代数系のべき等演算による分解と組み立て

東北大学理学研究科数学専攻
学振特別研究員ＤＣ１
井澤　昇平

２０１１年１２月１０日
数学基礎論若手の会

Outline

1. Algebra
2. Idempotent retract and minimum cover
3. Possibility of essential parts

What is Universal Algebra

Study of the pair of a set A and a set of operations S on A. It seems roughly classified 3 groups.

- Fix a language without relation symbols. Study possible models of the language.
- Fix a set. Study possible sets of operations (closed under composition).
- Study relations between different objects. (e.g. Stone duality)

This talk is a topic in the second group.

Essentially "same" algebras

Example

· Let $(B, 0, 1, \wedge, \vee, \neg)$ be a Boolean lattice. We define

$$a \cdot b := a \wedge b, \quad a + b := (a \wedge \neg b) \vee (\neg a \wedge b), \quad -a := \neg a.$$

Then $(B, +, \cdot, -, 0, 1)$ is a commutative ring which satisfies an identity $x^2 = x$ (Boolean ring).

· Conversely, if $(R, +, \cdot, -, 0, 1)$ is a Boolean ring and define

$$a \wedge b := a \cdot b, \quad a \vee b := a + b + (a \cdot b), \quad \neg a := -a$$

then $(R, 0, 1, \wedge, \vee, \neg)$ is a Boolean lattice.

These constructions are mutually inverse.

That means Boolean lattices and Boolean rings equal to each other. It seems natural that, in general, the sets S, S' of operations on A are said to be "the same" if all operations belong to S "are written" by operations belongs to S' and vice versa.

Definition

Let A be a set, C be a set of operations on A. C is a clone on A if

$\cdot$ Projection $(a_1, \cdots, a_m) \mapsto a_i$ belongs to C.

$\cdot$ If $f \in C_n, g_1, \cdots, g_n \in C_m$ then $(a_j)_{1 \leq j \leq m} \mapsto f(g_i(a_j)_{1 \leq j \leq m})_{1 \leq i \leq n}$ belongs to C.

($C_m :=$ m-ary operations belong to C)

An operation f on A "is written" by operations belong to S means $f \in C(S)$ (clone generated by S). In particular, S and S' are the same means $C(S) = C(S')$.

- We consider a pair (A, C) of a set A and a clone C on A.
- We only consider the case A is finite in this talk.

Definition

Algebra is a pair (A, C) which A is a set and C is a clone on A. Finite algebra is an algebra in which the universe A is finite.

Notation. We write "A is an algebra" for (A, C) is an algebra. The clone C on A is written $\mathrm{Clo}(A)$.

2.[Reduction to smaller algebras]

1. Algebra
2. Idempotent retract and minimum cover
3. Possibility of essential parts

Quotation

The purpose of this lecture is to describe the intuition behind tame congruence theory. (partly omitted) The theory is based on a method for selecting small subsets of an algebra, restricting structure to that subset, calculating locally, and piecing together local data to solve globally stated problems.

Lecture note: Tame congruence theory is a localization theory, Keith A. Kearnes

Tame Congruence: focus on $\mathrm{Con}(A)$ $\cdots$ roughly speaking, catch only information of less than 2-ary operations
Covering: focus on $\mathrm{Inv}(A)$ $\cdots$ catch complete structure

Definition

Let A be an algebra.
· $e \in \mathrm{Clo}_1(A)$ is said to be an idempotent term operation on A if $e^2 = e$.
$\mathbf{E}(A)$: set of all idempotent term operations.
· If $e \in E(A)$, $A|_{e(A)}$ is an algebra such that
- The universe is $e(A)$.
- $\mathrm{Clo}_m(A|_{e(A)}) := \{e \circ f \mid f \in \mathrm{Clo}_m(A)\}$.

The structure of $A|_{e(A)}$ is determined by $e(A)$.

Definition

Let $e_1, \cdots, e_n, e \in \mathbf{E}(A)$.
$\{e_1(A), \cdots, e_n(A)\}$ covers $e(A)$ if

$$\exists\lambda, f_1, \cdots, f_l\,;\, \lambda(e_{i_1} f_1(x), \cdots, e_{i_l} f_l(x)) = e(x).$$

This case $e(A)$ is "embedded" in $e_{i_1}(A) \times \cdots \times e_{i_l}(A)$ by term operations.
"Embedding": $x \mapsto (e_{i_1} f_1(x), \cdots, e_{i_l} f_l(x))$
"retraction": $(x_1, \cdots, x_l) \mapsto \lambda(x_1, \cdots, x_l)$

Example

If $\{U_1, \cdots, U_n\}$ is a cover of an algebra A, then arbitrary subalgebra of power of A is congruence permutable iff each $A|_{U_i}$ has the same property.

Definition

Algebra A is congruence permutable if for any congruence relations α, β of A $\alpha \circ \beta = \beta \circ \alpha$ (equivalent condition is $\alpha \circ \beta = \alpha \vee \beta$) holds.

Fact

Let A be an algebra. Arbitrary subalgebra of power of A is congruence permutable iff A has a ternary term p which satisfies $p(x, x, y) = y, p(x, y, y) = x$.

Definition

Let A be an algebra. $e_1, \cdots, e_l \in \mathbf{E}(A)$. $e_1(A) \boxtimes \cdots \boxtimes e_l(A)$ is an algebra such that

- the universe is $e_1(A) \times \cdots \times e_l(A)$.
- $\mathrm{Clo}_m(e_1(A) \boxtimes \cdots \boxtimes e_l(A))$ is a set of tuples $(e_1 t_1, \cdots, e_l t_l)$ where $t_i \in \mathrm{Clo}_{lm}(A)$.

Definition (revisited)

Let $e_1, \cdots, e_n, e \in \mathbf{E}(A)$. $\{e_1(A), \cdots, e_n(A)\}$ covers $e(A)$ if

$$\exists \lambda, f_1, \cdots, f_l\, ; \lambda(e_{i_1} f_1(x), \cdots, e_{i_l} f_l(x)) = e(x).$$

Fact

$\{e_1(A), \cdots, e_n(A)\}$ covers $e(A)$ iff $e(A)$ is an idempotent retract of $e_{i_1}(A) \boxtimes \cdots \boxtimes e_{i_l}(A)$ for some $i_1, \cdots, i_l$.

embedding: $x \mapsto (e_{i_1} f_1(x), \cdots, e_{i_l} f_l(x))$,
retraction: $(x_1, \cdots, x_l) \mapsto \lambda(x_1, \cdots, x_l)$.

Definition

A finite algebra A is irreducible if $\{e_1(A), \cdots, e_n(A)\}$ does not cover A except there is i such that $e_i(A) = A$.

Example

- Any algebra with cardinality 1 or 2 is irreducible.
- A finite lattice $(L, \wedge, \vee)$ is irreducible.
- A vector space over a finite field is irreducible.
- A group $(G, \cdot, e, *^{-1})$ is irreducible iff $|G|$ is prime power.

Definition

A cover $\{e_i(A)\}_{1\leq i\leq n}$ of A is minimum if $e_i(A)$ is irreducible for any i and $\{e_i(A)\}_i \setminus \{e_{i_0}(A)\}$ does not cover A for $i_0 = 1, \cdots, n$.

Definition

Let A be a finite algebra, $\{e_1(A), \cdots, e_n(A)\}$ be a minimum cover of A. We define essential part of A by
$\mathrm{Ess}(A) := e_1(A) \boxtimes \cdots \boxtimes e_n(A)$.

Theorem

A finite algebra has unique minimum cover and essential part “up to isomorphism”.

Example

- Essential part of Primal algebra $(P, \mathcal{O})$ is P_2.
- One of minimum cover of $M_2 = \{0, 1, a, b\}$ as bounded lattice $(\wedge, \vee, 0, 1)$ is $\{\{x \mid x \leq a\}, \{x \mid x \leq b\}\}$.
- A group G is an idempotent retract of $\mathrm{Ess}(G)$. $G = \mathrm{Ess}(G)$ iff G is nilpotent.

Definition (revisited)

Let $e_1, \cdots, e_n, e \in \mathbf{E}(A)$.
$\{e_1(A), \cdots, e_n(A)\}$ covers $e(A)$ if

$$\exists \lambda, f_1, \cdots, f_l\,; \lambda(e_{i_1} f_1(x), \cdots, e_{i_l}(x)) = e(x).$$

3.[“Reconstruction” from minimum cover]

1. Algebra
2. Idempotent retract and minimum cover
3. Possibility of essential parts

Theorem

Let A, B be finite algebras. Then $\mathrm{Ess}(A) \simeq \mathrm{Ess}(B)$ iff A is categorically equivalent to B.

Fact

A is categorically equivalent to B iff there exist $n \geq 1$ and $\sigma \in \mathbf{E}(A^{[n]})$ such that
- $\{\sigma(A^{[n]})\}$ covers $A^{[n]}$,
- $A^{[n]}|_{\sigma(A^{[n]})}$ is isomorphic to B.

Definition

$A^{[n]}$ is the algebra
- the universe is A^n,
- $\mathrm{Clo}_m(A^{[n]}) = (\mathrm{Clo}_{nm}(A))^n$. The action is $(t_1, \cdots, t_n) : ((a_{ij})_{1 \leq i \leq n})_{1 \leq j \leq m} \mapsto (t_i(a_{kj})_{k,j})_i$.

Example

1. Algebras categorically equivalent to n-dimensional $\mathbb{F}_q$-vector space are left $\mathrm{M}(\mathbb{F}_q, m)$-modules length n.
2. Algebras categorically equivalent to two element primal algebra are primal algebras.
3. If L is a lattice, then $\{(a, b) \in L^2 \mid a \leq b\}$ is categorically equivalent to L.

Thus the way of classification of finite algebras is decomposed 3 steps.

- Classifying irreducible algebras.
- Classifying matrix products for given family of irr. algebras.
- Classifying algebras cat. eq. to given essential algebras.

We consider 2nd step.

Proposition (Uniqueness of minimal idempotent retract)

Let A be a finite algebra. If U and V are minimal idempotent retracts of A then $A|_U$ is isomorphic to $A|_V$.

Theorem (Characterization of existence of matrix product)

Let $U_1, \cdots, U_n$ be irreducible algebras. There exists a finite algebra A such that the minimum cover of A is isomorphic to $\{U_1, \cdots, U_n\}$ iff minimal idempotent retracts of $U_1, \cdots, U_n$ are isomorphic to each other.

Proposition

Let G be a finite group, $|G| = N = p_1^{m_1} \cdots, p_n^{m_n}$.
$l_i \in \mathbb{N}$ s.t. $N | l_i(l_i - 1), p_i^{m_i} | l_i$. Then
- $G_i := \{x \in G \mid x^{p_i^{m_i}} = 1\} = [x \mapsto x^{l_i}](G)$ is an idempotent retract of G.
- $\{G_1, \cdots, G_n\}$ is a minimum cover of G.

Proposition

- Any finite G is an idempotent retract of $\mathrm{Ess}(G)$.
- A finite group G is essential if and only if G is nilpotent.

References

1. Keith A. Kearnes. Tame Congruence Theory is a localization theory, Lecture Notes from "A Course in Tame Congruence Theory" Workshop, Budapest, 2001.
2. Mike Behrisch. Relational Tame Congruence Theory and subalgebra primal algebras. Master's thesis, TU Dresden, 2009.
3. Ralph McKenzie, An algebraic version of categorical equivalence for varieties and more general algebraic categories, Logic and Algebra vol.180
4. K. Denecke, O. Lüders, Categorical equivalence of varieties and invariant relations, Algebra Universalis 46(2001)
5. David Hobby and Ralph McKenzie. The Structure of Finite algebras, Contemporary Mathematics 76 American Mathematical Society
6. Stanley N. Burris and H.P. Sankappanavar, A Course in Universal Algebra The Millennium Edition, Springer-Verlag