Universal Algebras

joseph.muscat@um.edu.mt
1 March 2013

1 Operations

A **universal algebra** is a set X with some **operations** $* : X^n \to X$ and **relations**[1] $\rightsquigarrow \subseteq X^m$.

For example, there may be specific *constants* c ($n = 0$), *functions* $x \mapsto x^*$ ($n = 1$), and *binary operations* $(x, y) \mapsto x * y$ ($n = 2$), etc. An n-ary operation is sometimes written as $x * y * \ldots$ instead of $*(x, y, \ldots)$, and an m-ary relation as $x \rightsquigarrow y \rightsquigarrow \ldots$ instead of $\rightsquigarrow (x, y, \ldots)$.

Elements are *indistinguishable* when

$$*(\ldots, x, \ldots) = *(\ldots, y, \ldots), \qquad \rightsquigarrow (\ldots, x, \ldots) \Leftrightarrow \rightsquigarrow (\ldots, y, \ldots).$$

A **subalgebra** is a subset closed under all the operations

$$x, y, \ldots \in Y \;\Rightarrow\; x * y * \ldots \in Y$$

(The relations are obviously inherited.)

If A_i are subalgebras, then $\bigcap_i A_i$ is a subalgebra.

$[\![A]\!]$, the subalgebra *generated* by A, is the smallest subalgebra containing A,

$$[\![A]\!] := \bigcap \{\, Y \subseteq X : A \subseteq Y, Y \text{ is a subalgebra} \,\}$$

Hence $A \subseteq Y \;\Leftrightarrow\; [\![A]\!] \subseteq Y$ (for any subalgebra Y).

$A \cap B$ is the largest subalgebra contained in the algebras A and B; $[\![A \cup B]\!]$ is the smallest containing them. The collection of subalgebras form a complete lattice.

For any subsets,

$$A \subseteq [\![A]\!], \qquad [\![[\![A]\!]]\!] = [\![A]\!]$$
$$A \subseteq B \;\Rightarrow\; [\![A]\!] \subseteq [\![B]\!],$$
$$[\![A]\!] \vee [\![B]\!] = [\![A \cup B]\!], \qquad [\![A \cap B]\!] \subseteq [\![A]\!] \cap [\![B]\!]$$

The map $A \mapsto [\![A]\!]$ is thus a 'closure' map on the lattice of subsets of X, with the 'closed sets' being the subalgebras.

[1] Relations are not usually included in the definition of universal algebras.

PROOF: Let $x, y, \ldots \in [\![A]\!]$, then for any sub-algebra $Y \supseteq A$, $x * y * \cdots \in Y$, so $x * y * \cdots \in [\![A]\!]$. Hence $A \subseteq B \subseteq [\![B]\!]$ gives $[\![A]\!] \subseteq [\![B]\!]$. In particular, $[\![A]\!] \subseteq [\![A]\!]$, so $[\![[\![A]\!]]\!] \subseteq [\![A]\!] \subseteq [\![[\![A]\!]]\!]$. $A, B \subseteq A \cup B$ so $[\![A]\!] \vee [\![B]\!] \subseteq [\![A \cup B]\!]$; $A, B \subseteq [\![A]\!] \vee [\![B]\!]$, so $[\![A \cup B]\!] \subseteq [\![A]\!] \vee [\![B]\!]$.

□

When the number of operations is finite, the generated subalgebra can be constructed recursively as $[\![A]\!] = \bigcup_{n\in\mathbb{N}} B_n$ where

$$B_0 := A, \qquad B_{n^+} := B_n \cup \bigcup_{*} *(B_n).$$

Proof: that $B_n \subseteq [\![A]\!]$ and $A = B_0 \subseteq B_n$ are obvious (by induction); if $x, \ldots, y \in \bigcup_n B_n$ then $x \in B_{n_1}, \ldots, y \in B_{n_k}$, so $\exists r, x, \ldots, y \in B_r$ and $*(x, \ldots, y) \in B_{r^+} \subseteq \bigcup_n B_n$; so $[\![A]\!] = \bigcup_n B_n$.

□

Hence if A is countable, so is $[\![A]\!]$.

The *free* algebra generated by A is that algebra in which $x*y*\ldots$ are distinct from each other, for any $x, y, \ldots \in A$, and there are no relations.

2 Morphisms

The **morphisms** (also called *homomorphisms*) between compatible universal algebras (i.e., with the same type of operations and relations) are those functions $\phi : X \to Y$ which preserve all the operations and relations

$$\phi(x * y * \ldots) = \phi(x) * \phi(y) * \ldots$$

$$x \rightsquigarrow y \rightsquigarrow \ldots \ \Rightarrow \ \phi(x) \rightsquigarrow \phi(y) \rightsquigarrow \ldots$$

For the special constants, functions, and binary operations, this means

$$\phi(c_X) = c_Y, \qquad \phi(x^*) = \phi(x)^*, \qquad \phi(x * y) = \phi(x) * \phi(y).$$

An algebra with its morphisms forms a category. When $\phi(x) \rightsquigarrow \cdots \Leftrightarrow x \rightsquigarrow \cdots$, a morphism is an *isomorphism* when it is bijective (since $\phi(\phi^{-1}(x) * \phi^{-1}(y) * \ldots) = x * y * \ldots$, so ϕ^{-1} is a morphism). The monomorphisms are the 1-1 morphisms; the epimorphisms are the onto morphisms.

Proposition 1

For a morphism $\phi : X \to Y$,

- **If A is a subalgebra of X, then so is ϕA**
- **For any subset $S \subseteq X$, $\phi[\![S]\!] = [\![\phi S]\!]$**
- **If B is a subalgebra of Y, then so is $\phi^{-1}B$**

PROOF: If $\phi(x), \phi(y), \ldots \in \phi A$, then

$$\phi(x) * \phi(y) * \cdots = \phi(x * y * \cdots) \in \phi A$$

since A is a subalgebra. Let $x, y, \ldots \in \phi^{-1}B$, i.e., $\phi(x), \phi(y), \ldots \in B$, then $\phi(x*y*\cdots) = \phi(x)*\phi(y)*\cdots \in B$, hence $x*y*\cdots \in \phi^{-1}B$. Finally, if $\phi A \subseteq C$ (a subalgebra of Y), then $A \subseteq [\![A]\!] \subseteq \phi^{-1}C$, so $[\![\phi A]\!] = \phi[\![A]\!]$.

□

Thus if morphisms agree on a set S, then they are equal on $[\![S]\!]$.

Products: $X \times Y$ can be given an algebra structure by defining the operations

$$(x_1, y_1) * (x_2, y_2) * \ldots := (x_1 * x_2 * \ldots, y_1 * y_2 * \ldots)$$

$$(x_1, y_1) \rightsquigarrow (x_2, y_2) \rightsquigarrow \ldots := (x_1 \rightsquigarrow x_2 \rightsquigarrow \ldots) \text{ AND } (y_1 \rightsquigarrow y_2 \rightsquigarrow \ldots)$$

More generally, X^A is an algebra with

$$(f * g * \ldots)(a) := f(a) * g(a) * \ldots,$$

$$f \rightsquigarrow g \rightsquigarrow \ldots := f(a) \rightsquigarrow g(a) \rightsquigarrow \ldots \quad \forall a \in A.$$

There is also a *coproduct* (or *free* product). An algebra is said to be *decomposable* when $X \cong Y \times Z$ with $Y, Z \ncong X$.

Quotients: An equivalence relation on X which is invariant under the operations and relations is called a *congruence* (or *stable* relation), i.e.,

$$\begin{aligned} x_1 \approx x_2, y_1 \approx y_2, \ldots \ \Rightarrow \ & (x_1 * y_1 * \ldots) \approx (x_2 * y_2 * \ldots) \\ & \text{AND } x_1 \rightsquigarrow y_1 \rightsquigarrow \ldots \ \Rightarrow \ x_2 \rightsquigarrow y_2 \rightsquigarrow \ldots \end{aligned}$$

The operations and relations can then be extended to act on the set $X/\approx$ of equivalence classes

$$[x] * [y] * \ldots := [x * y * \ldots]$$

$$[x] \rightsquigarrow [y] \rightsquigarrow \ldots := x \rightsquigarrow y \rightsquigarrow \ldots$$

i.e., the mapping $\pi : x \mapsto [x]$ is a morphism $X \to X/\approx$.

For example, indistinguishable elements form a congruent relation, that can be factored away.

An algebra X can be analyzed by looking for its congruence relations and then simplifying to get $X/\approx$; this process can be continued until perhaps an algebra is reached that has only trivial congruent relations ($x \approx y \Leftrightarrow x = y$ or $x \approx y \Leftrightarrow \text{TRUE}$), called *simple*: it has only trivial quotients. Simple algebras are the 'building blocks' of 'finitary-type' algebras.

Any morphism $\phi : X \to Y$ which preserves a congruence relation $x \approx y \Rightarrow \phi(x) \approx \phi(y)$, induces a morphism $X/\approx \to Y$, $[x] \mapsto \phi(x)$.

The following five "Isomorphism" theorems apply when the relations satisfy $x \rightsquigarrow y \rightsquigarrow \ldots \Leftrightarrow \phi(x) \rightsquigarrow \phi(y) \rightsquigarrow \ldots$:

First isomorphism theorem: For any morphism $\phi : X \to Y$, the relation $\phi(x) = \phi(y)$ is a congruence (called the kernel of ϕ), such that the associated quotient space

$$(X/\ker\phi) \cong \phi X.$$

Proof: That $\ker\phi$ is a congruence is trivial; so it induces a 1-1 morphism $X/\ker\phi \to \phi X$, thus an isomorphism.

Third isomorphism theorem: If a congruence $\approx_1$ is finer than another $\approx_2$, then $\approx_1$ induces a congruence $(\approx_2/\approx_1)$ on $X/\approx_2$, and

$$X/\approx_2 \cong (X/\approx_1)/(\approx_2/\approx_1).$$

Proof: The map $X/\approx_1 \to X/\approx_2$, $[x] \mapsto [[x]]$ is a well-defined onto morphism, with kernel $(\approx_2/\approx_1)$.

Second isomorphism theorem: If Y is a subalgebra of X, and $\approx$ is a congruence on X, then $\approx$ is a congruence on Y, and $Y/\approx$ is isomorphic to the subalgebra $Y' \subseteq X/\approx$, consisting of all the equivalence classes that contain an element of Y.

Proof: The map $Y \to X/\approx$, $y \mapsto [y]$, is a morphism with image Y' and kernel $\approx$.

Fourth isomorphism theorem: Given a congruence relation $\approx$, the subalgebras $Y \subseteq X$ that satisfy $y \in Y \Rightarrow [y] \subseteq Y$, are in correspondence with the subalgebras of $X/\approx$.

Proof: Clearly, $Y \subseteq Z \Rightarrow Y' \subseteq Z'$. Conversely, if $Y' \subseteq Z'$ and $y \in Y$, then $[y] \in Z'$, so $[y] = [z]$ for some $z \in Z$, thus $y \approx z \in Z$.

'Fifth' isomorphism theorem: Given congruences $\approx_1$, $\approx_2$ on X_1,X_2, the relation $(x_1, x_2)(\approx_1 \times \approx_2)(y_1, y_2) := (x_1 \approx_1 y_1)$ AND $(x_2 \approx_2 y_2)$ on $X_1 \times X_2$ is a congruence, and

$$\frac{X_1 \times X_2}{\approx_1 \times \approx_2} \cong \frac{X_1}{\approx_1} \times \frac{X_2}{\approx_2}.$$

Proof: Let $\phi : X_1 \times X_2 \to \frac{X_1}{\approx_1} \times \frac{X_2}{\approx_2}$, $(x_1, x_2) \mapsto ([x_1], [x_2])$. This is a morphism with kernel given by $([x_1], [x_2]) = ([y_1], [y_2]) \Leftrightarrow x_1 \approx_1 y_1$ AND $x_2 \approx_2 y_2$.

There are two senses in which a space X is 'contained' in a larger space Y:

1. Externally, by *embedding* X in Y, i.e., there is an isomorphism $\iota : X \to B \subseteq Y$, denoted $X \subsetneqq Y$ because X is, effectively, a subspace of Y;

2. Internally, by *covering* X by Y, i.e., there is an onto morphism $\pi : Y \to X$, so $X \cong Y/\ker\pi$; each element of X is refined into several in Y.

Then every morphism $\phi : X \to Y$ splits up into three parts with an inner core bijective morphism: $X \xrightarrow{\pi} X/\ker\phi \to \operatorname{im}\phi \xrightarrow{\iota} Y$. For example, $X \times Y \xrightarrow{\pi} X \xrightarrow{\iota} X \times Y$.

Theorem 2

> **Every finitely-generated algebra is a quotient of the finitely-generated free algebra.**

(the same is true if the operations have intrinsic properties, i.e., subalgebras, quotients and products have the same properties)

An *endomorphism* $\phi : X \to X$ induces a sequence of embeddings and partitions:

- A descending sequence of embedded spaces

$$X \supseteq \operatorname{im}\phi \supseteq \operatorname{im}\phi^2 \supseteq \cdots \supseteq \bigcap_n \operatorname{im}\phi^n$$

- An ascending sequence of partitions, where $x \sim_n y \Leftrightarrow \phi^n(x) = \phi^n(y)$,

$$0 \subseteq \ker\phi \subseteq \ker\phi^2 \subseteq \cdots \subseteq \bigcup_n \ker\phi^n$$

1. ϕ is said to be of *finite descent* down to n when $\operatorname{im}\phi^n = \operatorname{im}\phi^{n+1}$ ($= \operatorname{im}\phi^{n+2} = \cdots$), i.e., ϕ is onto $\operatorname{im}\phi^n$. In this case, every element can be represented, modulo $\sim_n$, by some element in $\operatorname{im}\phi^n$.

   Proof: $\phi^n(x) = \phi^{n+1}(y)$, so $x \sim_n \phi(y) \sim_n \cdots \sim_n \phi^n(z)$.

2. ϕ is of *finite ascent* up to n when $\ker\phi^n = \ker\phi^{n+1}$ ($= \ker\phi^{n+2} = \cdots$), i.e., ϕ is 1-1 on $\operatorname{im}\phi^n$. Then each n-equivalence class contains at most one element of $\operatorname{im}\phi^n$.

   Proof: $\phi^n(x) \sim_n \phi^n(y)$ implies $x \sim_{n+n} y$, so $x \sim_n y$, i.e., $\phi^n(x) = \phi^n(y)$.

3. If ϕ has finite ascent and descent, then the two sequences have the same length. Thus every element can be represented modulo $\sim_n$ by a unique element in $\operatorname{im}\phi^n$, and ϕ is bijective on $\operatorname{im}\phi^n$

   Proof: The ascent cannot be longer than the descent else $\phi^n(x_1) = \phi^n(y_1) = \phi^{n+1}(y_2)$ and $\phi^{n+1}(x_1) = \phi^{n+1}(y_1)$, so $x_1 \not\sim_n y_1$ but $x_1 \sim_{n+1} y_1$, and $x_2 \not\sim_{n+1} y_2$ but $x_2 \sim_{n+2} y_2$, etc. The descent cannot be longer than the ascent else if $\phi^m(x) = \phi^{m+1}(y)$ then $x \sim_m \phi(y)$, so $x \sim_n \phi(y)$.

3 Compatibility

An operation is **associative** when $*(x, y, \ldots)$ exists for every finite number of terms, such that

$$*(\ldots, *(x, y, \ldots), u, \ldots) = *(\ldots, x, y, \ldots, u, \ldots)$$

For example, $x * y * z = (x * y) * z$; so the operation reduces to three basic ones

$$0 := *(), \quad *(x), \quad *(x, y)$$

such that

$$0 * x = *(x), \qquad (x * y) * z = x * (y * z).$$

Note that $*(x) = *(y)$ is a stable equivalence relation (with respect to $*$), with related elements being *indistinguishable* algebraically; but can assume $*(x) = x$ by taking the quotient space and renaming; in this case, $0 * x = x$.

An operation is **distributive** over another when

$$*(\ldots, \circ(x, y, \ldots), z, \ldots) = \circ(*(\ldots, x, z, \ldots), *(\ldots, y, z, \ldots), \ldots)$$

For 0-,1-,2-operations, this means

	(0)	1	2
(0)	$(0 = 1)$	$(0 = 0^*)$	$(0 * x = 0 = x * 0)$
1	$(1^\circ = 1)$	$x^{*\circ} = x^{\circ *}$	$(x * y)^\circ = x^\circ * y = x * y^\circ$
2		$(x + y)^* = x^* + y^*$	$x * z + y * z = (x + y) * z$
			$z * x + z * y = z * (x + y)$

Two operations **commute** when

$$*(\circ(x_1, y_1, \ldots), \circ(x_2, y_2, \ldots), \ldots) = \circ(*(x_1, x_2, \ldots), *(y_1, y_2, \ldots))$$

For 1-,2-operations, this means

	0	1	2
0	$0 = 1$		
1		$x^{*\circ} = x^{\circ *}$	$(x + y)^* = x^* + y^*$
2			$(x_1 + y_1) * (x_2 + y_2) = x_1 * x_2 + y_1 * y_2$

Commuting 2-operations with identities must actually be the same, and must be commutative $x * y = y * x$ and associative.

Proof: The identities are the same: $1 = 11 = (1 + 0)(0 + 1) = 10 + 01 = 0 + 0 = 0$. $ab = (a + 0)(0 + b) = a0 + 0b = a + b$ so the operations are the same, and $(ab)(cd) = (ac)(bd)$. Hence $ab = (1a)(b1) = (1b)(a1) = ba$ and $a(bc) = (a1)(bc) = (ab)c$.

□

In particular if an operation with identity commutes with itself, it must be associative and commutative $x * y = y * x$.

3.1 Examples

1. The simplest example is a set with a single constant 0, sometimes called the field with one element.

2. A set with a constant and a 1-operation; properties may be $0^* = 0$, $x^{**} = x$.

3. A set with a constant, a 1-operation, and a 2-operation: e.g. $0 * x = x$, $(x * y)^* = y^* * x^*$.