Generalizing the clone–coclone Galois connection

Emil Jeřábek
jerabek@math.cas.cz
http://math.cas.cz/~jerabek/

Institute of Mathematics of the Academy of Sciences, Prague

Topology, Algebra, and Categories in Logic, June 2015, Ischia
Clones and coclones:
the classical case

1. Clones and coclones: the classical case
2. Interlude: reversible computing
3. Clones and coclones revamped
Fix a base set $B$

### Definition

A clone is a set $\mathcal{C}$ of functions $f : B^n \to B$, $n \geq 0$, s.t.

- the projections $\pi_{n,i} : B^n \to B$, $\pi_{n,i}(\vec{x}) = x_i$, are in $\mathcal{C}$
- $\mathcal{C}$ is closed under composition:
  
  if $g : B^m \to B$ and $f_i : B^n \to B$ are in $\mathcal{C}$, then
  
  $$h(\vec{x}) = g(f_0(\vec{x}), \ldots, f_{m-1}(\vec{x})) : B^n \to B$$

  is in $\mathcal{C}$
Clones (cont’d)

- Clone generated by a set of functions \( \mathcal{F} \)
  
  \[ \begin{align*}
&= \text{term functions of the algebra } \langle B, \mathcal{F} \rangle \\
&= \text{functions computable by circuits over } B \text{ using } \mathcal{F}\text{-gates}
\end{align*} \]
  
  - Classical computing: clones on \( B = \{0, 1\} \) completely classified by [Post41]

- Clones can be studied by means of relations they preserve
$f : B^n \rightarrow B$ preserves $r \subseteq B^k$: 

\[
\begin{array}{ccccccc}
  a_0 & \cdots & a_j & \cdots & a_{n-1} & b^0 \\
  \vdots & & \vdots & & \vdots & \\
  a_i^0 & \cdots & a_i^j & \cdots & a_i^{n-1} & b^i \\
  \vdots & & \vdots & & \vdots & \\
  a_i^{k-1} & \cdots & a_i^{k-1} & \cdots & a_i^{k-1} & b^{k-1} \\
  \vdots & & \vdots & & \vdots & \\
  a_i & \cdots & a_i & \cdots & a_i & \\
  \text{r} & \cdots & \text{r} & \cdots & \text{r} & \text{r} \\
\end{array}
\]

$\text{r} \subseteq B$
Galois connection

\( \mathcal{F} \) set of functions, \( \mathcal{R} \) set of relations

Invariants and polymorphisms:

\[
\begin{align*}
\text{Inv}(\mathcal{F}) &= \{ r : \forall f \in \mathcal{F} \text{ f preserves } r \} \\
\text{Pol}(\mathcal{R}) &= \{ f : \forall r \in \mathcal{R} \text{ f preserves } r \}
\end{align*}
\]

\( \implies \) Galois connection: \( \mathcal{R} \subseteq \text{Inv}(\mathcal{F}) \iff \mathcal{F} \subseteq \text{Pol}(\mathcal{R}) \)

- \( \text{Pol}(\text{Inv}(\mathcal{F})), \text{Inv}(\text{Pol}(\mathcal{R})) \) closure operators
  closed sets = range of \( \text{Pol}, \text{Inv} \) (resp.)

- \( \text{Inv}, \text{Pol} \) are mutually inverse dual isomorphisms of the complete lattices of closed sets
**Theorem [Gei68,BKKR69]**

If $B$ is finite:

- Galois-closed sets of functions = clones
- Galois-closed sets of relations = coclones

**Definition**

Coclone = set of relations closed under definitions by primitive positive FO formulas:

\[ R(x^0, \ldots, x^{k-1}) \iff \exists x^k, \ldots, x^l \bigwedge_{i < m} \varphi_i(x^0, \ldots, x^l) \]

where each $\varphi_i$ is atomic
Equivalently: a set of relations is a coclone if it contains the identity $x_0 = x_1$, and is closed under

- variable permutation and identification
- finite Cartesian products and intersections
- projection on a subset of variables

Closely related to constraint satisfaction problems
Variants

A host of generalizations of this Galois connection appear in the literature (e.g., [Isk71,Ros71,Ros83,Cou05,Ker12]):

- infinite base set
- partial functions, multifunctions
- functions $A^n \to B$
- categorial setting
- . . .
Interlude: reversible computing

1. Clones and coclones: the classical case

2. Interlude: reversible computing

3. Clones and coclones revamped
Computation in the physical world

Conventional models: computation can destroy the input on a whim

\[ \langle x, y \rangle \mapsto x + y \]

Reality check:

**Landauer’s principle**

Erasure of \( n \) bits of information incurs an \( n k \log 2 \) increase of entropy elsewhere in the system

\[ \implies \text{dissipates energy as heat} \]

The underlying time-evolution operators of quantum field theory are reversible
Reversible computing

Reversible computation models: only allow operations that can be inverted

\( \langle x, y \rangle \mapsto \langle x, x + y \rangle \)

Typical formalisms: circuits using reversible gates

- Classical computing:
  - motivated by energy efficiency
  - \( n \)-bit reversible gate = permutation \( \{0, 1\}^n \rightarrow \{0, 1\}^n \)

- Quantum computing:
  - \( n \) qubits of memory = Hilbert space \( \mathbb{C}^{2^n} \)
  - quantum gate = unitary linear operator
    \( \Rightarrow \) inherently reversible
Clones of reversible transformations

Reversible operations computable from a fixed set of gates:

- variable permutations, dummy variables
- composition
- ancilla bits: preset constant inputs, required to return to the original state at the end

⇒ notion of “reversible clones”

Recently: [AGS15] gave complete classification for $B = \{0, 1\}$ (≈ Post’s lattice for reversible operations)
Clones and coclones: the classical case

Interlude: reversible computing

Clones and coclones revamped
Goal

Generalize the clone–coclone Galois connection to encompass reversible clones

Let’s first have a look at some simple reversible clones on \( \{0, 1\} \)
Examples

- **Conservative operations** $f : \{0, 1\}^n \to \{0, 1\}^n$
  
  preserve Hamming weight

  $$f(\vec{a}) = \vec{b} \implies \sum_{i<n} a_i = \sum_{i<n} b_i$$

- **Mod-$k$ preserving operations**: Hamming weight modulo $k$

  $$f(\vec{a}) = \vec{b} \implies \sum_{i<n} a_i \equiv \sum_{i<n} b_i \pmod{k}$$

Permutations “can count”: invariants can’t be just relations
Examples (cont’d)

▶ **Affine** operations $f : \{0, 1\}^n \to \{0, 1\}^n$

$$f(\vec{x}) = A\vec{x} + \vec{c}, \text{ where } \vec{c} \in \mathbb{F}_2^n, \ A \in \mathbb{F}_2^{n \times n} \text{ non-singular}$$

▶ $\iff$ each component $f_i : \{0, 1\}^n \to \{0, 1\}$ affine

▶ classical invariant: $f_i$ affine $\iff$ preserves the relation $a + b + c + d = 0$ on $\mathbb{F}_2^4$

▶ let $w : \mathbb{F}_2^4 \to \mathbb{F}_2$, $w(a^0, a^1, a^2, a^3) = a^0 + a^1 + a^2 + a^3$

▶ identify $\mathbb{F}_2 = \{0, 1\} = \langle \{0, 1\}, 0, \lor \rangle$

▶ $f : \{0, 1\}^n \to \{0, 1\}^m$ affine $\iff$

$$f(a_0^0, \ldots, a_{n-1}^0) = \langle b_0^0, \ldots, b_{m-1}^0 \rangle, \ldots,$$

$$f(a_0^3, \ldots, a_{n-1}^3) = \langle b_0^3, \ldots, b_{m-1}^3 \rangle$$

implies

$$\bigvee_{i<n} w(a_i^0, a_i^1, a_i^2, a_i^3) \geq \bigvee_{i<m} w(b_i^0, b_i^1, b_i^2, b_i^3)$$
General case

We consider a preservation relation between

- partial multifunctions $f : B^n \Rightarrow B^m$
  - formally: $f \subseteq B^n \times B^m$, $n, m \geq 0$
  - $f(\vec{x}) \approx \vec{y}$ denotes $\langle \vec{x}, \vec{y} \rangle \in f$
  - $Pmf = \bigcup_{n,m} Pmf_{n,m}$

- “weight functions” $w : B^k \rightarrow M$
  - $\langle M, 1, \cdot, \leq \rangle$ partially ordered monoid, $k \geq 0$
  - $Wgt = \bigcup_k Wgt_k$
$f : B^n \Rightarrow B^m$ preserves $w : B^k \rightarrow M$:

\[
\begin{array}{ccc}
a_0 & \cdots & a_j & \cdots & a_{n-1} \\
\vdots & & \vdots & & \vdots \\
a_i^0 & \cdots & a_i^j & \cdots & a_i^{n-1} \\
\vdots & & \vdots & & \vdots \\
a_i^{k-1} & \cdots & a_i^{k-1} & \cdots & a_i^{n-1} \\
\end{array} \quad \xrightarrow{f} \quad 
\begin{array}{ccc}
b_0^0 & \cdots & b_0^{m-1} \\
\vdots & & \vdots \\
b_i^0 & \cdots & b_i^{m-1} \\
\vdots & & \vdots \\
b_i^{k-1} & \cdots & b_i^{k-1} \\
\end{array}
\]

\[
\begin{array}{c}
w(a_0) \cdots w(a_j) \cdots w(a_{n-1}) \\
w(b_0) \cdots w(b_{m-1})
\end{array}
\]
The preservation relation induces a Galois connection.

**Definition**

If $\mathcal{F} \subseteq \text{Pmf}$, $\mathcal{W} \subseteq \text{Wgt}$:

$$\text{Inv}(\mathcal{F}) = \{ w \in \text{Wgt} : \forall f \in \mathcal{F} \text{ } f \text{ preserves } w \}$$

$$\text{Pol}(\mathcal{W}) = \{ f \in \text{Pmf} : \forall w \in \mathcal{W} \text{ } f \text{ preserves } w \}$$

What are the **closed classes**?
Pol(\mathcal{W}) has the following properties:

**Definition**

\[ \mathcal{C} \subseteq \text{Pmf} \text{ is a pmf clone if} \]

- (identity) \[ \text{id}_n : B^n \to B^n \text{ is in } \mathcal{C} \]

- (composition) \[ f : B^n \Rightarrow B^m, \ g : B^m \Rightarrow B^r \text{ in } \mathcal{C} \]
  \[ \implies g \circ f : B^n \Rightarrow B^r \text{ in } \mathcal{C} \]

- (products) \[ f : B^n \Rightarrow B^m, \ g : B^n' \Rightarrow B^m' \text{ in } \mathcal{C} \]
  \[ \implies f \times g : B^{n+n'} \Rightarrow B^{m+m'} \text{ in } \mathcal{C} \]

\[ (f \times g)(x, x') \approx \langle y, y' \rangle \iff f(x) \approx y, g(x') \approx y' \]

- (topology) \[ \mathcal{C} \cap \text{Pmf}_{n,m} \text{ is topologically closed . . .} \]
Topological closure

Two interesting topologies on \( \{0, 1\} \):

- \( \{0, 1\}_H \) discrete (Hausdorff)
- \( \{0, 1\}_S \) Sierpiński: \( \{0\} \) closed, but \( \{1\} \) not

Lemma

Let \( C \subseteq \mathcal{P}(X) \simeq \{0, 1\}^X \). TFAE:

- \( C \) is closed in \( \{0, 1\}_S \)
- \( C \) is closed in \( \{0, 1\}_H \) and under subsets
- \( C \) is closed under directed unions and subsets
- \( Y \in C \) iff all finite \( Y' \subseteq Y \) are in \( C \)

Previous slide: apply to \( \text{Pmf}_{n,m} = \mathcal{P}(B^n \times B^m) \)
Coclones

Inv(𝒇) has the following properties:

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>D ⊆ Wgt is a weight coclone if</td>
</tr>
<tr>
<td>▶ (variable manipulation) w: B^k → M in D, ϱ: k → l</td>
</tr>
<tr>
<td>[⇒ w(x^{ϱ(0)}, \ldots, x^{ϱ(k−1)}): B^l → M in D ]</td>
</tr>
<tr>
<td>▶ (homomorphisms) w: B^k → M in D, ϕ: M → N</td>
</tr>
<tr>
<td>[⇒ ϕ ∘ w: B^k → N in D ]</td>
</tr>
<tr>
<td>▶ (direct products) w_α: B^k → M_α in D (α ∈ I)</td>
</tr>
<tr>
<td>[⇒ \langle w_α(x) \rangle_{α ∈ I}: B^k → \prod_{α ∈ I} M_α in D ]</td>
</tr>
<tr>
<td>▶ (submonoids) w: B^k → M in D, w[B^k] ⊆ N ⊆ M</td>
</tr>
<tr>
<td>[⇒ w: B^k → N in D ]</td>
</tr>
</tbody>
</table>
Galois connection

**Main theorem**

For any $B$:
- Galois-closed sets of pmf $= \text{pmf clones}$
- Galois-closed classes of weights $= \text{weight coclones}$

Emil Jeřábek

Generalizing the clone–coclone Galois connection | TACL 2015
Smaller invariants

Invariants of a pmf clone $C$ form a proper class

Better: $C = \text{Pol}(\mathcal{W})$ s.t. for each $w : B^k \to M$ in $\mathcal{W}$:

- $M$ is generated by $w[B^k]$
  - call such weights tight
  - $M$ finitely generated if $B$ finite

- $M$ is subdirectly irreducible (as a pomonoid)

Interesting case: (unordered) commutative monoids

- f.g. subdirectly irreducible are finite [Mal58]
- known structure [Sch66,Gri77]
Variants

We might want to restrict \textit{Pmf} or \textit{Wgt}, or impose additional \textit{closure conditions}, e.g.

\begin{itemize}
  \item \textbf{dimensions} of \( f : B^n \Rightarrow B^m \):
    \begin{itemize}
      \item \( n, m \geq 1, m = 1, n = m \)
    \end{itemize}
  \item \textbf{“shape”} of \( f \):
    \begin{itemize}
      \item (partial/total) functions, permutations
    \end{itemize}
  \item \textbf{constraints on monoids}:
    \begin{itemize}
      \item commutative, unordered
    \end{itemize}
  \item \textbf{constants, ancillas}
\end{itemize}
Dimension constraints

\( f : B^n \Rightarrow B^m \) with simple restrictions on \( n, m \) form clones
\( \iff \) correspond to inclusion of particular weights:

- \( n, m \geq 1 \): constant weight \( c_1 : B^0 \rightarrow \langle \{0, 1\}, 0, \lor, = \rangle \)
- \( n = m \): \( c_1 : B^0 \rightarrow \langle \mathbb{N}, 0, +, = \rangle \)

\( m = 1 \): a clone \( C \) is determined by \( f : B^n \Rightarrow B \) iff it contains the diagonal maps \( \Delta_n : B \rightarrow B^n, \Delta_n(x) = \langle x, \ldots, x \rangle \)

On the dual side:

- tight \( w : B^k \rightarrow M \) in \( \text{Inv}(C) \) are \( \{\land, \top\}\)-semilattices
- subdirectly irreducible: \( M = \langle \{0, 1\}, 1, \land, \leq \rangle \)
  \( \Rightarrow \) weight functions = relations
  \( \Rightarrow \) agrees with the classical description
Monoid restrictions

- Classes of weights \( w : B^k \to M \) with \( M \) commutative
  \( \iff \) clones containing variable permutations
  \[
  \langle x_0, \ldots, x_{n-1} \rangle \mapsto \langle x_{\pi(0)}, \ldots, x_{\pi(n-1)} \rangle
  \]

- Classes of weights \( w : B^k \to \langle M, 1, \cdot, = \rangle \)
  (i.e., unordered monoids)
  \( \iff \) clones closed under inverse
  \[
  f : B^n \Rightarrow B^m \text{ in } C \implies f^{-1} : B^m \Rightarrow B^n \text{ in } C
  \]
Uniqueness conditions

Partial functions form a clone \(\implies\)

\(\mathcal{C}\) consists of partial functions iff

\(\text{Inv}(\mathcal{C})\) includes a particular weight:

- Kronecker delta \(\delta: B^2 \to \langle\{0, 1\}, 1, \land, \leq\rangle\)

Symmetrically:

\(\mathcal{C}\) consists of injective pmf iff

\(\text{Inv}(\mathcal{C})\) includes

\[\delta: B^2 \to \langle\{0, 1\}, 1, \land, \geq\rangle\]
Totality conditions

In the classical case:

- **totality** of functions in $C \iff$ closure of $\text{Inv}(C)$ under existential quantification
- doesn’t work well over infinite (uncountable) $B$

**Definition**

$$w : B^{k+1} \to \langle M, 1, \cdot, \leq \rangle \text{ weight, } \langle M, 1, \cdot, 0, + \rangle \text{ semiring}$$

Define $w^+ : B^k \to \langle M, 1, \cdot, \leq \rangle$ by

$$w^+(x^0, \ldots, x^{k-1}) = \sum_{u \in B} w(x^0, \ldots, x^{k-1}, u)$$
Orders on semirings

**Definition**

- **positively ordered semiring** $= \langle M, 1, \cdot, 0, +, \leq \rangle$ s.t.
  - $\langle M, 1, \cdot, 0, + \rangle$ semiring
  - $\langle M, 1, \cdot, \leq \rangle$ and $\langle M, 0, +, \leq \rangle$ pomonoids, $0 \leq 1$

  $= \text{partially ordered semiring with least element } 0$

- **∨-semiring** $= \text{idempotent positively ordered semiring}$
  - $+ = \lor$

- **complete ∨-semiring:**
  - ∨-semiring, complete lattice
  - infinite distributive laws

\[
\left( \bigvee_{i \in I} x_i \right) y = \bigvee_{i \in I} x_i y \\
y \bigvee_{i \in I} x_i = \bigvee_{i \in I} y x_i
\]
Total clones

\[ C = \text{Pol}(D), \; D = \text{Inv}(C) \]

For \( B \) countable, the following are equivalent:

- \( C \) is generated by total multifunctions
- \( w : B^{k+1} \rightarrow M \) is in \( D \), \( M \) is a complete \( \lor \)-semiring
  \[ \implies w^+ : B^k \rightarrow M \text{ is in } D \]

A symmetric condition characterizes clones of surjective pmf

For \( B \) finite, TFAE:

- \( C \) is generated by mf extending a bijective function
- \( w : B^{k+1} \rightarrow M \) is in \( D \), \( M \) is a positively ordered semiring
  \[ \implies w^+ : B^k \rightarrow M \text{ is in } D \]
Ancillas

\[ C = \text{Pol}(D), \quad D = \text{Inv}(C) \]

The following are equivalent:

- **C supports ancillas**
  \[ a \in B, \quad f : B^{n+1} \Rightarrow B^{m+1} \text{ in } C \quad \iff \quad f_a : B^n \Rightarrow B^m \text{ in } C \]
  \[ f_a(\vec{x}) \approx \vec{y} \iff f(a, \vec{x}) \approx \langle a, \vec{y} \rangle \]

- **D is generated by** \( w : B^k \to M \) s.t. the diagonal weights \( z = w(u, \ldots, u) \) for \( u \in B \) are left-order-cancellative
  \[ zx \leq zy \implies x \leq y \]

Interferes with totality, but it mostly sorts itself out
The standard clone–coclone duality extends to a Galois connection between partial multifunctions $B^n \Rightarrow B^m$ and pomonoid-valued functions $B^k \rightarrow M$

Gracefully restricts to natural subclasses, such as total functions $B^n \rightarrow B^m$

Question

Does it generalize further?

Is it connected to some known duality involving pomonoids?
Thank you for attention!
References


- D. Geiger: *Closed systems of functions and predicates*, Pacific J. Math. 27 (1968), 95–100

References (cont’d)

- E. Jeřábek: Answer to [Aaronson14], Th. Comp. Sci. SE, 2014
- S. Kerkhoff: A general Galois theory for operations and relations in arbitrary categories, Algebra Universalis 68 (2012), 325–352
- E. L. Post: The two-valued iterative systems of mathematical logic, Princeton University Press, 1941