Autumn School of the Department of Algebra

Rybniště, November 15–18, 2018

BOOK OF ABSTRACTS

Cover image by openclipart.

Contents

Colouring knots

Tomáš Nagy

In the talk we will introduce knots and knot theory. We will discuss how can we distinguish knots by knot invariants and we will focus mostly on knot colouring. We will show that colouring of knots by algebraical structure called quandle is a knot invariant. The aim is to discuss an algorithm for distinguishing knots. We will show how can we transform knot colouring into the SAT-problem and we will shortly introduce the results of an computer experiment dealing with colouring several special types of knots.

1. Basic notions

Definition 1. *A knot* is an embedding of a circle in 3-dimensional Euclidean space.

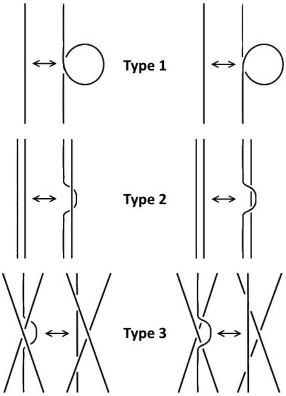
Two projection of a knot are called *equivalent* if there exists an ambient isotopy between them. This holds if and only if one projection can be obtained from the other by a final sequence of *Reidemeister moves.*

We represent knots by diagrams, e.g. projections with final number of crossings. We can get *PD notation* of a given knot diagram with n crossings as follows: Let us choose an orientation of the diagram and let us number the arcs of the projection by numbers $1, 2, \dots, n$. Then we represent a crossing with upper arc numbered by a, right arc (e.g. arc that is on the right side of the upper arc) with number b and left arc with number c by a triple (a, b, c). That means that we can represent this knot by n triples.

Knot invariants are properties that are common for all equivalent projections of a given knot.

2. Colouring and quandles

Definition 2. Let $K = \{(k_1, l_1, m_1), \dots, (k_n, l_n, m_n)\}$ be a representation of a knot diagram in PD notation and let C be a set with a binary operation $*$. We say that a mapping $f\colon C \longrightarrow K$ is a *colouring* of a diagram K by C if $f(k_i) * f(l_1) = f(m_1)$ for each $i \in \{1, \dots, n\}$.



We say that C is a set of *colours*. Let $Q = (C, *)$. We denote by $col_Q(K)$ the number of different colourings of the diagram K by Q.

Definition 3. Let C be a set and let $*$ be a binary operation on C. We say that $Q = (C, *)$ is a *quandle* if the operation $*$ satisfies following conditions:

(1) $a * a = a$;

(2) for each a, b there exists exactly one $x \in C$ such that $a * x = b$;

(3) $a * (b * c) = (a * b) * (a * c)$.

The colours used in colouring generate *algebraically connected quandles*, i.e., quandles $(C, *)$ where the group generated by left translations acts transitively on C. We can construct them from the pairs (G, ζ) where G is a group that acts transitively on C and $\zeta \in H$ (H is a stabilizer of an arbitrary element $e \in G$), such that $\langle g\zeta g^{-1}, g \in G\rangle = G$:

- Let (G, ζ) be as defined above.
- Let us chose for $y \in G$ some element $\hat{y} \in G$ such that $\hat{y}e = y$.
- We define the quandle operation $*$ on C as follows: $x * y = \hat{y}\zeta\hat{y}^{-1}x\hat{y}\zeta^{-1}\hat{y}^{-1}$.

Theorem 4. *Let $Q = (C, *)$ be a quandle. Then col_Q is a knot invariant.*

3. Distinguishing knots on the computer

In order to distinguish knots on the computer we will transform colouring into the Boolean satisfiability problem (SAT):

Let K be a projection of a knot with n arcs and let us denote these arcs by $a_1, a_2, \dots, a_n$. Let $Q = (\{1, 2, \dots, |Q|\}, *)$ be a quandle. We want to find a colouring f. We define $n|Q|$ many propositional variables $v_{i,j}$, where $i \in \{1, \dots, n\}$ and $j \in \{1, ..., |Q|\}$. We interpret $v_{i,j}$ as "arc i has a color j", i.e. $f(i) = j$.

We want following formulas to be satisfied:

(1) Each arc has exactly one color:
- Each arc has a color, i.e. $v_{i,1} \vee v_{i,2} \vee \cdots \vee v_{i,|Q|}$ for $i = 1, 2, \dots, n$.
- No arc has two colours, i.e. $\neg v_{i,l} \vee \neg v_{i,m}$ for $i = 1, 2, \dots, n, l = 1, 2, \dots, |Q|, m = l + 1, \dots, |Q|$.

(2) Each crossing satisfies the colouring condition, i.e. for a crossing (a_i, a_j, a_k) it holds that $f(i) * f(j) = f(k)$.
- Formulas of the form $(v_{i,l} \wedge v_{j,m}) \to v_{k,l*m}$, i.e. $\neg v_{i,l} \vee \neg v_{j,m} \vee v_{k,l*m}$ for $l, m = 1, 2, \dots, |Q|$.

(3) We want only non-trivial colourings.
- I.e. $\neg v_{1,l} \vee \neg v_{2,;} \vee \cdots \vee \neg v_{n,l}$ for $l = 1, 2, \dots, |Q|$.

(4) In order to simplify the result we can define that arc 1 has a color 1.
- I.e. $v_{1,1}$.

We get $col'_Q(K)$ many interpretations satisfying the given set of formulas. It can be easily seen that $col_Q(K) = |Q|(col'_Q(K) + 1)$ ("+1" for the trivial colouring,"$|Q|$-times" because we can choose $|Q|$ colours for the first arc).

Polynomial Closure of Classes of Regular Languages

Jana Bartoňová

The topic of this talk falls into the theory of regular languages. A *polynomial closure* is a certain operation on sets of regular languages. Its importance lies in the fact that it is used in defining so-called *concatenation hierarchies* of regular languages. The main problem concerning these hierarchies – the question of the decidability of their levels – is therefore closely connected with the question of the decidability of the polynomial closure.

1. Regular languages

Let A be a fixed finite set, called an *alphabet*. We denote by A^* a free monoid generated by A. Elements of A^* are called *words*, the monoid operation on A^* is a *concatenation*. A *language* over A is an arbitrary subset $L \subseteq A^*$.

A *regular language* over A is a language which can be created from languages of the form $\emptyset$ and $\{a\}$, where $a \in A$, by means of a finite number of applications of the following operations:

- union,
- *concatenation*: $K \cdot L = \{x \cdot y \mid x \in K, y \in L\}$,
- *iteration*: $L^* = \bigcup_{n=0}^{\infty} L^n$ (a submonoid of A^* generated by L).

Remark: The set of all regular language is closed also under complementation. (It is not obvious from the definition).

2. Polynomial closure

Definition 1. A *polynomial closure* $Pol(\mathcal{C})$ of a set of regular languages $\mathcal{C}$ is a set of regular languages which are finite unions of languages of the form

$$L_0 a_1 L_1 \ldots a_n L_n \qquad \text{where } a_i \in A, L_i \in \mathcal{C}.$$

3. Concatenation hierarchies

Definition 2. A *lattice* of regular languages is a set of regular languages containing $\emptyset$, A^* and closed under supremum $\cup$ (union) and infimum $\cap$ (intersection).

A *quotienting lattice* is a lattice of regular languages closed under *quotients* (a certain operation on regular languages).

$\mathcal{C}_0$ ... a given quotienting lattice of regular languages
$\mathcal{C}_{n+1/2} = Pol(\mathcal{C}_n) = Pol(\overline{\mathcal{C}_{n-1/2}})$ where $\overline{\mathcal{C}_{n-1/2}} = \{A^* \setminus L \mid L \in \mathcal{C}_{n-1/2}\}$
$\mathcal{C}_{n+1} = B(\mathcal{C}_{n+1/2})$ ... *Boolean* closure of the level $n + 1/2$ (closure under union and complementation)

The main question concerning half levels: How to decide whether a given regular language belongs to $\mathcal{C}_{n+1/2}$ for given $\mathcal{C}_0$ and $n \in \mathbb{N}_0$?

4. Syntactic monoid

Definition 3. A language $L \subseteq A^*$ is said to be *recognized* by a finite monoid M if there exist a homomorphism $\alpha\colon A^* \to M$ and a set $F \subseteq M$ such that $L = \alpha^{-1}(F)$.

Proposition 4. *A language L is regular iff it is recognized by a finite monoid.*

Definition 5. A *syntactic monoid* M_L of a regular language L is the smallest finite monoid recognizing L. The corresponding homomorphism $\alpha_L\colon A^* \to M_L$ is called a *syntactic homomorphism* of the language L.

Every syntactic monoid M_L is equipped with a distinguished partial order $\leq_L$.

5. An algebraic description of the polynomial closure

Theorem 6 (Branco, Pin, 2009; Place, Zeitoun, 2018)**.** *Let $\mathcal{C}$ be a quotienting lattice of regular languages, K a regular language. Then K belongs to $Pol(\mathcal{C})$ if and only if $e \leq_K ete$ for all $(e,t) \in \mathcal{C}[K] \subseteq (M_K)^2$ such that $e \in M_K$ is an idempotent.*

Computation of $\mathcal{C}[K] \subseteq (M_K)^2$:

(1) Stratification: $\mathcal{C} = \bigcup_{k=1}^{\infty} \mathcal{C}^k$ where all $\mathcal{C}^k$ are **finite** quotienting lattices such that $\mathcal{C}^1 \subseteq \mathcal{C}^2 \subseteq \mathcal{C}^3 \subseteq \cdots$. Then $\mathcal{C}[K] = \bigcap_{k=1}^{\infty} \mathcal{C}^k[K]$ where

$$\mathcal{C}^k[K] = \{(s,t) \in (M_K)^2 \mid \exists u, v \in A^* : \alpha_K(u) = s, \alpha_K(v) = t, u \leq_{\mathcal{C}^k} v\},$$

$$u \leq_{\mathcal{C}^k} v \quad \Leftrightarrow \quad \forall L \in \mathcal{C}^k :\ u \in L \ \Rightarrow\ v \in L.$$

(2) Find $m \in \mathbb{N}$ such that $\mathcal{C}^m[K] = \mathcal{C}[K]$ and compute $\mathcal{C}^m[K]$.

6. Example – Computation of $\mathcal{C}_{1/2}[K]$

Straubing–Thérien hierarchy:

$\mathcal{C}_0 = \{\emptyset, A^*\}$
$\mathcal{C}_{1/2}$ ... a set of finite unions of languages of the form

$$A^*a_1A^*a_2A^* \dots a_nA^* \quad \text{where } a_1, \dots, a_n \in A$$

(1) Stratification: $\mathcal{C}_{1/2} = \bigcup_{k=1}^{\infty} \mathcal{C}_{1/2}^k$ where $\mathcal{C}_{1/2}^k$ is a (quotienting) lattice of regular languages generated by languages of the form

$$A^*a_1A^*a_2A^* \dots a_nA^* \quad \text{where } \mathbf{n} \leq \mathbf{k}, a_1, \dots, a_n \in A.$$

(2) Let K be a regular language. Then $\mathcal{C}_{1/2}[K] = \mathcal{C}_{1/2}^{|M_K|}[K]$.

7. Conclusion

From the existence of an algorithm for the computation of $\mathcal{C}_{1/2}[K]$ we obtain the decidability of $\mathcal{C}_{3/2}$ of Straubing–Thérien hierarchy. The sets $\mathcal{C}_{3/2}[K]$, $\mathcal{C}_{5/2}[K]$ are known to be computable algorithmically as well (Place, Zeitoun 2014; Place, 2015). From these results we obtain the decidability of $\mathcal{C}_{5/2}$ and $\mathcal{C}_{7/2}$ of Straubing–Thérien hierarchy. The question of the decidability of the other half levels of this hierarchy is still an open problem.

Why is an elliptic curve a torus?

Ondrej Bínovský

We will show why elliptic curves over $\mathbb{C}$ are essentially the same objects as complex tori. Having established this correspondence, we will see that many nontrivial properties of elliptic curves become completely transparent, when viewed as the properties of complex tori. Moreover, these often remain valid for elliptic curves over other fields than $\mathbb{C}$.

1. Elliptic curves

Definition 1. An equation of the form

$$E\colon y^2 = 4x^3 - g_2x - g_3, \qquad g_2, g_3 \in \mathbb{C}$$

is called a Weierstrass equation over $\mathbb{C}$. A Weierstrass equation is called nonsingular if its discriminant $\Delta = g_2^3 - 27g_3^2$ does not vanish.

Definition 2. Let E be a nonsingular Weierstrass equation. The set

$$\mathcal{E} = \{(x, y) \in \mathbb{C}^2 \colon E(x, y) = 0\} \cup \{\infty\}$$

is called an elliptic curve over $\mathbb{C}$.

Definition 3. Let $\mathcal{E}$ be an elliptic curve and let $\mathcal{O}$ be the point at infinity of $\mathcal{E}$. Each line intersects the curve $\mathcal{E}$ exactly at three points (counted with multiplicity). We define the addition law of the elliptic curve $\mathcal{E}$ so that collinear triples of points sum to zero:

$$P + Q + R = \mathcal{O} \iff P, Q, R \text{ are collinear.}$$

Under this definition of addition, the elliptic curve $\mathcal{E}$ becomes an abelian group with $\mathcal{O}$ as the identity element. It is, however, not easy to show that the addition is indeed associative.

2. Complex tori

Definition 4. A lattice Λ is a set of the shape

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \colon m, n \in \mathbb{Z}\}$$

where ω_1 snd ω_2 are complex numbers which are linearly independent over the real numbers.

Definition 5. Let Λ be a lattice. Then the quotient group (of additive groups) $\mathbb{C}/\Lambda$ is called a complex torus.

3. Elliptic functions

Definition 6. Let Λ be a lattice. An elliptic function f for the lattice Λ is a function satisfying

(1) f is analytic on $\mathbb{C}$ except possibly at some isolated points (the poles of f).

(2) The lattice Λ is the lattice of periods of f, that is, $f(z+\lambda) = f(z)$ for all $z \in \mathbb{C}$, and all $\lambda \in \Lambda$.

Theorem 7 (Liouville)**.** *Let Λ be a lattice. Suppose that f is an elliptic function for Λ which is analytic on the whole complex plane (so it has no poles). Then f is constant.*

Theorem 8. *Let f be an elliptic function for a lattice Λ. Then there exists a positive integer n with the following property: for every $c \in \mathbb{C}$ the function $f(z) - c$ has exactly n zeros modulo Λ (the multiplicity of the zeros is taken into account). The number n is called the order of the elliptic function f, and it is denoted by* $\operatorname{ord}(f)$*.*

Definition 9. Let Λ be a lattice. The function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

is called the Weierstrass elliptic function.

Theorem 10. *Let Λ be a lattice. The function $\wp_\Lambda$ is an elliptic function for Λ. The Laurent expansion of $\wp_\Lambda$ around origin is*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}, \qquad \text{where } G_{2n}(\Lambda) = \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^{2n}}.$$

Theorem 11. *The function $\wp_\Lambda$ satisfies the differential equation*

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda), \qquad \text{where } g_2(\Lambda) = 60G_4(\Lambda) \text{ and } g_3(\Lambda) = 140G_6(\Lambda).$$

Theorem 12. *Let Λ be a lattice. The Weierstrass equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ is nonsingular, and so it defines an elliptic curve $\mathcal{E}$. The map*

$$\begin{aligned} \phi\colon \mathbb{C} &\longrightarrow \mathcal{E} \\ z &\longmapsto (\wp(z), \wp'(z)) \end{aligned}$$

induces a bijection between the complex torus $\mathbb{C}/\Lambda$ and the elliptic curve $\mathcal{E}$. Here $\phi(\Lambda)$ is to be interpreted as the point at infinity of $\mathcal{E}$.

Theorem 13. *The bijection ϕ from the previous theorem is a group isomorphism.*

Theorem 14. *Let $y^2 = 4x^3 - ax - b$ be a nonsingular Weierstrass equation. Then there exists a lattice Λ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$.*

4. Applications

Theorem 15. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$. Then the addition law of $\mathcal{E}$ defined in Definition 3 is associative.*

Theorem 16. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$. Let $\mathcal{E}[N]$ be the group of N-th torsion points of $\mathcal{E}$. Then $\mathcal{E}[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.*

Theorem 17. *Let $\mathcal{E}_1, \mathcal{E}_2$ be elliptic curves over $\mathbb{C}$. Let Λ_1, Λ_2 be the associated lattices. Then the homomorphisms from $\mathcal{E}_1$ to $\mathcal{E}_2$ correspond bijectively with complex numbers λ such that $\lambda\Lambda_1 \subset \Lambda_2$. In particular, $\mathcal{E}_1, \mathcal{E}_2$ are isomorphic if and only if $\lambda\Lambda_1 = \Lambda_2$ for some nonzero $\lambda \in \mathbb{C}$.*

Theorem 18. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$. Let $\mathrm{End}(\mathcal{E})$ be the endomorphism ring of $\mathcal{E}$. Then either $\mathrm{End}(\mathcal{E}) \cong \mathbb{Z}$ or $\mathrm{End}(\mathcal{E}) \cong R_K$, where R_K is an order in an imaginary quadratic field K.*

Pseudovarieties of semigroups and irreducibility

Jonatan Kolegar

In this talk I will introduce the theory of finite semigroups and the study of certain classes of semigroups. Early theorems regarding finite semigroups followed the general approach of algebra classifying structures up to isomorphism. There are just too many semigroups to characterize them this way, though. Asymptotically speaking, 3-nilpotent semigroups (i.e., semigroups satisfying $xyz = 0$) are almost all finite semigroups. Thus a revolution in thinking about semigroups was needed. This led to the study of classes of semigroups with additional properties. As these classes form a lattice, it is natural to aks for indecomposable elements of this lattice.

These classes of semigroups are called *pseudovarieties*. We will avoid a lot of structural theory of semigroups and dive directly into the study of pseudovarieties carried by useful examples with the goal of getting a good grasp for what a pseudovariety is. This is the main focus of the talk. Then we'll meet the notion of *irreducibility* in the lattice of pseudovarieties of finite semigroups and study one of the tools to show that a certain type of pseudovarieties is irreducible, *Rees extension semigroup.*

1. Reiterman theorem

Definition 1. Class V of finite semigroups is called *pseudovariety* if it is non-empty and satisfies the following conditions:

- If $S \in \mathsf{V}$ and $\varphi\colon S \to T$ is surjective homomorphism, then $T \in \mathsf{V}$.
- If T is a subsemigroup of $S \in \mathsf{V}$, then $T \in \mathsf{V}$.
- If S, T are semigroups in V, then $S \times T \in \mathsf{V}$.

In other words, pseudovarieties of semigroups are classes of semigroups closed under taking finite direct products, subsemigroups and homomorphic images.

By a pseudoidentity we mean a pair of two *implicit operations*. We denote Σ a set of pseudoidentites. Then $[\![\Sigma]\!]$ is a class of all semigroups satisfying all pseudoidentities from Σ. Omitting for now what an implicit operation is, we state the Reiterman theorem.

Theorem 2 (Reiterman, 1982)**.** *Class* V *of finite semigroups is pseudovariety if and only if there exists a set of pseudoidentities* Σ *such that* $\mathsf{V} = [\![\Sigma]\!]$*.*

Further, we define an operation for pseudovarieties of groups, *bar*.

Definition 3. Let H be pseudovariety of finite groups. Then $\bar{\mathsf{H}}$ is a pseudovariety of semigroups such that their subgroups belong to H.

2. Irreducibility

Definition 4. Pseudovariety V is *irreducible* if for any two pseudovarieties U, W holds

$$\mathsf{V} = \mathsf{U} \vee \mathsf{W} \Longrightarrow \mathsf{V} = \mathsf{U} \text{ or } \mathsf{V} = \mathsf{W},$$

where $\mathsf{U} \vee \mathsf{W}$ is the *join* of pseudovarieties, i.e., the supremum in the lattice of pseudovarieties (the smallest pseudovariety containg them both).

Now we introduce one of the tools to show some pseudovariety is irreducible. We denote S^1 smallest monoid containing S.

Definition 5. Let S and T be finite semigroups and $f\colon S^1 \to T^1$ be a function. On the set

$$M(S,T,f) = S \sqcup S^1 \times T^1 \times S^1$$

we define multiplication $\cdot$ for all $s, r \in S, s_1, s_1', s_2, s_2' \in S^1$ and $t, t' \in T^1$:

$$\begin{aligned} s \cdot r &= sr \\ s \cdot (s_1, t, s_2) &= (ss_1, t, s_2) \\ (s_1, t, s_2) \cdot s &= (s_1, t, s_2 s) \\ (s_1, t, s_2) \cdot (s_1', t', s_2') &= (s_1, tf(s_2 s_1')t', s_2'), \end{aligned}$$

and call it *Rees extension semigroup of S and T.*

Definition 6. For pseudovarieties U, V denote $\mathsf{U} \bullet \mathsf{V}$ pseudovariety generated by all Rees extention semigroups $M(S,T,f)$, where $S \in \mathsf{U}$ and $T \in \mathsf{V}$. We say that pseudovariety V is *bullet idempotent* if $\mathsf{V} = \mathsf{V} \bullet \mathsf{V}$.

Lemma 7. *Pseudovariety of groups* H *satisfies* $\bar{\mathsf{H}} = \bar{\mathsf{H}} \bullet \bar{\mathsf{H}}$.

Now we state the main result.

Theorem 8 (Almeida, Klíma, 2011)**.** *Let* V *be a bullet idempotent pseudovariety. Then* V *is irreducible.*

Corollary. *Pseudovariety* $\bar{\mathsf{H}}$ *is irreducible.*

Going further, it can be shown that

$$\mathsf{V} \bullet \mathsf{V} = \mathsf{V} \iff \mathsf{V} = \overline{\mathsf{V} \cap \mathsf{G}},$$

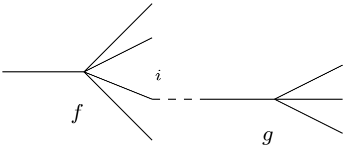
where G is the pseudovariety of all groups.

Operads and algebras over operads

Lada Peksová

Operads could be understood as an abstraction of composable functions.

Given functions $f\colon X^{\times n} \to X$ and $g\colon X^{\times m} \to X$, one may consider for $1 \leq i \leq n$ their composition $f(id,\dots,g,id,\dots,id)\colon X^{\times(m+n-1)} \to X$ where g is on the i-th place. This could be schematically illustrated by the following picture.



When composing several functions it obviously shouldn't matter in which order we realize these compositions. We can also consider a permutation of variables. And in such a case we want some kind of equivarinace[1]. And sometimes we also want to consider the identity map.

These observations lead us to the definition of operad:

Definition 1. An **operad** in category of $\mathbb{K}$-modules is a collection $P = \{P(n)\}_{n\geq 0}$ of right $\mathbb{K}[\Sigma_n]$-modules where Σ_n is symmetric group together with $\mathbb{K}$-linear maps called composition maps

$$\circ_i\colon P(m)\otimes P(n) \to P(m+n-1) \tag{1}$$

(where $1 \leq i \leq m$ and $0 \leq n$) such that the following two axioms are satisfied:

- **Associativity:** For each $1 \leq j \leq m$, $0 \leq n, 0 \leq k$ and $f \in P(m)$, $g \in P(n)$, $h \in P(k)$

$$(f \circ_i g) \circ_j h = \begin{cases} (f \circ_j h) \circ_{i+k-1} g & \text{if } 1 \leq j < i \\ f \circ_i (g \circ_{j-i+1} h) & \text{if } i \leq j < n+i \\ (f \circ_{j-n+1} h) \circ_i g & \text{if } i+n \leq j \leq m+n-1 \end{cases} \tag{2}$$

- **Equivariance:** For each $1 \leq i \leq m$, $0 \leq n$, $\tau \in \Sigma_m$ and $\sigma \in \Sigma_n$ let $\tau \circ_i \sigma$ be the permutation where pairs

$$(i, \tau \circ_i \sigma(i)), (i+1, \tau \circ_i \sigma(i+1)), \dots (i+n, \tau \circ_i \sigma(i+n))$$

corresponds to σ inserted on i-th place of τ[2]. Then for $f \in P(m), g \in P(n)$ we require

$$(f\tau) \circ_i (g\sigma) = \big(f \circ_{\tau(i)} g\big)(\tau \circ_i \sigma) \tag{3}$$

where the action of $\tau \in \Sigma_m$ on an element $f \in P(m)$ is denoted as $f\tau$.

[1] In this case, it means that the composition of functions with permuted variables should be the same as making first the composition and then applying some appropriate permutation.

[2] For example if we take permutation $\tau = (4,1,3,2) \in \Sigma_4$ and $\sigma = (2,1,3) \in \Sigma_3$ and insert σ as second argument of τ we get $\tau \circ_2 \sigma = (2,5,4,6,3,1) \in \Sigma_6$.

- **Unitality:** There exists $e \in P(1)$ such that for $f \in P(m)$ and $1 \leq i \leq m$: $f \circ_i e = f$. And for $g \in P(n)$: $e \circ_1 g = g$.

(The definitions and other constructions could be in most cases done for a general commutative ring K. We suggestively denote this ring in the same way as it is usual for a field of characteristic zero. This is because we mostly work with special K-modules, vector spaces.)

The definition of a homomorphism of operads is what one would intuitively think of.

And even not knowing, we are already familiar with one example of operads:

An *endomorphism operad* is a collection $End_V = \{End_V(n)\}_{n \geq 0}$ for a $\mathbb{K}$-module V (vector space) such that $End_V(n) = Hom_{\mathbb{K}}\left(V^{\otimes n}, V\right)$. For elements $f \in End_V(m)$ and $g \in End_V(n)$ is the composition defined as

$$f \circ_i g = f\left(\underbrace{\mathbb{1}_V \otimes \ldots \otimes \mathbb{1}_V}_{i-1 \text{ times}} \otimes g \otimes \mathbb{1}_V \otimes \ldots \otimes \mathbb{1}_V\right)$$

where $\mathbb{1}_V$ denotes identity morphism on V. The symmetric group action is defined as

$$(f\sigma)(v_1, v_2, \ldots v_m) = f\left(v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots v_{\sigma^{-1}(m)}\right)$$

where $v_1, v_2, \ldots v_m \in V$ and $\sigma \in \Sigma_m$.

But there are also other operads capturing the concepts of associativity, commutativity, Lie bracket structure…

Now, the homomorphism of operads $P \rightarrow End_V$ will give us an “evaluation” of an operad on the vector space V (given by the endomorphism operad). For example, for operad *Com* capturing commutativity, this gives us the usual commutative algebra.

Curvature and Cohomology

Josef Svoboda

In the lecture, I will start with basic notions of differential geometry. Then I will explain what is a circle bundle and its curvature and finally present basic topological T-duality.

1. Vector and forms

Definition 1. *Tangent vector X_p at point p of a surface S in $\mathbb{R}^3$ is a vector in tangent plane of S in p. For every function $f\colon S \to R$ defined around p, it gives the directional derivative $X_p(f)$ (real number) of f at point p.*

General variety M is not naturally embedded in Euclidean space $\mathbb{R}^n$, so we define *tangent vector* X in $p \in M$ as a "directional derivative", that is a linear map from real functions around p to $\mathbb{R}$ satisfying Leibniz rule:

$$X_p(fg) = X_p(f)g + fX_p(g).$$

Vector field is a smooth choice of tangent vectors in every point p of M.

Definition 2. *Differential form of degree k (k-form in p)* at p takes k tangent vectors in p and gives a real number so that it is linear in each variable and antisymmetric. Differential *k-form* on M is a smooth choice of k-form in every point p of M. Set of k-forms is denoted $\Omega^k(M)$, set of all forms $\Omega(M)$.

For any function f on M we have 1-form *df* defined by $df(V) = V(f)$ (directional derivative of f in the direction of V).

Definition 3. De Rham differential d (exterior derivative) is a unique map from $\Omega(M) \to \Omega(M)$ of degree one which is linear, it gives usual *df* on functions and satisfies Leibniz rule with respect to wedge product.

We can integrate k-forms over (oriented) k-dimensional objects (roughly we feed the k-form by k tangent vectors and get a function which we integrate).

Theorem 4 (Stokes)**.** *Integral of a differential form ω over the boundary of an orientable manifold M is equal to the integral of its exterior derivative d over the whole of M:*

$$\int_{\partial M} \omega = \int_M d\omega$$

2. Bundles

Bundle over M is a smooth choice of some type of object at every point of M. More formally it is a manifold P with a smooth map $\pi\colon P \to M$.

Example. (1) Vector bundle is a bundle so that at every point we have a vector space e.g. bundle consisting of all tangent vectors.

(2) Circle bundle is a bundle so that at every point there is a circle – e.g. circle of every possible "directions" – tangent vectors of length 1 on a Riemannian manifold M.

(3) We have trivial circle bundle $S^1 \times S^2 \to S^2$. An example of a nontrivial circle bundle is Hopf fibration $S^3 \to S^2$.

Theorem 5 (Gysin sequence). *For a fiber oriented circle bundle $P \to M$ with curvature F there is a long exact sequence:*

$$\cdots \longrightarrow H^k(M) \xrightarrow{\pi^*} H^k(P) \xrightarrow{\pi_*} H^{k-1}(M) \xrightarrow{\wedge F} H^{k+1}(M) \longrightarrow \ldots$$

where π_* is the pullback, π_* is the integration along fiber and $\wedge F$ is the wedge product with curvature.

Theorem 6 (Topological T-duality). *For every circle bundle $P \to M$ with curvature 2-form F and with a 3-form H on P there is a dual circle bundle $\hat{P} \to M$ with curvature form $\hat{F}$ and a three form $\hat{H}$ such that $\hat{F} = \pi_* H$ and $F = \pi_* \hat{H}$.*

Löb's Theorem and Self-Modifying Agents

Anna Gajdová

1. Introduction

Let's start with a paradox: *If this sentence is true, then Santa Claus exists.*

In this talk we will explore what does this paradox have to do with agents that are able to self-modify themselves.

2. Preliminaries

We will informally define some basic notions from mathematical logic.

A *formula* in the language of arithmetic is a well-formed expression using natural numbers, symbols $<, \cdot, +, =, \neg, \wedge, \vee, \rightarrow, \forall, \exists$, (,), a false symbol $\bot$, a true symbol $\top$ and a set of variables, e.g. $(\forall x)(x > 5) \wedge (x < 3)$ is a formula.

A *sentence* is a formula which has only variables that are quantified.

A *theory* is a set of sentences which are called *axioms*.

The theory of *Peano Arithmetic* (PA) is a theory given by the *Peano Axioms* which describe the properties of natural numbers, e.g. $(x + 1 = y + 1) \rightarrow (x = y)$.

We say that that a theory *$\mathcal{T}$ proves a formula ϕ* if we can derive ϕ from the axioms using some *rules of inference*, e.g. from $x \rightarrow y$ and $y \rightarrow z$ we can infer $x \rightarrow z$. We will denote this by $\mathcal{T} \vdash \phi$.

We will denote the existence of *a proof of a formula ϕ* by $\Box[\phi]$.

3. Gödel & Löb

Definition 1 (Consistency)**.** We say that a theory $\mathcal{T}$ is inconsistent if $\mathcal{T}$ proves the constant false sentence $\bot$:

$$\mathcal{T} \vdash \bot.$$

Otherwise we say that $\mathcal{T}$ is consistent.

Theorem 2 (Gödel's Second Incompleteness Theorem)**.** *If any theory $\mathcal{T}$ that is at least as powerful as Peano Arithmetic proves its own consistency then $\mathcal{T}$ is inconsistent:*

$$\mathcal{T} \vdash \neg\Box[\bot] \Rightarrow \mathcal{T} \vdash \bot.$$

Theorem 3 (Löb's Theorem)**.** *For any theory $\mathcal{T}$ that is at least as powerful as Peano Arithmetic and for any formula ϕ holds, that if $\mathcal{T}$ proves "If $\mathcal{T}$ proves ϕ than ϕ is true" than $\mathcal{T}$ proves ϕ:*

$$(\mathcal{T} \vdash (\Box[\phi] \rightarrow \phi)) \Rightarrow \mathcal{T} \vdash \phi.$$

4. Self-Modifying Agents

Definition 4 (Intelligent agent)**.** An intelligent agent is a goal oriented entity that acts upon the observation of its environment.

ADC-forms

Pavel Francírek

The aim of this talk is to introduce ADC-forms and to show how they can be useful for solving certain problems concerning the representation of integers by quadratic forms.

1. Representation of integers by quadratic forms

Definition 1. An integer m is (rationally) *represented* by an n-ary quadratic form $f \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ if there exists $u \in \mathbb{Q}^n$ such that

$$f(u) = m.$$

Moreover, if $u \in \mathbb{Z}^n$, we say that the integer m is *integrally represented* by the form f.

Note. The problem of (rational) representaion is completely resolved by the famous Hasse-Minkowski theorem.

Definition 2. An n-ary quadratic form $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ is an *ADC-form* if for all $a \in \mathbb{Z}$ the following holds:

$$a \text{ is represented by } f \Leftrightarrow a \text{ is integrally represented by } f.$$

Definition 3. A quadratic form $f \in \mathbb{Z}[x_1, \dots, x_n]$ is called *Euclidean* if for every $u \in \mathbb{Q}^n \smallsetminus \mathbb{Z}^n$ there exists $v \in \mathbb{Z}^n$ such that $0 < |f(u - v)| < 1$.

Proposition 4 (Aubry-Davenport-Cassels)**.** *Every Euclidean quadratic form is an ADC-form.*

To give an example of Euclidean form (thus ADC-form by Proposition 4) consider the form

$$\sum_{i=1}^{r} a_i x_i^2 - \sum_{i=r+1}^{k} a_i x_i^2$$

with $a_i \in \mathbb{N}$. It is not hard to see that this form is Euclidean if it is anisotropic and

$$\sum_{i=1}^{r} a_i \leq 3 \text{ and } \sum_{i=r+1}^{k} a_i \leq 3.$$

Using this observation, Proposition 4 and the Hasse-Minkowski theorem we can easily resolve some of classical problems: e.g. we can prove the Legendre's three-square theorem or we can show which integers are integrally represented by the form $x^2 + ny^2$ for $n \in \{\pm 1, \pm 2, -3\}$.

2. Binary quadratic forms

Let q be an odd prime number. We shall study the binary quadratic form

$$F_q(x, y) = x^2 - qy^2.$$

If F_q is an ADC-form then the class number of $\mathbb{Q}(\sqrt{q})$ is 1.

Note. For $q \equiv 3 \pmod 4$ the converse is also true.

We shall prove the following proposition:

Proposition 5. *Let $q \equiv 3 \pmod 4$ be a prime number. The form F_q is an ADC-form if and only if for every odd prime number $p < \sqrt{q}$ satisfying $\left(\frac{q}{p}\right) = 1$ the form F_q integrally represents $(-1)^{\frac{p-1}{2}} p$.*

Corollary. *Let $q \equiv 3 \pmod 4$ be a prime number. If $\left(\frac{q}{p}\right) = -1$ for every odd prime $p < \sqrt{q}$ then F_q is an ADC-form.*

p-adic numbers

Eva Hainzl

This talk will provide an introduction to the p-adic numbers $\mathbb{Q}_p$ which play a significant role in modern number theory and which will come up in a subsequent talk.
First, we will take an analytic approach and introduce $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to a newly defined metric d_p. Further on, we will explore algebraic properties of $\mathbb{Q}_p$, solve quadratic equations and eventually discuss *Hensel's lemma.*

1. p-adic numbers as a completion of $\mathbb{Q}$

Let p be a prime number. The p-adic order (or p-adic valuation) of $x \in \mathbb{Z}$ is defined as

$$\nu_p\, x = \begin{cases} \max\{n \in \mathbb{N} : \ p^n \mid x\} & \text{if } x \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

The definition can be extended to the rational numbers. For $x = \frac{a}{b} \in \mathbb{Q}$, define

$$\nu_p\, x = \nu_p\, a - \nu_p\, b$$

The p-adic absolute value of $x \in \mathbb{Q}$ is defined as

$$|x|_p = \begin{cases} p^{-\nu_p x} & \text{if } x \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

The p-adic absolute value induces an ultrametric $d_p(x, y) = |x - y|_p$ on $\mathbb{Q}$. We define the p-adic numbers, denoted by $\mathbb{Q}_p$, as the completion of the metric space $(\mathbb{Q}, d_p)$.
The ring of integers is defined as $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

2. algebraic properties of $\mathbb{Q}_p$

Conversely, we could have defined the p-adic integers $\mathbb{Z}_p$ as sequences $(a_n)_{n\geq 1}$, where $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ and $a_n \equiv a_m \mod p^n$, for $n \leq m$. Consequently,

$$\mathbb{Z}_p \hookrightarrow \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$$

After checking that $\mathbb{Z}_p$ is a ring without zero divisors, we would obtain $\mathbb{Q}_p$ as the field of fractions on $\mathbb{Z}_p$.

It is easy to see, that $\mathbb{Z}$ can be embedded into $\mathbb{Z}_p$. In fact, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and the ring of p-adic integers is uncountable.

Lemma 1. *Every $x \in \mathbb{Q}_p$ has a unique representation*

$$x = b_{-n_0}p^{-n_0} + \dots + b_0 + b_1 p + \dots b_n p^n + \dots = \sum_{n\geq n_0} b_n p^n$$

with $0 \leq b_n \leq p - 1$ for all $n \geq -n_0$ and $-n_0 = \nu_p\, x$.

Theorem 2 (Hensel's lemma). *Let* $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ *be a polynomial whose coefficients are in* $\mathbb{Z}_p$*. Suppose there exists a p-adic integer* α_1 *such that*

$$F(\alpha_1) \equiv 0 \mod p \qquad \textit{and} \qquad F'(\alpha_1) \not\equiv 0 \mod p$$

Then there exists a unique p-adic integer α *such that*

$$F(\alpha) = 0 \qquad \textit{and} \qquad \alpha \equiv \alpha_1 \mod p$$

Hilbert symbols

Pavel Surý

We will introduce Hilbert symbols, which can be considered as a generalisation of Legendre symbols. Without going through technical details, we will highlight the basic properties and Hilbert reciprocity.

We say that a positive definite quadratic form is universal, if it represents all natural numbers. We will use Hilbert reciprocity to show that no ternary positive definite quadratic form is universal.

1. Hilbert symbols

Definition 1. Let $F = \mathbb{Q}_p$ or $F = \mathbb{R}$. Let $a, b \in F$. We define the Hilbert symbol of a and b relative to the field F as

$$(a,b)_F = \begin{cases} 1, & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } F, \\ -1, & \text{otherwise.} \end{cases} \tag{1}$$

Basic properties.

- If a is a square, then $(a, b) = 1$ for any b.
- We have $(a, b) = (b, a)$ for any a, b.
- Multiplicativity in the form $(a, bc) = (a, b)(a, c)$. (difficult)

Theorem 2 (Hilbert reciprocity). *For every $a, b \in \mathbb{Q}^\star$, we have*

$$\prod_F (a,b)_F = 1,$$

where we take a product over all fields $\mathbb{Q}_p$, p prime, and $\mathbb{R}$.

2. No ternary positive definite quadratic form is universal

Definition 3. A n-ary quadratic form over a ring R is a polynomial of degree 2 of the form $q(x_1, \ldots, x_n) = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j$ with $a_{ij} \in R$.

- A quadratic form is positive definite, if $q(⊕) > 0$ for every $⊕ \neq 0$.
- A quadratic form is integral, if $R = \mathbb{Z}$.
- An integral quadratic form q is universal if it represents all positive integers over $\mathbb{Z}$. Formally, for every $k \in \mathbb{N}$ there exist $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that $q(x_1, x_2, \ldots, x_n) = k$.

Theorem 4. *No positive definite ternary integral quadratic form is universal.*

Proof. For contradiction, we will assume such form $q(x, y, z)$.

(1) We notice that q as a rational form is still positive definite and universal.
(2) We will obtain an equivalent diagonal form $d(x, y, z) = ax^2 + by^2 + cz^2$.
(3) From positive definiteness we conclude that $(-a/c, -b/c)_{\mathbb{R}} = -1$.
(4) From Hilbert reciprocity we obtain a prime p such that $(-a/c, -b/c)_{\mathbb{Q}_p} = -1$.

(5) We conclude that $d(x, y, z) = 0$ has only trivial solution in $\mathbb{Q}_p$.

(6) We notice that $d(x, y, z)$ as a p-adic form represents all p-adic numbers.

(7) In particular, we will see that $d(x, y, z)$ is equivalent in $\mathbb{Q}_p$ to $-abcx^2 + y^2 - z^2$.

(8) We will get a contradiction with (5), as this form represents 0 non-trivially.

□

Gelfand-Tsetlin Bases for Representations of the Symmetric Group

Petr Zima

The Schur-Weyl duality relates representation theories of the symmetric group $\mathsf{S}(k)$ and the general linear group $\mathsf{GL}(V)$ of a vector space V by considering their mutually commuting actions on the kth tensor power $V^{\otimes k}$ of V. A classical approach to describing irreducible components of $V^{\otimes k}$ is based on an explicit construction of suitable idempotents in the group algebra $\mathbb{Q}[\mathsf{S}(k)]$ called Young symmetrizers. Although effective this approach is indirect and gives only a limited insight into the role of *Young diagrams* which parametrize irreducible representations of $\mathsf{S}(k)$.

We review an alternative approach introduced by Okounkov and Vershik in [OV96]. They consider the whole chain of symmetric groups

$$\{1\} = \mathsf{S}(1) \subset \mathsf{S}(2) \subset \ldots \subset \mathsf{S}(k) \subset \ldots$$

and inductively construct the so called *Gelfand-Tsetlin bases* of the irreducible representations. These bases can be characterized as common eigenvectors of the Gelfand-Tsetlin algebra $\mathsf{GT}(k)$ which is a maximal commutative subalgebra in $\mathbb{Q}[\mathsf{S}(k)]$. This way the Young diagrams arise naturally from the spectra of distinguished generators of $\mathsf{GT}(k)$.

In the second part of the talk we present the results of our ongoing work which aims at extending this approach to study the tensor products $V^{\otimes k} \otimes V^{\otimes l}$. In particular, our original motivation is decomposing the product of two tensors with given symmetries to individual components with different symmetries. Analogously to the construction of the Gelfand-Tsetlin algebra the key step is finding suitable commuting elements in the centralizer of $\mathsf{S}(k)$ and $\mathsf{S}(l)$ inside $\mathbb{Q}[\mathsf{S}(k+l)]$.

1. Young diagrams

Definition 1. A *partition* of a positive integer k is a nonincreasing sequence $(k_1, \ldots, k_r)$ of positive integers such that $k = k_1 + \cdots + k_r$. A *Young diagram* corresponding to a partition $(k_1, \ldots, k_r)$ is a collection of k boxes arranged in r left justified rows such that ith row has k_i boxes.

For example, the Young diagrams corresponding to (4), $(3,1)$ and $(2,2)$ are:

$$\begin{array}{|c|c|c|c|}\hline & & & \\ \hline \end{array} \qquad \begin{array}{|c|c|c|}\hline & & \\ \hline \multicolumn{1}{|c|}{} & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array} \qquad \begin{array}{|c|c|}\hline & \\ \hline & \\ \hline \end{array}$$

Definition 2. A *Young tableau* is obtained by filling in the boxes of the Young diagram by numbers $1, \ldots, k$. A Young tableau is *standard* if the numbers in each row and each column are increasing.

All the possible standard Young tableaux obtained from the above diagrams are:

$$\begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline \end{array} \qquad \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline \multicolumn{1}{|c|}{4} & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array} \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline \multicolumn{1}{|c|}{3} & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array} \quad \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline \multicolumn{1}{|c|}{2} & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array} \qquad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array}$$

Theorem 3. *Irreducible representations of the symmetric group $\mathsf{S}(k)$ are up to isomorphism in one-to-one correspondence with partitions of k, or equivalently, with Young diagrams with k boxes.*

The dimension of the irreducible representation V_D corresponding to a diagram D is given by the number of standard Young tableaux obtained from D.

For example, there is only one possible standard Young tableau for the partitions (k) and $(1, \dots, 1)$. Those partitions correspond to the one-dimensional *trivial* and *alternating* representation respectively.

2. Gelfand-Tsetlin bases

Let us denote by $[i_1 i_2 \dots i_p]$ the cyclic permutation

$$i_1 \to i_2 \to \cdots \to i_p \to i_1.$$

Definition 4. The *Jucys-Murphy elements* are the following elements in $\mathbb{Q}[\mathsf{S}(k)]$,

$$X_i = [1i] + [2i] + \cdots + [(i-1)i], \qquad i = 2, \dots, k.$$

In other words, X_i is the sum of all transpositions in $\mathsf{S}(i)$ minus the sum of all transpositions in $\mathsf{S}(i-1)$.

Lemma 5. *The Jucys-Murphy elements commute and hence are simultaneously diagonalizable on every representation of $\mathsf{S}(k)$. They generate the so called Gelfand-Tsetlin algebra $\mathsf{GT}(k)$ which is a maximal commutative subalgebra in $\mathbb{Q}[\mathsf{S}(k)]$.*

Definition 6. Given a Young tableau T let us define a function $c_T \colon \{1, \dots, k\} \to \mathbb{Z}$ such that $c_T(i)$ is the column number minus the row number of the box of T which contains i.

For example:

$$T = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 & 7 \\ \hline 6 & 8 & 9 \\ \hline \end{array} \qquad \Rightarrow \qquad c_T\colon \begin{array}{ccc} 1 \mapsto 0 & 2 \mapsto 1 & 4 \mapsto 2 \\ 3 \mapsto -1 & 5 \mapsto 0 & 7 \mapsto 1 \\ 6 \mapsto -2 & 8 \mapsto -1 & 9 \mapsto 0 \end{array}$$

Theorem 7. *Let V_D be the irreducible representation of $\mathsf{S}(k)$ corresponding to a Young diagram D. The eigenvalues of the Jucys-Murphy elements X_i are given by $c_T(i)$ where T runs through all the standard Young tableaux obtained from D.*

The corresponding common eigenspaces of X_i are all one-dimensional and the nonzero vectors v_T characterized up to a scalar multiple by

$$X_i(v_T) = c_T(i)\, v_T, \qquad i = 2, \dots, k,$$

form a basis of V_D called the Gelfand-Tsetlin basis.

References

[OV96] Okounkov, A., Vershik, A. A new approach to representation theory of symmetric groups. *Selecta Mathematica* **2**(4) (1996), 581–605.

[OV05] Okounkov, A., Vershik, A. A new approach to the representation theory of the symmetric groups. II. *Journal of Mathematical Sciences* **131**(2) (2005), 5471–5494.

[Ve06] Vershik, A. A new approach to the representation theory of the symmetric groups. III. Induced representations and the Frobenius-Young correspondence. *Moscow Mathematical Journal* **6**(3) (2006), 567–585.

[CST10] Ceccherini-Silberstein, T., Scarabotti, F., Tolli, F. *Representation theory of the symmetric groups: the Okounkov-Vershik approach, character formulas, and partition algebras.* Vol. 121. Cambridge University Press (2010).

Introduction to universal homogeneous structures

Martin Raška

On the example of Urysohn's universal metric space, we will address the basic questions regarding universal homogeneous structures – existence, uniqueness and embeddings.

Positional Numeral Systems in Quaternions

Jakub Krásenský

1. Outline

In the first part of the talk the general concept of position numeral systems will be discussed. We introduce an important example due to Walter Penney (1955) – using radix $-1+\mathrm{i}$ and digits 0 and 1, it is possible to represent every element of the ring $\mathbb{Z}[\mathrm{i}]$ (and by allowing negative powers of the radix the whole complex plane). We will discuss similar ideas and results about positional numeral systems with the GNS property (unique representation property), especially in the complex plane. In the second part, position numeral systems in quaternions will be explored, in particular in the ring of Hurwitz and Lipschitz integers. GNSs with the smallest possible alphabet will be described. For every Hurwitz and Lipschitz integer it will be determined whether it can or cannot serve as a radix of some number system.

2. Positional numeral systems

Having a ring R, nonzero *radix* $\beta \in R$ and a finite *alphabet* $A \subset R$ containing zero, we try to represent elements of R using the positional numeral system (β, A). *Representation* of a nonzero $x \in R$ is a string $a_N \cdots a_0$ such that

$$x = \sum_{\ell=0}^{N} a_\ell \beta^\ell,$$

where $a_N \neq 0$ and all $a_\ell \in A$.

As in any fixed numeral system the set of all possible representations is countable, most rings are not suitable for examination of numeral systems. We will mostly work with discrete subsets of complex numbers – the lattices of Gaussian and Eisenstein integers. We are interested in a special type of numerals systems:

Definition 1. A *GNS* (numeral system with uniqueness property) in R is a numeral system where every nonzero element of R has a unique representation.

Observe that even the binary and decimal systems are not GNSs in $\mathbb{Z}$ since they do not enable to represent negative numbers. The numeral system $(-1+\mathrm{i}, \{0,1\})$ proposed by Walter F. Penney in 1955 is a GNS in $\mathbb{Z}[\mathrm{i}]$ (as will be explained). There are basic conditions which have to be satisfied for every GNS:

Proposition 2. *For every GNS (β, A) the following holds:*

1. *The alphabet A is a complete residue system modulo β.*
2. *Neither β nor $\beta - 1$ is a unit.*

The second condition is the reason why there is no GNS with radix 2 and in $\mathbb{Z}[\mathrm{i}]$ there is no GNS with radix $1 \pm \mathrm{i}$. On the other hand, Gabrielle Steidl showed in 1989 that in $\mathbb{Z}[\mathrm{i}]$ for every other radix β, $|\beta| > 1$ there is an alphabet A such that (β, A) is a GNS.

3. In Quaternions

The algebra of quaternions, denoted by $\mathbb{H}$, is a four-dimensional vector space over $\mathbb{R}$ spanned by four elements 1, i, j, k where multiplication is defined by $\mathrm{ij} = -\mathrm{ji} = \mathrm{k}$, $\mathrm{jk} = -\mathrm{kj} = \mathrm{i}$, $\mathrm{ki} = -\mathrm{ik} = \mathrm{j}$. It shares many properties with the complex numbers, e.g. it is a field (albeit a non-commutative one).

The ring of *Lipschitz integers*, denoted by $\mathbb{L}$, consist of quaternions with integer coefficients. The ring of *Hurwitz integers*, denoted by $\mathbb{W}$, can be defined as $\mathbb{L} \cup (\mathbb{L} + \psi)$ where $\psi = (1 + \mathrm{i} + \mathrm{j} + \mathrm{k})/2$; the fact that is is closed under multiplication is not immediately obvious. However, this strangely defined ring has in fact better properties than $\mathbb{L}$, e.g. every left (or right) ideal is principal. Our aim is to examine positional numeral systems in these two rings.

The main result is the following analogy of Gabriele Steidl's result:

Proposition 3. *Both in $\mathbb{L}$ and in $\mathbb{W}$, the element β is radix of some GNS if and only if $|\beta - 1| \neq 1$ and $|\beta| \neq 1$.*

A much more immediate result shows that in quaternions there is no GNS which is as nice as Penney's number system $(-1 + \mathrm{i}, \{0, 1\})$ in complex numbers:

Observation 4. *(1) A two-element alphabet enables to express only a two-dimensional subset of $\mathbb{H}$.*

(2) The same holds for an alphabet $A \subset \mathbb{R}$.

(3) The alphabet of a GNS in $\mathbb{L}$ or $\mathbb{W}$ has always at least 4 digits.

Greedy expansions and property (F)

Magdaléna Tinková

In this talk, we will focus on different representations of numbers. In our daily life, we use a decimal system and all of us know a binary system using digits 0 and 1. However, we can also choose any real or complex number as a base to express all elements of $\mathbb{R}$ or $\mathbb{C}$. More precisely, our aim is to rewrite some number x as

$$x = \sum_{n=-\infty}^{N} a_n \beta^n$$

where $N \in \mathbb{Z}$. Number β is called a base and coefficients a_n belong to a finite set of digits $\mathcal{A}$, which includes zero and is called an alphabet. In this talk, we will restrict to real bases $\beta > 1$ and $\mathcal{A} = \{0, 1, \dots, \lceil \beta \rceil - 1\}$.

Number x can have one, two or even infinitely many representations using β and our fixed alphabet $\mathcal{A}$. We will mention some of them and, finally, we will discuss so-called greedy expansions, which, in some sense, are the largest among these representations. To give an instance, we will show how to recognize them using the special expansion of number 1.

If we add or multiply two integers, we get a number belonging to $\mathbb{Z}$. Applying these operations on some numbers with a finite number of nonzero digits after a decimal point also leads to a number with the same property. However, a sum or a product of two numbers with a finite greedy expansion, i.e., with an expansion ended with infinitely many zeros, may have a greedy expansion with infinitely many nonzero digits.

If this situation does not occur, we say that β has so-called property (F). In the final part of this talk, we will show several either sufficient or necessary conditions related to the fulfillment of this property.

Biases amongst products of two primes

Filip Bialas

There is much more small numbers in the form pq, where p, q are prime numbers both congruent with 3 modulo 4 than numbers with these prime numbers both congruent with 1 modulo 4.

In this talk we will recall Prime number theorem and similar theorem for primes in arithmetic progression without proofs and then use them to prove *asymptotic formula*, which will in special case help us understand, why there is more numbers of the first type than of the second.

1. Main section

Definition 1. *Prime number function* is the function $\pi\colon ⋬ \to \&$, $\pi(n) = |\{p \text{ prime}, p \leq n\}|$. More generally if $a, b \in \&, (a, b) = 1$, then we define $\pi_{a,b}\colon ⋬ \to \&$, $\pi_{a,b}(n) = |\{p \text{ prime}, p \leq n, p \equiv b \pmod{a}\}|$.

Theorem 2 (Prime number theorem)**.** *Following equality holds*

$$\lim_{x\to+\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

More generally if a, b are coprime positive integers, then

$$\lim_{x\to+\infty} \frac{\pi_{a,b}(x)}{\frac{x}{\ln(x)}} = \frac{1}{\varphi(a)},$$

where φ is the Euler function.

Definition 3. Let n be a positive integer. We call a function $\chi\colon ¦ \to ⊞$ a *Dirichlet character* modulo n, iff it is periodic with period of length n, $\chi(d) = 0 \Leftrightarrow (n, d) > 1$ and it is multiplicative ($\forall a, b \in ¦\colon \chi(a)\chi(b) = \chi(ab)$). If $\operatorname{Im}(\chi) = \{-1, 0, 1\}$ we call the Dirichlet character χ *quadratic.*

Theorem 4. *Let n be a positive integer and χ a quadratic Dirichlet character modulo n, then for $\eta \in \{-1, 1\}$ following asymptotic formula holds*

$$\frac{|\{pq \leq x : \chi(p) = \chi(q) = \eta\}|}{\frac{1}{4}|\{pq \leq x : (p, d) = (q, d) = 1\}|} = 1 + \eta\frac{\mathcal{L}_\chi + o(1)}{\log\log x},$$

where $\mathcal{L}_\chi = \sum \frac{\chi(p)}{p}$, where p, q are always primes and the sum is taken over all primes.

2. Conclusion

We can see, that the difference between number of products of two primes with values 1 in χ and the products of primes with values -1 in χ is surprisingly large – asymptotically proportional to a constant times function $\frac{1}{\log\log x}$.

Similar methods can be used for computing asymptotics for products of more primes or for primes in defined arithmetic progressions instead with the same quadratic Dirichlet character.

Schedule

Thursday 15th.

13:30	*Lunch*
14:30	**Tomáš Nagy**: Colouring knots
15:15	**Jana Bartoňová**: Polynomial Closure of Classes of Regular Languages
16:00	**Ondrej Bínovský**: Why is an elliptic curve a torus?
16:45	*Break*
17:00	**Jonatan Kolegar**: Pseudovarieties of semigroups and irreducibility
17:45	**Lada Peksová**: Operads and algebras over operads
18:00	**Jan Čížek**: Talk
19:15	*Dinner*

Friday 16th.

8:15	*Breakfast*
9:00	**Josef Svoboda**: Curvature and Cohomology
9:45	**Anna Gajdová**: Löb's Theorem and Self-Modifying Agents
10:30	*Break*
10:45	**Pavel Francírek**: ADC-forms
11:30	**Eva Hainzl**: p-adic numbers
12:15	**Pavel Surý**: Hilbert symbols
13:00	*Lunch*
14:45	*Trip*
19:15	*Dinner*
20:00	**Marian Kechlibar**: Talk
20:45	*Rump session*

Saturday 17th.

8:15	*Breakfast*
9:00	**Petr Zima**: Gelfand-Tsetlin Bases for Representations of the Symmetric Group
9:45	**Martin Raška**: Introduction to universal homogeneous structures
10:30	*Break*
10:45	**Jakub Krásenský**: Positional Numeral Systems in Quaternions
11:30	**Magdaléna Tinková**: Greedy expansions and property (F)
12:15	**Filip Bialas**: Biases amongst products of two primes
13:00	*Lunch*
14:45	*Puzzlehunt*
19:15	*Dinner*

Sunday 18th.

10:00	*Breakfast*