

SPECSEMINĀRS

ALGEBRĀ,
ALGORITMU TEORIJĀ
UN
KRIPTOGRĀFIJĀ

Specseminārs domāts studentiem, kas saprot:

Specseminārs domāts studentiem, kas saprot:

- lai būvētu komiskos kuģus, jābūt attīstītai metalurģijai

Specseminārs domāts studentiem, kas saprot:

- lai būvētu komiskos kuģus, jābūt attīstītai metalurģijai;
- metalurģija [nav](#) kosmisko kuģu būvniecība

Specseminārs domāts studentiem, kas saprot:

- lai būvētu komiskos kuģus, jābūt attīstītai metalurģijai;
- metalurģija **nav** kosmisko kuģu būvniecība;
- jaunu sakausējumu izgudrošana drīzāk ir **teorētiska** zinātne

Specseminārs domāts studentiem, kas saprot:

- lai būvētu komiskos kuģus, jābūt attīstītai metalurģijai;
- metalurģija **nav** kosmisko kuģu būvniecība;
- jaunu sakausējumu izgudrošana drīzāk ir **teorētiska** zinātne;
- mēs nenodarbosimies nedz ar kosmisko kuģu būvi, nedz metalurģiju.

Seminārs

būs noderīgs visiem tiem,

kas vēlas tuvāk iepazīties ar jautājumu loku,

kas šobrīd ir

Seminārs

būs noderīgs visiem tiem,

kas vēlas tuvāk iepazīties ar jautājumu loku,

kas šobrīd ir

aktuāls

diskrētajā matemātikā

saistībā ar

teorētisko datorzinātni.

Šis seminārs var ieinteresēt tos, kas

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā;
 - doktorantūrā

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā;
 - doktorantūrā;
- vēlas

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā;
 - doktorantūrā;
- vēlas
 - darboties zinātnē

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā;
 - doktorantūrā;
- vēlas
 - darboties zinātnē;
 - radīt jaunus rezultātus

Šis seminārs var ieinteresēt tos, kas

- grib turpināt mācības
 - maģistratūrā;
 - doktorantūrā;
- vēlas
 - darboties zinātnē;
 - radīt jaunus rezultātus;
 - būt teorētiskās domas avangardā.

Tiem,

kas grib zināt precīzāk par semināra tematiku,

piedāvāju slaidus no savas uzstāšanās

starptautiskā konferencē Francijā.

11th Mons Days
of Theoretical Computer Science
30th August – 2nd September, 2006, Rennes

Jānis Buls

University of Latvia

**FROM BI-IDEALS TO
PERIODICITY**

◇ The repetitions (periodicities) of strings (words)

$$a_0 a_1 \dots a_n \dots$$

◇ The repetitions (periodicities) of strings (words)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

◇ The repetitions (periodicities) of strings (words)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

- word combinatorics

◇ The repetitions (periodicities) of strings (words)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

- word combinatorics

as well as in applications

◇ The repetitions (**periodicities**) of strings (**words**)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

- word combinatorics

as well as in applications, such as

- string matching algorithms

◇ The repetitions (**periodicities**) of strings (**words**)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

- word combinatorics

as well as in applications, such as

- string matching algorithms,
- text compression

◇ The repetitions (**periodicities**) of strings (**words**)

$$a_0 a_1 \dots a_n \dots$$

are fundamental objects in

- word combinatorics

as well as in applications, such as

- string matching algorithms,
- text compression,
- molecular biology.

◆ ω -words (right infinite words)

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$
- is called an ω -word.

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$
- is called an ω -word.

◇ Notation.

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$
- is called an ω -word.

◇ Notation.

- Let $x_i = x(i)$ then $x = x_0x_1 \dots x_i \dots$

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$
- is called an ω -word.

◇ Notation.

- Let $x_i = x(i)$ then $x = x_0x_1 \dots x_i \dots$
- A^ω — the set of all ω -words in alphabet A

◆ ω -words (right infinite words)

- Let $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Any total map $x : \mathbb{N} \rightarrow A$
- is called an ω -word.

◇ Notation.

- Let $x_i = x(i)$ then $x = x_0x_1 \dots x_i \dots$
- A^ω — the set of all ω -words in alphabet A
- $A^\infty = A^* \cup A^\omega$

◇ Metric

◇ Metric

- We introduce in A^∞ the so called **prefix metric** d as follows.

◇ Metric

- We introduce in A^∞ the so called **prefix metric** d as follows.
- Let $x, y \in A^\infty$.

◇ Metric

- We introduce in A^∞ the so called **prefix metric** d as follows.
- Let $x, y \in A^\infty$.
- Then $d(x, y) = \inf\{2^{-|u|} \mid u \in \text{Pref}(x) \cap \text{Pref}(y)\}$.

◇ Metric

- We introduce in A^∞ the so called **prefix metric** d as follows.
- Let $x, y \in A^\infty$.
- Then $d(x, y) = \inf\{2^{-|u|} \mid u \in \text{Pref}(x) \cap \text{Pref}(y)\}$.
- Here $|u|$ — the **length** of word u

◇ Metric

- We introduce in A^∞ the so called **prefix metric** d as follows.
- Let $x, y \in A^\infty$.
- Then $d(x, y) = \inf\{2^{-|u|} \mid u \in \text{Pref}(x) \cap \text{Pref}(y)\}$.
- Here $|u|$ — the **length** of word u ;
- $\text{Pref}(x)$ — the set of all prefixes of x .

◆ A sequence of words $v_0, v_1, \dots, v_n, \dots$

- ◆ A sequence of words $v_0, v_1, \dots, v_n, \dots$
- is called a **bi-ideal sequence**

◆ A sequence of words $v_0, v_1, \dots, v_n, \dots$

● is called a **bi-ideal sequence**

● if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♦ A sequence of words $v_0, v_1, \dots, v_n, \dots$

• is called a **bi-ideal sequence**

• if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♣ The sequence $v_0, v_1, \dots, v_n, \dots$

◆ A sequence of words $v_0, v_1, \dots, v_n, \dots$

- is called a **bi-ideal sequence**

- if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♣ The sequence $v_0, v_1, \dots, v_n, \dots$

- is a bi-ideal sequence

♦ A sequence of words $v_0, v_1, \dots, v_n, \dots$

- is called a **bi-ideal sequence**

- if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♣ The sequence $v_0, v_1, \dots, v_n, \dots$

- is a bi-ideal sequence

- if and only if

♦ A sequence of words $v_0, v_1, \dots, v_n, \dots$

- is called a **bi-ideal sequence**

- if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♣ The sequence $v_0, v_1, \dots, v_n, \dots$

- is a bi-ideal sequence

- if and only if

- there exists a sequence of words $u_0, u_1, \dots, u_n, \dots$

♦ A sequence of words $v_0, v_1, \dots, v_n, \dots$

- is called a **bi-ideal sequence**

- if $\forall i \ v_{i+1} \in v_i A^* v_i$.

♣ The sequence $v_0, v_1, \dots, v_n, \dots$

- is a bi-ideal sequence

- if and only if

- there exists a sequence of words $u_0, u_1, \dots, u_n, \dots$

- such that

$$\begin{aligned} v_0 &= u_0, \\ v_{i+1} &= v_i u_{i+1} v_i. \end{aligned}$$

◆ A word $x \in A^\omega$ is called a **bi-ideal**

◆ A word $x \in A^\omega$ is called a **bi-ideal**

- if there exists a bi-ideal sequence $v_0, v_1, \dots, v_n, \dots$

- ◆ A word $x \in A^\omega$ is called a **bi-ideal**
- if there exists a bi-ideal sequence $v_0, v_1, \dots, v_n, \dots$
- such that $\lim_{i \rightarrow \infty} v_i = x$.

◆ A word $x \in A^\omega$ is called a **bi-ideal**

• if there exists a bi-ideal sequence $v_0, v_1, \dots, v_n, \dots$

• such that $\lim_{i \rightarrow \infty} v_i = x$.

◆ Let $u_0, u_1, \dots, u_n, \dots$ be a sequence of words such that

$$\begin{aligned}v_0 &= u_0, \\v_{i+1} &= v_i u_{i+1} v_i.\end{aligned}$$

◆ A word $x \in A^\omega$ is called a **bi-ideal**

- if there exists a bi-ideal sequence $v_0, v_1, \dots, v_n, \dots$

- such that $\lim_{i \rightarrow \infty} v_i = x$.

◆ Let $u_0, u_1, \dots, u_n, \dots$ be a sequence of words such that

$$v_0 = u_0,$$

$$v_{i+1} = v_i u_{i+1} v_i.$$

- Then we say that the bi-ideal x is **generated** by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

◆ Let $x \in A^\omega$ then $x[i, j + 1) = x_i x_{i+1} \dots x_j$

◆ Let $x \in A^\omega$ then $x[i, j + 1) = x_i x_{i+1} \dots x_j$

• A factor $u \in F(x)$ is called **recurrent**

if the set $\{ i \mid u = x[i, |u|) \}$ has not upper bound.

◆ Let $x \in A^\omega$ then $x[i, j + 1) = x_i x_{i+1} \dots x_j$

- A factor $u \in F(x)$ is called **recurrent**

if the set $\{ i \mid u = x[i, |u|) \}$ has not upper bound.

- A word $x \in A^\omega$ is called **recurrent**

if any of its factors is recurrent.

◆ Let $x \in A^\omega$ then $x[i, j + 1) = x_i x_{i+1} \dots x_j$

• A factor $u \in F(x)$ is called **recurrent**

if the set $\{ i \mid u = x[i, |u|) \}$ has not upper bound.

• A word $x \in A^\omega$ is called **recurrent**

if any of its factors is recurrent.

♣ A word is recurrent if and only if it is a bi-ideal.

◆ Let $v \in A^+$ and $v^0 = \lambda$, $v^{n+1} = v^n v$ then $v^\omega = \lim_{n \rightarrow \infty} v^n$

◆ Let $v \in A^+$ and $v^0 = \lambda$, $v^{n+1} = v^n v$ then $v^\omega = \lim_{n \rightarrow \infty} v^n$

• We say that $x \in A^\omega$ is **ultimately periodic**

if $x = uv^\omega$ for some $u \in A^*$, $v \in A^+$.

- ◆ Let $v \in A^+$ and $v^0 = \lambda$, $v^{n+1} = v^n v$ then $v^\omega = \lim_{n \rightarrow \infty} v^n$
- We say that $x \in A^\omega$ is **ultimately periodic** if $x = uv^\omega$ for some $u \in A^*$, $v \in A^+$.
 - If $u = \lambda$ the word v^ω is called **periodic** of period $p = |v|$.

◆ Let $v \in A^+$ and $v^0 = \lambda$, $v^{n+1} = v^n v$ then $v^\omega = \lim_{n \rightarrow \infty} v^n$

• We say that $x \in A^\omega$ is **ultimately periodic**

if $x = uv^\omega$ for some $u \in A^*$, $v \in A^+$.

• If $u = \lambda$ the word v^ω is called

periodic of period $p = |v|$.

♣ Let $x \in A^\omega$ be an ultimately periodic.

If x is a bi-ideal then x is periodic.

◆ It is said a factor u occurs **syndetically** in $x \in A^\omega$
if there exists an integer k such that

- ◆ It is said a factor u occurs **syndetically** in $x \in A^\omega$ if there exists an integer k such that in any factor of x of length k there is at least one occurrence of u

◆ It is said a factor u occurs **syndetically** in $x \in A^\omega$

if there exists an integer k such that

in any factor of x of length k

there is at least one occurrence of u , namely,

$$\exists k [v \in F(x) \wedge |v| = k \Rightarrow u \in F(v)]$$

◆ It is said a factor u occurs **syndetically** in $x \in A^\omega$

if there exists an integer k such that

in any factor of x of length k

there is at least one occurrence of u , namely,

$$\exists k [v \in F(x) \wedge |v| = k \Rightarrow u \in F(v)]$$

• A word x is called **uniformly recurrent**

when all its factors occur syndetically in x .

◆ It is said a factor u occurs **syndetically** in $x \in A^\omega$

if there exists an integer k such that

in any factor of x of length k

there is at least one occurrence of u , namely,

$$\exists k [v \in F(x) \wedge |v| = k \Rightarrow u \in F(v)]$$

• A word x is called **uniformly recurrent**

when all its factors occur syndetically in x .

♣ If $x \in A^\omega$ is uniformly recurrent then x is a bi-ideal.

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

- The bi-ideal x is called **finitely generated** if

$$\exists m \forall i \forall j (i \equiv j \pmod{m} \Rightarrow u_i = u_j).$$

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

- The bi-ideal x is called **finitely generated** if

$$\exists m \forall i \forall j (i \equiv j \pmod{m} \Rightarrow u_i = u_j).$$

We say in this situation m -tuple $(u_0, u_1, \dots, u_{m-1})$

generates the bi-ideal x .

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

• The bi-ideal x is called **finitely generated** if

$$\exists m \forall i \forall j (i \equiv j \pmod{m} \Rightarrow u_i = u_j).$$

We say in this situation m -tuple $(u_0, u_1, \dots, u_{m-1})$

generates the bi-ideal x .

♣ If $x \in A^\omega$ is finitely generated

then x is uniformly recurrent.

◆ The factor v is called a **suffix** of $w \in A^*$
if $w = uv$ for any $u \in A^*$.

$\text{Suff}(w)$ — the set of all suffixes of w .

♦ The factor v is called a **suffix** of $w \in A^*$

if $w = uv$ for any $u \in A^*$.

$\text{Suff}(w)$ — the set of all suffixes of w .

♣ If $\bigcup_{i=0}^{m-1} \text{Pref}(u_i)$ or $\bigcup_{i=0}^{m-1} \text{Suff}(u_i)$

has at least two words with one and the same length

♦ The factor v is called a **suffix** of $w \in A^*$

if $w = uv$ for any $u \in A^*$.

$\text{Suff}(w)$ — the set of all suffixes of w .

♣ If $\bigcup_{i=0}^{m-1} \text{Pref}(u_i)$ or $\bigcup_{i=0}^{m-1} \text{Suff}(u_i)$

has at least two words with one and the same length

then a bi-ideal generated by $(u_0, u_1, \dots, u_{m-1})$

is not ultimately periodic.

♣ Let A be an alphabet and every letter $a \in A$ is chosen with one and the same probability $p(a) = \frac{1}{|A|}$.

♣ Let A be an alphabet and every letter $a \in A$ is chosen with one and the same probability $p(a) = \frac{1}{|A|}$.

Let p be a probability that a bi-ideal generated by (u_0, u_1, \dots, u_m) is ultimately periodic.

♣ Let A be an alphabet and every letter $a \in A$ is chosen with one and the same probability $p(a) = \frac{1}{|A|}$.

Let p be a probability that a bi-ideal generated by (u_0, u_1, \dots, u_m) is ultimately periodic.

If $\forall i |u_i| \geq n$ then $p \leq \frac{1}{|A|^{mn}}$.

♣ Let A be an alphabet and every letter $a \in A$ is chosen with one and the same probability $p(a) = \frac{1}{|A|}$.

Let p be a probability that a bi-ideal generated by (u_0, u_1, \dots, u_m) is ultimately periodic.

If $\forall i |u_i| \geq n$ then $p \leq \frac{1}{|A|^{mn}}$.

• Let $A = \{0, 1\}$ and $m = n = 10$

then probability $p \leq \frac{1}{2^{100}}$.

- Let x be a bi-ideal generated by $(0, 010)$

- Let x be a bi-ideal generated by $(0, 010)$ then

$$v_0 = 0,$$

$$v_1 = 00100,$$

$$v_2 = 00100000100,$$

$$v_3 = 0010000010001000100000100,$$

· · ·

$$x = \lim_{i \rightarrow \infty} v_i.$$

- Let x be a bi-ideal generated by $(0, 010)$ then

$$v_0 = 0,$$

$$v_1 = 00100,$$

$$v_2 = 00100000100,$$

$$v_3 = 0010000010001000100000100,$$

· · ·

$$x = \lim_{i \rightarrow \infty} v_i.$$

- This bi-ideal is not periodic

- Let x be a bi-ideal generated by $(0, 010)$ then

$$v_0 = 0,$$

$$v_1 = 00100,$$

$$v_2 = 00100000100,$$

$$v_3 = 0010000010001000100000100,$$

· · ·

$$x = \lim_{i \rightarrow \infty} v_i.$$

- This bi-ideal is not periodic nevertheless

$$\text{Pref}\{0, 010\} = \{0, 01, 010\},$$

$$\text{Suff}\{0, 010\} = \{0, 10, 010\},$$

- Let x be a bi-ideal generated by $(0, 010)$ then

$$v_0 = 0,$$

$$v_1 = 00100,$$

$$v_2 = 00100000100,$$

$$v_3 = 0010000010001000100000100,$$

· · ·

$$x = \lim_{i \rightarrow \infty} v_i.$$

- This bi-ideal is not periodic nevertheless

$$\text{Pref}\{0, 010\} = \{0, 01, 010\},$$

$$\text{Suff}\{0, 010\} = \{0, 10, 010\},$$

namely, these sets contain the words with different size only.

- Let $w \in A^+$ and $w^* = \bigcup_{n=0}^{\infty} \{w^n\}$.

- Let $w \in A^+$ and $w^* = \bigcup_{n=0}^{\infty} \{w^n\}$.
- ♣ The bi-ideal generated by the tuple $(u_0, u_1, \dots, u_{m-1})$ is **periodic**

- Let $w \in A^+$ and $w^* = \bigcup_{n=0}^{\infty} \{w^n\}$.
- ♣ The bi-ideal generated by the tuple $(u_0, u_1, \dots, u_{m-1})$ is **periodic** if and only if

- Let $w \in A^+$ and $w^* = \bigcup_{n=0}^{\infty} \{w^n\}$.
- ♣ The bi-ideal generated by the tuple $(u_0, u_1, \dots, u_{m-1})$ is **periodic** if and only if then

$$\exists w \forall i \in \overline{0, m-1} \quad u_i \in w^* .$$

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

- The bi-ideal x is called **bounded**

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

- The bi-ideal x is called **bounded** if

$$\exists l \forall i |u_i| \leq l.$$

◆ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

• The bi-ideal x is called **bounded** if

$$\exists l \forall i |u_i| \leq l.$$

♣ If $x \in A^\omega$ is bounded

then x is uniformly recurrent.

- Let x be a bi-ideal generated by sequence (u_i)

- Let x be a bi-ideal generated by sequence (u_i) , where

$$u_0 = 0,$$

$$u_1 = 1,$$

$$\forall i > 1 \quad u_i = 00100.$$

- Let x be a bi-ideal generated by sequence (u_i) , where

$$u_0 = 0,$$

$$u_1 = 1,$$

$$\forall i > 1 \quad u_i = 00100.$$

Then

- Let x be a bi-ideal generated by sequence (u_i) , where

$$\begin{aligned} u_0 &= 0, \\ u_1 &= 1, \\ \forall i > 1 \quad u_i &= 00100. \end{aligned}$$

Then

$$\begin{aligned} v_0 &= 0, \\ v_1 &= 010, \\ v_2 &= 010 00100 010, \\ v_3 &= 01000100010 00100 01000100010, \\ &\cdot \quad \cdot \quad \cdot \\ x &= \lim_{i \rightarrow \infty} v_i. \end{aligned}$$

- Thus x is the bounded bi-ideal

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.
- This demonstrates

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.
- This demonstrates that straightforward generalization

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.
- This demonstrates that straightforward generalization of Theorem

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.
- This demonstrates that straightforward generalization of Theorem
- ♣ The bi-ideal generated by the tuple $(u_0, u_1, \dots, u_{m-1})$ is **periodic** if and only if then

$$\exists w \forall i \in \overline{0, m-1} \quad u_i \in w^* .$$

- Thus x is the bounded bi-ideal,
- besides $x = (0100)^\omega$.
- This demonstrates that straightforward generalization of Theorem
- ♣ The bi-ideal generated by the tuple $(u_0, u_1, \dots, u_{m-1})$ is **periodic** if and only if then

$$\exists w \forall i \in \overline{0, m-1} \quad u_i \in w^* .$$

for bounded bi-ideals is not valid.

♣ Let x be a bi-ideal generated by the sequence

♣ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

♣ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

A bi-ideal x is **periodic**

♣ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

A bi-ideal x is **periodic**

if and only if

♣ Let x be a bi-ideal generated by the sequence

$$u_0, u_1, \dots, u_n, \dots$$

A bi-ideal x is **periodic**

if and only if

$$\exists n \in \mathbb{N} \exists u \exists v (v_n u \in v^* \wedge \forall i \in \mathbb{Z}_+ u_{n+i} \in uv^*).$$

**Thank You
very much!**