Clones (3&4)

Martin Goldstern

Discrete Mathematics and Geometry,
TU Wien

TACL Olomouc, June 2017

Galois connections

Let A, B be sets, $R \subseteq A \times B$.
For any $S \subseteq A$ and any $T \subseteq B$ let

- $S^u := \{b \in B \mid \forall a \in S : aRb\}$
- $T^\ell := \{a \in A \mid \forall b \in T : aRb\}$.

Then

- the maps $T \mapsto T^\ell$ and $S \mapsto S^u$ are $\subseteq$-antitone.
- the maps $S \mapsto \bar{S} := S^{u\ell}$ and $T \mapsto \bar{T} := T^{\ell u}$ are closure operators ($S \subseteq \bar{S} = \bar{\bar{S}}$)
- $S^{u\ell u} = S^u$, $T^{\ell u \ell} = \ell$.

Usually it is of interest to characterize the family of *closed* sets $\{S \mid S = \bar{S}\}$ and the closure operator "from below".

Galois connections, examples

Let A, B be sets, $R \subseteq A \times B$.
$S^u := \{b \in B \mid \forall a \in S : aRb\} = \bigcap_{a \in S}\{b \in B \mid aRb\}$
$T^\ell := \{a \in A \mid \forall b \in T : aRb\} = \bigcap_{b \in T}\{a \in A \mid aRb\}$

Examples

- A = vector space, B = dual space = set of linear forms.
  $aRb \Leftrightarrow b(a) = 0$.
  $S \subseteq A \Rightarrow S^{u\ell}$ = linear hull of S.
- A = all formulas, B = all structures,
  $aRb \Leftrightarrow b \models a$ (the formula a holds in the structure b).
  $\bar{S}$ = all consequences of $S = \{a : S \models a\}$
- A = operations on X, B = relations, $fR\rho \Leftrightarrow f \rhd \rho$.
  $S^{u\ell} = \langle S \rangle$ = clone generated by S.

k-ary clones, clones

$\mathcal{O}^{(k)} := \{f \mid f : X^k \to X\}$. $\mathcal{O}_X := \bigcup_{k=1}^{\infty} \mathcal{O}_X^{(k)}$.

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.

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.

Definition (Composition)

Let $f \in \mathcal{O}^{(k)}$, $g_1, \ldots, g_k \in \mathcal{O}_X^{(m)}$.
$f(g_1, \ldots, g_k)(\vec{x}) := f(\, g_1(\vec{x}), \ldots, g_k(\vec{x})\,)$ for all $\vec{x} \in X^m$.
If C is a clone, then $C^{(k)} := C \cap \mathcal{O}^{(k)}$ is a k-ary clone, the k-ary fragment of C.

Vector-valued operations

C is a clone: $f, g_1, \ldots, g_k \in C \Rightarrow f(g_1, \ldots, g_k) \in C$).
We can view $(g_1, \ldots, g_k)$ as a single function $\vec{g} : X^m \to X^k$, and write $f \circ \vec{g}$ instead of $f(g_1, \ldots, g_k)$.

Definition

For any set $S \subseteq \mathcal{O}_X$ let $\tilde{S}$ be the set of all operations $f : X^k \to X^n$ with the property that all "components" are in S:

$$\tilde{S} := \bigcup_{k,n} \{f : X^k \to X^n \mid \forall i \in \{1, \ldots, n\} : \ \pi_i^n \circ f \in S)\}$$

where $\pi_i^n : X^n \to X$ is the i-th projection function.
The set S is a clone iff $\tilde{S}$ contains all projection functions and is closed under composition:

$$\forall g : X^m \to X^k \ \ \forall f : X^k \to X^n : (f, g \in \tilde{S} \Rightarrow f \circ g \in \tilde{S})$$

Examples of clones

- Every subset $S \subseteq \mathcal{O}_X$ will *generate* a clone $\langle S \rangle$, the smallest clone containing S.
- For any relation $\rho \subseteq X^n$: $\mathrm{Pol}(\rho) := \{f \in \mathcal{O}_X^{(|f)} \rhd \rho\}$ is a clone.
- For any relation $\rho \subseteq X^K$ (K infinite), $\mathrm{Pol}(\rho)$ is a clone.
- For any set R of relations, $\mathrm{POL}(R) := \bigcap_{\rho \in R} \mathrm{Pol}(\rho)$ is a clone.
- $\langle C \rangle = \mathrm{POL}(\mathrm{INV}(C))$, where $\mathrm{INV}(C) := \bigcap_{f \in C} \mathrm{Inv}(f)$, $\mathrm{Inv}(f) := \{\rho \mid f \rhd \rho\}$.
  (For infinite X, need to allow infinitary relations; operations still have finite arity!)

The lattice of all clones on X

For finite X, $\mathcal{O}_X$ is countable.
For infinite X of size κ, $\mathcal{O}_X$ has 2^κ elements.

Definition

For any nonempty set X let $Cl(X)$ be the set of all clones on X.
($Cl(X)$ is a subset of the power set of $\mathcal{O}_X$.)

- $Cl(X)$ is a complete lattice. (meet = intersection, join = clone generated by union)
- $Cl(X)$ is Countable for $|X| = 2$.
  (Post's lattice. wikipedia!)
- $Cl(X)$ is of size $|\mathbb{R}| = 2^{\aleph_0}$ for X finite with > 2 elements.
- For infinite X of size κ: $|Cl(X)| \leq 2^{2^\kappa}$.
  In fact: $= 2^{2^\kappa}$. (Later)

Minimal clones

Definition

We call a clone M *minimal* if $J \subsetneq M$ (J is the smallest clone, containing only the projections), but there is no clone D with $J \subsetneq D \subsetneq M$.

The minimal clones are the atoms of the clone lattice.

An operation m is minimal iff $\langle m \rangle$ is a minimal clone.

Instead of minimal clones we consider minimal operations.

If m is minimal, then $\forall f \in \langle m \rangle \setminus J : m \in \langle f \rangle$.

- If m is unary, then have $m \in \langle m^j \rangle$ for all j except if $m^j = id$. Hence $j^2 = id$ (“retraction”), or m is a permutation of prime order.
- If m not essentially unary, then m must be idempotent. $m(x, \ldots, x) = m$.

Minimal operations, examples

- Every constant operation.
- Every permutation whose order is a prime number.
- The meet operation of any meet-semilattice.
- The median operation in any linear order.
- ... (many more. Some necessary conditions known, but no explicit criterion.)

Fact

If X is finite, then there are finitely many minimal operations. Every clone $\neq J$ contains a minimal clone.

(This is not true for infinite sets. Let $s : \mathbb{Z} \to \mathbb{Z}$ be defined by $s(x) = x + 1$, then every non-projection in $\langle s \rangle$ is of the form s^j ($j \in \{1, 2, \ldots\}$, and none of them is minimal, as $\langle s^{2j} \rangle \subsetneq \langle s^j \rangle$.)

Complete sets

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

Proof for infinite X.

- Let $p_2 : X^2 \to X$ be a bijection.
- Find bijections $p_j : X^j \to X$ for $j = 3, 4, \ldots$, with $p_j \in \langle \mathcal{O}^{(2)} \rangle$.
  For example, $p_3(x, y, z) := p_2(x, p_2(y, z))$.
- For every $f : X^k \to X$, let $\hat{f} := f \circ p_k^{-1}$.
  So $f(\vec{x}) = \hat{f}(p_k(\vec{x}))$ for all $\vec{x} \in X^k$. As $\hat{f}$ is unary, $\hat{f} \in \langle \mathcal{O}^{(2)} \rangle$.
- From $\hat{f} \in \langle \mathcal{O}^{(2)} \rangle$ and $p_k \in \langle \mathcal{O}^{(2)} \rangle$ conclude $f \in \langle \mathcal{O}^{(2)} \rangle$.

Complete sets

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

Proof for finite X (“Lagrange interpolation”).

Let $(X, +, \cdot, 0, 1)$ be a finite lattice with smallest element 0 and greatest element 1. So $x + 0 = 0 + x = x = 1 \cdot x$ for all x.

- For each $a \in X$ let $\chi_a : X \to X$ be the characteristic function of the set $\{a\}$. So $\chi_a \in \mathcal{O}^{(1)} \subseteq \langle \mathcal{O}^{(2)} \rangle$.
- For each $\vec{a} \in X^k$ let $\chi_{\vec{a}} : X^k \to X$ be the characteristic function of $\{\vec{a}\}$: $\chi_{\vec{a}} = \prod_i \chi_{a_i}(x_i)$. So $\chi_{\vec{a}} \in \langle \mathcal{O}^{(2)} \rangle$.
- For any $b \in X$ let $c_b \in \mathcal{O}^{(1)}$ be constant with value b.
- Every operation $f \in \mathcal{O}^{(k)}$ can now be written as $f = \sum_{\vec{a} \in X^k} (\chi_{\vec{a}} \cdot c_{f(\vec{a})})$. So $f \in \langle \mathcal{O}^{(2)} \rangle$.

(Remark: This proof also works for strongly amorphous sets.)

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

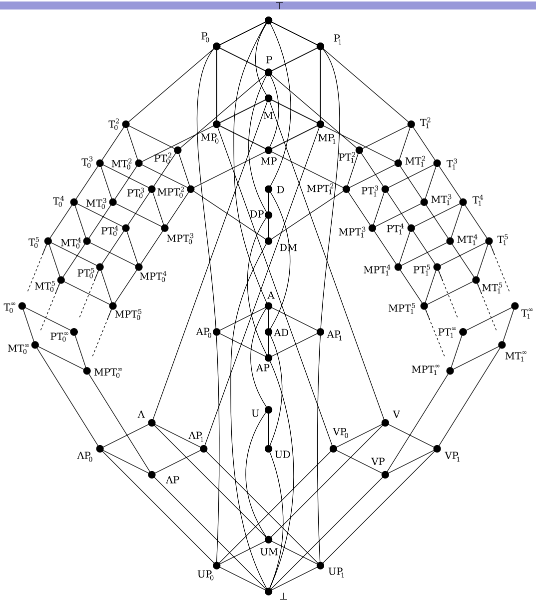
For any clone $C \subsetneq \mathcal{O}_X$ there is a precomplete clone C' with $C \subseteq C'$.

(Remark: Not true for infinite sets! At least if the continuum hypothesis holds.)

Post's lattice

The lattice of all clones on a 2-element set is countably infinite.

It has 5 coatoms ("precomplete" clones) and 7 atoms.



Precomplete clones, example 1

Let ρ be a nontrivial unary relation, i.e. $\emptyset \subsetneq \rho \subsetneq X$.
Then $\mathrm{Pol}(\rho)$ is the set of all operations f such that ρ is a subalgebra of (X, f). This clone is precomplete.

Proof.
Let $g : X^k \to X$, $g \notin \mathrm{Pol}(\rho)$. Let $C := \langle \mathrm{Pol}(\rho) \cup \{g\} \rangle$. We show $C = \mathcal{O}_X$. Sufficient: $C \supseteq \mathcal{O}_X^{(2)}$.
For $v \in X$, let c_v be the constant function with value v.
There are $\vec{a} = (a_1, \dots, a_k) \in \rho^k$, $b \notin \rho$ with $g(\vec{a}) = b$,
So $c_b = g(c_{a_1}, \dots, c_{a_k})$ is in C.
For $f \in \mathcal{O}_X^{(2)}$ define $\hat{f}(x_1, x_2, y) := \begin{cases} x_1 & \text{if } y \in \rho \\ f(x_1, x_2) & \text{if } y \notin \rho \end{cases}$. So $\hat{f} \in C$.
Now $f = \hat{f}(\pi_1^2, \pi_2^2, c_b)$, i.e., $f(x_1, x_2) = \hat{f}(x_1, x_2, b)$. So $f \in C$.

Precomplete clones, example 2

$\sim$ a nontrivial equivalence relation $\Rightarrow$ Pol($\sim$) is precomplete.

Proof.
For $\vec{a}, \vec{b} \in X^k$ write $\vec{a} \sim \vec{b}$ iff $\forall i\ a_i \sim b_i$. This is an equivalence relation on X^k.
Let $g : X^k \to X$, $g \notin \mathrm{Pol}(\sim)$. Let $C := \langle \mathrm{Pol}(\sim) \cup \{g\} \rangle$. We have to show $C = \mathcal{O}_X$. Sufficient: $C \supseteq \mathcal{O}_X^{(2)}$.
There is k and $\vec{a} \sim \vec{b} \in X^k$ with $1 := g(\vec{a}) \not\sim g(\vec{b}) =: 0$.
We claim that for each $p \in X^2$ there is a function $\chi_p : X^2 \to X$ which maps p to 1, everything else to $0 \not\sim 1$.
For each $p \in X^2$ let $h_p : X^2 \to X^k$ be defined by $h_p(p) = \vec{a}$, $h_p(x) = \vec{b}$ otherwise. Clearly $h_p \in \mathrm{Pol}(\widetilde{\sim})$. So $\chi_p := g \circ h_p \in C$.
(continued on next page)

Proof that Pol($\sim$) is precomplete, continued.

We started with a clone $C \supsetneq \mathrm{Pol}(\sim)$.
For each $p \in X^2$ we have found $\chi_p \in C$, $\chi_p : X^2 \to X$ with $\chi_p(p) = 1$, $\chi_p(x) = 0$ for $x \neq p$. (And $0 \not\sim 1$)
Define $\chi : X^2 \to X^{|X|^2}$ by $\chi(\vec{x}) = (\chi_p(x) : p \in X^2)$. So $\chi \in \tilde{C}$.
Let $f \in \mathcal{O}_X^{(2)}$ be arbitrary. We will show $f \in C$.
Define $\hat{f} : X^{2+|X|^2} \to X$ as follows:

- $\hat{f}$ is constant on each $\sim$-class. (So $\hat{f} \in \mathrm{Pol}(\sim) \subseteq C$)
- $\hat{f}(\vec{x}, \chi(\vec{x})) = f(\vec{x})$.

This two requirements are compatible, as $\vec{x} \neq \vec{x}'$ implies that $\chi(\vec{x}) \not\sim \chi(\vec{x}')$.
Clearly $f(\vec{x}) = \hat{f}(\vec{x}, \chi(\vec{x}))$. So $f \in C$.

Precomplete clones, example 3

Definition

Let $r : X \to X$, $f : X^k \to X$. We say that f commutes with r if:

$$\forall x_1, \ldots, x_k \in X : f(\, r(x_1), \ldots, r(x_k)\,) = r(\, f(x_1, \ldots, x_k)\,)$$

Writing $r^\bullet$ for the relation $\{(x, r(x)) \mid x \in X\}$, f commutes with r iff $f \rhd r^\bullet$. (We may write $f \rhd r$ instead of $f \rhd r^\bullet$)

Clearly $f \rhd r \Rightarrow f \rhd r^j$ for all j. Hence e.g. $\mathrm{Pol}(r) \subseteq \mathrm{Pol}(r^2)$. But if r is a permutation of order p, then $\mathrm{Pol}(r) = \mathrm{Pol}(r^j)$ whenever p does not divide j.

Theorem

Assume that $r : X \to X$ is a permutation and all cycles have the same prime length. Then $\mathrm{Pol}(r)$ is precomplete.

Precomplete clones, examples 4,5

- "monotone": Let $\rho \subseteq X \times X$ be a partial order with smallest and greatest element.
  Pol(ρ) is the set of all pointwise monotone operations.
- "affine" Assume $|X| = p^m$, so wlog X is a finite field $X = GF(p^m)$.
  Let $\rho = \{(a, b, c, d) \in X^4 \mid a + b = c + d\}$. Then Pol($\rho$) is the set of all operations f of the form

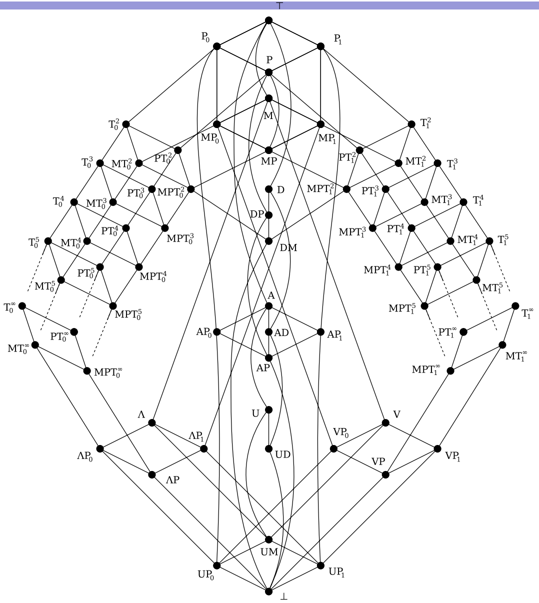
$$f(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} \sum_{j=0}^{m-1} x_i^{p^j}$$

All these clones are precomplete.

Post's lattice, again

The 5 precomplete clones in $Cl(\{0,1\})$:

- operations preserving $\{0\}$.
- operations preserving $\{1\}$.
- monotone operations
- "commuting": $f(\neg x) = \neg f(x)$.
- affine operations



Rosenberg's list

Theorem

Let $X = \{1, \ldots, k\}$. Then there is an explicit finite list of relations $\rho_1, \ldots, \rho_m$ such that every precomplete clone on X is one of $\mathrm{Pol}(\rho_1)$, ..., $\mathrm{Pol}(\rho_m)$.
The list includes

- *all "central relations" (generalisations of $\rho \subsetneq X$)*
- *all nontrivial equivalence relations ($\nexists$ if $|X| = 2$)*
- *all prime permutations*
- *All bounded partial orders*
- *affine relations (only if $|X| = p^n$)*
- *(others. more complicated but still explicit)*

Rosenberg's list

Theorem

Let $X = \{1, \ldots, k\}$. Then there is an explicit finite list of relations $\rho_1, \ldots, \rho_m$ such that every precomplete clone on X is one of Pol(ρ_1), *…,* Pol(ρ_m)*.*

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

A complicated interval in the clone lattice

Definition

Let C_{idem} be the clone of all idempotent operations: $f(x, \dots, x) = x$. (Assume $|X| \geq 3$.)

Find all clones between C_{idem} and $\mathcal{O}_X$!

Example

Let $Y \subseteq X$. Then $C_{\mathrm{idem}\restriction Y} := \{f \mid \forall x \in Y : f(x, \dots, x) = x\}$ is a clone $\supseteq C_{\mathrm{idem}}$.

Theorem

Every clone between C_{idem} and $\mathcal{O}_X$ is of the form $C_{\mathrm{idem}\restriction Y}$.
Hence: the interval $[C_{\mathrm{idem}}, \mathcal{O}_X]$ is (anti-)isomophic to the power set of X.
(Precomplete clones correspond to singletons, $\mathcal{O}_X$ to $\emptyset$.)

$[C_{\mathrm{idem}}, \mathcal{O}_X]$, proof sketch

Let C be a clone containing all idempotent operations $f(x,\dots,x) = x$.
We want to find Y such that
$C = C_{\mathrm{idem}\restriction Y}$ = $\{f \mid \forall y \in Y : f(y,\dots,y) = y\}$. .

- $\mathrm{fix}(f) := \{a \in X \mid f(a,\dots,a) = a\}$, $\mathrm{nix}(f) := X \setminus fix(f)$.
- Let $R := \{\mathrm{nix}(f) \mid f \in C\}$.
- R is downward closed.
- R is upward directed, hence an ideal.
- Let Z be the largest element of R, $Y := X \setminus Z$.
- So $C \subseteq C_{\mathrm{idem}\restriction Y}$.
- If $\mathrm{nix}(f) \subseteq \mathrm{nix}(g)$ and $g \in C$, then $f \in C$.
- Hence $C = C_{\mathrm{idem}\restriction Y}$.

A complicated interval, continued

C_{idem} = the clone of all idempotent operations: $f(x, \ldots, x) = x$.

Theorem (X finite)

Every clone between C_{idem} and $\mathcal{O}_X$ is of the form $C_{\mathrm{idem}\restriction Y}$.

For infinite X:

Definition

For every filter $\mathcal{F}$ on X, let

$$C_{\mathcal{F}} := \bigcup_{Y \in \mathcal{F}} C_{\mathrm{idem}\restriction Y} = \{f \mid \exists Y \in \mathcal{F}\ \forall y \in Y\ f(y, \ldots, y) = y\}$$

Each $C_{\mathcal{F}}$ is a clone above C_{idem}.

A complicated interval, conclusion

$$C_{\mathcal{F}} := \{f \mid \exists Y \in \mathcal{F}\ \forall y \in Y\ f(y, \ldots, y) = y\}$$

Theorem

Let X be any set. Then the map $\mathcal{F} \mapsto C_{\mathcal{F}}$ is an order-preserving bijection between the filters on X and the clones above $C_{\mathcal{F}}$. Ultrafilters correspond to precomplete clones in this interval, and the improper filter corresponds to $\mathcal{O}_X$. (For finite sets, all filters are principal.)

Translation to topology: the interval $[C_{\mathrm{idem}}, \mathcal{O}_X]$ is anti-isomorphic to the family of closed sets of βX, the Čech-Stone compactification of the discrete space X. (Precomplete clones correspond to points, $\mathcal{O}_X$ to $\emptyset$.)

Another complicated interval

Let X be infinite. We will find "very many" clones with trivial unary fragment, i.e., below C_{idem}, the clone of all idempotent operations. (Unfortunately: no complete classification.)
In fact all our operations will be "conservative":
$f(x_1, \dots, x_k) \in \{x_1, \dots, x_k\}$.

- Let $(A_i : i \in I)$ be a family of sufficiently independent sets. (In particular: we demand that for any finite $I_0 \subseteq I$ and any $j \in I \setminus I_0$ the set $(\cup_{i \in I_0} A_i) \cap (X \setminus A_j)$ contains at least 2 elements. It is possible to find such a family with $2^{|X|}$ elements, in particular: an uncountable such family.)
- Fix a linear order $\leq_i$ on A_i, with minimum operation $\wedge_i$.
- Extend $\wedge_i$ to X by requiring $x \wedge_i y = x$ outside A_i.
- For any $I' \subseteq I$ let $C_{I'} := \langle\{\wedge_i \mid i \in I'\}\rangle$. Then all $C_{I'}$ are distinct. (Note: the numbers of such clones = $2^{2^{|X|}}$!)

Local clones

Let X be infinite. A clone C is local if each fragment $C \cap \mathcal{O}_X k$ is closed in the product topology (pointwise convergence) on X^{X^k} (with discrete X). Equivalently: If there is a set R of relations of finite arity such that $C = \text{POL}(R)$.

The lattice of local clones has only $2^{|X|}$ elements; the lattice of all clones: $2^{2^{|X|}}$.

Example:

On a finite set with k elements, the intervall $[\mathcal{O}_X^{(1)}, \mathcal{O}_X]$ has $k+1$ elements.

On any infinite set X, the intervall $[\mathcal{O}_X^{(1)}, \mathcal{O}_X]$ in the lattice of all clones has at least $2^{2^{|\mathbb{N}|}}$ elements.

On any infinite set X, the intervall $[\mathcal{O}_X^{(1)}, \mathcal{O}_X]$ in the lattice of *local clones* has at only countably many elements.

Bonus round: non-AC

We used $X \times X \approx X$ to show that $\langle \mathcal{O}_X^{(2)} \rangle = \mathcal{O}_X$ (for infinite sets X). But $X \times X \approx X$ uses the axiom of choice (and in fact $\forall X$ infinite : $X \times X \approx X$ is equivalent to AC). Was that necessary?
Yes, probably.

Proof sketch. Really: a hint. An idea of a hint. No satisfaction guaranteed.

Let (M, R_3) be the "random 3-uniform hypergraph". That is, R_3 is a totally symmetric totally irreflexive relation which is "as random as possible". For example: For all (reasonable) finite sets $\{a_1, b_1, \ldots, a_k, b_k, c_1, d_1, \ldots, c_n, d_n\} \subseteq M$ there is some $e \in M$ with $R(a_i, b_i, e)$ for all i, and $\neg R(c_j, d_j, e)$ for all j.
(Technically: the Fraïssé limit of all finite 3-uniform hypergraphs.)

non-AC, continued

Continuation of the proof.

Let (M, R_3) be the "random 3-uniform hypergraph". (M countable, $R_3 \subseteq M^3$ is "random" or "generic".)
Let $f_1, \dots, f_m$ be first order definable binary operations, say definable from $m_1, \dots, m_k$ in the structure (M, R). Then the set $X \times X$ can be partitioned into finitely many sets according to the "type" a pair (x, y) can have over $m_1, \dots m_k$. On each type each operation f_i must be either constant or a projection, so the same is true for any element of $\langle f_1, \dots, f_k \rangle$. But the function χ_R is neither a projection or a constant on any type. So we have found a definable ternary function not in the clone generated by the definable binary functions.

non-AC, conclusion

We have found a definable ternary function on (M, R), definable from R, but not in the clone generated by the definable binary functions.

Now construct a model of ZF+$\neg$AC in which all operations on M are definable from R and finitely many parameters. In this model, all binary operations are trivial on a large set, but not all ternary operations.

Summary

- The clone lattice on $\{0, 1\}$ is well understood. (But nontrivial.)
- $Cl(X)$ for larger finite sets X: many fragments are explicitly known (certain intervals, coatoms, ...), others only partially (atoms), or only for very small sets (say, $|X| \leq 4, 5$).
- To analyse k-ary operations, it is often helpful to consider $k+1$-ary operations. (Or $2k$-ary. or $(k + |X|^2)$-ary, etc.)
- Many open questions.
- For infinite X: set theory kicks in. Local clones more interesting than all clones?

Thank you
for your attention!
and for your questions!
. . . and for your corrections!!