INSTITUTE OF MATHEMATICS

THE CZECH ACADEMY OF SCIENCES

Galois connection for multiple-output operations

Emil Jeřábek

Preprint No. 47-2017

PRAHA 2017

Galois connection for multiple-output operations

Emil Jeřábek*

Institute of Mathematics of the Czech Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: `jerabek@math.cas.cz`

July 29, 2017

Abstract

It is a classical result from universal algebra that the notions of polymorphisms and invariants provide a Galois connection between suitably closed classes (clones) of finitary operations $f\colon B^n \to B$, and classes (coclones) of relations $r \subseteq B^k$. We will present a generalization of this duality to classes of (multi-valued, partial) functions $f\colon B^n \to B^m$, employing invariants valued in partially ordered monoids instead of relations. In particular, our set-up encompasses the case of permutations $f\colon B^n \to B^n$, motivated by problems in reversible computing.

1 Introduction

One of the pivotal notions in universal algebra is the concept of a *clone*: a set of finitary operations $f\colon B^n \to B$ on a base set B, closed under composition (superposition), and containing all projections. A typical clone is the set of term operations of an algebra with underlying set B; in a sense, clones can be thought of as algebras with their signature abstracted away. Apart from universal algebra, clones have numerous applications in logic and computer science, many owing to the celebrated work of Post [21] who classified all clones on a two-element base set.

An important tool in the study of clones is the *clone–coclone duality*, originally discovered by Geiger [8] and Bodnarchuk, Kaluzhnin, Kotov, and Romov [4, 5]. In its most basic form valid for finite base sets B, it states that the natural preservation relation between operations $f\colon B^n \to B$ and relations $r \subseteq B^k$ induces a Galois connection that provides a dual isomorphism of the lattice of clones to the lattice of *coclones*: sets of relations closed under definability by primitive positive (pp) formulas.

Many variants and extensions of the clone–coclone Galois connection appear in the literature; let us mention just a few without attempting to make an exhaustive list. The use of

*The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no. 339691. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

relational invariants was pioneered by Krasner (see e.g. [14, 15]), who developed a duality theory for endofunctions $f\colon B \to B$. The above-mentioned seminal paper by Geiger [8] considers not just the case of functions $f\colon B^n \to B$ for finite B, but also partial multi-valued functions, and he briefly indicates possible generalizations to infinite base sets B. Iskander [10] describes, for arbitrary B, the closed classes dual to sets of partial operations $B^n \to B$. Rosenberg [22, 23] develops, for arbitrary B, a duality for clones of total or partial operations $B^n \to B$ using infinitary relations as invariants. Pöschel [20] describes Galois-closed sets of finitary relations and operations for arbitrary B. Kerkhoff [13] develops the duality in more general categories than Set. Couceiro [7] presents a duality for sets of heterogeneous (partial, multi-valued) operations $A^n \to B$ with two base sets A and B.

In this paper, we present a new generalization of this Galois connection: rather than classes of operations $f\colon B^n \to B$, we consider (partial, multi-valued) functions $f\colon B^n \to B^m$, where $m \geq 0$; that is, operations with multiple outputs, just like usual operations already may have multiple inputs. On the dual side, we use functions $w\colon B^k \to \mathbf{M}$ valued in partially ordered monoids $\mathbf{M}$ as invariants; note that other variants of the Galois connection mentioned above generally stick to ordinary relations or something close in spirit (e.g., infinitary relations, or pairs of relations).

Let us briefly explain the primary motivation for this generalization, which comes from the work of Aaronson, Grier, and Schaeffer [2] (anticipated in [1], where a preliminary version of some results of the present paper were posted [12]).

One way to model conventional computation is with Boolean circuits $C\colon \{0,1\}^n \to \{0,1\}$. We may consider families of circuits using various sets of basic gates, and then the class of Boolean functions definable by circuits over some basis is a clone on $B = \{0,1\}$. Such clones were classified by Post [21], and their description becomes relevant when discussing circuits for restricted classes of functions.

In conventional computing, we may freely destroy or duplicate information: for example, on input x, y we may compute $x + y$. In *reversible computing* [18], this is disallowed: computation is required to be (in principle) step-by-step invertible. (The addition example above could be made reversible by computing the pair $x, x + y$ instead.) One motivation to study reversible computing comes from consideration of physical constraints. Since the underlying time-evolution operators of quantum mechanics are invertible, any physical realization of irreversible computation must "store" the excess information in the form of side-effects; more specifically, the second law of thermodynamics implies *Landauer's principle*, which states that erasure of n bits of information incurs a certain increase of entropy proportional to n elsewhere in the system. In practical terms, this means the computer must draw the corresponding amount of energy and dissipate it in the environment as heat. In contrast, there are no known theoretical limits on the energy efficiency of reversible computation.

Going a step further, models of *quantum computing* [11] are inherently reversible, as all computation steps perform unitary (hence invertible) operators.

Now, reversible computation can be modelled using a suitable kind of circuits made of reversible gates, which are permutations (bijections) $f\colon B^n \to B^n$. A class of functions computable by circuits over some basis of reversible gates forms a "clone" of permutations satisfying a handful of natural closure properties. The main result of [2] is a description of all such closed classes of permutations on $B = \{0, 1\}$, which can be thought of as an analogue of Post's classification for reversible computing.

Thus, one of the design goals of the present paper is to develop a duality that applies as a special case to the kind of closed classes of permutations $f\colon B^n \to B^n$ studied in [2], providing it with a broader framework. Of course, it is highly desirable to include the classical case of functions $f\colon B^n \to B$ as well. This naturally leads to consideration of functions $f\colon B^n \to B^m$ as a common generalization. We do not have a particular reason to consider also partial multi-valued functions, except that it happens to work; in fact, the basic Galois connection is easier to study for partial multi-valued functions, while requirements of totality bring in extra complications.

The paper is organized as follows. We begin with a handful of motivating examples in Section 2. We recall some preliminary facts about partially ordered structures and Galois connections in Section 3. In Section 4, we present our main Galois connection between partial multi-valued multi-output functions and pomonoid-valued weight functions in its most general form. In Section 5, we discuss variants of our Galois connection for restricted classes of multi-output functions or weights that might be important for applications, in particular, we give Galois connections for classes of *total* multi-output functions in Section 5.1, and for classes of permutations closed under the ancilla rule as in [2] in Section 5.2. We discuss the merits of using weights in subdirectly irreducible pomonoids in Section 6, including a brief description of finitely generated subdirectly irreducible commutative monoids as classified by Grillet [9]. A few concluding words are included in Section 7.

2 Initial examples

The Galois connection we are going to introduce involves more complicated invariants on the "coclone" side in contrast to the classical clone–coclone duality and many of its known generalizations: rather than some form of relations, we need to use functions valued in partially ordered monoids. Before we get to the formal business, we will present a few examples to show that this is in fact a necessary move that follows the nature of multiple-output functions, and to have something easily graspable in mind to illustrate the subsequent abstract definitions.

First, let us recall the preservation relation from the standard Galois connection. A function $f\colon B^n \to B$ *preserves* a relation $r \subseteq B^k$ if for every pair of matrices[1]

$$a = \begin{pmatrix} a_0^0 & a_1^0 & \cdots & a_{n-1}^0 \\ a_0^1 & a_1^1 & \cdots & a_{n-1}^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{k-1} & a_1^{k-1} & \cdots & a_{n-1}^{k-1} \end{pmatrix} \in B^{k\times n}, \qquad b = \begin{pmatrix} b_0^0 \\ b_0^1 \\ \vdots \\ b_0^{k-1} \end{pmatrix} \in B^{k\times 1},$$

[1]We index tuples and matrices starting from 0, so that e.g., an n-tuple is written as $(x_0, \dots, x_{n-1})$. Accordingly, we write $\mathbb{N} = \{0, 1, 2, \dots\}$, and index variables such as i and j are implicitly taken in $\mathbb{N}$; for instance, a quantifier over $i < n$ stands for $i = 0, \dots, n-1$.

if all rows represent values of f:

$$f(a_0^j, \dots, a_{n-1}^j) = b_0^j, \quad j < k,$$

and if all columns of a are in r:

$$(a_i^0, \dots, a_i^{k-1}) \in r, \quad i < n,$$

then the (unique in this case) column of b is in r as well:

$$(b_0^0, \dots, b_0^{k-1}) \in r.$$

In order to make the notation more concise, we will denote a matrix a as above by $(a_i^j)_{i<n}^{j<k}$; its rows and columns will be denoted $a^j = (a_i^j : i < n)$ and $a_i = (a_i^j : j < k)$, respectively. Thus, we can state the definition of the preservation relation as follows: for all $a \in B^{k\times n}$ and $b \in B^{k\times 1}$, if $f(a^j) = b_0^j$ for every $j < k$, and $a_i \in r$ for every $i < n$, then $b_0 \in r$. (So far it would have been simpler to treat b as a vector rather than a 1-column matrix, but we will shortly realize this is an artifact of f having unary output.)

We will now have a look at some of the closed classes of reversible operations on two-element base set, considered in [2].

Example 2.1 The class of all *conservative* permutations $f \colon B^n \to B^n$ for $B = \{0, 1\}$: that is, bijective functions such that $f(x)$ and x have the same Hamming weight (= the number of 1s) for any $x \in B^n$. We can express this condition as follows: a permutation $f \colon B^n \to B^n$ is conservative iff

(1) $$f(a^0) = b^0 \implies \sum_{i<n} a_i^0 = \sum_{i<n} b_i^0$$

holds for all matrices $a, b \in B^{1\times n}$, where the sum is computed in the integers, viewing B as a subset of $\mathbb{N}$.

Example 2.2 (Still $B = \{0, 1\}$.) The class of all *mod-c-preserving* permutations $f \colon B^n \to B^n$ for a constant $c > 1$: that is, permutations such that the Hamming weights of $f(x)$ and x are congruent modulo c for any $x \in B^n$. A permutation $f \colon B^n \to B^n$ is mod-c-preserving iff it satisfies the property (1) for all matrices $a, b \in B^{1\times n}$, where the sum is now computed in the group $\mathbb{Z}/c\mathbb{Z}$.

The previous two examples show that multi-output functions, and specifically permutations, can "count"—they are capable of preserving numerical quantities associated with the input (as opposed to yes/no properties as given by relations $r \subseteq B^k$), expressible as certain "sums" over the input elements.

In the general definition in Section 4, we will actually employ multiplicative notation, so the "sums" will be written as "products"; this is partly to emphasize that we will allow the aggregation operation to be noncommutative, but mostly because we will at some point need to make this "multiplication" operation interact in a ring-like fashion with another kind of "addition". In any case, this is just a matter of notation.

The next example also appears in [2] when restricted to permutations, but we will state it for general functions in order to showcase new features. In particular, in the first two examples, the "sums" (to become "products") were preserved by equality; but in the general case, they will only be preserved by inequality.

Example 2.3 ($B = \{0, 1\}$) The class of *affine functions* $f\colon B^n \to B^m$, i.e., $f(x) = Ax + c$ for some $A \in B^{m\times n}$ and $c \in B^m$, identifying B with the field $\mathbb{F}_2$. In order to characterize this class in a similar spirit to Examples 2.1 and 2.2, notice first that f is affine if and only if each of its m components $f_i\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is affine. This gets us in the realm of the classical clone–coclone duality: we know that f_i is affine iff it preserves the relation

$$r = \{(a^0, a^1, a^2, a^3) \in \mathbb{F}_2^4 : a^0 + a^1 + a^2 + a^3 = 0\}$$

(the sum being computed in $\mathbb{F}_2$). Thus, let $w\colon \mathbb{F}_2^4 \to \{0, 1\}$ denote the characteristic function of r, i.e.,

$$w(x^0, x^1, x^2, x^3) = x^0 + x^1 + x^2 + x^3 + 1$$

(still using $\mathbb{F}_2$ addition). Then $f\colon B^n \to B^m$ is affine iff for all $a \in B^{4\times n}$ and $b \in B^{4\times m}$,

$$\forall j < 4\, f(a^j) = b^j \wedge \forall i < n\, w(a_i) = 1 \implies \forall i < m\, w(b_i) = 1.$$

We can recast this as preservation of a product: f is affine iff for all $a \in B^{4\times n}$ and $b \in B^{4\times m}$,

$$\forall j < 4\, f(a^j) = b^j \implies \prod_{i<n} w(a_i) \le \prod_{i<m} w(b_i).$$

In a similar way, any classical relational invariant $r \subseteq B^k$ can be expressed as preservation of a product of certain functions valued in the two-element meet-semilattice $(\{0, 1\}, 1, \cdot, \le)$.

Invariants of a similar syntactic shape as above can be defined for functions $w\colon B^k \to \mathbf{M}$, where $\mathbf{M}$ is a structure in which we can compute products of finite sequences of elements, and we have a suitable order relation. That is, we are led to the class of *partially ordered monoids.*

3 Preliminaries

3.1 Ordered structures

Since partially ordered monoids and other ordered structures are omnipresent in this paper, this section presents a summary of some background information on such structures.

We might as well start from the beginning, even though the reader must have seen monoids and partial orders before. So, recall that a binary relation $\le \subseteq X \times X$ is a *preorder* on X if it is reflexive and transitive. If it is additionally antisymmetric ($x \le y \wedge y \le x \to x = y$), it is a *partial order.*

Let $\le$ be a partial order on X. A set $Y \subseteq X$ is a *down-set* if $x \le y$ and $y \in Y$ implies $x \in Y$, and an *up-set* if it satisfies the dual condition. For any $Y \subseteq X$, $Y{\downarrow}$ denotes the generated down-set $\{x \in X : \exists y \in Y\, x \le y\}$, and $Y{\uparrow}$ the generated up-set $\{x \in X : \exists y \in Y\, y \le x\}$.

A structure $\mathbf{M} = (M, 1, \cdot)$ in a signature with one constant, and one binary operation, is a *monoid* if $\cdot$ is associative, and 1 is a two-sided unit ($1 \cdot x = x \cdot 1 = x$). We often write just xy for $x \cdot y$. Associativity allows us to unambiguously refer to iterated products

$$x_0 x_1 \cdots x_{n-1} = \prod_{i<n} x_i.$$

This product is understood to be 1 if $n = 0$. We will also sometimes write monoids in the additive signature $(M, 0, +)$, particularly when commutative.

A *partially ordered monoid* (*pomonoid* for short) is a structure $\mathbf{M} = (M, 1, \cdot, \leq)$ such that $(M, 1, \cdot)$ is a monoid, and $\leq$ is a partial order on M compatible with multiplication, i.e., satisfying

$$x \leq y \to xz \leq yz,$$
$$x \leq y \to zx \leq zy$$

for all $x, y, z \in M$.

Apart from the class of pomonoids, we will also need to work e.g. with its subvarieties, and expansions such as semirings. Thus, it will be helpful to have a general framework for ordered structures. While we will assume the reader is familiar with basic notions from universal algebra—such as varieties, equational logic, and subdirect irreducibility—in the standard set-up of purely algebraic structures (see e.g. [6]), the corresponding theory for partially ordered structures and inequational logic is much less commonly known, hence we review the relevant concepts below. The results we need can be found in [19], but various parts of the theory appear e.g. in [3, 17].

Let us fix an algebraic signature Σ (in our application, it will most often be the signature of monoids with extra constants). A *partially ordered* Σ*-algebra* (short: poalgebra) is a Σ-algebra $\mathbf{A}$ endowed with a partial order $\leq_{\mathbf{A}}$ that makes all functions from Σ monotone (nondecreasing) in every argument[2]. Homomorphisms, subalgebras, products, and restricted products of poalgebras are defined in the expected way, using the corresponding algebraic and order-theoretic notions on the respective parts of the structure.

If $\phi\colon \mathbf{A} \to \mathbf{B}$ is a homomorphism between two poalgebras, its *order kernel* is the relation $\operatorname{oker}(\phi) = \{(a, a') \in A^2 : \phi(a) \leq_{\mathbf{B}} \phi(a')\}$. The order kernel is an *invariant preorder* on $\mathbf{A}$: a preorder $\preceq$ extending $\leq_{\mathbf{A}}$ such that for each $f \in \Sigma$, $f^{\mathbf{A}}$ is nondecreasing with respect to $\preceq$ in every argument. Conversely, let $\preceq$ be an invariant preorder on $\mathbf{A}$. The relation $\sim\, = \,\preceq \cap \succeq$ is a congruence of the algebraic part of $\mathbf{A}$, hence we can form the quotient structure $\mathbf{B} = \mathbf{A}/{\sim}$, and make it a poalgebra ordered by $\preceq/{\sim}$. The quotient map $\phi\colon \mathbf{A} \to \mathbf{B}$ is a (surjective) homomorphism, and $\operatorname{oker}(\phi) = \,\preceq$. We will denote $\mathbf{B}$ as $\mathbf{A}/{\preceq}$.

Since invariant preorders are closed under arbitrary intersections, they form an algebraic complete lattice $\operatorname{OCon}\mathbf{A}$, which plays much the same role as the congruence lattice for unordered algebras.

[2] More generally, we could specify for each argument a *polarity* indicating whether the function is nondecreasing or nonincreasing in the given argument, see [19].

A poalgebra $\mathbf{A}$ is a *subdirect product* of a family of poalgebras $\{\mathbf{A}_i : i \in I\}$ if there exists an embedding

$$\varphi\colon \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i \tag{2}$$

such that $\pi_i \circ \varphi\colon \mathbf{A} \to \mathbf{A}_i$ is surjective for each $i \in I$, where π_i denotes projection to the ith coordinate. A poalgebra $\mathbf{A}$ is *subdirectly irreducible* if for every subdirect product (2), there exists $i \in I$ such that $\pi_i \circ \varphi$ is an isomorphism. An intrinsic characterization is that a poalgebra $(\mathbf{A}, \le_{\mathbf{A}})$ is subdirectly irreducible iff it has a least invariant preorder properly extending $\le_{\mathbf{A}}$. Every poalgebra can be written as a subdirect product of subdirectly irreducible poalgebras.

A class of Σ-poalgebras is a (*partially ordered*) *variety* if it can be axiomatized by a set of (implicitly universally quantified) inequalities $t(\vec{x}) \le s(\vec{x})$, where t and s are Σ-terms, over the theory of all Σ-poalgebras. Equivalently, a povariety is a class of poalgebras closed under subalgebras, products, and homomorphic images (i.e., quotients by invariant preorders). If a poalgebra $\mathbf{A}$ from a variety V is a subdirect product of a family of poalgebras $\{\mathbf{A}_i : i \in I\}$, then each $\mathbf{A}_i$ is in V, too; thus, every $\mathbf{A} \in V$ is a subdirect product of subdirectly irreducible poalgebras from V.

More generally, a class of poalgebras is a (*partially ordered*) *quasivariety* if it can be axiomatized by a set of *quasi-inequalities*

$$\bigwedge_{i<n} t_i(\vec{x}) \le s_i(\vec{x}) \to t(\vec{x}) \le s(\vec{x}),$$

where $n \in \omega$, and t, s, t_i, s_i are terms. Equivalently, a class of poalgebras is a quasivariety iff it is closed under isomorphic images, subalgebras, products, and ultraproducts (or: restricted products).

If Q is a quasivariety, and $\mathbf{A}$ a poalgebra, a *Q-preorder* is an invariant preorder $\preceq$ on $\mathbf{A}$ such that $\mathbf{A}/{\preceq} \in Q$. The set of Q-preorders is closed under arbitrary intersections, hence it forms an algebraic complete lattice $\operatorname{OCon}_Q \mathbf{A}$. (If Q is a povariety, then $\operatorname{OCon}_Q \mathbf{A}$ is a principal filter of $\operatorname{OCon} \mathbf{A}$.) An algebra $\mathbf{A} \in Q$ is *subdirectly irreducible relative to Q* if for every subdirect product (2) with $\{\mathbf{A}_i : i \in I\} \subseteq Q$, there is $i \in I$ such that $\pi_i \circ \varphi$ is an isomorphism. Equivalently, there is a least Q-preorder properly extending $\le_{\mathbf{A}}$. Every $\mathbf{A} \in Q$ can be written as a subdirect product of a family of poalgebras $\mathbf{A}_i \in Q$, subdirectly irreducible relative to Q.

An unordered Σ-algebra $\mathbf{A}$ can be identified with the poalgebra $(\mathbf{A}, =_{\mathbf{A}})$, which we will call *trivially ordered*. Notice that the class of trivially ordered poalgebras is a quasivariety, being axiomatized by $x \le y \to y \le x$.

3.2 Galois connections

In order to ensure that we are all on the same page, let us also recall basic facts about closure operators and Galois connections.

Let $(P, \le)$ be a partially ordered set. A *closure operator* on P is a function $\operatorname{cl}\colon P \to P$ such that

$$X \le \operatorname{cl} Y \quad \text{iff} \quad \operatorname{cl} X \le \operatorname{cl} Y \tag{3}$$

for all $X, Y \in P$. (In our applications, P will be typically the powerset lattice $(\mathcal{P}(U), \subseteq)$ for some set U; in this case, we will also call cl a closure operator *on* U for simplicity.) The definition (3) is equivalent to the conjunction of the three conditions

$$\begin{gathered} X \leq \operatorname{cl} X, \\ X \leq Y \implies \operatorname{cl} X \leq \operatorname{cl} Y, \\ \operatorname{cl} X = \operatorname{cl} \operatorname{cl} X. \end{gathered}$$

If cl is a closure operator, an $X \in P$ is *closed* if $X = \operatorname{cl} X$. Let $C \subseteq P$ be the collection of all closed elements. The definition of a closure operator implies that for any $X \in P$, $\operatorname{cl} X$ is the least closed element above X:

$$\operatorname{cl} X = \min\{Y \in C : X \leq Y\}. \tag{4}$$

That is, we can recover cl from C.

A subset $C \subseteq P$ with the property that (4) exists for all $X \in P$ is called a *closure system* on P. For any closure system C, the function cl defined by (4) is a closure operator. The constructions of closure systems from closure operators and vice versa described above are mutually inverse, hence the two definitions can be considered different presentations of the same concept. If P is a complete lattice (e.g., a powerset lattice), closure systems have a simpler characterization: $C \subseteq P$ is a closure system iff it is closed under arbitrary meets (including the empty meet, which yields the top element of P). In particular, any such closure system is itself a complete lattice.

Now, let $(P, \leq)$ and $(Q, \preceq)$ be two partially ordered sets (again, typically powersets for us). A *Galois connection* between P and Q is a pair of mappings $F \colon P \to Q$ and $G \colon Q \to P$ such that

$$X \leq G(Y) \quad \text{iff} \quad Y \preceq F(X) \tag{5}$$

for all $X \in P$ and $Y \in Q$. This is equivalent to the conditions

$$\begin{gathered} X \leq G(F(X)), \\ Y \preceq F(G(Y)), \\ X \leq X' \implies F(X') \preceq F(X), \\ Y \preceq Y' \implies G(Y') \leq G(Y) \end{gathered}$$

for $X, X' \in P$ and $Y, Y' \in Q$.

A Galois connection as above induces closure operators $\operatorname{cl}_P = G \circ F \colon P \to P$ and $\operatorname{cl}_Q = F \circ G \colon Q \to Q$ on P and Q, respectively. Elements of P or Q are called *closed* with respect to the Galois connection (for short: *Galois-closed*) if they are closed under cl_P or cl_Q, respectively.

The images of F and G consist of closed elements. Moreover, F and G restricted to the collections of closed elements of P and Q (respectively) are mutually inverse antitone isomorphisms.

The Galois connections discussed in this paper arise by means of the following simple but powerful observation. Let U and V be sets, and $R \subseteq U \times V$ a binary relation. Then the mappings

$$\begin{aligned} F(X) &= \{v \in V : \forall x \in X\, R(x, v)\}, \\ G(Y) &= \{u \in U : \forall y \in Y\, R(u, y)\} \end{aligned} \tag{6}$$

form a Galois connection between the powerset lattices $(\mathcal{P}(U), \subseteq)$ and $(\mathcal{P}(V), \subseteq)$: indeed, either of $X \subseteq G(Y)$ and $Y \subseteq F(X)$ is equivalent to the symmetric condition

$$\forall x \in X\, \forall y \in Y\, R(x, y),$$

hence (5) holds.

We will not be too fussy about applying the concepts above to proper classes instead of sets, even though a "powerclass lattice" is not an honest object. In such cases, we will take care to only work with maps from classes to classes that are definable, and refrain from problematic steps like explicit quantification over subclasses, so it should be straightforward to formalize all our reasoning in ZFC.

4 Multiple-output clones and coclones

Let us fix a base set B for the rest of the paper. (While some results will only apply if B is finite, the general set-up allows arbitrary B. It may even be empty.)

As we already mentioned, we are going to study classes of *partial multi-valued functions* (*pmf*) from B^n to B^m for some $n, m \in \omega$. Formally speaking, a pmf from X to Y is just a relation $f \subseteq X \times Y$; however, we view it as a nondeterministic operation that maps $x \in X$ to one of the values $y \in Y$ such that $(x, y) \in f$ (if any). In order to stress this interpretation (while at the same time distinguishing it in notation from "proper" functions), we will use the symbol $f \colon X \rightrightarrows Y$ to mean that f is a pmf from X to Y, and we will write $f(x) \approx y$ for $(x, y) \in f$.

Definition 4.1 For any $n, m \in \omega$, let $\mathrm{Pmf}_{n,m}$ denote the set of all partial multi-valued functions (pmf) from B^n to B^m (that is, formally, $\mathrm{Pmf}_{n,m} = \mathcal{P}(B^n \times B^m)$). We also put $\mathrm{Pmf} = \dot{\bigcup}_{n,m} \mathrm{Pmf}_{n,m}$.

Following the examples in Section 2, we will characterize suitably closed classes of pmf by preservation of certain "weighted products" in pomonoids. Thus, our invariants will be the following kind of objects:

Definition 4.2 If $k \in \omega$, Wgt_k denotes the class of k-ary *weight functions,* i.e., mappings $w \colon B^k \to \mathbf{M}$ where $\mathbf{M} = (M, 1, \cdot, \leq)$ is any pomonoid. Let $\mathrm{Wgt} = \dot{\bigcup}_k \mathrm{Wgt}_k$.

Without further ado, here is our fundamental preservation relation. (Keep in mind the notational conventions for matrices from Section 2.)

Definition 4.3 Let $n, m, k \in \omega$. A pmf $f\colon B^n \Rightarrow B^m$ *preserves* a weight $w\colon B^k \to \mathbf{M}$, written $f \triangleright w$, if the following holds for all $a = (a_i^j)_{i<n}^{j<k} \in B^{k\times n}$ and $b = (b_i^j)_{i<m}^{j<k} \in B^{k\times m}$:

$$\forall j < k\, f(a^j) \approx b^j \implies \prod_{i<n} w(a_i) \le \prod_{i<m} w(b_i). \tag{7}$$

When $f \triangleright w$, we also say that w is an *invariant* of f, and f is a *polymorphism* of w. If $C \subseteq \mathrm{Pmf}$ and $D \subseteq \mathrm{Wgt}$, we will write $C \triangleright D$ as a shorthand for $\forall f \in C\, \forall w \in D\, f \triangleright w$.

Using (6), the preservation relation induces a Galois connection between sets $C \subseteq \mathrm{Pmf}$, and classes $D \subseteq \mathrm{Wgt}$:

$$\begin{aligned}\mathrm{Inv}(C) &= \{w \in \mathrm{Wgt} : C \triangleright w\},\\ \mathrm{Pol}(D) &= \{f \in \mathrm{Pmf} : f \triangleright D\}.\end{aligned}$$

Corollary 4.4 $\mathrm{Pol} \circ \mathrm{Inv}$ *and* $\mathrm{Inv} \circ \mathrm{Pol}$ *are closure operators on* Pmf *and* Wgt*, respectively.* Inv *and* Pol *are mutually inverse antitone isomorphisms between Galois-closed subsets of* Pmf*, and Galois-closed subclasses of* Wgt*.* $\mathrm{Inv}(C)$ *and* $\mathrm{Pmf}(D)$ *are Galois-closed for each* $C \subseteq \mathrm{Pmf}$ *and* $D \subseteq \mathrm{Wgt}$*.* □

Our fundamental task in this section is to find an intrinsic characterization of Galois-closed subsets of Pmf, and subclasses of Wgt.

Before we do that, we need to clarify one minor issue. The description of Galois-closed sets involves a condition that says, roughly, that whether a pmf belongs in such a set depends only on its finite parts. In the literature, this condition appears in several formulations under several names, such as *local closure*. We prefer to think of it as a topological closure property, however we include a few equivalent forms of the condition below for the benefit of the reader.

Definition 4.5 Let $\mathbf{2}$ be the set $\{0, 1\}$; $\mathbf{2}_H$ denotes $\mathbf{2}$ endowed with the discrete Hausdorff topology, and $\mathbf{2}_S$ denotes $\mathbf{2}$ endowed with the Sierpiński topology where $\{1\}$ open, but $\{0\}$ is not.

Lemma 4.6 *Let A be a family of subsets of X, identified with their characteristic functions (i.e., elements of $\mathbf{2}^X$). The following are equivalent.*

(i) A is closed in $\mathbf{2}_S^X$.

(ii) A is closed in $\mathbf{2}_H^X$ and closed under subsets.

(iii) A is closed under directed unions and subsets.

(iv) A is of finite character: i.e., a $Y \subseteq X$ is in A iff all finite subsets of Y are in A.

Proof:

(i) → (ii): A is closed in $\mathbf{2}_H^X$ as $\mathbf{2}_H$ is finer than $\mathbf{2}_S$. Moreover, the basic open sets in $\mathbf{2}_S^X$ are of the form $\{Y : Y \supseteq Y_0\}$ where $Y_0 \subseteq X$ is finite, hence every $\mathbf{2}_S^X$-open set is closed upwards, and every closed set is closed downwards.

(ii) → (iii): Let $S \subseteq A$ be directed, and $Y = \bigcup S$. For every finite $X_0 \subseteq X$, there is $Y' \in S$ such that $Y' \supseteq Y \cap X_0$ by directedness, which implies $Y' \cap X_0 = Y \cap X_0$. Thus, every $\mathbf{2}_H^X$-open neighbourhood of Y intersects A, whence $Y \in A$.

(iii) → (iv): Left to right follows from closure under subsets. Right to left: Y is a directed union of its finite subsets.

(iv) → (i): Let $Y \notin A$. By finite character, there is a finite $Y_0 \subseteq Y$ such that $Y_0 \notin A$, and then the basic 2_S^X-open neighbourhood $\{Y' : Y' \supseteq Y_0\}$ of Y is disjoint from A. □

Remark 4.7 The closure of $A \subseteq \mathcal{P}(X)$ in $\mathbf{2}_S^X$ is

$$\{Y \subseteq X : \forall Y_0 \subseteq Y \text{ finite } \exists Z \in A\, Y_0 \subseteq Z\}.$$

One more notational clarification: in (A) below and elsewhere, we view $k \in \omega$ as a von Neumann numeral, that is, $k = \{0, \dots, k-1\}$.

Definition 4.8 A set $C \subseteq \mathrm{Pmf}$ is a *pmf clone* if the following hold for all $n, m, r, n', m' \in \omega$:

(I) $C \cap \mathrm{Pmf}_{n,m}$ is topologically closed as a subset of $\mathbf{2}_S^{B^n \times B^m}$.

(II) C contains the identity function $\mathrm{id}_n \colon B^n \to B^n$.

(III) C is closed under composition: if $f \colon B^n \Rightarrow B^m$ and $g \colon B^m \Rightarrow B^r$ are in C, then so is the pmf $g \circ f \colon B^n \Rightarrow B^r$ given by

$$(g \circ f)(x) \approx z \quad \text{iff} \quad \exists y \in B^m\, (f(x) \approx y \wedge g(y) \approx z).$$

(IV) If $f \colon B^n \Rightarrow B^m$ and $g \colon B^{n'} \Rightarrow B^{m'}$ are in C, then so is $f \times g \colon B^{n+n'} \Rightarrow B^{m+m'}$, where $(f \times g)(x, x') \approx (y, y')$ iff $f(x) \approx y$ and $g(x') \approx y'$.

A class $D \subseteq \mathrm{Wgt}$ is a *weight coclone* if it satisfies the following conditions for any $k, k' \in \omega$:

(A) If $w \colon B^k \to \mathbf{M}$ is in D, and $\varrho \colon k \to k'$, the weight $w \circ \tilde{\varrho} \colon B^{k'} \to \mathbf{M}$ is in D, where $\tilde{\varrho}(x^0, \dots, x^{k'-1}) = (x^{\varrho(0)}, \dots, x^{\varrho(k-1)})$.

(B) If $w \colon B^k \to \mathbf{M}$ is in D, and $\varphi \colon \mathbf{M} \to \mathbf{M}'$ is a pomonoid homomorphism (not necessarily onto), then the weight $\varphi \circ w \colon B^k \to \mathbf{M}'$ is in D.

(C) If $w_\alpha \colon B^k \to \mathbf{M}_\alpha$ is in D for every $\alpha \in I$, the weight $w \colon B^k \to \prod_{\alpha \in I} \mathbf{M}_\alpha$ defined by $w(x) = (w_\alpha(x) : \alpha \in I)$ is in D.

(D) If $w \colon B^k \to \mathbf{M}$ is in D, and $\mathbf{M}' \subseteq \mathbf{M}$ is a submonoid including the image of w, then $w \colon B^k \to \mathbf{M}'$ is in D.

Remark 4.9 The smallest pmf clone is the clone $C_{\min}$ consisting of all subidentity partial functions $f \colon B^n \Rightarrow B^n$, $f \subseteq \mathrm{id}_n$. Its dual coclone $\mathrm{Inv}(C_{\min})$ is Wgt.

The index set I in condition (C) may be empty, in which case the result is the weight $w \colon B^k \to \mathbf{1}$ into the trivial pomonoid. In particular, every weight coclone is nonempty. The smallest weight coclone $D_{\min}$ consists of all *trivial weights* $\mathrm{c}_1 \colon B^k \to \mathbf{M}$, i.e., constant weights mapping to the unit of $\mathbf{M}$. The dual of $D_{\min}$ is $\mathrm{Pol}(D_{\min}) = \mathrm{Pmf}$.

Remark 4.10 Preservation of weights by pmf can be put in the framework of ordered universal algebra in the following way. For fixed $k \in \omega$, let Σ_k denote the signature of pomonoids expanded with a set of extra constants $\{c_u : u \in B^k\}$. A weight $w\colon B^k \to \mathbf{M}$ can be represented by a Σ_k-structure, namely $\mathbf{M}$ expanded with $w(u)$ as a realization of the constant c_u for each $u \in B^k$. Let us denote this structure as $(\mathbf{M}, w)$. We see from (7) that for any $C \subseteq \mathrm{Pmf}$, there is a set I_C of inequalities between closed (variable-free) Σ_k-terms such that $C \triangleright w$ iff $(\mathbf{M}, w) \vDash I_C$. In this way, $\mathrm{Inv}(C) \cap \mathrm{Wgt}_k$ becomes a partially ordered variety.

Remark 4.11 Let D be a weight coclone, $\mathbf{M}$ a monoid, and $w\colon B^k \to \mathbf{M}$. Then the set of partial orders $\leq$ such that $w\colon B^k \to (\mathbf{M}, \leq)$ is in D, is either empty, or a principal filter in the poset of partial orders compatible with $\mathbf{M}$; that is, it is closed under order extensions (by (B)), and nonempty intersections (by (C) and (D), using the diagonal embedding of $(\mathbf{M}, \bigcap_\alpha \leq_\alpha)$ in $\prod_\alpha (\mathbf{M}, \leq_\alpha)$).

This can be even more naturally stated for invariant preorders in place of partial orders: that is, for any pomonoid $\mathbf{M}$, and $w\colon B^k \to \mathbf{M}$, the set of invariant preorders $\preceq$ such that $w\colon B^k \to \mathbf{M}/{\preceq}$ is in D, is a principal filter in $\mathrm{OCon}\,\mathbf{M}$. Indeed, it is just $\mathrm{OCon}_{D_k}(\mathbf{M}, w)$, where D_k denotes $D \cap \mathrm{Wgt}_k$ as a Σ_k-povariety in the set-up of Remark 4.10.

The main results of this section state that the notions of pmf clones and weight coclones faithfully describe the closure systems of our Galois connection.

Theorem 4.12 *Galois-closed sets of pmf are exactly the pmf clones.*

Proof: First, we show that any Galois-closed set of pmf is a pmf clone. Assume that $\mathrm{Pol}(D)$ is such a set. Let $n, m, k \in \omega$, f be in the topological closure of $\mathrm{Pol}(D) \cap \mathrm{Pmf}_{n,m}$, $w \in D \cap \mathrm{Wgt}_k$, and $a \in B^{k \times n}$, $b \in B^{k \times m}$ be such that $f(a^j) \approx b^j$ for all $j < k$. There exists $f' \in \mathrm{Pol}(D)$ in the basic open neighbourhood $\{f' : \forall j < k\, f'(a^j) \approx b^j\}$ of f; since $f' \triangleright w$, we obtain

$$\prod_{i<n} w(a_i) \leq \prod_{i<m} w(b_i).$$

This shows that $\mathrm{Pol}(D)$ satisfies (I). Reflexivity and transitivity of $\leq$ readily implies (II) and (III). Finally, if $f, g \in \mathrm{Pol}(D)$, $w \in D$, and $(f \times g)(a^j, a'^j) \approx (b^j, b'^j)$ for each $j < k$, then

$$\prod_{i<n+n'} w((a, a')_i) = \Big(\prod_{i<n} w(a_i)\Big)\Big(\prod_{i<n'} w(a'_i)\Big) \leq \Big(\prod_{i<m} w(b_i)\Big)\Big(\prod_{i<m'} w(b'_i)\Big) = \prod_{i<m+m'} w((b, b')_i)$$

as $\cdot$ is nondecreasing in both arguments, which verifies (IV).

On the other hand, let C be a pmf clone; we will prove C is Galois-closed. In fact, we will construct a canonical sequence of weights $\{w_k : k < \omega\}$ that characterize C. For any $k < \omega$, let $\mathbf{F}_k = (F_k, 1, \cdot)$ be the monoid freely generated by B^k (i.e., the monoid of finite words over alphabet B^k), and define a relation $\lesssim$ on F_k by

$$a_0 \dots a_{n-1} \lesssim b_0 \dots b_{m-1} \quad \text{iff} \quad \exists g \in C \cap \mathrm{Pmf}_{n,m}\ \forall j < k\, g(a^j) \approx b^j. \tag{8}$$

Conditions (II) and (III) imply that $\lesssim$ is a preorder, and (IV) shows that $x \lesssim y$ implies $xz \lesssim yz$ and $zx \lesssim zy$. Thus, the relation $x \sim y \Leftrightarrow x \lesssim y \wedge y \lesssim x$ is a congruence on $\mathbf{F}_k$, and

$\mathbf{M}_k = (M_k, 1, \cdot, \leq) := (F_k, 1, \cdot, \lesssim)/{\sim}$ is a pomonoid. Let $w_k \colon B^k \to \mathbf{M}_k$ be the quotient map composed with the natural inclusion of B^k in $\mathbf{F}_k$. For any $a \in B^{k\times n}$, we have

$$\prod_{i<n} w_k(a_i) = (a_0 \dots a_{n-1})/{\sim},$$

thus

$$\prod_{i<n} w_k(a_i) \leq \prod_{i<m} w_k(b_i) \quad \text{iff} \quad a_0 \dots a_{n-1} \lesssim b_0 \dots b_{m-1}. \tag{9}$$

This implies immediately $C \triangleright w_k$ for all $k < \omega$.

Now, assume $f \in \mathrm{Pmf}_{n,m}$ is in $\mathrm{Pol}(\mathrm{Inv}(C))$, which implies $f \triangleright \{w_k : k < \omega\}$; we want to show $f \in C$. By (I) and Remark 4.7, it suffices to verify that for any $k < \omega$, $a \in B^{k\times n}$, and $b \in B^{k\times m}$, if $f(a^j) \approx b^j$ for all $j < k$, then there exists $g \in C \cap \mathrm{Pmf}_{n,m}$ such that $g(a^j) \approx b^j$ for all $j < k$. This is indeed true: if $f(a^j) \approx b^j$ for all $j < k$, then $f \triangleright w_k$ implies $a_0 \dots a_{n-1} \lesssim b_0 \dots b_{m-1}$ by (9), hence the required g exists by (8). □

Theorem 4.13 *Galois-closed classes of weights are exactly the weight coclones.*

Proof: Let $\mathrm{Inv}(C)$ be any Galois-closed class of weights, we will show it is a weight coclone. In view of Remark 4.10, for each fixed k, $\mathrm{Inv}(C) \cap \mathrm{Wgt}_k$ is a povariety, and as such it is closed under homomorphic images, products, and substructures. Moreover, since it is axiomatized by variable-free inequalities on top of the theory of pomonoids, it is also closed under embedding into structures that are expansions of pomonoids, whence under non-surjective homomorphisms into such structures. This shows that $\mathrm{Inv}(C)$ satisfies conditions (B)–(D). As for (A), let $f \in C \cap \mathrm{Pmf}_{n,m}$, and $a' \in B^{k'\times n}$, $b' \in B^{k'\times m}$ be such that $f(a'^j) \approx b'^j$. Define $a \in B^{k\times n}$ and $b \in B^{k\times m}$ by putting $a_i^j = a_i'^{\varrho(j)}$, $b_i^j = b_i'^{\varrho(j)}$ for $j < k$. Then $f \triangleright w$ implies

$$\prod_{i<n} w(\tilde\varrho(a'_i)) = \prod_{i<n} w(a_i) \leq \prod_{i<m} w(b_i) = \prod_{i<m} w(\tilde\varrho(b'_i)).$$

Conversely, we prove that any weight coclone D is Galois-closed. Let $v \colon B^k \to \mathbf{N}$ be in $\mathrm{Inv}(\mathrm{Pol}(D))$, we will show $v \in D$. Let I denote the set of pairs $\alpha = ((a_i^j)_{i<n}^{j<k}, (b_i^j)_{i<m}^{j<k})$ such that

$$\prod_{i<n} v(a_i) \nleq \prod_{i<m} v(b_i).$$

For each such α, let $f_\alpha \colon B^n \Rightarrow B^m$ denote the pmf $\{(a^j, b^j) : j < k\}$. Since $f_\alpha \not\triangleright v \in \mathrm{Inv}(\mathrm{Pol}(D))$, there is $w'_\alpha \colon B^{k'} \to \mathbf{M}_\alpha$ in D such that $f_\alpha \not\triangleright w'_\alpha$. By the definition of f_α, this means there is $\varrho \colon k' \to k$ such that

$$\prod_{i<n} w'_\alpha(a_i^{\varrho(0)}, \dots, a_i^{\varrho(k'-1)}) \nleq \prod_{i<m} w'_\alpha(b_i^{\varrho(0)}, \dots, b_i^{\varrho(k'-1)}).$$

Thus, $w_\alpha = w'_\alpha \circ \tilde\varrho \colon B^k \to \mathbf{M}_\alpha$, which is in D by (A), satisfies

$$\prod_{i<n} w_\alpha(a_i) \nleq \prod_{i<m} w_\alpha(b_i). \tag{10}$$

Let $\mathbf{M}' = \prod_{\alpha \in I} \mathbf{M}_\alpha$, $w' \colon B^k \to \mathbf{M}'$ be as in (C), $\mathbf{M}$ be the submonoid of $\mathbf{M}'$ generated by $\operatorname{im}(w')$, and $w \colon B^k \to \mathbf{M}$ be w' reconsidered as a mapping to $\mathbf{M}$. We have $w \in D$ by (C) and (D).

If $\prod_{i<n} w(a_i)$ and $\prod_{i<m} w(b_i)$ are two elements of M such that

(11) $$\prod_{i<n} w(a_i) \le \prod_{i<m} w(b_i),$$

we must have $\prod_{i<n} v(a_i) \le \prod_{i<m} v(b_i)$: otherwise $\alpha = ((a_i^j), (b_i^j)) \in I$, thus (10) contradicts (11). It follows that

$$\varphi\Bigl(\prod_{i<n} w(a_i)\Bigr) = \prod_{i<n} v(a_i)$$

is a well-defined pomonoid homomorphism $\varphi \colon \mathbf{M} \to \mathbf{N}$, hence $v = \varphi \circ w \in D$ by (B). □

For any set $C \subseteq \mathrm{Pmf}$, the least Galois-closed set containing C is $\mathrm{Pol}(\mathrm{Inv}(C))$. By Theorem 4.12, $\mathrm{Pol}(\mathrm{Inv}(C))$ is exactly the pmf clone generated by C, that is, the closure of C under conditions (I)–(IV). This is, on the face of it, a rather opaque operation, as in principle we might need to cycle through the individual closure conditions and iterate them over and over. In fact, we will see that it is enough to close the set under each condition once, in a judiciously chosen order, and similarly for the Galois closure of classes of weights.

Definition 4.14 If $C \subseteq \mathrm{Pmf}$, let $\mathrm{cl}_\cup C$ denote the closure of C under directed unions, $\mathrm{cl}_\subseteq C$ the closure under subfunctions, and $\mathrm{cl}_{\mathrm{id}} C$, $\mathrm{cl}_\circ C$, and $\mathrm{cl}_\times C$ the closure under (II), (III), and (IV), respectively. If $D \subseteq \mathrm{Wgt}$, $\mathrm{cl}_{\mathrm{var}} D$, $\mathrm{cl}_M D$, $\mathrm{cl}_P D$, and $\mathrm{cl}_S D$ denote the closure of D under (A), (B), (C), and (D), respectively.

The M in cl_M stands for "morphism". While cl_M, cl_S, and cl_P are reminiscent of the H, S, and P closure operators from universal algebra, condition (B) also applies to non-surjective homomorphisms; for this reason, we chose a different letter to forestall confusion.

Corollary 4.15 $\mathrm{Pol}(\mathrm{Inv}(C)) = \mathrm{cl}_\cup \mathrm{cl}_\subseteq \mathrm{cl}_\circ \mathrm{cl}_\times \mathrm{cl}_{\mathrm{id}} C$, *and* $\mathrm{Inv}(\mathrm{Pol}(D)) = \mathrm{cl}_M \mathrm{cl}_S \mathrm{cl}_P \mathrm{cl}_{\mathrm{var}} D$.

Proof: The $\supseteq$ inclusions are clear, and the proof of Theorem 4.13 shows directly that any $w \in \mathrm{Inv}(\mathrm{Pol}(D))$ is in $\mathrm{cl}_M \mathrm{cl}_S \mathrm{cl}_P \mathrm{cl}_{\mathrm{var}} D$. Let $f \in \mathrm{Pol}(\mathrm{Inv}(C))$, and C^+ be the closure of C under (II), (III), and (IV). The argument in Theorem 4.12 shows that any finite subfunction of f is included in some $g \in C^+$, hence $\mathrm{Pol}(\mathrm{Inv}(C)) \subseteq \mathrm{cl}_\cup \mathrm{cl}_\subseteq C^+$. Clearly, $\mathrm{cl}_\circ \mathrm{cl}_\times \mathrm{cl}_{\mathrm{id}} C$ contains $\mathrm{cl}_{\mathrm{id}} C$, and it is closed under composition. It is also closed under $\times$, as

$$(f_r \circ \dots \circ f_1) \times (g_s \circ \dots \circ g_1) = (\mathrm{id}_m \times g_s) \circ \dots \circ (\mathrm{id}_m \times g_1) \circ (f_r \times \mathrm{id}_n) \circ \dots \circ (f_1 \times \mathrm{id}_n),$$

where m is the arity of the output of f_r, and n of the input of g_1. Thus, $C^+ = \mathrm{cl}_\circ \mathrm{cl}_\times \mathrm{cl}_{\mathrm{id}} C$. □

5 Restricted cases

The generality of the Galois connection described in Section 4 reflects more what we *can* do than what is *useful* to do. In potential applications, we may be interested in restricted classes of pmf or weights, for example:

- We may want to discuss only bona fide functions $f\colon B^n \to B^m$ (total, univalued) rather than pmf.
- In the context of reversible operations, we want them further to be bijective, and we require $n = m$. On the other hand, in the classical case we require $m = 1$.
- In essentially any reasonable context, we want to allow permutation of variables.
- Some readers may prefer to disallow pesky corner cases involving B^0, and only deal with pmf $B^n \Rightarrow B^m$ and weights $B^k \to \mathbf{M}$ where $n, m, k \geq 1$.
- We may need to impose extra closure conditions, such as closure under inverse, or under usage of ancillary inputs (see below).

We would like to adapt our Galois connection to such restricted contexts. Some cases are very easy to handle as an immediate consequence of our main theorem:

Example 5.1 Let us investigate the Galois connection induced by the preservation relation restricted to pmf $f\colon B^n \Rightarrow B^n$ (i.e., with the same number of inputs and outputs). The class of all such pmf itself forms a clone, say $C_=$; its dual is a coclone $D_=$. It follows that the preservation relation restricted to $f \in C_=$ induces a Galois connection whose closed classes are exactly the pmf clones $C \subseteq C_=$ on the one side, and weight coclones $D \supseteq D_=$ on the other side. In order to complete the description, it only remains to determine $D_=$, ideally by presenting a simple generating set. This is given in Proposition 5.2 below: $D_=$ is generated by the constant-1 weight function $\mathrm{c}_1\colon B^0 \to (\mathbb{N}, 0, +, =)$. (In fact, $D_=$ consists of all constant weight functions.) Thus, the closed classes of weights under this restricted Galois connection are weight coclones that contain c_1.

Several similarly easy cases can be dealt with using Propositions 5.2 and 5.5 below.

Other cases turn out to be more complicated. In particular, the very important restriction of the Galois connection to *total* functions requires substantial work, and we will tackle it in Section 5.1. Likewise, in Section 5.2 we investigate closure conditions imposed on classes of permutations in the work of Aaronson, Grier, and Schaeffer [2], in particular closure under ancillas.

For the next statement, recall that the Kronecker delta function is defined by

$$\delta(u, v) = \begin{cases} 1 & u = v, \\ 0 & u \neq v. \end{cases}$$

For any pmf $f\colon B^n \Rightarrow B^m$, its inverse $f^{-1}\colon B^m \Rightarrow B^n$ is defined by $f^{-1}(x) \approx y \Leftrightarrow f(y) \approx x$. A pmf f is injective (sometimes called left-unique) if $f(x) \approx y$ and $f(x') \approx y$ implies $x = x'$.

Proposition 5.2 *Let $C = \mathrm{Pol}(D)$ and $D = \mathrm{Inv}(C)$. If $w\colon B^k \to \mathbf{M}$ is a weight, let $\mathbf{M}_{(w)}$ denote the submonoid of $\mathbf{M}$ generated by $\mathrm{im}(w)$.*

(*i*) *All $f\colon B^n \Rightarrow B^m$ in C satisfy $n \le m$ ($n \ge m$; $n = m$) iff D contains the constant weight $\mathrm{c}_1\colon B^0 \to (\mathbb{N}, 0, +)$, where $\mathbb{N}$ is ordered by $\le$ ($\ge$; $=$; resp.).*

(*ii*) *All $f \in C$ are partial functions (injective; both) iff D contains Kronecker $\delta\colon B^2 \to (\mathbf{2}, 1, \wedge)$, where the monoid is ordered by $\le$ ($\ge$; $=$; resp.).*

(*iii*) *C contains the swap function $B^2 \to B^2$, $(x, y) \mapsto (y, x)$ (and consequently all variable permutations $B^n \to B^n$) iff $\mathbf{M}_{(w)}$ is commutative for every $w \in D$.*

(*iv*) *C contains all (constant) functions $B^0 \to B$ iff for every $w\colon B \to \mathbf{M}$ in D, 1 is a bottom element in $\mathbf{M}_{(w)}$.*

(*v*) *C contains the diagonal mappings $\Delta_m\colon B \to B^m$, $\Delta_m(x) = (x, \dots, x)$, for $m = 0, 2$ (and consequently, for all $m \ge 0$), and variable permutations, iff for every $w \in D$, $\mathbf{M}_{(w)}$ is a meet-semilattice with a top element $(M_{(w)}, \top, \wedge, \le)$.*

(*vi*) *$f \in C$ implies $f^{-1} \in C$ iff for every $w\colon B^k \to (\mathbf{M}, \le)$ in D, also $w\colon B^k \to (\mathbf{M}, =)$ is in D.*

Proof: (i)–(iii) are straightforward.

(iv): A straightforward computation shows that C contains all functions $B^0 \to B^1$ iff for every $w\colon B^k \to \mathbf{M}$ in D, and for every $u \in B$, we have $1 \le w(u, \dots, u)$. This is equivalent to the special case $k = 1$ given in (iv), since for any $w \in D$ as above, the unary weight $w'\colon B^1 \to \mathbf{M}$ defined by $w'(u) = w(u, \dots, u)$ is also in D by condition (A).

(v): As long as $\mathbf{M}_{(w)}$ is commutative, w is preserved by diagonal maps iff $\mathbf{M}_{(w)}$ satisfies $x \le x^m$ for all $m \ge 0$; that is, $x \le 1$ and $x \le x^2$. On the one hand, this gives $xy \le x, y$. On the other hand, $z \le x, y$ implies $z \le z^2 \le xy$. Thus, $(\mathbf{M}, \le)$ is a semilattice with meet $\cdot$, and top element 1.

(vi), right-to-left: if $f \in C$, and $w \in D$, we may assume $w\colon B^k \to (\mathbf{M}, =)$. Then condition (7) is symmetric in a and b, hence $f \rhd w$ implies $f^{-1} \rhd w$. Left-to-right: let $w\colon B^k \to (\mathbf{M}, \le)$ be in D, and consider any $f \in C$ and $(a_i^j), (b_i^j)$ such that $f(a^j) \approx b^j$ for all $j < k$. Since $f \rhd w$, we have

$$\prod_{i<n} w(a_i) \le \prod_{i<m} w(b_i).$$

By assumption, also $f^{-1} \in C$, and $f^{-1}(b^j) \approx a^j$ for all $j < k$, hence

$$\prod_{i<m} w(b_i) \le \prod_{i<n} w(a_i).$$

Thus, f preserves the weight $w\colon B^k \to (\mathbf{M}, =)$. □

The various cases in (i) and (ii) of Proposition 5.2 give rise to variants of the clone–coclone duality where Pmf is restricted to a smaller class in the same way as in Example 5.1. Conversely, (iii)–(vi) lead to variants where Wgt is restricted, such as:

Example 5.3 Consider the Galois connection induced by the preservation relation restricted to $\mathrm{Wgt}_{\mathrm{comm}}$—weights $w\colon B^k \to \mathbf{M}$ with $\mathbf{M}$ a commutative pomonoid. We claim that the closed classes of this Galois connection are, on the one side, pmf clones containing the swap function, and on the other side, classes of weights $w\colon B^k \to \mathbf{M}$ from $\mathrm{Wgt}_{\mathrm{comm}}$ satisfying conditions (A)–(D), where (B) is restricted to $\mathbf{M}'$ commutative (let us call them "commutative coclones").

Indeed, Proposition 5.2 (iii) shows immediately that $C \subseteq \mathrm{Pmf}$ is of the form $\mathrm{Pol}(D)$ for some $D \subseteq \mathrm{Wgt}_{\mathrm{comm}}$ iff it is a clone containing the swap. It is also clear that since $\mathrm{Inv}(C)$ is a coclone, $\mathrm{Inv}(C) \cap \mathrm{Wgt}_{\mathrm{comm}}$ is a commutative coclone. On the other hand, if D is a commutative coclone, then the class D' of weights $w\colon B^k \to \mathbf{M}'$ such that $w\colon B^k \to \mathbf{M}$ is in D for some (commutative) subpomonoid $\mathbf{M} \subseteq \mathbf{M}'$ is a coclone, and $D = D' \cap \mathrm{Wgt}_{\mathrm{comm}}$, thus $D = \mathrm{Wgt}_{\mathrm{comm}} \cap \mathrm{Inv}(C)$ for some $C \subseteq \mathrm{Pmf}$.

Let us also state explicitly one more case as it involves a nontrivial closure condition on C:

Example 5.4 Let $\mathrm{Wgt}_{\mathrm{unord}}$ be the class of functions $w\colon B^k \to \mathbf{M}$ where $\mathbf{M}$ is an (unordered) monoid, identified with the trivially ordered pomonoid $(\mathbf{M}, =)$. Consider the Galois connection induced by the preservation relation between $f \in \mathrm{Pmf}$ and $w \in \mathrm{Wgt}_{\mathrm{unord}}$. Using Proposition 5.2 (vi), and the argument in Example 5.3, it is easy to see that the closed classes of this Galois connection are, on the one side, clones $C \subseteq \mathrm{Pmf}$ closed under taking inverses (for every $f\colon B^n \Rightarrow B^m$ in C, also $f^{-1}\colon B^m \Rightarrow B^n$ is in C), and on the other side, classes $D \subseteq \mathrm{Wgt}_{\mathrm{unord}}$ closed under (A)–(D), where in (B), $\varphi\colon \mathbf{M} \to \mathbf{M}'$ is a monoid homomorphism.

The restrictions of the Galois connection corresponding to the cases of Proposition 5.2 can be combined where it makes sense.

Although quite similar in spirit to Proposition 5.2, we discuss the following restrictions separately.

Proposition 5.5 *Let $C = \mathrm{Pol}(D)$ and $D = \mathrm{Inv}(C)$. Let us say that a pmf $f\colon B^n \Rightarrow B^m$ has the* right shape *if $n > 0$ ($m > 0$; both).*

(i) C is generated by a set of pmf of the right shape iff all $f \in C$ are of the right shape except for id_0 and $\varnothing\colon B^0 \Rightarrow B^0$ iff D contains the constant weight $\mathrm{c}_0\colon B^0 \to (\mathbf{2}, 1, \wedge)$ with the monoid ordered by $\leq$ ($\geq$; $=$; resp.).

(ii) D is generated by $w\colon B^k \to \mathbf{M}$ with $k > 0$ iff all nontrivial $w\colon B^k \to \mathbf{M}$ in D have $k > 0$ iff C contains the empty pmf $\varnothing\colon B^0 \Rightarrow B^1$ and $\varnothing\colon B^1 \Rightarrow B^0$ (hence $\varnothing\colon B^n \Rightarrow B^m$ for all n, m).

Proof: Straightforward. □

Corollary 5.6

(i) The preservation relation restricted to pmf of the right shape induces a Galois connection whose closed classes are, on the one side, sets of pmf of the right shape satisfying the appropriate restrictions of (I)–(IV), and on the other side, weight coclones that include $\mathrm{c}_0\colon B^0 \to (\mathbf{2}, 1, \wedge)$ ordered by $\leq$ ($\geq$; $=$; resp.).

(*ii*) *The preservation relation restricted to weights* $w\colon B^k \to \mathbf{M}$ *with* $k > 0$ *induces a Galois connection whose closed classes are, on the one side, pmf clones that include* $\varnothing\colon B^n \Rightarrow B^m$ *for all* $n, m \geq 0$*, and on the other side, classes of said weights satisfying the appropriate restrictions of (A)–(D).*

(*iii*) *Let us consider the preservation relation simultaneously restricted to pmf of the right shape, and to weights* $w\colon B^k \to \mathbf{M}$ *with* $k > 0$*. The closed classes of the induced Galois connection are, on the one side, classes of pmf of the right shape satisfying the appropriate restrictions of (I)–(IV), and including all* $\varnothing\colon B^n \Rightarrow B^m$ *of the right shape; on the other side, classes of said weights satisfying the appropriate restrictions of (A)–(D), and including the constant weight* $\mathrm{c}_0\colon B^1 \to (\mathbf{2}, 1, \wedge)$ *ordered by* $\leq$ *(*$\geq$*;* $=$*; resp.).*

Proof: (i) and (ii) follow from Proposition 5.5 in a similar way as in Examples 5.1, 5.3, and 5.4. However, let us prove (iii) in more detail as the two conditions from Proposition 5.5 somewhat contradict each other, the weight in Proposition 5.5 (i) being nullary.

Clearly, a closed set of pmf must satisfy the restricted versions of (I)–(IV), and contain all empty pmf of the right shape by Proposition 5.5. Likewise, a closed class of weights satisfies the restricted versions of (A)–(D), and contains all weights $w\colon B^k \to \mathbf{M}$ with $k > 0$ that are in the coclone generated by $\mathrm{c}_0\colon B^0 \to (\mathbf{2}, 1, \wedge)$ (ordered in the indicated fashion), one of which being $\mathrm{c}_0\colon B^1 \to (\mathbf{2}, 1, \wedge)$.

On the other hand, let C be a set of pmf satisfying the conditions in the statement of (iii), and let C' be C together with $\mathrm{id}_0\colon B^0 \Rightarrow B^0$, and all empty pmf. Then C' is a pmf clone, and by Proposition 5.5, its dual $\mathrm{Inv}(C')$ is generated by a class D of weights $w\colon B^k \to \mathbf{M}$ with $k > 0$. Thus, $C' = \mathrm{Pol}(D)$, and C is the restriction of $\mathrm{Pol}(D)$ to the set of pmf of the right shape, as we added into C' only pmf of wrong shapes.

Similarly, let D be a class of weights satisfying the conditions in the statement of (iii). Let D' denote D together with all weights $w\colon B^0 \to \mathbf{M}$ such that the unique element $a \in \mathrm{im}(w)$ is an idempotent, and satisfies $a \leq 1$ ($1 \leq a$; nothing; respectively). Then D' is a weight coclone: in particular, for any weight $w\colon B^0 \to \mathbf{M}$ as just described, the corresponding constant weight $B^1 \to \mathbf{M}$ is already in D by property (B), as it factors through $\mathrm{c}_0\colon B^1 \to (\mathbf{2}, 1, \wedge)$. By Proposition 5.5, $D' = \mathrm{Inv}(C)$ for a set C of pmf of the right shape. Again, the same holds for D under the restricted preservation relation as we only added nullary weights into D'. □

Remark 5.7 In general, nullary weights in $\mathrm{Inv}(C)$ describe possible shapes of pmf in C, where by the shape of $f\colon B^n \Rightarrow B^m$ we mean the numbers n, m of inputs and outputs. To see this, consider a weight $w\colon B^0 \to \mathbf{M}$. Let $a \in M$ be the single value of w, and $\varphi\colon (\mathbb{N}, 0, +) \to \mathbf{M}$ the unique monoid homomorphism mapping 1 to a. The order kernel $\mathrm{oker}(\varphi)$ is an invariant preorder $\preceq$ on $\mathbb{N}$, which faithfully represents the relevant part of w in that the restricted-image weight $w\colon B^0 \to \mathbf{M}_{(w)}$ (with the same polymorphisms) is isomorphic to the weight $\mathrm{c}_1\colon B^0 \to \mathbb{N}/{\preceq}$ with single value $1/{\preceq}$. Now, for any pmf $f\colon B^n \Rightarrow B^m$, we have

$$f \rhd w \quad \text{iff} \quad n \preceq m.$$

On a related note, recall from Remark 4.11 that for any pmf clone C, there is the smallest invariant preorder $\preceq$ on $\mathbb{N}$ such that $\mathrm{c}_1\colon B^0 \to \mathbb{N}/{\preceq}$ is in $\mathrm{Inv}(C)$. It follows from the discussion above that

$$n \preceq m \quad \text{iff} \quad C \cap \mathrm{Pmf}_{n,m} \neq \varnothing.$$

Remark 5.8 Case (v) of Proposition 5.2 directly gives a restricted version of the Galois connection with weights in semilattices in the spirit of Example 5.3. However, the real reason we mention it is that it can be used to recover the classical clone–coclone Galois connection, or more precisely, its version for partial multifunctions $B^n \to B$ as given in the original paper by Geiger [8] (we have yet to handle total functions). We will describe the reduction now.

If a pmf clone C contains variable permutations and the diagonal maps Δ_m, it also contains all projections $\pi_{n,i}\colon B^n \to B$, $\pi_{n,i}(x_0, \dots, x_{n-1}) = x_i$ (using Δ_0). We claim that for any $f \in \mathrm{Pmf}_{n,m}$,

$$f \in C \quad \text{iff} \quad \forall i < m\, \pi_{m,i} \circ f \in C. \tag{12}$$

The left-to-right implication follows from (III), as $\pi_{m,i} \in C$. For the right-to-left implication, if $f_i = \pi_{m,i} \circ f \in C$ for each $i < m$, then $f_0 \times \cdots \times f_{m-1}\colon B^{nm} \Rightarrow B^m$ is in C. By using Δ_n and variable permutations, C includes the function $B^n \to B^{nm}$, $x \mapsto (x, \dots, x)$, hence also the pmf $f' = (f_0, \dots, f_{m-1})\colon B^n \Rightarrow B^m$ defined by

$$f'(x) \approx (y_0, \dots, y_{m-1}) \quad \text{iff} \quad \forall i < m\, f_i(x) \approx y_i.$$

If f were a function, then simply $f' = f$; for a general pmf f, we still have that $f(x) \approx y$ implies $f_i(x) \approx y_i$, hence $f \subseteq f'$, and $f \in C$ by (I).

Thus, C is determined by its unary-output fragment $C_1 = \dot{\bigcup}_n (C \cap \mathrm{Pmf}_{n,1})$. Now, C_1 satisfies (I), contains all $\pi_{n,i}$, and it is closed under composition in the sense that whenever it contains $g\colon B^{n'} \Rightarrow B$, and $f_i\colon B^n \Rightarrow B$ for $i < n'$, it also contains $g \circ (f_0, \dots, f_{n'-1})\colon B^n \Rightarrow B$. Conversely, if C_1 satisfies these three conditions, then (12) defines a pmf clone C containing Δ_m and variable permutations whose unary-output fragment is C_1. Let us call such C_1 *unary clones.*

On the dual side, if $w\colon B^k \to \mathbf{M}$ is a weight such that $\mathbf{M}_{(w)}$ is a meet semilattice with a top, we can write $\mathbf{M}_{(w)}$ as a subdirect product of subdirectly irreducible such semilattices, i.e., $(\mathbf{2}, \top, \wedge, \leq)$. Such weights $w\colon B^k \to \mathbf{2}$ can be identified with relations $r \subseteq B^k$, and it is easy to see that for $f\colon B^n \Rightarrow B$, $f \triangleright r$ coincides with the classical preservation relation as in Section 2. Weight coclones D corresponding to unary clones are thus determined by classes D_1 of relations $r \subseteq B^k$. The class D_1 is closed under variable manipulations as in (A). Conditions (B)–(D) boil down to the following: If $r_\alpha \subseteq B^k$ is in D_1 for all $\alpha \in I$, and F is a filter on $\mathcal{P}(I)$, the relation $r \subseteq B^k$ defined by

$$r(x) \quad \text{iff} \quad \{\alpha \in I : r_\alpha(x)\} \in F \tag{13}$$

is in D_1 (this describes when the weight corresponding to r can be obtained as a homomorphic image of a subsemilattice of a direct product of weights corresponding to r_α). Notice that principal filters F give closure of D_1 under intersections. In general, one can check that D_1 is closed under (13) iff it is closed in the Hausdorff topology, and under (finite, hence infinite) intersections. We thus obtain a Galois connection whose closed classes are unary clones on one side, and classes of relations D_1 closed under (A) and intersections, and topologically closed, on the other side. This recovers the results of [8].

5.1 Totality conditions

In contrast to the set-up of partial multifunctions that we worked with so far, our two original motivating examples (classical clones of operations on a set, and reversible operations) deal exclusively with *total* functions, it is thus imperative to investigate how the duality is affected if we impose this restriction. That is, the preservation relation $f \triangleright w$ induces a Galois connection between classes of *total* multifunctions, and classes of weights: can we determine what are the closed classes in this connection? Notice that unlike conditions like injectivity that we handled in Propositions 5.2 and 5.5, the class of all total pmf is not a clone in our sense (it is obviously not closed downwards), which considerably complicates the answer.

Closed classes of total mf are easy to guess; it is straightforward to formulate a version of the notion of pmf clones for total mf (we will do this in Definition 5.11). Moreover, it will mesh fairly well with the theory of pmf clones, in that a clone of total mf can be identified with the pmf clone it generates by closing it downwards. The pmf clones C we get in this way are those with the property that each pmf in C extends to a total mf in C.

Description of the corresponding coclones is more difficult. Recall that in the classical case, coclones on a finite set are sets of relations closed under positive primitive definitions, and in particular, totality corresponds to closure under *existential quantification.* (This correspondence does not work that well on infinite—especially uncountable—sets, and we will encounter similar cardinality difficulties, too.) A natural generalization of existential quantification to weight functions is as follows: if $w\colon B^{k+1} \to \mathbf{M}$ is a weight function, let us define a weight $w^+\colon B^k \to \mathbf{M}$ by

$$w^+(x^0, \dots, x^{k-1}) = \sum_{u \in B} w(x^0, \dots, x^{k-1}, u). \tag{14}$$

However, first we need to make sense of the sum in (14). If B is finite, it is enough to stipulate that $\mathbf{M}$ be a *semiring*: a structure $(M, 1, \cdot, 0, +)$ where $(M, 1, \cdot)$ is a monoid, $(M, 0, +)$ is a commutative monoid, and the finite distributive laws

$$(x + y)z = xz + yz \qquad z(x + y) = zx + zy$$
$$0z = 0 \qquad z0 = 0$$

hold. If B is infinite, we will also need some sort of completeness to make sense of infinite sums. We introduce the relevant notions below.

The above discussion of totality applies symmetrically to classes of *surjective* (*onto*) pmf, and we will treat both cases, as well as their combination, in parallel.

Definition 5.9 A *partially ordered semiring* (*posemiring*) is a structure $(M, 1, \cdot, 0, +, \leq)$ such that $(M, 1, \cdot, 0, +)$ is a semiring, and $(M, 1, \cdot, \leq)$ and $(M, 0, +, \leq)$ are pomonoids.[3]

When $\mathbf{M}$ is a posemiring, we will abuse the language to speak of weight functions $w\colon B^k \to \mathbf{M}$ with the understanding that this refers to the multiplicative pomonoid $(M, 1, \cdot, \leq)$.

A *positive* (*negative*) *semiring* is a posemiring $(M, 1, \cdot, 0, +, \leq)$ such that $0 \leq 1$ ($1 \leq 0$, resp.). This in fact implies that 0 is a smallest (largest, resp.) element of $\mathbf{M}$.

A semiring is *idempotent* if it satisfies $x + x = x$. The additive structure of an idempotent semiring is a semilattice, thus it can be interpreted as a pomonoid in two ways: a $\vee$-*semiring* is an idempotent semiring ordered so that $+$ is $\vee$, and a $\wedge$-*semiring* is an idempotent semiring ordered so that $+$ is $\wedge$. Equivalently, a $\vee$-semiring ($\wedge$-semiring) is an idempotent positive (negative, resp.) semiring. An idempotent semiring is *continuous* if either of these two partial orders makes it a complete lattice, satisfying the infinite distributive laws

$$\Bigl(\sum_{\alpha\in I} x_\alpha\Bigr) z = \sum_{\alpha\in I} x_\alpha z, \qquad z \sum_{\alpha\in I} x_\alpha = \sum_{\alpha\in I} z x_\alpha. \tag{15}$$

More generally, an idempotent semiring is κ-*continuous* for a cardinal κ, if $\sum_{\alpha\in I} x_\alpha$ exists and satisfies (15) whenever $|I| < \kappa$. Notice that every idempotent semiring is ω-continuous.

Continuous $\vee$-semirings are commonly known in the literature as *unital quantales.*

The next theorem is the main technical result in this section: it characterizes pmf clones C whose dual coclones are closed under the w^+ operation in continuous $\vee$-semirings. It turns out that on the fundamental level, this operation does not precisely correspond to totality, but to the possibility of extending the domains of finite pmf in C by one new element. (This also agrees with the effects of existential quantification in the classical duality.) Only if the base set B is additionally *countable* (including finite), we can repeat this extension countably many times to obtain that each finite pmf from C extends to a total mf in C.

Theorem 5.10 *Let $C = \mathrm{Pol}(D)$ and $D = \mathrm{Inv}(C)$. The following are equivalent.*

(i) For every finite $f\colon B^n \Rightarrow B^m$ in C, and $a \in B^n$, there exists $b \in B^m$ such that $f \cup \{(a, b)\} \in C$.

(ii) Whenever $w\colon B^{k+1} \to \mathbf{M}$ is in D, where $\mathbf{M}$ is a continuous $\vee$-semiring, then also $w^+\colon B^k \to \mathbf{M}$ is in D.

In condition (ii), it would be enough to demand that $\mathbf{M}$ be $|B|^+$-continuous.

The symmetric condition $\forall f \in C\, \forall b\, \exists a\, f \cup \{(a, b)\} \in C$ is similarly characterized using continuous $\wedge$-semirings.

Proof:

[3] We warn the reader that while this terminology is convenient for our purposes, and fits well in the general framework of partially ordered varieties, it clashes with another commonly used definition whereby ordered semirings, and in particular rings, satisfy the implication $x \leq y \to xz \leq yz \wedge zx \leq zy$ only for $z \geq 0$, so the multiplicative monoid is not a pomonoid. On the other hand, they are additionally required to satisfy $0 \leq 1$.

(i) $\to$ (ii): Assume $w \in D$, we will show $C \rhd w^+$. Let $f \in C$, $f\colon B^n \Rightarrow B^m$, and $(a_i^j)_{i<n}^{j<k}$, $(b_i^j)_{i<m}^{j<k}$ be such that $f(a^j) \approx b^j$ for all $j < k$. We may assume that f is finite. Fix $a^k \in B^n$, and let $b^k \in B^m$ be such that $g = f \cup \{(a^k, b^k)\} \in C$. Since $g \rhd w$,

$$\prod_{i<n} w(a_i^0, \dots, a_i^k) \leq \prod_{i<m} w(b_i^0, \dots, b_i^k) \leq \prod_{i<m} w^+(b_i^0, \dots, b_i^{k-1}).$$

As a^k was arbitrary, distributivity gives

$$\begin{aligned}\prod_{i<n} w^+(a_i^0, \dots, a_i^{k-1}) &= \prod_{i<n} \bigvee_{u\in B} w(a_i^0, \dots, a_i^{k-1}, u)\\ &= \bigvee_{a^k\in B^n} \prod_{i<n} w(a_i^0, \dots, a_i^k)\\ &\leq \prod_{i<m} w^+(b_i^0, \dots, b_i^{k-1}).\end{aligned}$$

(ii) $\to$ (i): Assume for contradiction that $(a_i^j)_{i<n}^{j\leq k}$, $(b_i^j)_{i<m}^{j<k}$ are such that the pmf $f = \{(a^j, b^j) : j < k\}$ is in C, but $f \cup \{(a^k, b^k)\} \notin C$ for all $b^k \in B^m$. For each such b^k, we can pick $w_{b^k} : B^{k+1} \to \mathbf{M}_{b^k}$ in D such that

$$\prod_{i<n} w_{b^k}(a_i^0, \dots, a_i^k) \nleq \prod_{i<m} w_{b^k}(b_i^0, \dots, b_i^k)$$

using (A). Let $\mathbf{M} = \prod_{b^k\in B^m} \mathbf{M}_{b^k}$, and $w\colon B^{k+1} \to \mathbf{M}$ be as in (C), so that $w \in D$, and

$$\prod_{i<n} w(a_i^0, \dots, a_i^k) \nleq \prod_{i<m} w(b_i^0, \dots, b_i^k) \tag{16}$$

for every $b^k \in B^m$.

Let $\overline{M}$ be the complete lattice of down-sets of $\mathbf{M}$, which we make into a pomonoid $(\overline{M}, 1{\downarrow}, \cdot, \subseteq)$ by putting $X \cdot Y = \{xy : x \in X, y \in Y\}{\downarrow}$. It is easy to check that

$$Y \cdot \bigcup_{\alpha\in I} X_\alpha = \bigcup_{\alpha\in I} Y \cdot X_\alpha,$$

and similarly for multiplication from the right, hence $\overline{\mathbf{M}} = (\overline{M}, 1{\downarrow}, \cdot, \varnothing, \cup, \subseteq)$ is in fact a continuous $\vee$-semiring. The mapping $x \mapsto x{\downarrow}$ is an embedding of $\mathbf{M}$ into $\overline{\mathbf{M}}$, whose composition with w is a weight $\overline{w}\colon B^{k+1} \to \overline{\mathbf{M}}$ in D by (B). By assumption, the weight $\overline{w}^+\colon B^k \to \overline{\mathbf{M}}$ given by

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

is also in D. We have

$$\prod_{i<n} w(a_i^0, \dots, a_i^k) \in \prod_{i<n} \overline{w}^+(a_i^0, \dots, a_i^{k-1}),$$

but (16) implies

$$\prod_{i<n} w(a_i^0,\ldots,a_i^k) \notin \Big\{\prod_{i<m} w(b_i^0,\ldots,b_i^k) : b^k \in B^m\Big\}\Big\downarrow = \prod_{i<m} \overline{w}^+(b_i^0,\ldots,b_i^{k-1}),$$

thus

$$\prod_{i<n} \overline{w}^+(a_i^0,\ldots,a_i^{k-1}) \nsubseteq \prod_{i<m} \overline{w}^+(b_i^0,\ldots,b_i^{k-1}).$$

This contradicts $f \in C$. □

Definition 5.11 A *total* (*surjective; total surjective*) *clone* is a set C of total multifunctions (surjective pmf; total surjective mf; resp.) that satisfies (I)–(IV), where condition (I) is understood relative to the subspace of $\mathbf{2}_S^{B^n\times B^m}$ of all total (surjective; both; resp.) pmf.

A *total* (*surjective; total surjective*) *coclone* is a weight coclone that satisfies condition (ii) of Theorem 5.10 (the dual condition for $\wedge$; both; resp.).

Lemma 5.12 *Assume that B is countable, and let C be a pmf clone.*

(*i*) *If C satisfies condition* (*i*) *from Theorem 5.10, then for every finite $f\colon B^n \Rightarrow B^m$ in C, there exists a total mf $\overline{f}\colon B^n \Rightarrow B^m$ in C such that $f \subseteq \overline{f}$.*

(*ii*) *If C satisfies condition* (*i*) *from Theorem 5.10 and its symmetric condition, then for every finite $f\colon B^n \Rightarrow B^m$ in C, there exists a total surjective mf $\overline{f}\colon B^n \Rightarrow B^m$ in C such that $f \subseteq \overline{f}$.*

Proof:

(i): The statement is trivial if $B^n = \varnothing$; otherwise, let us fix a (not necessarily injective) enumeration $B^n = \{a^j : j \in \omega\}$. By repeated application of condition (i), we build an increasing chain of finite pmf

$$f = f_0 \subseteq f_1 \subseteq f_2 \subseteq f_3 \subseteq \cdots \tag{17}$$

such that $f_j \in C$, and $a^j \in \mathrm{dom}(f_{j+1})$. Then $\overline{f} = \bigcup_{j\in\omega} f_j \in C$ is a total extension of f.

(ii) is similar: we enumerate $B^n = \{a^j : j \in \omega\}$ and $B^m = \{b^j : j \in \omega\}$, and we construct a chain (17) such that $a^j \in \mathrm{dom}(f_{2j+1})$, and $b^j \in \mathrm{im}(f_{2j+2})$. □

Corollary 5.13 *The preservation relation induces a Galois connection between sets of total* (*surjective; total surjective*) *pmf, and classes of weights. In this connection, the Galois-closed sets of pmf are exactly the total* (*surjective; total surjective; resp.*) *clones. All Galois-closed classes of weights are total* (*surjective; total surjective; resp.*) *coclones, and if B is countable, the converse also holds.*

Proof: We will discuss the total case, the other two cases are completely analogous.

Since the class of weights is unrestricted, the Galois-closed sets of pmf of this connection are exactly the intersections of pmf clones with the set Tmf of all total mf by Theorem 4.12. These are just the total clones: on the one hand, if C is a clone, then $C \cap \mathrm{Tmf}$ clearly satisfies the closure conditions (I)–(IV) restricted to Tmf; on the other hand, if C is a total clone, let $\overline{C}$ be the set of all pmf $g\colon B^n \Rightarrow B^m$ such that every finite $f \subseteq g$ is included in some $h \in C$. Then using Corollary 4.15, we see that $\overline{C}$ is a pmf clone (that is, it is the clone generated by C), while the restricted condition (I) ensures that $\overline{C} \cap \mathrm{Tmf} = C$.

Galois-closed classes of weights of the restricted connection are thus classes of the form $D = \mathrm{Inv}(C)$, where C is a total clone. Clearly, any such D is a weight coclone. Moreover, since $D = \mathrm{Inv}(\overline{C})$, and any finite pmf in $\overline{C}$ is included in some $f \in C$, which is total, we see that the pmf clone $\overline{C}$ satisfies condition (i) of Theorem 5.10, thus D is a total coclone.

Conversely, if D is a total coclone, then $\mathrm{Pol}(D)$ is a pmf clone satisfying condition (i) of Theorem 5.10. Thus, if B is countable, then $\mathrm{Pol}(D)$ is generated by $C = \mathrm{Pol}(D) \cap \mathrm{Tmf}$ by Lemma 5.12, and as such $D = \mathrm{Inv}(C)$ is a closed class of the restricted Galois connection. □

We remark that the Galois connections from Corollary 5.13 can be combined with the restrictions from Propositions 5.2 and 5.5: for example, we obtain (for countable B) a duality between total clones consisting of total *functions*, and total coclones that include the Kronecker delta weight $\delta\colon B^2 \to (\mathbf{2}, 1, \wedge, \leq)$.

Example 5.14 Neither Lemma 5.12 nor Corollary 5.13 holds if we drop the requirement of B being countable. (Another version of the example also applies to Theorem 5.18 below.)

Assume that B is uncountable, and fix a dense linear order $<$ on B such that there are copies of $\mathbb{Q}$ at both ends of $(B, <)$. Let C be the pmf clone generated by all strictly order-preserving partial functions $B \Rightarrow B$, the diagonal functions Δ_m, and variable permutations. (The last two are not really necessary; we only include them so that the example can be realized as a clone of partial operations $B^n \Rightarrow B$ in the classical set-up of Geiger [8], cf. Remark 5.8.) Explicitly, C consists of subfunctions of partial functions $f\colon B^n \Rightarrow B^m$ of the form

$$f(x_0, \dots, x_{n-1}) = (f_0(x_{i_0}), f_1(x_{i_1}), \dots, f_{m-1}(x_{i_{m-1}})),$$

where $i_0, \dots, i_{m-1} < n$, and each $f_j\colon B \Rightarrow B$ is a strictly order-preserving partial function.

The pmf clone C satisfies condition (i) of Theorem 5.10: we can extend each f_j separately if it is finite, using the density of $<$.

However, C does not satisfy the conclusion of Lemma 5.12. Using the properties of $<$, we can find two elements $a, b \in B$ such that $a{\uparrow}$ is uncountable, and $b{\uparrow}$ is countable. Then the partial function $f\colon B \Rightarrow B$ mapping a to b is in C, but it has no total extension in C, as a total strictly order-preserving extension of f would need to embed $a{\uparrow}$ in $b{\uparrow}$, which is impossible.

Furthermore, let $D = \mathrm{Inv}(C)$. By Theorem 5.10, D is a total coclone. However, D is not a Galois-closed class in the Galois connection restricted to total mf from Corollary 5.13: indeed, if it were, then $C = \mathrm{Pol}(D)$ would be generated as a pmf clone by a set of total mf (a total clone), and as such it would satisfy condition (i) from Lemma 5.12 (cf. the proof of Corollary 5.13). We have just seen this is not the case. (We remark that D is generated by relations $r \subseteq B^k$ definable without parameters in the structure $(B, <)$, identified with weights in $(\mathbf{2}, 1, \wedge, \leq)$ as in Remark 5.8.)

Because of the application to reversible operations, we are particularly interested in clones determined by permutations. At least for finite B, their invariants are easily seen to be closed under the w^+ operation even when the target posemiring is not idempotent. We will now investigate this closure condition more closely.

Theorem 5.15 *Assume B is finite, and let $C = \mathrm{Pol}(D)$ and $D = \mathrm{Inv}(C)$. The following are equivalent.*

(i) *For every $f\colon B^n \Rightarrow B^m$ in C, there is an injective function $g\colon B^n \to B^m$ such that $f \cup g \in C$ (which implies $n \le m$ unless $|B| \le 1$).*

(ii) *For every $w\colon B^{k+1} \to \mathbf{M}$ in D where $\mathbf{M}$ is a positive semiring, the weight $w^+\colon B^k \to \mathbf{M}$ is in D.*

Proof:

(i) → (ii): Assume $w\colon B^{k+1} \to \mathbf{M}$ is in D, we will verify $C \rhd w^+$. Let $f\colon B^n \Rightarrow B^m$ be in C, and $(a_i^j)_{i<n}^{j<k}$, $(b_i^j)_{i<m}^{j<k}$ be such that $f(a^j) \approx b^j$. We may assume that f includes an injection $g\colon B^n \to B^m$. Since $f \rhd w$, we have

$$\begin{aligned}\prod_{i<n} w^+(a_i) &= \sum_{u\in B^n}\prod_{i<n} w(a_i,u_i)\\ &\le \sum_{u\in B^n}\prod_{i<m} w(b_i,g(u)_i)\\ &= \sum_{v\in g[B^n]}\prod_{i<m} w(b_i,v_i)\\ &\le \sum_{v\in B^m}\prod_{i<m} w(b_i,v_i)\\ &= \prod_{i<m} w^+(b_i),\end{aligned}$$

using positivity of the semiring.

(ii) → (i): Let $f\colon B^n \Rightarrow B^m$ in C be $\subseteq$-maximal; we need to show that f includes an injection. Using Hall's marriage theorem, it suffices to verify that $|f[X]| \ge |X|$ for every $X \subseteq B^n$.

Let us fix an enumeration $f = \{(a^j, b^j) : j < k\}$. As in the proof of Theorem 5.10, we can find a weight $w\colon B^{k+1} \to \mathbf{M}$ in D such that

$$\prod_{i<n} w(a_i,c_i) \nleq \prod_{i<m} w(b_i,d_i) \tag{18}$$

for all $(c,d) \in (B^n \times B^m) \smallsetminus f$. We consider the monoidal semiring $\mathbb{N}[\mathbf{M}]$, whose elements are formal sums

$$x = \sum_{u\in M} x_u u,$$

where $x_u \in \mathbb{N}$, and $x_u = 0$ for all but finitely many $u \in M$. We define a relation $\le$ on $\mathbb{N}[\mathbf{M}]$ by

$$x \le y \quad \text{iff} \quad \forall U \subseteq M \text{ up-set: } \sum_{u\in U} x_u \le \sum_{u\in U} y_u. \tag{19}$$

We readily see that $\leq$ is a partial order, and $x \leq y$ implies $x + z \leq y + z$. If $x \leq y$, $v \in M$, and $U \subseteq M$ is an up-set, then $U' = \{u : uv \in U\}$ is also an up-set, and we have

$$\sum_{u \in U} (xv)_u = \sum_{u' \in U'} x_{u'} \leq \sum_{u' \in U'} y_{u'} = \sum_{u \in U} (yv)_u,$$

hence $xv \leq yv$. The set $\{z \in \mathbb{N}[\mathbf{M}] : xz \leq yz\}$ thus contains 0, 1, and it is closed under + and right multiplication by elements of M, hence it is all of $\mathbb{N}[\mathbf{M}]$. Symmetrically, one can prove $zx \leq zy$, thus $\mathbb{N}[\mathbf{M}]$ is a positive semiring. The natural inclusion $\mathbf{M} \subseteq \mathbb{N}[\mathbf{M}]$ is a pomonoid embedding, hence we can treat w as a weight $w \colon B^{k+1} \to \mathbb{N}[\mathbf{M}]$.

By assumption, the weight $w^+ \colon B^k \to \mathbb{N}[\mathbf{M}]$ is also in D, in particular

$$\sum_{c \in B^n} \prod_{i<n} w(a_i, c_i) = \prod_{i<n} w^+(a_i) \leq \prod_{i<m} w^+(b_i) = \sum_{d \in B^m} \prod_{i<m} w(b_i, d_i). \tag{20}$$

Let $X \subseteq B^n$, and

$$U = \Big\{ \prod_{i<n} w(a_i, c_i) : c \in X \Big\} \Big\uparrow.$$

Then (18), (19) and (20) give

$$|X| \leq \left| \Big\{ c \in B^n : \prod_{i<n} w(a_i, c_i) \in U \Big\} \right| \leq \left| \Big\{ d \in B^m : \prod_{i<m} w(b_i, d_i) \in U \Big\} \right| = \big| f[X] \big|.$$

Since X was arbitrary, Hall's theorem implies there exists an injection $g \subseteq f$. □

Symmetrically, Theorem 5.15 also has a version with injective surjective partial functions in place of injective (total) functions, and negative semirings in place of positive semirings. More interestingly, we can combine both:

Corollary 5.16 *Assume B is finite, and let $C = \operatorname{Pol}(D)$ and $D = \operatorname{Inv}(C)$. The following are equivalent.*

- *(i) For every $f \colon B^n \rightrightarrows B^m$ in C, there is a bijection $g \colon B^n \to B^m$ such that $f \cup g \in C$ (which implies $n = m$ unless $|B| \leq 1$).*
- *(ii) For every $w \colon B^{k+1} \to \mathbf{M}$ in D where $\mathbf{M}$ is a posemiring, the weight $w^+ \colon B^k \to \mathbf{M}$ is in D.*

Proof:

(i) → (ii): When g is onto, the calculation in the proof of (i) → (ii) of Theorem 5.15 is sound even if the posemiring $\mathbf{M}$ is not positive.

(ii) → (i): We obtain an injective function g by Theorem 5.15. Any coclone D contains the constant-1 weight $\mathrm{c}_1 \colon B \to (\mathbb{N}, 1, \cdot, 0, +, \geq)$, where the target is a (negative) posemiring. Thus by our assumption, D also contains the weight $\mathrm{c}_1^+ \colon B^0 \to \mathbb{N}$ whose single value is $|B|$. Since $f \triangleright \mathrm{c}_1^+$, we obtain $|B|^n \geq |B|^m$, hence any injection $g \colon B^n \to B^m$ is onto. □

Still having reversible operations in mind, we close Section 5.1 by formulating a natural version of our Galois connection for classes of permutations $B^n \to B^n$: we want closed classes of permutations to be groups for each fixed n (in particular, to be closed under inverse), and to always include variable permutations. These are in fact the demands on closed classes of reversible operations imposed by Aaronson, Grier, and Schaeffer [2], except for closure under the ancilla rule, which we will handle in the next section. On the dual side, the constraints on permutation clones allow us to only consider weights in commutative unordered monoids, which simplifies the set-up.

Definition 5.17 A set of permutations $C \subseteq \dot{\bigcup}_{n\in\omega} \mathrm{Sym}(B^n)$ is a *permutation clone* if every $C \cap \mathrm{Sym}(B^n)$ is a closed subgroup of $\mathrm{Sym}(B^n)$ under its natural Hausdorff topology, C is closed under $\times$, and contains all variable permutations.

A *permutation weight* is a weight $w\colon B^k \to \mathbf{M}$, where $\mathbf{M}$ is a commutative monoid, considered as a trivially ordered pomonoid. A class D of permutation weights is a *permutation coclone*, if it satisfies (A)–(D) (with (B) restricted to $\mathbf{M}'$ commutative and trivially ordered), contains the weights $\mathrm{c}_1\colon B^0 \to (\mathbb{N}, 0, +)$ and $\delta\colon B^2 \to (\mathbf{2}, 1, \wedge)$ from Proposition 5.2, and is closed under the following version of condition (ii) of Theorem 5.10: if $w\colon B^{k+1} \to \mathbf{M}$ is in D, where $\mathbf{M}$ is a continuous idempotent commutative semiring, then D also contains $w^+\colon B^k \to \mathbf{M}$. (If B is finite, we may state this condition more generally with arbitrary commutative semirings.)

Theorem 5.18 *The preservation relation induces a Galois connection between sets of permutations, and classes of permutation weights. In this connection, the Galois-closed sets of permutations are exactly the permutation clones. All Galois-closed classes of permutation weights are permutation coclones, and if B is countable, the converse also holds.*

Proof: If D is a class of permutation weights, the set of all permutations in $\mathrm{Pol}(D)$ is a permutation clone by Theorem 4.12 and Proposition 5.2.

Conversely, let C be a permutation clone, and $h \in \mathrm{Sym}(B^n) \smallsetminus C$. Let $\overline{C}$ be the set of pmf $g\colon B^m \Rightarrow B^m$ such that every finite subset of g is contained in some $f \in C$. By Corollary 4.15, $\overline{C} = \mathrm{Pol}(\mathrm{Inv}(C))$. We have $h \notin \overline{C}$, hence there exists a weight $w\colon B^k \to (\mathbf{M}, \leq)$ such that $\overline{C} \rhd w$, and $h \not\rhd w$. We may assume $\leq$ is $=$ by condition (vi) of Proposition 5.2, and that $\mathbf{M}$ is commutative by condition (iii), hence w is in fact a permutation weight.

If C is a permutation clone, the class of permutation weights in $\mathrm{Inv}(C) = \mathrm{Inv}(\overline{C})$ is a permutation coclone by Theorem 4.13, Proposition 5.2, and Theorem 5.10 (and Theorem 5.15 if we use the extended definition for B finite).

On the other hand, let D be a permutation coclone, and $\overline{D} = \mathrm{Inv}(\mathrm{Pol}(D))$. Using Corollary 4.15, $\overline{D}$ consists of weights $w\colon B^k \to (\mathbf{M}, \leq)$ for which there exists a (necessarily commutative) submonoid $\mathrm{im}(w) \subseteq \mathbf{M}' \subseteq \mathbf{M}$ such that $w\colon B^k \to (\mathbf{M}', =)$ is in D; in particular, all permutation weights in $\overline{D}$ are in D. Thus, if $w \notin D$ is a permutation weight, there is $f \in \mathrm{Pol}(D)$ such that $f \not\rhd w$; we may assume f is finite. The description of $\overline{D}$ and Proposition 5.2 implies that $\mathrm{Pol}(D)$ is closed under $\cdot^{-1}$, and that $\overline{D}$ satisfies condition (ii) of Theorem 5.10 (whence also its symmetric version). Thus, if B is countable, we can extend f

to a total surjective $\overline{f} \in \mathrm{Pol}(D)$ by Lemma 5.12. By Proposition 5.2, $\overline{f}$ is also an injective function, hence it is in fact a permutation, and still $\overline{f} \not\triangleright w$. □

5.2 Ancillas and masters

There is another natural closure condition on clones commonly employed in reversible computing that we have not discussed yet: the use of *ancilla inputs*. The idea is that when we want to compute a permutation $B^n \to B^n$, we may, along with the given input elements $x_0, \dots, x_{n-1}$, also work with auxiliary elements (ancillas) $x_n, \dots, x_{n+m-1}$ that are initialized to a fixed string $a \in B^m$, as long as we guarantee to return these extra elements to their original value at the end of the computation.

More formally, the (total) ancilla rule allows to construct a permutation $g\colon B^n \to B^n$ from a permutation $f\colon B^{n+m} \to B^{n+m}$ if there exists $a \in B^m$ such that for all $x \in B^n$,

$$f(x, a) = (g(x), a).$$

The usefulness of this rule in reversible circuit classes stems from the facts that on the one hand, it is considered available for implementation, and on the other hand, it makes construction of circuits much more flexible; in particular, there is no other way of producing a reversible circuit with a smaller number of inputs than what we started with.

While it is suggested in [2] that ancillas are similar to fixing inputs to constants in classical circuit classes, this is only a loose analogy; in our set-up, we can formulate both, and closure under the ancilla rule turns out to behave rather differently from closure under substitution of constants. In fact, we already dealt with the latter: due to closure under composition, a pmf clone is closed under fixing inputs to constants iff it contains all constant functions $B^0 \to B^1$, which is in our duality equivalent to a restriction on unary weights presented in Proposition 5.2 (iv).

The ancilla rule as such is somewhat difficult to fit in our framework. For one thing, the rule is "semantic"[4] in that we need to know that all $x \in B^n$ satisfy a certain property before being allowed to construct the new function. It is also not very clear how the rule should be generalized outside permutations. In order to get started, we characterize below in Theorem 5.20 pmf clones that are closed under its modified form—a *partial* ancilla rule which is always applicable (relying on no semantic promises), at the expense that it may produce partial functions in a way which does not play nice with totality conditions as in Section 5.1.

Definition 5.19 An element z of a pomonoid $(M, 1, \cdot, \leq)$ is *right-order-cancellative* if $xz \leq yz$ implies $x \leq y$ for every $x, y \in M$.

Theorem 5.20 *Let $C = \mathrm{Pol}(D)$ and $D = \mathrm{Inv}(C)$. The following are equivalent.*

(*i*) *For all $f\colon B^{n+1} \Rightarrow B^{m+1}$ in C, and $c \in B$, the pmf $g\colon B^n \Rightarrow B^m$ defined by*

$$g(x) \approx y \quad \textit{iff} \quad f(x, c) \approx (y, c)$$

is in C.

[4] In the sense used in "syntactic vs. semantic complexity classes".

(*ii*) *For every* $w\colon B^k \to \mathbf{M}$ *in* D*, there is* $w'\colon B^k \to \mathbf{M}'$ *in* D*, and a homomorphism* $\varphi\colon \mathbf{M}' \to \mathbf{M}$ *such that* $w = \varphi \circ w'$*, and the diagonal weights* $w'(c,\dots,c)$ *are right-order-cancellative in* $\mathbf{M}'$ *for all* $c \in B$*.*

Proof:

(ii) → (i): Let f and g be as in (i), and $w\colon B^k \to \mathbf{M}$ in D. Let $w'\colon B^k \to \mathbf{M}'$ and φ be as in (ii); in particular, $w'(c^{(k)})$ is right-order-cancellative in $\mathbf{M}'$, where $c^{(k)} = (c,\dots,c) \in B^k$. If $(a_i^j)_{i<n}^{j<k}$, $(b_i^j)_{i<m}^{j<k}$ are such that $g(a^j) \approx b^j$, we have

$$\prod_{i<n} w'(a_i)\cdot w'(c^{(k)}) \le \prod_{i<m} w'(b_i)\cdot w'(c^{(k)})$$

as $f \triangleright w'$, hence

$$\prod_{i<n} w'(a_i) \le \prod_{i<m} w'(b_i)$$

by cancellativity. Since φ is a pomonoid homomorphism and $w = \varphi \circ w'$, this implies

$$\prod_{i<n} w(a_i) \le \prod_{i<m} w(b_i).$$

(i) → (ii): Let D' denote the class of weights $w'\colon B^k \to \mathbf{M}'$ in D such that $w'(c^{(k)})$ is right-order-cancellative in $\mathbf{M}'$ for all $c \in B$. Let $w_k\colon B^k \to \mathbf{M}_k$ be as in the proof of Theorem 4.12. Condition (i) ensures that $w_k \in D'$, and the proof of Theorem 4.12 shows that $C = \mathrm{Pol}(\{w_k : k \in \omega\})$, hence

$$D = \mathrm{Inv}(\mathrm{Pol}(\{w_k : k \in \omega\})) = \mathrm{cl}_M \, \mathrm{cl}_S \, \mathrm{cl}_P \, \mathrm{cl}_{\mathrm{var}}\{w_k : k \in \omega\}$$

by Corollary 4.15. It is easy to see that D' is closed under cl_S, cl_P, and $\mathrm{cl}_{\mathrm{var}}$, hence $D = \mathrm{cl}_M(D')$. □

Reversible gate classes as defined in [2] are permutation clones closed under the *total* ancilla rule. We call them *master clones* below, in accordance with the terminology used in [12], where a rudimentary form of our Galois connection was first presented. We present in Theorem 5.23 a convenient variant of our Galois connection for master clones on a finite base set B. As in Definition 5.17, we will only deal with unordered weights in commutative monoids.

If we take a master clone, and close it under subfunctions to generate a pmf clone in a minimal way, there is no reason to expect the generated clone to be closed under the partial ancilla rule. However, we can get there in a roundabout way: given a master clone C, we close it under the partial ancilla rule (and subfunctions); we obtain a pmf clone that is closed under the partial ancilla rule by definition, and crucially, that does not contain any new total functions outside C—this is precisely what the closure of C under the *total* ancilla rule tells us. (However, the pmf clone we get in this way does not have the property of extendability to total functions as in Theorem 5.10 or Theorem 5.15, even though it was "generated" from a set of total functions!)

Thus, we will be able to describe master clones by weights satisfying a property that actually corresponds to the partial ancilla rule as in Theorem 5.20. In the context of unordered commutative monoids, right order-cancellativity is equivalent to plain cancellativity. We will in fact impose a stronger requirement, namely that the monoid elements in question have an inverse; this makes the condition somewhat simpler, and as a technical advantage, stable under homomorphisms. We rely here on the basic fact that cancellative elements of a commutative monoid can be made invertible in a (commutative) extension of the monoid by a variant of the Grothendieck group construction:

Lemma 5.21 *If* $\mathbf{M}$ *is a commutative monoid, and* $U \subseteq \mathbf{M}$ *a set of cancellative elements, there exists a commutative monoid* $\mathbf{N} \supseteq \mathbf{M}$ *such that every* $u \in U$ *has an inverse in* $\mathbf{N}$.

Proof: Let $\mathbf{M}_U$ be the submonoid of $\mathbf{M}$ generated by U. Since the elements of $\mathbf{M}_U$ are cancellative, the relation

$$(x, u) \sim (y, v) \quad \text{iff} \quad xv = yu$$

on $\mathbf{M} \times \mathbf{M}_U$ is easily seen to be a congruence, thus we can form the quotient $\mathbf{N} = (\mathbf{M} \times \mathbf{M}_U)/{\sim}$. The monoid $\mathbf{M}$ embeds in $\mathbf{N}$ via $x \mapsto (x, 1)/{\sim}$, and for $u \in \mathbf{M}_U$, $(u, 1)/{\sim}$ has an inverse $(1, u)/{\sim}$. □

Because of the complicated interference of the ancilla rules with totality conditions, we are not able to precisely describe the closed classes of weights in the Galois connection for master clones; we only know some necessary conditions.

Definition 5.22 Assume that B is finite. A permutation clone C is a *master clone* if it is closed under the total ancilla rule: if $f \in C \cap \mathrm{Sym}(B^{n+m})$, $a \in B^m$, and $g \in \mathrm{Sym}(B^n)$ are such that $f(x, a) = (g(x), a)$ for all $x \in B^n$, then $g \in C$.

A permutation weight $w\colon B^k \to \mathbf{M}$ is a *master weight* if the diagonal weights $w(x^{(k)})$ are invertible in $\mathbf{M}$ for all $x \in B$. A *master proto-coclone* is a class of master weights that contains $\mathrm{c}_1\colon B^0 \to (\mathbb{Z}, 0, +)$, $\delta\colon B^2 \to (\mathbf{2}, 1, \wedge)$, and is closed under conditions (A)–(D) relative to the class of all master weights.

Theorem 5.23 *If* B *is finite, the preservation relation induces a Galois connection between sets of permutations and classes of master weights such that Galois-closed sets of permutations are exactly the master clones. Galois-closed classes of master weights are master proto-coclones.*

Proof: The set of permutations preserving a class of master weights is a permutation clone by Theorem 5.18, and it satisfies the ancilla rule by the argument in the proof of Theorem 5.20. Likewise, the class of master weights preserving a set of permutations is a master proto-coclone, being the intersection of a permutation coclone with the class of all master weights.

Let C be a master clone, and h a permutation not in C. Let $\overline{C}$ be the set of pmf $g\colon B^n \Rightarrow B^n$ such that there are $m \in \omega$, $a \in B^m$, and $f \in C \cap \mathrm{Sym}(B^{n+m})$ such that $f(x, a) = (y, a)$ whenever $g(x) \approx y$. We have $h \notin \overline{C}$. We can check easily that $\overline{C}$ is a pmf clone closed under $\cdot^{-1}$, hence there is a permutation weight $w\colon B^k \to \mathbf{M}$ in $\mathrm{Inv}(\overline{C})$ such that $h \not\triangleright w$ as in the proof of Theorem 5.18. Moreover, $\overline{C}$ satisfies condition (i) of Theorem 5.20, hence we can assume that $w(x^{(k)}) \in M$ is cancellative for every $x \in B$. By Lemma 5.21, we can embed $\mathbf{M}$ in a commutative monoid $\mathbf{N}$ where every $w(x^{(k)})$ is invertible, thus $w\colon B^k \to \mathbf{N}$ is a master weight. $\square$

Remark 5.24 It is not clear what other properties do Galois-closed classes of master weights satisfy. Extending the argument in the proof of Theorem 5.23, we can show that the following are equivalent for a master proto-coclone D:

(i) D is Galois-closed in the connection from Theorem 5.23.

(ii) All master weights in the least permutation coclone containing D are already in D.

(iii) For every pmf $g\colon B^n \Rightarrow B^n$ such that $g \triangleright D$, there are $m \in \omega$, $f \in \mathrm{Sym}(B^{n+m})$, and $a \in B^m$ such that $f \triangleright D$, and $f(x,a) = (y,a)$ whenever $g(x) \approx y$.

Unfortunately, these conditions are fairly opaque. We can at least infer additional necessary closure conditions on D from (ii), in particular the following: if $w\colon B^{k+l} \to \mathbf{M}$ is in D, where $\mathbf{M}$ is a semiring, let $w^{+l}\colon B^k \to \mathbf{M}$ be the permutation weight defined by

$$w^{+l}(x) = \sum_{y \in B^l} w(x,y)$$

(i.e., the w^+ construction l times iterated), let

$$u \sim v \quad \text{iff} \quad \exists n \in \omega\, \exists x \in B^n\; u \prod_{i<n} w^{+l}(x_i^{(k)}) = v \prod_{i<n} w^{+l}(x_i^{(k)})$$

be the least congruence on $\mathbf{M}$ that makes the diagonal w^{+l}-weights cancellative, and let $\mathbf{N} \supseteq \mathbf{M}/{\sim}$ be the Grothendieck monoid from Lemma 5.21 where they are made invertible. Then $w^{+l}\colon B^k \to \mathbf{N}$ is in D.

However, we see no evidence to suggest that this condition is sufficient.

Problem 5.25 *Describe Galois-closed classes of master weights by means of transparent closure conditions.*

6 Subdirectly irreducible weights

Coclones with weights in arbitrary pomonoids, as we discussed so far, are convenient for the abstract theory because of their rich closure properties, but not so much for applications, as such invariants are absurdly large: any nontrivial coclone is a proper class that includes pomonoids of arbitrary cardinality, most of which are clearly redundant. In contrast, the classical clone–coclone duality only involves finitary relations on the base set B, which are small finite objects for finite B.

In light of this, we would like to identify a smaller class of weights that suffice to characterize every clone. The price we are willing to pay is that we resign on the idea of coclones having sensible closure conditions: in particular, we drop closure under products, and in the process we will also lose closure properties such as in Section 5.1. In fact, we will in a sense make closure conditions work backwards, to decompose any weight into small pieces that generate it.

Recall from Remark 4.10 that any weight $w\colon B^k \to \mathbf{M}$ can be identified with an expansion $(\mathbf{M}, w)$ of the pomonoid $\mathbf{M}$ by extra constants describing the values of w. If D is a coclone, this makes $D \cap \mathrm{Wgt}_k$ into a povariety. Furthermore, we only care about the validity of variable-free inequalities in its inequational theory. This suggests two ways to obtain a small generating set in a coclone:

- We can restrict attention to weights $w\colon B^k \to \mathbf{M}$ such that $\mathbf{M}$ is generated by $\mathrm{im}(w)$ as a monoid (that is, $(\mathbf{M}, w)$ is 0-generated). In particular, if B is finite, this makes $\mathbf{M}$ finitely generated.
- As in any povariety, $(\mathbf{M}, w)$ can be written as a subdirect product of subdirectly irreducible poalgebras; thus, we can restrict attention to weights with the pomonoid $\mathbf{M}$ subdirectly irreducible (subdirect irreducibility is unaffected by expansions by constants).

Let us state the result explicitly for the record.

Proposition 6.1 *Every pmf clone C can be written in the form $C = \mathrm{Pol}(D)$, where D is a set of weights $w\colon B^k \to \mathbf{M}$ such that the pomonoid $\mathbf{M}$ is subdirectly irreducible, and generated by $\mathrm{im}(w)$.* □

The same principle also applies to variants of the Galois connection with restricted classes of weights, as discussed in Section 5. Most cases of interest can be handled by the following generalization of Proposition 6.1:

Proposition 6.2 *Let Q be a poquasivariety of pomonoids, and $P \subseteq \mathrm{Pmf}$. Consider the Galois connection induced by the preservation relation between pmf $f \in P$, and weights $w\colon B^k \to \mathbf{M}$ with $\mathbf{M} \in Q$. Then every Galois-closed set of pmf is of the form $P \cap \mathrm{Pol}(D)$, where D is a set of weights as above with $\mathbf{M}$ subdirectly irreducible relative to Q, and generated by $\mathrm{im}(w)$.*

Even more generally, we can use possibly different quasivarieties Q_k for each $k \in \omega$. □

The various restrictions on weights mentioned in 5.1–5.7, as well as permutation weights from Definition 5.17, can be defined using quasi-inequalities, hence they are in the scope of Proposition 6.2. (Allowing Q_k to depend on k is useful e.g. if we want to disable nullary weights as in Corollary 5.6.) Notice that we have already implicitly used a form of Proposition 6.2 in Remark 5.8.

The one remaining exception is the class of master weights from Definition 5.22: these do not form a quasivariety, as the invertibility of the diagonal weights $w(x, \dots, x)$ needs an existential quantifier to state. We can adapt our approach to this case anyway: we can assume that $\mathbf{M}$ is generated by $\mathrm{im}(w)$ together with inverses of the diagonal weights, which again makes it finitely generated if B is finite; and we can restrict attention to $\mathbf{M}$ subdirectly irreducible (in the ordinary algebraic sense).

These considerations are particularly useful for classes of weights whose finitely generated subdirectly irreducible pomonoids are finite, in which case we can characterize all clones by finite invariants if B is finite. In particular, this happens for *permutation weights*, which can describe all permutation clones, and more generally, all pmf clones containing variable permutations and being closed under inverses.

The fact that finitely generated subdirectly irreducible commutative monoids (or semigroups) are finite was proved by Mal'cev [16], and their structure has been investigated by Schein [24] and Grillet [9]. For completeness, we include a simplified description below.

Definition 6.3 A *nilsemigroup* is a semigroup $(N, \cdot)$ with an absorbing element 0 (i.e., $0x = x0 = 0$ for all $x \in N$) such that for every $x \in N$, there is $n \in \mathbb{N}_{>0}$ such that $x^n = 0$.

Let $(G, 1, \cdot)$ be an abelian group, $(\Omega, \cdot, 0)$ a commutative nilsemigroup, and Ω^1 the monoid $\Omega \cup \{1\}$. A *factor set* on Ω with values in G is $\sigma = \{\sigma_{\alpha,\beta} : \alpha, \beta \in \Omega^1, \alpha\beta \neq 0\} \subseteq G$ satisfying

$$\begin{aligned}\sigma_{\alpha,\beta} &= \sigma_{\beta,\alpha},\\ \sigma_{\alpha,1} &= 1,\\ \sigma_{\alpha,\beta}\,\sigma_{\alpha\beta,\gamma} &= \sigma_{\alpha,\beta\gamma}\,\sigma_{\beta,\gamma}\end{aligned}$$

for all $\alpha, \beta, \gamma \in \Omega^1$ such that $\alpha\beta\gamma \neq 0$. We define a commutative monoid $[\Omega, G, \sigma]$ whose underlying set is

$$\{0\} \cup \{(g, \alpha) : g \in G, \alpha \in \Omega^1, \alpha \neq 0\},$$

with unit $(1, 1)$, absorbing element 0, and multiplication of nonzero elements defined by

$$(g, \alpha)(h, \beta) = \begin{cases} 0 & \alpha\beta = 0,\\ (gh\sigma_{\alpha,\beta}, \alpha\beta) & \text{otherwise.}\end{cases}$$

Note that $[\Omega, G, \sigma]$ is a disjoint union of a copy of G, and a nilsemigroup N which is an ideal of $[\Omega, G, \sigma]$, such that the semigroup of orbits $N/{\equiv}$ is isomorphic to Ω, where $u \equiv v$ iff $u = gv$ for some $g \in G$. In particular, Ω and G are determined by $[\Omega, G, \sigma]$ up to isomorphism. The factor set σ, however, is not: $[\Omega, G, \sigma] \simeq [\Omega, G, \sigma']$ if

$$\sigma'_{\alpha,\beta} = \sigma_{\alpha,\beta} u_\alpha u_\beta u_{\alpha\beta}^{-1}$$

for some $\{u_\alpha : \alpha \in \Omega \smallsetminus \{0\}\} \subseteq G$ with $u_1 = 1$.

Ω carries a canonical partial order, defined by $x \leq y$ iff $x = uy$ for some $u \in \Omega^1$. Assume that Ω has a unique minimal element μ. We say that N is *weakly irreducible* when the following condition holds for all $\alpha, \beta \in \Omega$ (or Ω^1): if

$$\{\tau \in \Omega : \tau\alpha = \mu\} = \{\tau \in \Omega : \tau\beta = \mu\},$$

and the mapping $\tau \mapsto \sigma_{\alpha,\tau}\sigma_{\beta,\tau}^{-1}$ is constant on $\{\tau \in \Omega : \tau\alpha = \mu\}$, then $\alpha = \beta$.

Theorem 6.4 (Grillet [9]) *Let G be a abelian group, Ω a finite commutative nilsemigroup, and σ a factor set on Ω with values in G such that:*

(i) G is trivial, or a cyclic group C_{p^k} of prime power order.

(ii) Ω is trivial, or it has a unique minimal element μ, and N is weakly irreducible.

Then $[\Omega, G, \sigma]$ is a finite subdirectly irreducible commutative monoid.

Conversely, every finite (= finitely generated) subdirectly irreducible commutative monoid is isomorphic to some $[\Omega, G, \sigma]$ as above, or to C_{p^k} (which equals $[0, C_{p^k}, 1]$ minus its zero element).

An example of a nilsemigroup with a unique minimal element is $(\{1, \ldots, d\}, \min\{d, x + y\})$ for $d > 1$: here d is a zero element, and $\mu = d - 1$.

7 Conclusion

We have demonstrated that the usual notion of clones of multiple-input single-output functions has a natural generalization to multiple-output (partial multi-valued) functions. The clone–coclone Galois connection admits a parallel generalization: multiple-output clones are determined by preservation of invariants in the shape of weighted products in partially ordered monoids. Closed classes of invariants, generalizing the usual coclones, are likewise characterized by suitable closure conditions resembling properties of varieties, and admit a form of decomposition into subdirectly irreducible invariants.

We have also seen that the Galois connection is flexible enough to accommodate various natural modifications of the set-up: for example, if we desire clones to be always closed under variable permutations, it suffices to switch to commutative monoids; constraining clones to partial uni-valued functions corresponds to inclusion of a specific weight as an invariant; and closure of clones under inverse can be obtained by using unordered monoids. Most importantly, we can adapt the Galois connection to classes of total functions (multi-valued or uni-valued), in which case coclones get closed under sums in certain semirings, generalizing the closure under existential quantification from the classical case. By suitable restrictions on weights, we can also take care of the ancilla rule as employed in reversible computing, although we could not exactly determine the corresponding closure conditions on the coclone side.

This work opens up the possibility to study multiple-output clones with tools of universal algebra, generalizing the standard framework of clones to a set-up where domains and codomains of operations receive a fully symmetrical treatment.

References

[1] Scott Aaronson, *Classifying reversible gates*, Theoretical Computer Science Stack Exchange, 2014, `http://cstheory.stackexchange.com/q/25730`.

[2] Scott Aaronson, Daniel Grier, and Luke Schaeffer, *The classification of reversible bit operations*, arXiv:1504.05155 [quant-ph], 2015, `http://arxiv.org/abs/1504.05155`.

[3] Stephen L. Bloom, *Varieties of ordered algebras*, Journal of Computer and System Sciences 13 (1976), no. 2, pp. 200–212.

[4] V. G. Bodnarchuk, L. A. Kaluzhnin, V. N. Kotov, and B. A. Romov, *Galois theory for Post algebras. I*, Cybernetics 5 (1969), no. 3, pp. 243–252, translated from: Kibernetika 5 (1969), no. 3, pp. 1–10.

[5] ———, *Galois theory for Post algebras. II*, Cybernetics 5 (1969), no. 5, pp. 531–539, translated from: Kibernetika 5 (1969), no. 5, pp. 1–9.

[6] Stanley N. Burris and Hanamantagouda P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics vol. 78, Springer, 1981.

[7] Miguel Couceiro, *Galois connections for generalized functions and relational constraints*, in: Contributions to General Algebra (Chajda, Dorfer, Eigenthaler, Halaš, Müller, and Pöschel, eds.), vol. 16, Verlag Johannes Heyn, Klagenfurt, 2005, pp. 35–54.

[8] David Geiger, *Closed systems of functions and predicates*, Pacific Journal of Mathematics 27 (1968), no. 1, pp. 95–100.

[9] Pierre Antoine Grillet, *On subdirectly irreducible commutative semigroups*, Pacific Journal of Mathematics 69 (1977), no. 1, pp. 55–71.

[10] A. A. Iskander, *Subalgebra systems of powers of partial universal algebras*, Pacific Journal of Mathematics 38 (1971), no. 2, pp. 457–463.

[11] Gregg Jaeger, *Quantum information: An overview*, Springer, New York, 2007.

[12] Emil Jeřábek, *Answer to [1]*, Theoretical Computer Science Stack Exchange, 2014, `http://cstheory.stackexchange.com/a/25791`.

[13] Sebastian Kerkhoff, *A general Galois theory for operations and relations in arbitrary categories*, Algebra Universalis 68 (2012), no. 3–4, pp. 325–352.

[14] Marc Krasner, *Généralisation abstraite de la théorie de Galois*, in: Algèbre et théorie des nombres, Paris 25. 9.–1. 10. 1949, Colloques Internationaux du Centre National de la Recherche Scientifique vol. 24, 1950, pp. 163–168.

[15] ———, *Abstract Galois theory and endotheory. I*, Acta Scientiarum Mathematicarum 50 (1986), pp. 253–286.

[16] Anatolij I. Mal'cev, *On homomorphisms onto finite groups*, Uchen. Zap. Ivanov. Gos. Ped. Inst. 18 (1958), pp. 49–60 (in Russian).

[17] ———, *Algebraic systems*, Die Grundlehren der mathematischen Wissenschaften vol. 192, Springer, 1973, translated from Russian by B. D. Seckler and A. P. Doohovskoy.

[18] Kalyan S. Perumalla, *Introduction to reversible computing*, Computational Science Series, Chapman and Hall/CRC, 2013.

[19] Don Pigozzi, *Partially ordered varieties and quasivarieties*, Lecture notes, `http://orion.math.iastate.edu/dpigozzi`, 2004.

[20] Reinhard Pöschel, *A general Galois theory for operations and relations and concrete characterization of related algebraic structures*, Technical Report R-01/80, Akademie der Wissenschaften der DDR, Zentralinstitut für Mathematik und Mechanik, Berlin, 1980.

[21] Emil L. Post, *The two-valued iterative systems of mathematical logic*, Annals of Mathematics Studies no. 5, Princeton University Press, Princeton, 1941.

[22] Ivo G. Rosenberg, *A classification of universal algebras by infinitary relations*, Algebra Universalis 1 (1971), no. 1, pp. 350–354.

[23] ———, *Galois theory for partial algebras*, in: Universal Algebra and Lattice Theory (R. S. Freese and O. C. Garcia, eds.), Lecture Notes in Mathematics vol. 1004, Springer, 1983, pp. 257–272.

[24] Boris M. Schein, *Homomorphisms and subdirect decompositions of semigroups*, Pacific Journal of Mathematics 17 (1966), no. 3, pp. 529–547.