Abstrakty

Lubomíra Balková: *Combinatorics on Words and Random Number Generation*

Random number generators (RNGs) based on infinite words will be described. We will then introduce a certain combinatorial property of infinite words that guarantees absence of lattice structure of the related RNGs. The famous Fibonacci word or Arnoux-Rauzy words have the WDO property. Moreover, surprisingly good results in statistical tests of such RNGs will be pointed out.

Daniel Dombek: *On coding of $(\pm\beta)$-integers by conjugated morphisms*

In this contribution we study the expansions of real numbers in positive and negative real base. In particular, we consider the sets $\mathbb{Z}_\beta^+$ and $\mathbb{Z}_{-\beta}$ of nonnegative β-integers and $(-\beta)$-integers respectively. It is well known that, in numerous cases, these two sets can be completely unrelated to $\mathbb{Z}_\beta^+$. We manage to precisely describe all bases $(\pm\beta)$ for which $\mathbb{Z}_\beta^+$ and $\mathbb{Z}_{-\beta}$ can be coded by infinite words with the same language.

Josef Florian: *Domněnka 4n*

V příspěvku si představíme konstrukci nekonečných slov pomocí řídící posloupnosti a palindromického uzávěru. Dále se podíváme na některé vlastnosti takto konstruovaných slov, týkající se především faktorové komplexity, a na závěr ještě uvedeme jeden otevřený problém, který s danou problematikou souvisí.

Tomáš Hejda: *Balanced S-adic Words and Multi-Dimensional Continuted Fractions*

Sturmian words are strongly related to the one-dimensional continued fractions and Gauss algorithm in $\mathbb{R}_+^2$. It is well-known that they are 1-balanced. There exist several multi-dimensional continued fraction algorithms and we can assign certain S-adic systems to them. The Arnoux-Rauzy (AR) algorithm is nice but it does not allow the expansion of all directions from $\mathbb{R}_+^3$. A typical example of an AR word is the Tribonacci word, which is known to be 3-balanced. However, there are AR words which are not finitely balanced. Still, we prove that almost all AR words are finitely balanced.
The Brun algorithm has very nice properties and allows the expansion of all directions in 3 dimensions. We show that almost all Brun words are finitely balanced, yet there are uncountably many Brun words that are not.

Tatiana Jajcayová: *Generalized Difference Sets on Positive Integers*

The main topic of this talk is a generalization of the classical concept of difference sets: Given a non-empty set of positive integers $S \subseteq N$, consider the multiset $D(S) = \{s - t \mid s, t \in S, s > t\}$ of all positive differences of elements from S together with its frequency sequence $\Lambda(S) = \{\lambda_i \mid i \in N\}$, where λ_i represents the number of times the positive natural number i appears as a difference in $D(S)$.

While every non-empty subset of N has a corresponding frequency sequence, it is not hard to discover that while one frequency sequence may correspond to infinitely many subsets S of N, there also exist numerous examples of infinite sequences Λ that do not correspond to any set S at all.

In our talk, we address two basic problems concerning the frequency sequences of generalized difference sets: the problem of the *classification of sequences* Λ *that allow for the existence of* S satisfying $\Lambda(S) = \Lambda$, and the problem of the *minimal density* of such a set S.

We intend the talk to be non-technical, and to emphasize the fun side of the good old natural numbers.

Karel Klouda: *Bispecial factors in D0L languages*

We explain the importance of bispecial factors for understanding the structure of D0L languages. Usually, it is not difficult to describe all bispecial factors for a given particular D0L system; however, our goal is to find a general algorithm. Such an algorithm is known for D0L languages not containing repetitions. In this talk we mainly focus on the case of repetitive D0L systems: we give a brief survey of what is known and also some hints how it could help us to find a general algorithm for describing all bispecial factors.

Adam Kožaný: *Structural properties of PM colonies*

PM colonies are cooperating grammar systems. In this paper we point on structural properties of PM colonies, especially on changes in its behaving (generative power and decidability questions).

Petr Kůrka: *Dynamika celulárních automatů*

Přehled různých typů dynamického chování celulárních automatů, charakteristika celulárních automatů pomocí jazyků.

Markéta Lopatková: *Unstructured Data: How to Describe a Natural Language?*

The talk focuses on basic syntactic relations, namely on dependency and word order, and on their mutual interplay. We present a formal framework that gives us a possibility of an economic and linguistically adequate description of these relations as well as their automatic processing. Finally, we shortly mention the application of the framework in language resources and NLP tools.

Zuzana Masáková: *About spectra of Pisot numbers*

The spectrum of a real number $\beta > 1$ is the set of $p(\beta)$ where p ranges over all polynomials with coefficients restricted to a finite set of consecutive integers, in particular,

$$X^r(\beta) = \Big\{ \sum_{j=0}^{n} a_j \beta^j : n \in \mathbb{N},\, a_j \in \mathcal{A} = \{0, 1, \ldots, r\} \Big\} = \{0 = x_0 < x_1 < x_2 < x_3 < \cdots\}\,.$$

The study of such sets for $\beta \in (1, 2)$ was initiated by Erdős et al. and since then, many authors have contributed to the description of $X^r(\beta)$, especially in case that β is a Pisot number. A general result by Feng and Wen states that for a Pisot number β and $r + 1 > \beta$, the sequence of distances $x_{n+1} - x_n$ in $X^r(\beta)$ can be generated by a substitution. The alphabet of the substitution grows rapidly with r. However, neither the explicit prescription for the substitution, nor the values of distances and their frequencies are known in general. The only case of base β, for which the minimal distance in $X^r(\beta)$ is known for any r is when β is a quadratic Pisot unit. For the same class of β, we show that recasting of the spectra in the frame of the cut-and-project scheme may bring new insight into the problem. We determine the values of all distances between consecutive points and their corresponding frequencies. We also show that shifting the set $\mathcal{A}$ of digits so that it contains at least one negative element, or considering negative base $-\beta$ instead of β, the generalized spectrum coincides with a cut-and-project sequence. As a consequence, we can show that the spectrum can be generated by a substitution over an alphabet at most five letters. Joint work with E. Pelantová and K. Pastirčáková.

Tomáš Masopust: *When can two regular word languages K and L be separated by a simple language?*

We investigate this question and consider separation by piecewise-testable and suffix-testable languages and variants thereof. We give characterizations of when two languages can be separated and present an overview of when these problems can be decided in polynomial time if K and L are given by nondeterministic finite automata.

Dana Pardubská: *Parallel communicating grammar systems with regular control and Restarting automata*

We introduce Parallel communicating grammar systems with regular control (RPCGS), which are obtained from returning regular parallel communicating grammar systems by restricting the derivations through a regular control language. For the class of languages that are generated by RPCGSs with constant communication complexity we derive a characterisation in terms of a restricted type of freely rewriting restarting automaton. From this characterisation we obtain that these languages are semi-linear, and that for RPCGSs with constant communication complexity, the centralised variant has the same generative power as the non-centralised variant.
Motivation for this work comes from computational linguistics. The talk is mainly based on paper
D. Pardubská, M. Plátek, F. Otto: Parallel communicating grammar systems with regular control and skeleton preserving FRR automat. Theoretical Computer Science 412 (2011) 458–477

Kateřina Pastirčáková: *Spectra of quadratic Pisot units and cut-and-project sets*

We follow the presentation of Z. Masáková about spectra of quadratic Pisot units, i.e. sets

$$X^m(\beta) = \Big\{ \sum_{j=0}^{n} a_j \beta^j : n \in \mathbb{N},\, a_j \in \mathcal{A} = \{0, 1, \ldots, m\} \Big\},$$

where $\beta > 1$ is a root of $x^2 - px - 1$, $p \geq 1$, or $x^2 - px + 1$, $p \geq 3$. Thanks to the approach using a cut-and-project scheme, we can show that, up to finitely many exceptions, the values of distances between consecutive points are three, just as in the corresponding cut-and-project sequence $\Sigma(\Omega)$. Nevertheless, we show that there are infinitely many elements of $\Sigma(\Omega)$ outside of the spectrum.

Edita Pelantová: *Výměna intervalů a itineráře návratů*

Studujeme nekonečná slova kódující výměnu dvou nebo tří intervalů, tzv. 2iet- a 3iet-slova. Ukážeme, jak znalost itinerářů návratu do obecného podintervalu přispívá k řešení následujících otázek:

1. struktura návratových slov pro 3iet-slova;
2. struktura abelovských slov návratu pro 2iet-slova;
3. tvar morfizmu, který má za svůj pevný bod nějaké 3iet-slovo;
4. vztah k domněnce Hofa, Knilla a Simona.

Martin Plátek: *Analysis by Reduction by Meta-Instructions*

The talk provides linguistic motivation for analysis by reduction and concentrates on a formal description of the whole mechanism through a special class of restarting automata consisting from a set of meta-instructions. The automata define gradually inreasing finite sets of sentences and their reductions, in order to obtain their (in general) infinite covering languages and sets of reductions (reduction languages). The analysis by reduction is modeled by reduction languages. Reduction languages create a refinement of (string) languages. We obtain similar infinite hierarchies for finite and infinite (reduction) languages. In that way we obtain a linguistically relevant tool for uniform clasifications of finite and infinite (reduction) languages. We discuss some of the formal and linguistic relevance of the presented notions.

Lukáš Pohanka: *Optimizing Serpent block cipher on ARM processors*

ARM processors are one of the most common CPU's in today's mobile devices and portable computers. This presentation shows the possibilities of optimizing cryptographic primitives on these processors, while utilizing most of the processor's features. These concepts are shown on Serpent block cipher which is one of the most secure but slowest AES candidates.

Petr Sosík: *DNA Computing versus Formal Language Theory*

The talk summarizes connections between the two mentioned research areas. The origins of DNA computing are intimately interconnected with the formal language theory, as the abstraction of DNA single-stranded molecules are strings over the alphabet A,C,T,G. Many new DNA-inspired operations over strings and languages have been introduced and their theoretical properties have been studied in the last 20 years. After introducing basic abstract operations used in the DNA computing, we describe several DNA computing models with clearly defined formal language background, including sticker systems, insertion-deletion systems, Watson-Crick automata and splicing systems. We conclude with an overview of the recent progress in the DNA computing field.

Štěpán Starosta: *Generalized pseudostandard words*

Let $\mathcal{A}$ a finite alphabet and Ψ be an involutive antimorphism over $\mathcal{A}^*$. A Ψ-*palindromic closure* of a word w is the shortest Ψ-palindrome having w as a prefix. The Ψ-palindromic closure of w is denoted by w^{Ψ}.
Let $\mathcal{I}$ be a finite set of involutive antimorphism. Let $\Theta = \vartheta_1\vartheta_2\vartheta_3\ldots \in \mathcal{I}^{\mathbb{N}}$ and $\Delta = \delta_1\delta_2\delta_3\ldots \in \mathcal{A}^{\mathbb{N}}$. Denote

$$w_0 = \varepsilon \quad \text{and} \quad w_n = \Big(w_{n-1}\delta_n\Big)^{\vartheta_n} \quad \text{for every} \quad n \in \mathbb{N}, n \geq 1.$$

The word

$$\mathbf{u}_{\Theta}(\Delta) = \lim_{n\to\infty} w_n$$

is called a *generalized pseudostandard word* with the directive sequence of letters Δ and the directive sequence of antimorphisms Θ.
We give an overview of known results of generalized pseudostandard words. We start with $\#\mathcal{I} = 1$ and then follow with larger sets. A relation to palindromic richness is also given.

Milena Svobodová: *k-block versus* 1*-block Parallel Addition in Non-standard Numeration Systems*

A positional numeration system is given by a base β in $\mathbb{C}$, $|\beta| > 1$, and a finite alphabet $\mathcal{A}$ of contiguous integers containing 0. We focus on the question whether, for a given numeration system, there exists a parallel algorithm performing addition of numbers with finite $(\beta, \mathcal{A})$-representations. By parallel algorithms we mean algorithms which perform the addition $x+y$ in constant time, independently of the lengths of the representations of x and y. This is equivalent to say that addition is a local function (or a sliding block code) from the alphabet $\mathcal{B} = \mathcal{A}+\mathcal{A}$ to $\mathcal{A}$. Recently, it has been shown that for any algebraic number β, $|\beta| > 1$, which has no conjugates of modulus 1, there exists an alphabet $\mathcal{A}$ allowing parallel addition. In general, the cardinality of $\mathcal{A}$ is unnecessarily large. In 1999, Kornerup suggested to consider a more general type of parallel algorithms, which, instead of treating each digit separately, manipulate blocks of digits of length $k \geq 1$. In that setting addition is a local function from $\mathcal{B}^k$ to $\mathcal{A}^k$.
In this talk we present an easy-to-check property of $(\beta, \mathcal{A})$ which guarantees the possibility of block parallel addition. We apply this result to the bases β which are Parry numbers, i.e., numbers whose Rényi expansion of unity $d_\beta(1) = t_1 t_2 t_3 \ldots$ is finite or eventually periodic. We show that if β additionally satisfies the property (F) or (PF), then block parallel addition is possible on the alphabet $\{0, \ldots, 2t_1\}$ or $\{-t_1, \ldots, t_1\}$. Specifically, we prove the usefulness of this concept on the d-bonacci base, where $\beta > 1$ is a root of the polynomial $f(X) = X^d - X^{d-1} - X^{d-2} - \cdots - X - 1$, by showing that k-block parallel addition is possible on the alphabets $\{0, 1, 2\}$ and $\{-1, 0, 1\}$ for some convenient k. However, if we require $k = 1$ (i.e., the standard parallel algorithm working with single digits), the cardinality of any alphabet allowing parallel addition in the d-bonacci base must be at least $d + 1$.

Jan Trávníček: *Space optimal indexing trees for pattern matching*

Indexing trees for all subtrees is a well investigated problem with an optimal algorithmic solution. There are some open questions regarding indexing trees for tree patterns. Given a tree with n nodes, the numbers of distinct tree patterns which match the tree can be at most $2^{n-1} + n$. The nondeterministic tree pattern pushdown automaton accepting all tree patterns of the given tree is of size $\mathcal{O}(n)$. The size of its deterministic variant is an open question. A new approach of tree indexing for tree patterns is presented. The presented approach posesses the property of the index of linear size, the time of the locating of all occurrences of an input tree pattern does not depend on the size of the subject tree. One step of the algorithm will be presented for a discussion.

Tomáš Vávra: *On Ito-Sadahiro number systems associated to confluent Pisot numbers*

Confluent Pisot numbers are roots $\beta > 1$ of polynomials $x^k - mx^{k-1} - \cdots - mx - n,\ k \geq 1, m \geq n \geq 1$. There are many specific properties of Rényi number systems are related to these bases. The most notable one is that any integer combination of non-negative powers of the base with coefficients in $\{0, 1, \ldots, \lceil \beta \rceil - 1\}$ is a β-integer, although a sequence of coefficients may be forbidden in the corresponding number system. We show that in Ito-Sadahiro number systems an analogical property holds. We also show that arithmetical properties of Rényi and Ito-Sadahiro number systems with confluent Pisot bases are very different.