EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

CTU
CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

# SEMINAR

## Czech Institute of Informatics, Robotics and Cybernetics

**Lecturer:** Mathieu Chanavat
**Title:** Loops of Csörgő type and the AIM conjecture

**Project name:** Artificial Intelligence and Reasoning
**Project Registration Number:** CZ.02.1.01/0.0/0.0/15_003/0000466

**Venue:** CIIRC (room A-623) + Zoom
**Date:** 7. 7. 2021, 16:00 - 16:45

# Table of contents I

# Loops and definitions

# Definition

## Definition (Loop)

A loop $Q$ is a magma where:

- $\exists 1 \in Q \; \forall a \in Q, \quad a = 1 \cdot a = a \cdot 1$
- $\forall a, b \in A, \; \exists ! x, y \in Q, \quad a \cdot x = b \wedge \; y \cdot a = b$

Alternatively, if one considers $\forall q \in Q, \quad L_q : x \mapsto q \cdot x$ and $\forall q \in Q, \quad R_q : x \mapsto x \cdot q$, then

# Definition

## Definition (Loop)

A loop $Q$ is a magma where:

- $\exists 1 \in Q \; \forall a \in Q, \quad a = 1 \cdot a = a \cdot 1$
- $\forall a, b \in A, \; \exists! x, y \in Q, \quad a \cdot x = b \wedge y \cdot a = b$

Alternatively, if one considers $\forall q \in Q, \quad L_q : x \mapsto q \cdot x$ and $\forall q \in Q, \quad R_q : x \mapsto x \cdot q$, then

## Definition (Alternative definition)

A loop $Q$ is a magma where:

- $\exists 1 \in Q, \quad L_1$ and $R_1$ are identity functions.
- $\forall q \in Q, \quad L_q$ and $R_q$ are bijections.

# Inner Mapping Group

Let $Q$ be a loop.

**Definition (Multiplication and Inner Mapping Group)**

- $\mathrm{Mlt}(Q) = \langle L_q, R_q \mid q \in Q \rangle$
- $\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mlt}(Q) \mid \phi(1) = 1\}$

# Inner Mapping Group

Let $Q$ be a loop.

## Definition (Multiplication and Inner Mapping Group)

- $\mathrm{Mlt}(Q) = \langle L_q, R_q \mid q \in Q \rangle$
- $\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mlt}(Q) \mid \phi(1) = 1\}$

$\mathrm{Inn}(Q)$ is a generalization of $\mathrm{Inn}(G) = \{x \mapsto g^{-1}xg \mid g \in G\} \trianglelefteq \mathrm{Aut}(G)$.

# Nilpotency Class

Let $Q$ be a loop.

**Definition (Nucleus and Center)**

- $\mathrm{Nuc}(Q) = \{a \in Q \,|\, \forall x, y \in Q, \;\; ax \cdot y = a \cdot xy \;\wedge\; xa \cdot y = x \cdot ay \;\wedge\; xy \cdot a = x \cdot ya\}$
- $Z(Q) = \mathrm{Nuc}(Q) \cap \{a \in Q \mid x \in Q, \;\; a \cdot x = x \cdot a\}$

# Nilpotency Class

Let $Q$ be a loop.

## Definition (Nucleus and Center)

- $\mathrm{Nuc}(Q) = \{a \in Q \,|\, \forall x, y \in Q,\ \ ax \cdot y = a \cdot xy \wedge xa \cdot y = x \cdot ay \wedge xy \cdot a = x \cdot ya\}$
- $Z(Q) = \mathrm{Nuc}(Q) \cap \{a \in Q \mid x \in Q,\ \ a \cdot x = x \cdot a\}$

## Definition (Nilpotency Class)

$\mathrm{Nilp}(Q)$ is the smallest integer $n$ such that $Z_n(Q) = Q$, where:

- $Z_0 = \{1\}$
- $Z_{i+1} = \pi^{-1}(Z(Q/Z_i))$ where $\pi : Q \mapsto Q/Z_i$

# Nilpotency Class

Let $Q$ be a loop.

## Definition (Nucleus and Center)

- $\mathrm{Nuc}(Q) = \{a \in Q \,|\, \forall x, y \in Q, \;\; ax \cdot y = a \cdot xy \,\wedge\, xa \cdot y = x \cdot ay \,\wedge\, xy \cdot a = x \cdot ya\}$
- $Z(Q) = \mathrm{Nuc}(Q) \cap \{a \in Q \mid x \in Q, \;\; a \cdot x = x \cdot a\}$

## Definition (Nilpotency Class)

$\mathrm{Nilp}(Q)$ is the smallest integer $n$ such that $Z_n(Q) = Q$, where:

- $Z_0 = \{1\}$
- $Z_{i+1} = \pi^{-1}(Z(Q/Z_i))$ where $\pi : Q \mapsto Q/Z_i$

## Abelian, nilpotent

If $\mathrm{Nilp}(Q) = 1$ then $Q = Z_1 = \pi^{-1}(Z(Q/\{1\})) = Z(Q)$. That is, $Q$ is an abelian group.

# AIM conjecture and Csörgő Type Loops

# AIM Conjecture

Let Q be a loop.

**AIM Conjecture (weak version)**

If $\mathrm{Inn}(Q)$ is abelian then $\mathrm{Nilp}(Q) \leq 3$.

# AIM Conjecture

Let Q be a loop.

## AIM Conjecture (weak version)

If $\mathrm{Inn}(Q)$ is abelian then $\mathrm{Nilp}(Q) \leq 3$.

## Group theory equivalent

Let $G$ be a group.

- $\mathrm{Inn}(G) \simeq G/Z(G)$
- So $\mathrm{Nilp}(G) = 1 + \mathrm{Nilp}(\mathrm{Inn}(G))$
- If $\mathrm{Inn}(G)$ is abelian, then $\mathrm{Nilp}(G) = 1 + \mathrm{Nilp}(\mathrm{Inn}(G)) = 1 + 1 = 2$

# AIM Conjecture

Let Q be a loop.

## AIM Conjecture (weak version)

If $\mathrm{Inn}(Q)$ is abelian then $\mathrm{Nilp}(Q) \leq 3$.

## Group theory equivalent

Let $G$ be a group.

- $\mathrm{Inn}(G) \simeq G/Z(G)$
- So $\mathrm{Nilp}(G) = 1 + \mathrm{Nilp}(\mathrm{Inn}(G))$
- If $\mathrm{Inn}(G)$ is abelian, then $\mathrm{Nilp}(G) = 1 + \mathrm{Nilp}(\mathrm{Inn}(G)) = 1 + 1 = 2$

## Some result (Niemenmaa, 2009) [3]

If $\mathrm{Inn}(Q)$ is nilpotent then $\mathrm{Nilp}(Q)$ is finite.

# Csörgő Type Loops

**Initial AIM conjecture (false)**

If $\mathrm{Inn}(Q)$ is nilpotent then $\mathrm{Nilp}(Q) \leq 2$.

# Csörgő Type Loops

## Initial AIM conjecture (false)

If $\mathrm{Inn}(Q)$ is nilpotent then $\mathrm{Nilp}(Q) \leq 2$.

## Csörgő counter example

In 2004, Csörgő constructed a loop $C$ of order 128 such that [1]:

- $\mathrm{Inn}(C)$ is abelian

# Csörgő Type Loops

## Initial AIM conjecture (false)

If $\mathrm{Inn}(Q)$ is nilpotent then $\mathrm{Nilp}(Q) \leq 2$.

## Csörgő counter example

In 2004, Csörgő constructed a loop $C$ of order 128 such that [1]:

- $\mathrm{Inn}(C)$ is abelian
- $\mathrm{Nilp}(C) = 3$

# Csörgő Type Loops

## Initial AIM conjecture (false)

If $\mathrm{Inn}(Q)$ is nilpotent then $\mathrm{Nilp}(Q) \leq 2$.

## Csörgő counter example

In 2004, Csörgő constructed a loop $C$ of order 128 such that [1]:

- $\mathrm{Inn}(C)$ is abelian
- $\mathrm{Nilp}(C) = 3$

## Definition (Csörgő Type Loop)

A loop $Q$ is called a Csörgő type loop if

- $\mathrm{Inn}(C)$ is abelian
- $\mathrm{Nilp}(C) \geq 3$

# Open problems

**Is there a Csörgő type loop**

- of order less that 128?
- of odd order?
- of nilpotency class bigger than 3?

# Finding smaller Csörgő type loops: Cocycles, central and abelian extensions

# Central extensions

Let $A$ be an abelian group and $B$ be a loop.

## Definition (Central extension)

If $\theta : B \times B \mapsto A$, we can construct $A :_\theta B, = (A \times B, \cdot)$

- $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2 + \theta(b_1, b_2), b_1 + b_2)$

# Central extensions

Let $A$ be an abelian group and $B$ be a loop.

## Definition (Central extension)

If $\theta : B \times B \mapsto A$, we can construct $A :_\theta B, = (A \times B, \cdot)$

- $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2 + \theta(b_1, b_2), b_1 + b_2)$

If $\theta$ is such that $\forall x \in B,\ \ \theta(0, x) = \theta(x, 0) = 0$, then $A :_\theta B$ is a loop [4].

In this case, we call $\theta$ a cocycle.

# Central extensions

Let $A$ be an abelian group and $B$ be a loop.

## Definition (Central extension)

If $\theta : B \times B \mapsto A$, we can construct $A :_\theta B, = (A \times B, \cdot)$

- $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2 + \theta(b_1, b_2), b_1 + b_2)$

If $\theta$ is such that $\forall x \in B,\ \ \theta(0, x) = \theta(x, 0) = 0$, then $A :_\theta B$ is a loop [4].

In this case, we call $\theta$ a cocycle.

## Definition (Abelian extension)

A more general definition is abelian extension: If $\theta : B \times B \mapsto A$, $\phi, \psi : B \times B \mapsto \mathrm{Aut}(A)$, and $\Gamma = (\phi, \psi, \theta)$ we can construct $A :_\Gamma B, = (A \times B, \cdot)$ where

- $(a_1, b_1) \cdot (a_2, b_2) = (\phi_{b_1,b_2}(a_1) + \psi_{b_1,b_2}(a_2) + \theta(b_1, b_2), b_1 + b_2)$

# Central extensions

Let $A$ be an abelian group and $B$ be a loop.

## Definition (Central extension)

If $\theta : B \times B \mapsto A$, we can construct $A :_\theta B, = (A \times B, \cdot)$

- $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2 + \theta(b_1, b_2), b_1 + b_2)$

If $\theta$ is such that $\forall x \in B, \ \ \theta(0, x) = \theta(x, 0) = 0$, then $A :_\theta B$ is a loop [4].

In this case, we call $\theta$ a cocycle.

## Definition (Abelian extension)

A more general definition is abelian extension: If $\theta : B \times B \mapsto A$, $\phi, \psi : B \times B \mapsto \mathrm{Aut}(A)$, and $\Gamma = (\phi, \psi, \theta)$ we can construct $A :_\Gamma B, = (A \times B, \cdot)$ where

- $(a_1, b_1) \cdot (a_2, b_2) = (\phi_{b_1, b_2}(a_1) + \psi_{b_1, b_2}(a_2) + \theta(b_1, b_2), b_1 + b_2)$

If $\theta = 0$ and $\phi(b_1, b_2) = \mathrm{Id}_A$, we have, for a good choice of $\psi$, a semidirect product between $A$ and $B$.

# Constructing Csörgő type loops of nilpotency class 3

**Nilpotency class and iterated central extension [4]**

A loop is nilpotent if and only if it is an iterated central extension.

# Constructing Csörgő type loops of nilpotency class 3

**Nilpotency class and iterated central extension [4]**

A loop is nilpotent if and only if it is an iterated central extension.

Because our desired loops are nilpotent of class 3, we can hope (?) to construct them by taking three abelian groups $A, B$ and $C$, two cocycles $\theta$ and $\sigma$ and creating $C = A :_\theta (B :_\sigma C)$.

# Constructing Csörgő type loops of nilpotency class 3

## Nilpotency class and iterated central extension [4]

A loop is nilpotent if and only if it is an iterated central extension.

Because our desired loops are nilpotent of class 3, we can hope (?) to construct them by taking three abelian groups $A, B$ and $C$, two cocycles $\theta$ and $\sigma$ and creating $C = A :_\theta (B :_\sigma C)$.

## Smallest Csörgő type loops

Currently, the smallest known Csörgő type loops (constructed in [2]) can be decomposed as follow:

- $A = Z_2, B = Z_2 \times Z_2 \times D_8, C = Z_2$
- Then for some morphism $\phi : C \mapsto \mathrm{Aut}(B)$ and for some cocycle $\mu$, $C = A :_\mu (B \times_\phi C)$ is a Csörgő type loop of order 128.

# Constructing Csörgő type loops of nilpotency class 3

## Nilpotency class and iterated central extension [4]

A loop is nilpotent if and only if it is an iterated central extension.

Because our desired loops are nilpotent of class 3, we can hope (?) to construct them by taking three abelian groups $A, B$ and $C$, two cocycles $\theta$ and $\sigma$ and creating $C = A :_\theta (B :_\sigma C)$.

## Smallest Csörgő type loops

Currently, the smallest known Csörgő type loops (constructed in [2]) can be decomposed as follow:

- $A = Z_2, B = Z_2 \times Z_2 \times D_8, C = Z_2$
- Then for some morphism $\phi : C \mapsto \mathrm{Aut}(B)$ and for some cocycle $\mu$, $C = A :_\mu (B \times_\phi C)$ is a Csörgő type loop of order 128.

Because a semidirect product is an abelian extension, this decomposition is an iterated abelian extension. How to find an iterated central extension?

# Finding smaller Csörgő type loops

## What kind of loop?

If a smaller Csörgő type loop exists, it seems reasonable to suppose that it has order 64. It's then all about finding $A, B, C$ abelian groups, $\theta, \sigma$ cocycles such that $C = A :_\theta (B :_\sigma C)$ has order 64 and $\mathrm{Inn}(C)$ abelian.

# Finding smaller Csörgő type loops

## What kind of loop?

If a smaller Csörgő type loop exists, it seems reasonable to suppose that it has order 64. It's then all about finding $A, B, C$ abelian groups, $\theta, \sigma$ cocycles such that $C = A :_\theta (B :_\sigma C)$ has order 64 and $\mathrm{Inn}(C)$ abelian.

## Definition (Derived subgroup)

If $G$ is a group, $G'$ is the smallest normal subgroup of $G$ such that $G/G'$ is abelian.
Equivalently, $G' = \langle [g, h], \ \ g, h \in G \rangle$.
$|G'|$ measure the *abelianess* of a group.

# Finding smaller Csörgő type loops

## What kind of loop?

If a smaller Csörgő type loop exists, it seems reasonable to suppose that it has order 64. It's then all about finding $A, B, C$ abelian groups, $\theta, \sigma$ cocycles such that $C = A :_\theta (B :_\sigma C)$ has order 64 and $\mathrm{Inn}(C)$ abelian.

## Definition (Derived subgroup)

If $G$ is a group, $G'$ is the smallest normal subgroup of $G$ such that $G/G'$ is abelian.
Equivalently, $G' = \langle [g, h], \;\; g, h \in G \rangle$.
$|G'|$ measure the *abelianess* of a group.

## Measuring how "AIM" a loop is

If $Q$ is a loop, then $\dfrac{|\mathrm{Inn}(Q)'|}{|\mathrm{Inn}(Q)|}$ can be used as a metric of how well the loop satisfies the AIM hypothesis.

# Why it doesn't work very well

## Big space

Let's fix the abelian groups $A, B$ and $C$ such that $C = A :_\theta (B :_\sigma C)$ has order 64. The space size of the different $\theta, \sigma$ is $2^n$ where $n \in \{27, 72, 54, 98, 196, 450\}$, depending on $A, B, C$.

# Why it doesn't work very well

## Big space

Let's fix the abelian groups $A, B$ and $C$ such that $C = A :_\theta (B :_\sigma C)$ has order 64. The space size of the different $\theta, \sigma$ is $2^n$ where $n \in \{27, 72, 54, 98, 196, 450\}$, depending on $A, B, C$.

## Uniform metric

For fixed $A, B, C$ and over thousands of samples of $\sigma, \theta$, the metric usually takes 2-3 different values. How to differentiate the *good* loops from the *bad* loops?

# Why it doesn't work very well

## Big space

Let's fix the abelian groups $A, B$ and $C$ such that $C = A :_\theta (B :_\sigma C)$ has order 64. The space size of the different $\theta, \sigma$ is $2^n$ where $n \in \{27, 72, 54, 98, 196, 450\}$, depending on $A, B, C$.

## Uniform metric

For fixed $A, B, C$ and over thousands of samples of $\sigma, \theta$, the metric usually takes 2-3 different values. How to differentiate the *good* loops from the *bad* loops?

## Cocycle and loop properties

It is moreover not clear how the properties of the cocycle are related to the properties of the loop and how to control the loop properties via the cocycles.

# How to make it work?

- Find better metrics (the list of 54 interesting properties?)

# How to make it work?

- Find better metrics (the list of 54 interesting properties?)
- Study the link between the cocycles and the resulting loops

# How to make it work?

- Find better metrics (the list of 54 interesting properties?)
- Study the link between the cocycles and the resulting loops
- Find the iterated central extensions that lead to the Csörgő type loops of order 128.

# References


- Piroska Csörgő. "Abelian inner mappings and nilpotency class greater than two". In: *European Journal of Combinatorics* 28.3 (2007), pp. 858–867. ISSN: 0195-6698. DOI: https://doi.org/10.1016/j.ejc.2005.12.002. URL: https://www.sciencedirect.com/science/article/pii/S0195669805001708.
- Aleš Drápal and Petr Vojtěchovský. *Small loops of nilpotency class three with commutative inner mapping groups*. 2015. arXiv: 1509.05723 [math.GR].
- MARKKU NIEMENMAA. "FINITE LOOPS WITH NILPOTENT INNER MAPPING GROUPS ARE CENTRALLY NILPOTENT". In: *Bulletin of the Australian Mathematical Society* 79.1 (2009), pp. 109–114. DOI: 10.1017/S0004972708001093.
- David Stanovský and Petr Vojtěchovský. *Abelian extensions and solvable loops*. 2015. arXiv: 1509.05733 [math.GR].

Thanks!