Clones (1&2)

Martin Goldstern

Discrete Mathematics and Geometry,
TU Wien

TACL Olomouc, June 2017

Base set X

Let X be a (nonempty) set.

- Often finite:
  - $X = \{0, 1\}$.
  - $X = \{0, *, 1\}$.
  - $X = \{\,\{\}, \{a\}, \{b\}, \{a, b\}\,\}$.
  - $X = \{1, \dots, n\}$.
  - Etc.
- Sometimes countably infinite:
  - $X = \mathbb{N} = \{0, 1, 2, \dots\}$.
- Sometimes uncountably infinite:
  - $X = \mathbb{R}$, etc.

Operations on X

$X =$ our base set.

- A unary operation is a (total) function $f : X \to X$.
- A binary operation is a function $f : X^2 \to X$.
- ternary, quaternary, ...
- A k-ary operation is a function $f : X^k \to X$ (for $k \geq 1$).
- We write $\mathcal{O}^{(k)}$ or $\mathcal{O}_X^{(k)}$ for the set of all k-ary operations on X. (Sometimes also written X^{X^k}.)
- We let $\mathcal{O}_X := \bigcup_{k=1}^{\infty} \mathcal{O}_X^{(k)}$.

(For simplicity we will assume that the sets X^k are pairwise disjoint. We will ignore the 0-ary functions and replace them by constant 1-ary functions.)

Transformation monoids

Definition ((abstract) monoid)

A *monoid* or *abstract monoid* is a structure $(M, *, 1)$, where

- $*$ is a binary operation on M, associative
- $\ldots$ together with a neutral element 1 ($1 * a = a * 1 = a$).

Definition (transformation/concrete monoid, unary clone)

A *transformation monoid* is a subset $T \subseteq \mathcal{O}_X^{(1)}$ (for some X) which is closed under composition and contains the identity function $id : X \to X$. ($(T, \circ, id)$ will be an abstract monoid.)

Conversely, a variant of Cayley's theorem shows that every abstract monoid is isomorphic to a transformation monoid.

Binary clones

A *transformation monoid* or *unary clone* on X is a subset $T \subseteq \mathcal{O}_X^{(1)}$ which is closed under composition and contains the identity function $id : X \to X$.

Definition

A *binary clone* on X is a set $T \subseteq \mathcal{O}_X^{(1)}$ which is closed under "‘composition"’ and contains the two projections $\pi_1, \pi_2 : X^2 \to X$.

Definition (Composition)

Let $f, g_1, g_2 \in \mathcal{O}_X^{(2)}$. The composition $f(g_1, g_2)$ is the function from X^2 to X defined by

$$f(g_, g_2)(x, y) := f(\ g_1(x, y), g_2(x, y)\ )$$

k-ary clones

Definition (k-ary clone)

A *k-ary clone* on X is a set $T \subseteq \mathcal{O}_X^{(k)}$ which is closed under "‘composition"’ and contains the k projections $\pi_1, \dots, \pi_k : X^k \to X$.

Definition (Composition)

Let $f, g_1, \dots, g_k \in \mathcal{O}_X^{(k)}$. The composition $f(g_1, \dots, g_k)$ is the function from X^k to X defined by

$$\forall \vec{x} \in X^k : f(g_1, \dots, g_k)(\vec{x}) := f(\ g_1(\vec{x}), \dots, g_k(\vec{x})\ )$$

(“Plugging $g_1, \dots, g_k$ into f”)

Clones

Definition (Clone)

A *clone* on X is a set $T \subseteq \mathcal{O}_X = \bigcup_{k=1}^{\infty} \mathcal{O}_X^{(k)}$ which is closed under "'composition"' and contains all projections $\pi_k^n : X^n \to X$, $n = 1, 2, \ldots, 1 \leq k \leq n$.

Definition (Composition)

Let $f \in \mathcal{O}^{(k)}$, $g_1, \ldots, g_k \in \mathcal{O}_X^{(m)}$. The composition $f(g_1, \ldots, g_k)$ is the function from X^m to X defined by

$$\forall \vec{x} \in X^m : f(g_1, \ldots, g_k)(\vec{x}) := f(\ g_1(\vec{x}), \ldots, g_k(\vec{x})\ )$$

("Plugging $g_1, \ldots, g_k$ into f")

If C is a clone, then $C^{(k)} := C \cap \mathcal{O}^{(k)}$ is a k-ary clone, the k-ary fragment of C.

Examples of clones

- The smallest clone J_X contains only the projections.
- The largest clone $\mathcal{O}_X$ contains all operations.
- Every subset $S \subseteq \mathcal{O}_X$ will *generate* a clone $\langle S \rangle$, the smallest clone containing S. The clone $\langle S \rangle$ can be obtained from below by closing S under composition, or from above as $\langle S \rangle = \bigcap \{ M \mid S \subseteq M \subseteq \mathcal{O}_X, M \text{ is a clone} \}$.
- If V is a vector space over the field K, then the set of all linear functions $f_{\vec{a}} : V^k \to V$

  $$f_{\vec{a}}(v_1, \ldots, v_k) := a_1 v_1 + \cdots + a_k v_k$$

  (with $\vec{a} = (a_1, \ldots, a_k) \in K^k$) is a clone.

Examples of clones, continued

For every algebra $\mathcal{X} = (X, f, g, \ldots)$ (=universe X with operations f, g, ... — for example $\mathcal{X}$ might be a group, a ring, etc) we consider

- the clone of *term operations* on X, the smallest clone containing all the basic operations $f, g, \ldots$ of $\mathcal{X}$;
- the clone of *polynomial operations* on X, the smallest clone containing all terms as well as all constant unary functions on X.

Many properties of the algebra $\mathcal{X}$ depend only on the clone of term functions, and not on the specific set of basic operations which generates this clone. (E.g. subalgebras, congruence relations, automorphisms, etc)

For example, a Boolean algebra will have the same clone as the corresponding Boolean ring.

The family of all clones

For any nonempty set X let $Cl(X)$ be the set of all clones on X.

- The intersection of any subfamily of $Cl(X)$ is again in $Cl(X)$.
- $(Cl(X), \subseteq)$ is a complete lattice.
  Meet = intersection, join = generated by union.
- J_X is the smallest clone, $\mathcal{O}_X$ the largest.
- If $X = \{0\}$, then there is a unique clone: $J_X = \mathcal{O}_X$.
- If $X = \{0, 1\}$, then $Cl(X)$ is countably infinite.
- If X is finite and has at least three elements, then $Cl(X)$ is uncountable. (In fact: $|Cl(X)| = |\mathbb{R}|$.)
- If X is infinite, then ... (later)

Uncountably many clones

If $X = \{0, 1, 2\}$, then $Cl(X)$ is uncountable.

Proof sketch.

- We call a k-tuple $(a_1, \ldots, a_k) \in \{0, 1, 2\}^k$ proper, if exactly one of the a_i is equal to 1, and all the others are 2.
- For every $k \geq 3$ let $f_k : X^k \to X$ be the function that assigns 1 to every proper k-tuple, and 0 to everything else.
- For every $A \subseteq \{3, 4, \ldots\}$ let $C_A := \langle\{f_i \mid i \in A\}\rangle$.
- Check that for $k \notin A$ we have $f_k \notin C_A$.
  (Every composition of functions $f_i, i \neq k$ will assign 0 to some proper k-tuple.)
- Hence the map $A \mapsto C_A$ is 1-1.

Completeness

Fix a base set X.

Definition

A set $S \subseteq \mathcal{O}_X$ is *complete* if $\langle S \rangle = \mathcal{O}_X$, i.e., if every operation on X is term function of the algebra with operations S.

Example

Let $X = \{0, 1\}$, $\mathcal{X} = (X, \vee, \wedge, \neg, 0, 1)$.

- The set $\{\vee, \wedge, \neg\}$ is complete.
- The set $\{\wedge, \neg\}$ is complete.
- The set $\{|\}$ is complete, where $x|y := \neg(x \wedge y)$.
  (Sheffer stroke)

Completeness, more examples

Theorem

For every X: $\langle \mathcal{O}_X^{(2)} \rangle = \mathcal{O}_X$.

Proof.

- finite: Lagrange interpolation
- infinite: use $X \times X \approx X$.

Caution: Most clones C are NOT generated by their binary fragment $C \cap \mathcal{O}^{(2)}$. (Not even finitely generated.)

Theorem

If $X = \{1, \ldots, k\}$, *then there is a single function* $f \in \mathcal{O}_X^{(2)}$ *with* $\langle f \rangle = \mathcal{O}_X^{(2)}$*: Let* $f(x, x) = x + 1$ *(modulo k),* $f(x, y) = 0$ *otherwise.*

(Completeness on infinite sets)

If X is infinite, then $\mathcal{O}_X$ is uncountable. Hence a finite/countable set of operations cannot generate all of $\mathcal{O}_X$.
However:

Theorem

Let $X \neq \emptyset$. For any finite or countable set $T \subseteq \mathcal{O}_X$ there is a single function f_T (not necessarily in T) such that $T \subseteq \langle f \rangle$.

Theorem

- *If X is countable, then there is a countable dense subset of $\mathcal{O}_X$ (in the natural topology), hence there is a single function f such that the topological closure of $\langle f \rangle$ is all of $\mathcal{O}_X$.*
- *If X is uncountable, then $\mathcal{O}_X$ will not be separable any more.*

Completeness, continued

Let $X = \{0, 1\}$ be the 2-element Boolean algebra, with Boolean operations $\wedge, \vee, \neg, \to, |, \ldots$.

Example

The set $\{\vee, \wedge, \to\}$ is not complete.

Proof.

Each of the three operations preserves the set $\{1\}$, i.e., this set is a subalgebra of the algebra $(\{0, 1\}, \wedge, \vee, \to)$.
Hence every function in $\langle\{\wedge, \vee, \to\}$ will also preserve this set, but $\neg$ does not. So $\neg \notin \langle\{\wedge, \vee, \to\}\rangle$.

Polymorphisms, example

Example

The set $\{\vee, \wedge, 0, 1\}$ is not complete.

Proof.

All four functions are monotone in both arguments.

Definition

Let $\rho \subseteq X \times X$ be a relation (Example: $\leq$ on $\{0, 1\}$.)
A function $f : X^k \to X$ *preserves* ρ iff:
for all $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \ldots, \begin{pmatrix} x_k \\ y_k \end{pmatrix} \in \rho$, we have $\begin{pmatrix} f(x_1, \ldots, x_k) \\ f(y_1, \ldots, y_k) \end{pmatrix} \in \rho$.

Lemma

If all $f \in S \subseteq \mathcal{O}_X$ preserve ρ, then all $f \in \langle S \rangle$ preserve ρ.

Polymorphisms, definition

Definition

Let $\rho \subseteq X^m$ be an m-ary relation, and let $f : X^k \to X$ be a k-ary function. We say that "f preserves ρ" ($f \triangleright \rho$, $f \in \mathrm{Pol}(\rho)$) if:

- for all $(a_{i,j} : i \leq m, j \leq k) \in X^{m \times k}$:

  whenever $a_{*,1} \in \rho, \ldots, a_{*,k} \in \rho$, then also $\begin{pmatrix} f(a_{1,*}) \\ \vdots \\ f(a_{m,*}) \end{pmatrix} \in \rho$.

(We let $a_{*,j} := \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix}$, similarly $a_{i,*} = (a_{i,1}, \ldots, a_{i,k})$.)

Equivalently: Letting $(X^m, f^{[m]})$ be the m-th power of (X, f):
$f \triangleright \rho$ iff ρ is a subalgebra of $(X^m, f^{[m]})$.

Polymorphisms, examples

- Let ρ be a nontrivial unary relation, i.e. $\emptyset \subsetneq \rho \subsetneq X$. Then Pol($\rho$) is the set of all operations f such that ρ is a subalgebra of (X, f).
- Let $\rho \subseteq X \times X$ be an equivalence relation. Then Pol(ρ) is the set of all operations f such that ρ is a congruence relation of the algebra (X, f).
- Let $\rho \subseteq X \times X$ be a (reflexive) partial order. Then Pol(ρ) is the set of all pointwise monotone operations.
- Let $\rho \subseteq X \times X$ be the graph of a function r:
  $\rho = \{(x, r(x)) : x \in X\}$.
  Then Pol(ρ) is the set of all functions f such that r is an endomorphism of (X, f), i.e., f commutes with r.

Fix a finite base set X.

Definition

For any relation $\rho \subseteq X^m$ let $\mathrm{Pol}(\rho)$ be the set of all operations preserving ρ: $\mathrm{Pol}(\rho) := \{f \in \mathcal{O}_X \mid f \rhd \rho\}$
For a set R of relations, let $\mathrm{POL}(R) := \bigcap_{\rho \in R} \mathrm{Pol}(\rho)$.

Lemma

If $S \subseteq \mathrm{Pol}(\rho)$, then also $\langle S \rangle \subseteq \mathrm{Pol}(\rho)$. In particular, $\mathrm{Pol}(\rho)$ and also $\mathrm{POL}(R)$ are always clones.

Theorem

For every clone $C \subseteq \mathcal{O}_X$ there exists:

- *A set $S \subseteq \mathcal{O}_X$ such that $C = \langle S \rangle$. (Trivial)*
- *A set R of relations such that $C = \mathrm{POL}(R)$.*

(Helpful to show incompleteness.)

Galois connection

Theorem

For every clone $C \subseteq \mathcal{O}_X$ there exists a set R of relations such that $C = \mathrm{POL}(R) = \{f \mid \forall \rho \in R : f \rhd \rho\}$.

Proof sketch.

The largest set R satisfying $\forall \rho \in R : C \subseteq \mathrm{Pol}(\rho)$ is the set

$$\mathrm{INV}(C) := \{\rho \mid \forall f \in C : f \rhd \rho\}$$

For finite sets X, we can check that $C = \mathrm{POL}(\mathrm{INV}(C))$.

even: $\langle S \rangle = \mathrm{POL}(\mathrm{INV}(S))$ for all $S \subseteq \mathcal{O}_X$.
We will see a construction of a “better” set R with $C = \mathrm{POL}(R)$ later.

Pol: completeness criterion

Fix a finite base set X.

Theorem

For every clone $C \subseteq \mathcal{O}_X$ there exists a set R of relations such that $C = \mathrm{POL}(R)$.

Corollary

If $S \subseteq \mathcal{O}_X$ is not complete (i.e., $\langle S \rangle \neq \mathcal{O}_X$),
then there is a nontrivial relation ρ such that $S \subseteq \mathrm{Pol}(\rho)$, hence $\langle S \rangle \subseteq \mathrm{Pol}(\rho)$.

(But there are so many candidates for ρ! Want to search a small set. $\rightarrow$ precomplete clones)

Precomplete clones

Definition

A clone $C \subseteq \mathcal{O}_X$ is "precomplete" (or "maximal") if $C \neq \mathcal{O}_X$, but there is no clone D satisfying $C \subsetneq D \subsetneq \mathcal{O}_X$.

Theorem

For any clone $C \subsetneq \mathcal{O}_X$ there is a precomplete clone C' with $C \subseteq C'$.

(Remark: Not true for infinite sets!)

Proof.

(Use Zorn's lemma??) Let $\mathcal{O}_X = \langle f \rangle$. Among all clones D with $C \subseteq D$, $f \notin D$, find a maximal element.
(Better proof: later)

Examples of precomplete clones

Example

Let $\emptyset \subsetneq \rho \subsetneq X$. Then $\mathrm{Pol}(\rho)$ is precomplete.

Proof.

Assuming $g \notin \mathrm{Pol}(\rho)$, we let $C := \langle \mathrm{Pol}(\rho) \cup \{g\} \rangle$; we show $C = \mathcal{O}_X$.

First show that there is $b \notin \rho$ such that the constant operation c_b with value b is in C.

For any function $f : X^k \to X$ let $\hat{f} : X^{k+1} \to X$ be defined by $\hat{f}(\vec{x}, b) = f(\vec{x})$, and $\hat{f}(\vec{x}, y) \in \rho$ arbitrary for $y \neq b$. Then $\hat{f} \in C$, and $f(\vec{x}) = \hat{f}(\vec{x}, c_b(x_1))$, so $f \in C$.

Example

Let ρ be a bounded partial order. Then $\mathrm{Pol}(\rho)$ is precomplete.

Rosenberg's list

Theorem
Let $X = \{1, \ldots, k\}$*. Then there is an explicit finite list of relations* $\rho_1, \ldots, \rho_m$ *(including, for example, all nontrivial unary relations, all bounded partial orders) such that every precomplete clone on* X *is one of* $\mathrm{Pol}(\rho_1)$*, ...,* $\mathrm{Pol}(\rho_m)$*.*

Completeness criterion If $\langle S \rangle \neq \mathcal{O}_X$ iff there is some i with $\forall f \in S : f \rhd \rho_i$.

k-ary fragments

Let D be a k-ary clone. The smallest clone C with $C \cap \mathcal{O}_X^{(k)} = D$ is $\langle D \rangle$.

$D \subseteq X^{X^k}$ can be viewed as a relation on X.

The largest clone C with $C \cap \mathcal{O}_X^{(k)} = D$ is

$$\mathrm{Pol}(D) = \bigcup_n \{ f \in \mathcal{O}_X^{(n)} \mid \forall d_1, \ldots, d_n \in D : f(d_1, \ldots, d_n) \in D \}$$

For any clone E, the clones $\mathrm{Pol}(E \cap \mathcal{O}_X^{(k)})$ approximate E from above, agreeing with E on larger and larger sets: $\mathrm{Pol}(E \cap \mathcal{O}_X^{(k)}) \cap \mathcal{O}_X^{(k)} = E \cap \mathcal{O}_X^{(k)}$.

Theorem

For all clones E: $E = \bigcap_k \mathrm{Pol}(E \cap \mathcal{O}_X^{(k)})$.

$Cl(X)$ is dually atomic

Theorem

Let X be finite, $C \neq \mathcal{O}_X$ a clone.
Then there is a precomplete clone $D \supseteq C$.

Proof.

Let $C' \supseteq C$ be such that $C' \cap \mathcal{O}_X^{(2)}$ is maximal. (finite!)
Let $D := \mathrm{Pol}(C')$.