitis Ozols
University of Latvia

Calvin Pärn
Cybernetica AS

Kateryna Pavlyk
Simula UiB, Norway

Krišjānis Prūsis
University of Latvia, Faculty of Computing

Martin Puškin
University of Tartu

Raul-Martin Rebane
University of Tartu, Institute of Computer Science

Ago-Erik Riet
University of Tartu, Institute of Mathematics and Statistics

Aleksandrs Rivošs
University of Latvia, Faculty of Computing, Center for Quantum Computer Science

Artjoms Šinkarovs
Heriot-Watt University

Vitaly Skachek
University of Tartu, Institute of Computer Science

Juris Smotrovs
University of Latvia, Faculty of Computing

Nikita Snetkov
Cybernetica AS

Igors Stepanovs

Dominique Unruh
University of Tartu

Tarmo Uustalu
Tallinn University of Technology, Dept. of Software Science

Jelizaveta Vakarjuk
Cybernetica AS

Niccolò Veltri
Tallinn University of Technology

Jevgēnijs Vihrovs
University of Latvia

Niels Voorneveld
Tallinn University of Technology

Cheng-Syuan Wan
Tallinn University of Technology

Zhaowei Xu
University of Tartu

Bahdan Yanovich
Tallinn University of Technology, School of Information Technologies, Department of Software Science

Michał Zając
Nethermind