Representation of self-distributive systems on digraphs

Graduate Algebra and Representation Theory Seminar

Fanxin Wu

March 10, 2023

Representation theory is all of mathematics. —Israel Gelfand

LD-system

A binary operation $(M, *)$ is *left self-distributive* (LD) if it satisfies $a * (b * c) = (a * b) * (a * c)$.

LD-system

A binary operation $(M, *)$ is *left self-distributive* (LD) if it satisfies $a * (b * c) = (a * b) * (a * c)$.

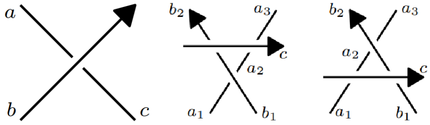
Examples:

If G is a group, define $g * h := ghg^{-1}$.

$(g * h) * (g * k) = (ghg^{-1}) * (gkg^{-1}) = (ghg^{-1})(gkg^{-1})(ghg^{-1}) = ghkh^{-1}g^{-1} = g * (h * k)$

This is in fact a *quandle*: $g * g = g$ and $\forall g, k \exists ! h \; g * h = k$.

LD-system



An oriented knot diagram consists of a set of arcs. The *knot quandle* is the quandle generated by the arcs and the relations $a * b = c$; it is right self-distributive. It is a complete knot invariant up to orientation.

LD-system

Theorem

The word problem for free LD-systems on finitely many generators is decidable.

LD-system

Theorem

The word problem for free LD-systems on finitely many generators is decidable.

Outline:

1. Assuming there is an elementary embedding $j : V_\lambda \to V_\lambda$, show that in the LD-system generated by j, left division has no cycle.

2. Consequently, left division in free LD-systems has no cycle.

3. Given two expressions t_1, t_2, enumerate all possible ways to expand them using LD; use 2 to argue that if t_1, t_2 aren't equivalent, eventually we will find t'_1, t'_2 s.t. one of them is a proper subterm of the other.

Structure

A *structure* is a set equipped with some (finitary) functions, relations and constants (distinguished elements).

Examples:

1. A group $(G, \cdot, e)$ has one binary operation and one constant. Not all structures $(X, \cdot, e)$ are groups, e.g., $(\mathbb{N}, +, 0)$ or $(\mathbb{Z}, +, 1)$.

2. ring $(R, +, \cdot, 0, 1)$

3. linear order $(X, <)$

4. digraph (G, E)

5. ordered field $(R, +, \cdot, 0, 1, <)$

6. A category can be viewed as a structure with two *sorts*, objects and morphisms. Composition of morphisms is viewed as a ternary relation.

Structure

A *substructure* is a subset containing all constants and closed under all functions; the relations are restricted to the subset.

Examples:

1. A substructure of $(G, \cdot, e)$ is only a semigroup. A substructure of $(G, \cdot, ^{-1}, e)$ is a group.

2. If there is no function then any subset can be viewed as a substructure. A subset of $(X, <)$ is naturally a sub-linear order. A subset of (G, E) is an *induced* subgraph.

3. An embedding $j : \mathcal{A} \to \mathcal{B}$ is an isomorphism with a substructure of $\mathcal{B}$.

Satisfaction

For a fixed list of functions, relations and constants, we can define what it means for a structure to *satisfy* a statement about those functions, relations and constants.

$(G, \cdot, e)$ is a group if it satisfies:

(i) $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;

(ii) $\forall x\ x \cdot e = e \cdot x = x$;

(iii) $\forall x \exists y\ x \cdot y = y \cdot x = e$.

$(X, <)$ is a partial order if it satisfies:

(i) $\forall x \forall y \forall z (x < y \wedge y < z \rightarrow x < z)$;

(ii) $\forall x \forall y\ \neg(x < y \wedge y < x)$.

Satisfaction

How to express that $(G, \cdot, e)$ is torsion-free? A naive attempt:

$\forall n > 1 \forall x (x \neq e \to x^n \neq e)$

This doesn't work because $x^n \neq e$ is the abbreviation of

$\underbrace{x \cdot x \cdot x \cdot \cdots \cdot x}_{n \text{ times}} \neq e$,

which is a different formula for each natural number n.

Satisfaction

How to express that $(G, \cdot, e)$ is torsion-free? A naive attempt:

$\forall n > 1 \forall x (x \neq e \rightarrow x^n \neq e)$

This doesn't work because $x^n \neq e$ is the abbreviation of

$\underbrace{x \cdot x \cdot x \cdot \dots \cdot x}_{n \text{ times}} \neq e$,

which is a different formula for each natural number n.

The correct way: a group is torsion-free iff it satisfies all the following statements.

$\forall x (x \neq e \rightarrow x \cdot x \neq e)$

$\forall x (x \neq e \rightarrow x \cdot x \cdot x \neq e)$

$\forall x (x \neq e \rightarrow x \cdot x \cdot x \cdot x \neq e)$

$\vdots$

Satisfaction

Similarly, $(G, \cdot, e)$ is infinite iff it satisfies all of the following statements.

$\exists x_1 \exists x_2 \; x_1 \neq x_2$

$\exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3)$

$\vdots$

Satisfaction

Similarly, $(G, \cdot, e)$ is infinite iff it satisfies all of the following statements.

$\exists x_1 \exists x_2 \; x_1 \neq x_2$

$\exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3)$

$\vdots$

Properties about groups expressible in formal language (possibly with infinitely many statements): torsion-free, infinite, abelian, trivial, having exactly 60 elements...

Properties not expressible: torsion, finite, free, simple, finitely generated...

Satisfaction

A field is algebraically closed iff it satisfies all of the following statements.

$\forall a_0 \forall a_1 \exists x (x^2 + a_1 x + a_0 = 0)$

$\forall a_0 \forall a_1 \forall a_2 \exists x (x^3 + a_2 x^2 + a_1 x + a_0 = 0)$

$\vdots$

Satisfaction

A field is algebraically closed iff it satisfies all of the following statements.

$\forall a_0 \forall a_1 \exists x (x^2 + a_1 x + a_0 = 0)$

$\forall a_0 \forall a_1 \forall a_2 \exists x (x^3 + a_2 x^2 + a_1 x + a_0 = 0)$

$\vdots$

An ordered field is *real closed* iff it satisfies:

(i) every positive element has a square root;

(ii) every odd degree polynomial has a root.

Elementary substructure

A substructure $\mathcal{N} \subseteq \mathcal{M}$ is *elementary* if it satisfies exactly the same (formal) properties as $\mathcal{M}$, where "properties" allow parameters from $\mathcal{N}$.

More precisely, if $a_1, \ldots, a_n \in \mathcal{N}$ and $\varphi(x_1, \ldots, x_n)$ is some statement, then

$\mathcal{N}$ satisfies $\varphi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{M}$ satisfies $\varphi(a_1, \ldots, a_n)$

Elementary substructure

Non-examples:

1. $(\mathbb{Z}, +)$ satisfies $\exists x \; x + x = 2$ but $(2\mathbb{Z}, +)$ doesn't, despite that the parameter 2 belongs to $2\mathbb{Z}$; so $(2\mathbb{Z}, +)$ is not an elementary substructure. Note that $(2\mathbb{Z}, +) \simeq (\mathbb{Z}, +)$, so they satisfy the same parameter-free statements (aka sentences).

2. $([0, 2], <)$ satisfies $\exists x \; 1 < x$ but $([0, 1], <)$ doesn't, so $([0, 1], <)$ is not an elementary substructure.

3. $(\mathbb{Q}, +, \cdot, 0, 1)$ satisfies the sentence $\forall x \neq 0 \exists y \; x \cdot y = 1$, while $(\mathbb{Z}, +, \cdot, 0, 1)$ doesn't. To tell $\mathbb{Q}$ and $\mathbb{C}$ apart, note that the former isn't algebraically closed.

Elementary substructure

Examples:

1. (Lefschetz transfer principle) If $E \subseteq F$ are both algebraically closed, then E is an elementary substructure. We say that the theory of ACF is *model-complete*.

In particular, if a system of polynomial equations with parameters from E has solution in F, then it has solution in E.

Elementary substructure

Examples:

1. (Lefschetz transfer principle) If $E \subseteq F$ are both algebraically closed, then E is an elementary substructure. We say that the theory of ACF is *model-complete*.

In particular, if a system of polynomial equations with parameters from E has solution in F, then it has solution in E.

2. (Tarski-Seidenberg) The theory of real closed field (RCF) is model-complete.

3. (Löwenheim-Skolem-Tarski) Any infinite structure $\mathcal{M}$ has elementary substructures of any infinite size below $|\mathcal{M}|$.

Elementary substructure

$j : \mathcal{A} \to \mathcal{B}$ is an elementary embedding if it is an embedding, and the image is an elementary substructure. Equivalently, for any $a_1, \ldots, a_n \in \mathcal{A}$ and statement $\varphi(x_1, \ldots, x_n)$,

$\mathcal{A}$ satisfies $\varphi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{B}$ satisfies $\varphi(j(a_1), \ldots, j(a_n))$

In a model-complete theory, any embedding is elementary.

Application of model-completeness: ACF

We prove the weak Nullstellensatz: if k is ACF and $I \subseteq k[X_1, \ldots, X_n]$ is a proper ideal then $V(I) \neq \emptyset$. The full Nullstellensatz can be proved similarly.

Application of model-completeness: ACF

We prove the weak Nullstellensatz: if k is ACF and $I \subseteq k[X_1, \ldots, X_n]$ is a proper ideal then $V(I) \neq \emptyset$. The full Nullstellensatz can be proved similarly.

WLOG I is maximal. By Hilbert basis theorem $I = \langle f_1, \ldots, f_m \rangle$. Let K be the algebraic closure of the field $k[X_1, \ldots, X_n]/I$. $\overline{X}_1, \ldots, \overline{X}_n$ are a solution to I in K.

"The system $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ has a solution" can be expressed as a single statement with parameters from k. Since it is true in K, by model completeness it is true in k.

Application of model-completeness: RCF

A polynomial $f(X_1, \ldots, X_n)$ is *positive semidefinite* if $f(a_1, \ldots, a_n) \geq 0$ for $a_1, \ldots, a_n \in \mathbb{R}$.

Hilbert's 17th: f is a sum of square of rational functions.

Application of model-completeness: RCF

A polynomial $f(X_1, \ldots, X_n)$ is *positive semidefinite* if $f(a_1, \ldots, a_n) \geq 0$ for $a_1, \ldots, a_n \in \mathbb{R}$.

Hilbert's 17th: f is a sum of square of rational functions.

Fact: an element of $\mathbb{R}(X_1, \ldots, X_n)$ is a sum of squares iff it is positive under any field ordering of $\mathbb{R}(X_1, \ldots, X_n)$.

So it suffices to show that $f \geq 0$ under any field ordering of $\mathbb{R}(X_1, \ldots, X_n)$. Given such an ordering, let K be the real closure of $\mathbb{R}(X_1, \ldots, X_n)$. Since $\forall a_1 \cdots \forall a_n \; f(a_1, \ldots, a_n) \geq 0$ is true in $\mathbb{R}$, it is true in K, so in particular $f(X_1, \ldots, X_n) \geq 0$.

Other applications of model theory

1. (complex/real/arithmetic/differential) algebraic geometry, in particular a proof of Mordell-Lang conjecture (Hrushovski);

2. non-standard analysis;

3. some results on representation growth,

etc.

Von-Neumann hierarchy

A *set* is a set of sets. More precisely:

$V_0 = \emptyset$

$V_1 = \mathcal{P}(V_0) = \{\emptyset\}$

$V_2 = \mathcal{P}(V_1) = \{\emptyset, \{\emptyset\}\}$

$V_3 = \mathcal{P}(V_2) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

$\vdots$

$V_\omega = \bigcup_{n<\omega} V_n$

$V_{\omega+1} = \mathcal{P}(V_\omega)$

$\vdots$

$V_{\omega+\omega} = \bigcup_{n<\omega} V_{\omega+n}$

$\vdots$

Large cardinal

A set X is *singular* if it can be written as $X = \bigcup_{i \in I} X_i$ where $|X_i| < |X|$ for each i, and also $|I| < |X|$. Otherwise it is *regular*.

X is *inaccessible* if it is regular and whenever $|A| < |X|$, $|\mathcal{P}(A)| < |X|$.

Large cardinal

A set X is *singular* if it can be written as $X = \bigcup_{i \in I} X_i$ where $|X_i| < |X|$ for each i, and also $|I| < |X|$. Otherwise it is *regular*.

X is *inaccessible* if it is regular and whenever $|A| < |X|$, $|\mathcal{P}(A)| < |X|$.

Examples:

1. A countable set is inaccessible since it's not a finite union of finite sets, and power set of a finite set is finite. The existence of an uncountable inaccessible set is a *large cardinal axiom*, which is so powerful that it implies the consistency of ZFC set theory.

2. $V_{\omega+\omega}$ is singular since $V_{\omega+\omega} = \bigcup_{n<\omega} V_{\omega+n}$, and for each n $|V_{\omega+n}| < |V_{\omega+\omega}|$, although $V_{\omega+\omega}$ satisfies the second requirement of inaccessibility.

Large cardinal

Provably one cannot prove that inaccessible set is consistent, i.e., assuming it exists doesn't lead to contradiction. Most set theorists believe in its consistency, so they kept strengthening the assumption...

Large cardinal

Provably one cannot prove that inaccessible set is consistent, i.e., assuming it exists doesn't lead to contradiction. Most set theorists believe in its consistency, so they kept strengthening the assumption...

Recall that an elementary embedding is an isomorphism with an elementary substructure.

Large cardinal

Provably one cannot prove that inaccessible set is consistent, i.e., assuming it exists doesn't lead to contradiction. Most set theorists believe in its consistency, so they kept strengthening the assumption...

Recall that an elementary embedding is an isomorphism with an elementary substructure.

The existence of a non-identity elementary embedding $j : (V_\lambda, \in) \to (V_\lambda, \in)$ is called I3, the third-closest-to-inconsistency large cardinal axiom. There are many inaccessible von-Neumann levels below V_λ, although V_λ itself isn't inaccessible.

LD-system of elementary embeddings

If $j, k : (V_\lambda, \in) \to (V_\lambda, \in)$ are elementary embeddings, we can form the composition $j \circ k$. We can also *apply* j to k as follows. k is not an element of V_λ, but k_α, the restriction of k to some V_α for $\alpha < \lambda$, is a function with domain V_α. Since j is an elementary embedding,

k_α is a function with domain $V_\alpha \Rightarrow j(k_\alpha)$ is a function with domain $V_{j(\alpha)}$.

Also, for $\beta > \alpha$

k_β extends $k_\alpha \Rightarrow j(k_\beta)$ extends $j(k_\alpha)$

Therefore the various $j(k_\alpha)$ are compatible, and cohere to a map $V_\lambda \to V_\lambda$, which is denoted $j * k$. It is an elementary embedding.

LD-system of elementary embeddings

Proposition

If $j, k, l : (V_\lambda, \in) \to (V_\lambda, \in)$ *are elementary embeddings, then* $j * (k * l) = (j * k) * (j * l)$.

Essentially this is because by elementarity, the function f sends x to $y \Rightarrow$ the function $j(f)$ sends $j(x)$ to $j(y)$, in other words,

$j(f(x)) = j(f)(j(x))$

LD-system of elementary embeddings

Proposition

If $j, k, l : (V_\lambda, \in) \to (V_\lambda, \in)$ *are elementary embeddings, then* $j * (k * l) = (j * k) * (j * l)$.

Essentially this is because by elementarity, the function f sends x to $y \Rightarrow$ the function $j(f)$ sends $j(x)$ to $j(y)$, in other words,

$j(f(x)) = j(f)(j(x))$

Let $\mathcal{E}_\lambda$ be the set of non-identity elementary embeddings from V_λ to V_λ. We say that j is left divisible by j' if $j = j' * k$ for some k.

Theorem

$\mathcal{E}_\lambda$ *is an LD-system where left division has no cycle, i.e., there is no* $j_1, j_2, \ldots, j_n$ *where* j_{i+1} *is left divisible by* j_i.

LD-system of elementary embeddings

Corollary

Assuming the existence of a non-identity elementary embedding $j : V_\lambda \to V_\lambda$ for some λ, the word problem for free LD-systems is decidable.

LD-system of elementary embeddings

Corollary

Assuming the existence of a non-identity elementary embedding $j : V_\lambda \to V_\lambda$ for some λ, the word problem for free LD-systems is decidable.

Theorem (Dehornoy)

The large cardinal assumption can be dropped.

In fact the large cardinal-free proof yielded more: it revealed the close relation between LD-systems and braid groups, and showed that braid groups are orderable.

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

By (i):

$*$	1	2	3	4	5
1	2				
2	3				
3	4				
4	5				
5	1				

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

$N * (b * 1) = (N * b) * (N * 1) = (N * b) * 1$

$*$	1	2	3	4	5
1	2				
2	3				
3	4				
4	5				
5	1	2	3	4	5

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

$(4 * (b * 1) = (4 * b) * 5$

$*$	1	2	3	4	5
1	2				
2	3				
3	4				
4	5	5	5	5	5
5	1	2	3	4	5

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

$(3 * (b * 1) = (3 * b) * 4$

$*$	1	2	3	4	5
1	2				
2	3				
3	4	5	4	5	4
4	5	5	5	5	5
5	1	2	3	4	5

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

$(2 * (b * 1) = (2 * b) * 3$

$*$	1	2	3	4	5
1	2				
2	3	4	5	3	4
3	4	5	4	5	4
4	5	5	5	5	5
5	1	2	3	4	5

Laver table

Fact: for each N there is a unique binary operation $*$ defined on $\{1, 2, \ldots, N\}$ such that:

(i) $a * 1 = a + 1$ for $1 \leq a \leq N - 1$, and $N * 1 = 1$;

(ii) $a * (b * 1) = (a * b) * (a * 1)$.

Inductively can show $a * b > a$ for $a < N$, so the strategy works.

$*$	1	2	3	4	5
1	2	4	5	2	4
2	3	4	5	3	4
3	4	5	4	5	4
4	5	5	5	5	5
5	1	2	3	4	5

Laver table

Fact: This is an LD-system iff $N = 2^n$, called the n-th Laver table and denoted A_n. Each row of A_n is periodic, and the periods are powers of 2. The period of the i-th row of A_n is non-decreasing with n.

A_n is a certain quotient of the subset of $\mathcal{E}_\lambda$ generated by any fixed j under application and composition; it originated as a tool to calculate the effects of elementary embeddings on so-called critical points. A_ns are "building blocks" of finite LD-systems.

Laver table

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Laver table

Theorem

The period of the i-th row in A_n tends to infinity with n.

The proof uses the relation between A_n and elementary embeddings.

Laver table

Theorem

The period of the i-th row in A_n tends to infinity with n.

The proof uses the relation between A_n and elementary embeddings.

Remarks:

1. Unlike word problem, this theorem hasn't been proved without large cardinal.

2. It is known that if the period indeed tends to infinity, it does so extremely slowly. The period of the first row reaches 16 at $n = 9$, but it cannot reach 32 (if ever) until $n > A(9, A(8, A(8, 254)))$, where $A(m, n)$ is the Ackermann function.

Reference

- David Marker (2002) *Model Theory : An Introduction*, Springer New York, NY
- Patrick Dehornoy (1994) *Braid groups and left distributive operations*
- Patrick Dehornoy (2010) *Elementary Embeddings and Algebra*, in Handbook of Set Theory