Galois connection for multiple-output operations

Emil Jeřábek

jerabek@math.cas.cz

http://math.cas.cz/~jerabek/

Institute of Mathematics of the Czech Academy of Sciences, Prague

96. Arbeitstagung Allgemeine Algebra, June 2018, Darmstadt

Clones and coclones: the classical case

Clones

Fix a base set B

Definition

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

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

Clones (cont'd)

- Clone generated by a set of functions $\mathcal{F}$

  $=$ term functions of the algebra $(B, \mathcal{F})$

  $=$ functions computable by circuits over B using $\mathcal{F}$-gates

  - Classical computing: clones on $B = \{0, 1\}$ completely classified by [Post41]

- Clones can be studied by means of relations they preserve

Preservation

$f\colon B^n \to B$ preserves $r \subseteq B^k$:

$$
\begin{array}{ccccccc}
a_0^0 & \cdots & a_j^0 & \cdots & a_{n-1}^0 & & b^0 \\
\vdots & & \vdots & & \vdots & f & \vdots \\
a_0^i & \cdots & a_j^i & \cdots & a_{n-1}^i & \longrightarrow & b^i \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_0^{k-1} & \cdots & a_j^{k-1} & \cdots & a_{n-1}^{k-1} & & b^{k-1} \\
 & & & & & & \\
\rotatebox{90}{$\in$} & \cdots & \rotatebox{90}{$\in$} & \cdots & \rotatebox{90}{$\in$} & \Longrightarrow & \rotatebox{90}{$\in$} \\
r & & r & & r & & r
\end{array}
$$

Galois connection

$\mathcal{F}$ set of functions, $\mathcal{R}$ set of relations

Invariants and polymorphisms:

$$\mathrm{Inv}(\mathcal{F}) = \{r : \forall f \in \mathcal{F}\ f \text{ preserves } r\}$$
$$\mathrm{Pol}(\mathcal{R}) = \{f : \forall r \in \mathcal{R}\ f \text{ preserves } r\}$$

$\Longrightarrow$ Galois connection: $\mathcal{R} \subseteq \mathrm{Inv}(\mathcal{F}) \iff \mathcal{F} \subseteq \mathrm{Pol}(\mathcal{R})$

- $\mathrm{Pol}(\mathrm{Inv}(\mathcal{F}))$, $\mathrm{Inv}(\mathrm{Pol}(\mathcal{R}))$ closure operators
  closed sets = range of Pol, Inv (resp.)
- Inv, Pol are mutually inverse dual isomorphisms of the complete lattices of closed sets

Basic correspondence

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:

$$R(x^0, \dots, x^{k-1}) \Leftrightarrow \exists x^k, \dots, x^l \bigwedge_{i<m} \varphi_i(x^0, \dots, x^l)$$

where each φ_i is atomic

Coclones (cont'd)

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,Pös80,Ros83,Cou05,Ker12]):

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

Interlude: reversible computing

Computation in the physical world

Conventional models:

computation can destroy the input on a whim

$$(x, y) \mapsto x + y$$

Reality check:

Landauer's principle

Erasure of n bits of information incurs an $n\,kT\log 2$ increase of entropy elsewhere in the system

$\implies$ dissipates energy as heat

Time-evolution operators in quantum mechanics are reversible

Reversible computing

Reversible computation models:
only allow operations that can be inverted

$$(x, y) \mapsto (x, x + y)$$

Typical formalisms: circuits using reversible gates

- Classical computing:
  - motivated by energy efficiency
  - n-bit reversible gate = permutation $\{0,1\}^n \to \{0,1\}^n$
- Quantum computing:
  - n qubits of memory = Hilbert space $\mathbb{C}^{2^n}$
  - quantum gate = unitary linear operator
    $\implies$ 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

$\Longrightarrow$ notion of "reversible clones"

Recently: [AGS15] gave complete classification for $B = \{0, 1\}$

($\approx$ Post's lattice for reversible operations)

Clones and coclones revamped

$\downarrow$

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 $f\colon \{0,1\}^n \to \{0,1\}^n$ 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 $f\colon \{0,1\}^n \to \{0,1\}^n$
  $f(\vec{x}) = A\vec{x} + \vec{c}$, where $\vec{c} \in \mathbb{F}_2^n$, $A \in \mathbb{F}_2^{n\times n}$ non-singular
  - $\iff$ each component $f_i\colon \{0,1\}^n \to \{0,1\}$ affine
  - classical invariant: f_i affine $\iff$ preserves the relation $a+b+c+d=0$ on $\mathbb{F}_2^4$
  - let $w\colon \mathbb{F}_2^4 \to \mathbb{F}_2$, $w(a^0,a^1,a^2,a^3) = a^0+a^1+a^2+a^3$
  - identify $\mathbb{F}_2 = \{0,1\} = (\{0,1\},0,\vee)$
  - $f\colon \{0,1\}^n \to \{0,1\}^m$ affine $\iff$
    $f(a^0_0,\dots,a^0_{n-1}) = (b^0_0,\dots,b^0_{m-1}),\dots,$
    $f(a^3_0,\dots,a^3_{n-1}) = (b^3_0,\dots,b^3_{m-1})$
    implies
    $$\bigvee_{i<n} w(a_i^0,a_i^1,a_i^2,a_i^3) \ge \bigvee_{i<m} w(b_i^0,b_i^1,b_i^2,b_i^3)$$

General case

We consider a preservation relation between

- partial multifunctions $f\colon B^n \rightrightarrows B^m$
  - formally: $f \subseteq B^n \times B^m$, $n, m \geq 0$
  - $f(\vec{x}) \approx \vec{y}$ denotes $(\vec{x}, \vec{y}) \in f$
  - $\mathrm{Pmf} = \bigcup_{n,m} \mathrm{Pmf}_{n,m}$
- "weight functions" $w\colon B^k \to M$
  - $(M, 1, \cdot, \leq)$ partially ordered monoid, $k \geq 0$
  - $\mathrm{Wgt} = \bigcup_k \mathrm{Wgt}_k$

Preservation

$f\colon B^n \rightrightarrows B^m$ preserves $w\colon B^k \to M$:

$$
\begin{array}{ccccccccc}
a_0^0 & \cdots & a_j^0 & \cdots & a_{n-1}^0 & & b_0^0 & \cdots & b_{m-1}^0 \\
\vdots & & \vdots & & \vdots & f & \vdots & & \vdots \\
a_0^i & \cdots & a_j^i & \cdots & a_{n-1}^i & \longrightarrow & b_0^i & \cdots & b_{m-1}^i \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
a_0^{k-1} & \cdots & a_j^{k-1} & \cdots & a_{n-1}^{k-1} & & b_0^{k-1} & \cdots & b_{m-1}^{k-1}
\end{array}
$$

$$\downarrow w \qquad\qquad \downarrow$$

$$w(a_0) \cdots w(a_j) \cdots w(a_{n-1}) \quad \le \quad w(b_0) \cdots w(b_{m-1})$$

Invariants and polymorphisms

The preservation relation induces a Galois connection

Definition

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

$$\begin{aligned}
\mathrm{Inv}(\mathcal{F}) &= \{w \in \mathrm{Wgt} : \forall f \in \mathcal{F}\ f \text{ preserves } w\} \\
\mathrm{Pol}(\mathcal{W}) &= \{f \in \mathrm{Pmf} : \forall w \in \mathcal{W}\ f \text{ preserves } w\}
\end{aligned}$$

What are the closed classes?

Clones

Pol($\mathcal{W}$) has the following properties:

Definition

$\mathcal{C} \subseteq \mathrm{Pmf}$ is a pmf clone if

- (identity) $\mathrm{id}_n \colon B^n \to B^n$ is in $\mathcal{C}$
- (composition) $f \colon B^n \Rightarrow B^m$, $g \colon B^m \Rightarrow B^r$ in $\mathcal{C}$ $\implies g \circ f \colon B^n \Rightarrow B^r$ in $\mathcal{C}$
- (products) $f \colon B^n \Rightarrow B^m$, $g \colon B^{n'} \Rightarrow B^{m'}$ in $\mathcal{C}$ $\implies f \times g \colon B^{n+n'} \Rightarrow B^{m+m'}$ in $\mathcal{C}$

  $$(f \times g)(x, x') \approx (y, y') \iff f(x) \approx y, g(x') \approx y'$$

- (topology) $\mathcal{C} \cap \mathrm{Pmf}_{n,m}$ is topologically closed ...

Topological/local closure

Two interesting topologies on $\{0,1\}$:

- $\mathbf{2}_H$ discrete (Hausdorff)
- $\mathbf{2}_S$ Sierpiński: $\{0\}$ closed, but $\{1\}$ not

Lemma

Let $C \subseteq \mathcal{P}(X) \approx \mathbf{2}^X$. TFAE:

- C is closed in $\mathbf{2}_S^X$
- C is closed in $\mathbf{2}_H^X$ 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 $\mathrm{Pmf}_{n,m} = \mathcal{P}(B^n \times B^m)$

Coclones

$\mathrm{Inv}(\mathcal{F})$ has the following properties:

Definition

$\mathcal{D} \subseteq \mathrm{Wgt}$ is a weight coclone if

- (variable manipulation) $w\colon B^k \to M$ in $\mathcal{D}$, $\varrho\colon k \to l$
  $\Longrightarrow w(x^{\varrho(0)}, \dots, x^{\varrho(k-1)})\colon B^l \to M$ in $\mathcal{D}$
- (homomorphisms) $w\colon B^k \to M$ in $\mathcal{D}$, $\varphi\colon M \to N$
  $\Longrightarrow \varphi \circ w\colon B^k \to N$ in $\mathcal{D}$
- (direct products) $w_\alpha\colon B^k \to M_\alpha$ in $\mathcal{D}$ $(\alpha \in I)$
  $\Longrightarrow (w_\alpha(x))_{\alpha\in I}\colon B^k \to \prod_{\alpha\in I} M_\alpha$ in $\mathcal{D}$
- (submonoids) $w\colon B^k \to M$ in $\mathcal{D}$, $w[B^k] \subseteq N \subseteq M$
  $\Longrightarrow w\colon B^k \to N$ in $\mathcal{D}$

Galois connection

Main theorem

For any B:

- Galois-closed sets of pmf $=$ pmf clones
- Galois-closed classes of weights $=$ weight coclones

Smaller invariants

Invariants of a pmf clone $\mathcal{C}$ form a proper class

Better: $\mathcal{C} = \mathrm{Pol}(\mathcal{W})$ s.t. for each $w\colon B^k \to M$ 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 Pmf or Wgt,
or impose additional closure conditions, e.g.

- dimensions of $f \colon B^n \Rightarrow B^m$:
  - $n, m \geq 1$, $m = 1$, $n = m$
- "kind" of f:
  - (partial/total) functions, permutations
- constraints on monoids:
  - commutative, unordered
- constants, ancillas

Monoid restrictions

- Classes of weights $w\colon B^k \to M$ with M commutative
  $\iff$ clones containing variable permutations

$$(x_0, \dots, x_{n-1}) \mapsto (x_{\pi(0)}, \dots, x_{\pi(n-1)})$$

  generated by swap $(x, y) \mapsto (y, x)$
- Classes of weights $w\colon B^k \to (M, 1, \cdot, =)$
  (i.e., unordered monoids)
  $\iff$ clones closed under inverse

$$f\colon B^n \Rightarrow B^m \text{ in } \mathcal{C} \implies f^{-1}\colon B^m \Rightarrow B^n \text{ in } \mathcal{C}$$

Dimension constraints

$f\colon B^n \rightrightarrows B^m$ with simple restrictions on n, m form clones ←lie
$\Longrightarrow$ correspond to inclusion of particular weights:

- $n, m \geq 1$: constant weight $c_1\colon B^0 \to (\mathbf{2}, 1, \wedge, =)$
- $n = m$: $c_1\colon B^0 \to (\mathbb{N}, 0, +, =)$

$m = 1$: clone $\mathcal{C}$ determined by $f\colon B^n \rightrightarrows B$ iff contains swap & diagonal maps $\Delta_n\colon B \to B^n$, $\Delta_n(x) = (x, \dots, x)$

On the dual side:

- tight $w\colon B^k \to M$ in $\mathrm{Inv}(\mathcal{C})$ are $\{\wedge, \top\}$-semilattices
- subdirectly irreducible: $M = (\mathbf{2}, 1, \wedge, \leq)$
  $\Longrightarrow$ weight functions = relations
  $\Longrightarrow$ agrees with the classical description

Uniqueness conditions

Partial functions form a clone $\implies$

$\mathcal{C}$ consists of partial functions iff
$\mathrm{Inv}(\mathcal{C})$ includes a particular weight:

- Kronecker delta $\delta\colon B^2 \to (\mathbf{2}, 1, \wedge, \leq)$

Symmetrically:

$\mathcal{C}$ consists of injective pmf iff
$\mathrm{Inv}(\mathcal{C})$ includes

$$\delta\colon B^2 \to (\{0,1\}, 1, \wedge, \geq)$$

Totality conditions

In the classical case:

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

Definition

$w\colon B^{k+1} \to (M, 1, \cdot, \le)$ weight, $(M, 1, \cdot, 0, +)$ semiring
Define $w^+\colon B^k \to (M, 1, \cdot, \le)$ by

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

Orders on semirings

Definition

- posemiring $= (M, 1, \cdot, 0, +, \leq)$ s.t.
  - $(M, 1, \cdot, \leq)$ and $(M, 0, +, \leq)$ pomonoids
  - $(M, 1, \cdot, 0, +)$ semiring
- positive semiring $=$ posemiring s.t. $0 \leq 1$
  negative semiring $=$ posemiring s.t. $1 \leq 0$
- idempotent semiring: $x + x = x$
  semilattice $\implies$ can be ordered in two ways:
  - $\vee$-semiring: $+$ is $\vee$
    $=$ idempotent positive semiring
  - $\wedge$-semiring: $+$ is $\wedge$
    $=$ idempotent negative semiring

Completeness of posemirings

Definition

- complete idempotent semiring ($\vee$-semiring, $\wedge$-semiring):
  - complete lattice
- continuous idempotent semiring ($\vee$-semiring, $\wedge$-semiring):
  - complete
  - infinite distributive laws

$$\Big(\sum_{i\in I} x_i\Big) y = \sum_{i\in I} x_i y \qquad y \sum_{i\in I} x_i = \sum_{i\in I} y x_i$$

Continuous $\vee$-semirings = unital quantales

Total clones

$\mathcal{C} = \mathrm{Pol}(\mathcal{D})$, $\mathcal{D} = \mathrm{Inv}(\mathcal{C})$

For B countable, the following are equivalent:

- $\mathcal{C}$ is generated by total multifunctions
- $w \colon B^{k+1} \to M$ is in $\mathcal{D}$, M is a continuous $\vee$-semiring
  $\implies w^+ \colon B^k \to M$ is in $\mathcal{D}$

Symmetrically: clones of surjective pmf characterized using continuous $\wedge$-semirings

For B finite, TFAE:

- $\mathcal{C}$ is generated by mf extending a bijective function
- $w \colon B^{k+1} \to M$ is in $\mathcal{D}$, M is a posemiring
  $\implies w^+ \colon B^k \to M$ is in $\mathcal{D}$

Ancillas

$\mathcal{C} = \mathrm{Pol}(\mathcal{D})$, $\mathcal{D} = \mathrm{Inv}(\mathcal{C})$

The following are equivalent:

- $\mathcal{C}$ supports ancillas
  $c \in B$, $f \colon B^{n+1} \Rightarrow B^{m+1}$ in $\mathcal{C} \implies f_c \colon B^n \Rightarrow B^m$ in $\mathcal{C}$

$$f_c(\vec{x}) \approx \vec{y} \iff f(\vec{x}, c) \approx (\vec{y}, c)$$

- $\mathcal{D}$ is generated by $w \colon B^k \to M$ s.t. the diagonal weights $z = w(u, \dots, u)$ for $u \in B$ are right-order-cancellative

$$xz \le yz \implies x \le y$$

Warning: Interferes badly with totality

Summary

- The standard clone–coclone duality extends to a Galois connection between partial multifunctions $B^n \Rightarrow B^m$ and pomonoid-valued functions $B^k \to M$
- Gracefully restricts to natural subclasses, such as total functions $B^n \to B^m$

Thank you for attention!

References

- S. Aaronson: Classifying reversible gates, Th. Comp. Sci. SE, 2014, `http://cstheory.stackexchange.com/q/25730`
- S. Aaronson, D. Grier, L. Schaeffer: The classification of reversible bit operations, 2015, arXiv:1504.05155 [quant-ph]
- V. G. Bodnarchuk, L. A. Kaluzhnin, V. N. Kotov, B. A. Romov: Galois theory for Post algebras I & II, Cybernetics 5 (1969), no. 3, 243–252, and no. 5, 531–539
- M. Couceiro: Galois connections for generalized functions and relational constraints, in: Contributions to General Algebra 16, Heyn, Klagenfurt 2005, 35–54
- D. Geiger: Closed systems of functions and predicates, Pacific J. Math. 27 (1968), 95–100
- P. A. Grillet: On subdirectly irreducible commutative semigroups, Pacific J. Math. 69 (1977), 55–71

References (cont'd)

- A. A. Iskander: Subalgebra systems of powers of partial universal algebras, Pacific J. Math. 38 (1971), 457–463
- E. Jeřábek: Galois connection for multiple-output operations, Algebra Universalis 79 (2018), art. no. 17
- S. Kerkhoff: A general Galois theory for operations and relations in arbitrary categories, Algebra Universalis 68 (2012), 325–352
- A. I. Mal'cev: On homomorphisms onto finite groups, Uchen. Zap. Ivanov. Gos. Ped. Inst. 18 (1958), 49–60, in Russian
- E. L. Post: The two-valued iterative systems of mathematical logic, Princeton University Press, 1941
- R. Pöschel: A general Galois theory for operations and relations and concrete characterization of related algebraic structures, Tech. Rep. R-01/80, Akademie der Wissenschaften der DDR, Zentralinstitut für Mathematik und Mechanik, 1980

References (cont'd)

- I. G. Rosenberg: A classification of universal algebras by infinitary relations, Algebra Universalis 1 (1971), 350–354
- ________: Galois theory for partial algebras, in: Universal Algebra and Lattice Theory, LNM 1004, Springer, 1983, 257–272
- B. M. Schein: Homomorphisms and subdirect decompositions of semigroups, Pacific J. Math. 17 (1966), 529–547