Completeness in coalgebras

B. ČSÁKÁNY*

To Professor Károly Tandori on his sixtieth birthday

1. Preliminaries. For a set $A$ and $n$ positive integer, denote by $A^{(n)}$ the $n$th copower (i.e., the union of $n$ disjoint copies) of $A$. Dualizing the notion of an $n$-ary operation we obtain that of an $n$-ary co-operation on $A$: this is a mapping $f: A \rightarrow A^{(n)}$. The corresponding notion may be introduced in any well-copowered category, cf. [4], [6], [10]. For $A$ non-empty and $F$ a set of co-operations on $A$, the pair $(A; F)$ is called a coalgebra. Coalgebras were considered by Drbohlav [2]; he introduced the common algebraic notions and proved the Birkhoff variety theorem for them. Here we shall study completeness of sets of co-operations on finite sets.

Let $n$ stand for $\{0, \ldots, n-1\}$. One can introduce $A^{(n)}$ as $n \times A$, and so each co-operation $f: A \rightarrow A^{(n)}$ is uniquely determined by a pair of mappings $(f_0, f_1)$ where $f_0: A \rightarrow n$ and $f_1: A \rightarrow A$. We call $f_0$ and $f_1$ the labelling and the mapping of $f$, respectively. We can imagine co-operations — as well as other mappings — by means of graphs, e.g., Fig. 1 displays the ternary co-operation on $3$ having the cycle $(012)$ as labelling and the transposition $(01)$ as mapping.

The $n$-ary coprojections may be defined by dualizing the notion of the $n$-ary projection. We write $p_i^f$ for the $i$th $n$-ary coprojection $(i=0, \ldots, n-1)$; then $p_i^0(a) = i$ and $p_i^1(a) = a$ for each $a \in A$.

The superposition $f(g_0, \ldots, g_{n-1})$ of an operation $f: A^n \rightarrow A$ and $n$ operations $g_i: A \rightarrow A^n$ may be considered as follows. There exists a (unique) $g: A^n \rightarrow A$ such that $g_i = g_i^ek_i$ for each $i \in n$. Then $f(g_0, \ldots, g_{n-1}) = g$. Dually, for arbitrary co-operations $f: A \rightarrow A^{(n)}$, $g^{(0)}: A^n \rightarrow A^{(n)}$ and $g^{(0)}: A \rightarrow A^{(n)}$ (where $a = 0, \ldots, n-1$) there exists a (unique) mapping $g: A^{(n)} \rightarrow A^{(n)}$ such that $g^{(0)} = p_a^0 g$. The co-operation $fg: A \rightarrow A^{(n)}$ is called the superposition of $f$ and $g^{(0)}$; we denote it by $f(g_0, \ldots, g^{(n-1)})$.

Fig. 2 and 3 display $f(g_0, g^{(0)}, g^{(2)})$ with $f, g^{(0)}, g^{(2)}$ the co-operation on Fig. 1, and $g^{(2)} = p_a^4$. For the labelling and mapping of a superposition $s = f(g_0, \ldots, g^{(n-1)})$
we have
\begin{align}
\psi(a) &= g(f_s(a), f_t(a)), \\
\phi(a) &= g(f_s(a), f_t(a)).
\end{align}

Fig. 1

Fig. 2

Fig. 3

Analogously to the case of operations, a set of co-operations on a set \( A \) is called \textit{a clone} if it is closed under superpositions and contains all coprojections. A clone of co-operations is also an abstract clone, i.e., it is a heterogeneous clone in the sense of Taylor [13]. Indeed, it satisfies the identities (2.8.1)–(2.8.3) in the definition of heterogeneous clone in [13]; they may be written in the form
\begin{align}
f(g^0(h^{(0)}), \ldots, h^{(k^{(0)})}), g^{(n^{(0)})}(h^{(0)}, \ldots, h^{(k^{(0)})})) &= \\
&= f(g(h^{(0)}, \ldots, h^{(n^{(0)})}))(h^{(0)}, \ldots, h^{(k^{(0)})})
\end{align}
for arbitrary \( f, g^0, h^{(0)} \) of appropriate arities;
\begin{align}f(p^{n}, \ldots, p^{(n^{(0)})}) &= f
\end{align}
for \( f \)-ary; and
\begin{align}p^{(k^{(0)})}(f^{(0)}, \ldots, f^{(n^{(0)})}) &= f^{(0)}
\end{align}
for \( f^{(0)}, \ldots, f^{(n^{(0)})} \) of the same arity. Denote, e.g., the left and right side of (2.1) by \( p \) and \( q \), and let \( f \) and \( g \) stand for \( g^0(h^{(0)}, \ldots, h^{(n^{(0)})}) \) and \( g^0(h^{(0)}, \ldots, h^{(k^{(0)})}) \), respectively. Then, for every \( a \in A \), the equations (1) give
\begin{align}p_0(a) &= g_0(f_s(a), f_t(a)) = h_0^0(f_s(a), f_t(a)) = \\
&= h_0^0(f_t(a)) = g_0(a),
\end{align}
and similarly we obtain \( p_1(a) = g_1(a) \). One can verify also (2.2) and (2.3).

We shall denote the clone of all co-operations on \( A \) by \( \mathcal{C}_A \), and the set of all \( n \)-ary co-operations of \( A \) by \( \mathcal{C}^n_A \).

An \( n \)-ary operation \( f \) on \( A \) depends on its \( i \)-th variable iff there is an \( n \)-ary \( g \) on \( A \) such that \( f(e_i^1, \ldots, e_i^{n_i}, \ldots, e_i^{n_i}) \neq f \). Accordingly, an \( f \in \mathcal{C}^n_A \) depends on its \( i \)-th variable if there exists a \( g \in \mathcal{C}_A \) with \( f(p^{i}, \ldots, p^{i^{(0)}}, \ldots, p^{i^{(0)}}, \ldots, p^{i^{(n^{(0)})}}) \neq f \). It is easy to verify that \( f \) depends on its \( i \)-th variable if \( f^{i+}(i) \) is not void. We say that \( f \in \mathcal{C}^n_A \) is essentially \( k \)-ary if there exist exactly \( k \) elements \( a \in A \) such that \( f \) depends on its \( i \)-th variable, i.e., \( f \) has \( k \)-element range.

2. Complete sets of co-operations. We shall study co-operations on finite sets \( A \) \( (n=1) \). For \( C \subseteq \mathcal{C}_A \), the least clone in \( \mathcal{C}_A \) containing \( C \) will be denoted by \( \left[ C \right] \) and called the \textit{clone generated by} \( C \). If \( \left[ C \right] = \mathcal{C}_A \) (i.e., every co-operation on \( n \) may be obtained from those in \( C \) and co-operations using superposition) then \( C \) is said to be \textit{complete}. In this case we call also the co-algebra \( (n; C) \) \textit{primai}.

We shall need terms and notations for special co-operations. The \textit{diagonal co-operation} \( d \) on \( n \)-ary with \( a_0, a_1 \) identical. The \( n \)-ary \( (i, j) \)-constant co-operation \( f^{i,j} \) is determined by \( f^{i,j}(k)=f \) for each \( i, j \in n \) and for each \( k \in n \). An \( (i, j) \)-translation is a co-operation \( t \) with \( t_i(i)=j \). If \( a \) is \( m \)-ary then \( f^{i,b_1, \ldots, b_m} \) is an \( n \)-ary \( (i, j) \)-translation (which is essentially \( f_{(r_0, \ldots, r_{m-1})}^{i,j} \)). Similarly, from an \( (i, j) \)-translation we can get an \( (i, j) \)-constant of arbitrary arity. We call a co-operation \( g \) \( (i, j) \)-gluing if \( g_k(i)=g_k(j) \) for all \( k \); \( g \) is \textit{gluing} if it is \( (i, j) \)-gluing for some \( i, j \in n \). Thus, \( g \) is not gluing iff the mapping \( h \mapsto (g_0(h), g_1(h)) \) is \( 1 \rightarrow 1 \) on \( n \).

The following observations are trivial:

\textbf{Proposition 0.} An essentially \( k \)-ary co-operation is a superposition of a \( k \)-ary co-operation and some coprojections. If a co-operation on \( n \) is essentially \( k \)-ary then \( k \in n \).

This implies

\textbf{Proposition 1.} The set of all at most \( n \)-ary co-operations on \( n \) is complete.

Thus, studying completeness on \( n \), we can restrict ourselves to co-operations with arity \( \leq n \).

The mappings of a set \( C \) of co-operations on \( n \) generate a semigroup \( \mathcal{S}(C) \) of self-mappings of \( n \), called the \textit{semigroup of} \( C \). We call \( C \) \textit{transitive} if \( \mathcal{S}(C) \) is transitive. Note that each self-mapping in \( \mathcal{S}(C) \) is the mapping of some (unary) co-operation on \( \left[ C \right] \), i.e., \( \mathcal{S}(C) \subseteq \mathcal{S}(\left[ C \right]) \). Indeed, for co-operations \( f \) and \( g \) of arbitrary arities, let \( h=\mathcal{S}(C)(g(p^{0}, \ldots, p^{n}), \ldots, g(p^{0}, \ldots, p^{n})) \). Then for each \( i \in n \), \( h_i(i)=g_i(f_i(i)) \), proving that \( \mathcal{S}(C) \) is closed under products of mappings, whence the assertion follows.
Proposition 2. A transitive set of co-operations on \( n \) is complete provided it contains an essentially \( n \)-ary co-operation.

Proof. By Proposition 1, we have to prove that, for a set of co-operations \( C \) satisfying the conditions of Proposition 2, every at most \( n \)-ary co-operation \( g \) on \( n \) is a composition of some co-operations in \( C \). Let \( f \in C \) be essentially \( n \)-ary. Then the labelling of \( f \) is onto, hence it is a permutation of \( n \). Form \( f(p_1, p_2, \ldots, p_n) = f^* \); then, for each \( i \in n \), we have \( f^*(i) = p_i \). Let \( f \) be essentially \( n \)-ary, i.e., the arity and labelling of \( f \) are the same as those of \( g \), while its mapping is the mapping of \( g \) for each \( i \in n \), \( f^*(i) = p_i \). Let \( f \) be cyclic, since \( f \) is transitive; hence \( f \) is not gluung.

Now we show that, for each pair \( i, j \) of different elements from \( n \), there exists a non-negative integer \( k \) such that \( f(k(i)) = f(j) \). Write \( \theta(i) \) for \( i \), and \( \theta \) for \( j \). Suppose that \( f(k(i)) = f(j) \) for every integer \( k \), contrary to the claim; in particular, \( f(0(i)) = f(j) \). As \( f \) is cyclic, there is a least natural number \( t = n \) such that \( f(t(i)) = f(j) \), and \( f(t(i)) = f(j) \) for every non-negative integer \( r \). If \( t = 1 \), then \( f(i) = f(j) \), \( f \) is constant, a contradiction, because \( f \) is at least binary. Hence \( 1 < t \). Now we see that \( f(t(i)) = f(j) \) whenever \( t = n \); this is a refinement of the equivalence induced by \( f \). Also, clearly, is preserved by \( f \). Since \( f \) preserves the (non-trivial) partition of this equivalence, a contradiction again.

Given an integer \( k \), there exists a unary co-operation \( h \) in \( f \) such that, for each \( i \in n \), \( h(i) = f(i) \). Hence for the \( n \)-ary co-operation \( k \)-ary \( h(f) \) we have \( k(i) = f(i) \). Now, if \( 2k < n \), for every non-gluung essentially \( k \)-ary co-operation \( c \) in \( f \) we construct a non-gluung essentially at least \( (k+1) \)-ary co-operation \( c' \) as follows.

Since \( k < n \), and \( c \) is not gluung, there exist \( i, j \in n \) such that \( c(i) = c(j) \), and \( c(i) \neq c(j) \). Let \( c \) be (formally) \( i \)-ary. Put

\[
c' = c(p^{+1}, 0, ..., p^{+1} \cdot 0, 0, ..., p^{+1}, 0, ..., p^{+1}, 0, 0, ..., p^{+1}, 0, 0, ..., p^{+1}, 0).
\]

Assume that \( c \) depends on its \( q \) variable. Then there is a \( r \in x \) such that \( c(i) = q \). If \( q \neq c(i) \) then \( c(i) = p^{(q+1)}(c(i)) = q \), and if \( q = c(i) \) then \( c(i) = p^{(q+1)}(c(i)) = p^{(q+1)}(c(i)) = p^{(q+1)}(c(i)) = p^{(q+1)}(c(i)) = q \). I.e., \( c' \) also depends on its \( q \)-ary variable. In addition, \( c' \) depends on its \( l \) variable, too: \( c_i(j) = p^{(q+1)}(c_i(j)) = q \).

Completeness in coalgebras
We have shown that \( c' \) is essentially at least \((k+1)\)-ary. It remains to show that \( c' \) is not gluing. Observe that, for \( a \in \mathfrak{n} \), \( c'_0(a) = 1 \) if \( a = 1 \) and \( c_0(a) = c_1(a) \), while \( c'_0(a) = c'_1(a) \) otherwise; further \( c'_2(a) = c'_2(0, c_1(a)) \) if \( c_1(a) = c_0(1) \), and \( c'_2(a) = c'_1(a) \) otherwise. Since \( s^{0,1}_n \) is a permutation of \( \mathfrak{n} \), we obtain that, for \( a, b \in \mathfrak{n} \), \( c'_0(a) = c'_0(b) \), \( c'_1(a) = c'_1(b) \) whenever \( c_1(a) = c_1(b) \). This means that \( c' \) is \((a, b, gluing)\)-gluing only if \( c \) is \((a, b, gluing)\). Thus, \( c' \) is not gluing, as required.

Using this construction, from \( f \) we get an essentially \( n \)-ary co-operation in \( f \) in a finite number of steps, proving the sufficiency.

Necessity. We have to show that if a co-operation \( f \) preserves a non-trivial partition \( \pi \) of \( \mathfrak{n} \) then every co-operation in \( [f] \) also preserves \( \pi \), and the same holds for non-empty subsets instead of non-trivial partitions. As the coprojections preserve everything, it is enough to show that any composition \( f(g^0, \ldots, g^{k-1}) \) preserves the partition \( \pi \) provided \( f, g^0, \ldots, g^{k-1} \) preserve it.

Let \( h = f(g^0, \ldots, g^{k-1}) \), and let \( a \equiv b(\pi) \). Then \( h(a) = g^k(f(a)) = f_1(a)(b) = g^k(h(b)) \). Here \( f_1(a) = f_1(b) \) for \( a \equiv b(\pi) \) and \( f_2(a) = f_2(b) \), hence \( g^k(f_1(a)) = g^k(f_1(b)) \), as needed. Also we have \( h_1(a) = h_1(b) \), again by \( (1) \) and the definition of preservation. The case of subsets is equally simple. Thus, Proposition 3 is proved.

Consider the case when \( n \) is a prime number. Then the non-preserving of non-empty proper subsets by \( f \) means that \( f_1 \) is a prime-order cycle, hence it preserves no non-trivial partition with more than one block. Thus we have to exclude the preservation of the one-block partition only. This can be done by requiring that \( f \) is essentially at least binary. Hence it follows:

**Corollary 3.** Let \( n \) be a prime number. A co-operation \( f \) on \( n \) is Sheffer if and only if it is essentially at least binary and \( f_1 \) is a cyclic permutation of \( n \).

Introducing some natural algebraic notions for coalgebras, we can give a more formal version of Proposition 3. Let \( A = (A; F) \) be a coalgebra. If the subset \( B \) of \( A \) is preserved by \( F \), we can obtain a subcoalgebra \( B = (B; F') \) of \( A \) by putting \( F' = \{ f' : f \in F \} \) where \( f' \) is the restriction of \( f \) to \( B \). A subcoalgebra \( B \) of \( A \) is proper if \( B \) is a proper subset of \( A \).

Furthermore, if the partition \( \pi \) of \( A \) is preserved by \( F \), we can obtain a coalgebra \( \overline{A} = (\overline{A}; F) \), where \( \overline{A} = \{ a \in A : a \in \pi \} \) is the set of blocks of \( \pi \), while \( F = \{ f : f \in F \} \) and \( f \) is defined by \( f_0(a) = f_0(b) \), \( f_1(a) = f_1(b) \) for each \( a \in \pi \). Coalgebras \( \overline{A} \) arising in such a way are called factorcoalgebras of \( (A; F) \); \( \overline{A} \) is a proper if it is induced by a partition with at least one non-trivial block. As is usual for algebras, a coalgebra \( B \) which may be obtained from another coalgebra \( A \) by forming a subcoalgebra of a factorcoalgebra is called a factor of \( A \). A factor of \( A \) is proper if in the process of its formation we take a proper sub- or factoralgebra. Using just the introduced notions, Proposition 3 states:

**Proposition 3.** A finite coalgebra with one co-operation is primal if and only if it has no proper factors.

This is the coalgebraic version of Rousseau's theorem (a finite algebra with one operation is primal if it has no proper factors and is rigid [8], [7]).

The following proposition corresponds to Shupeck's completeness criterion for operations [12], [7]. Call a co-operation essential if it is essentially at least binary and non-gluing.

**Proposition 4.** The set consisting of all unary co-operations and an arbitrary essential co-operation is complete on any \( n \).

**Proof.** Denote the set and the essential co-operation in the proposition by \( S \) and \( f \), respectively. We show that there is a Sheffer co-operation in \( S \). For this aim we prove the following two claims:

(a) There exists a Sheffer co-operation \( g \) on \( n \) such that \( g_0 = f_0 \).

(b) If \( g \) is a co-operation on \( n \) such that \( g_0 = f_0 \), then \( g \in S \).

**Proof of (a).** A co-operation \( g \) on \( n \) with \( g_0 = f_0 \) is fully determined by its mapping \( g_1 \). We have to define \( g_1 \) such that neither non-empty proper subsets nor non-leaf partitions would be preserved by \( g \). Concerning the subsets, it is sufficient to choose \( g_1 \) a cyclic permutation of \( n \). As for the partitions, the co-operation \( g \) may preserve only refinements of the partition \( \lambda \) induced by its labelling. Thus, we have to show that under appropriate choice of the cycle \( g_1 \), no non-trivial refinement of \( \lambda \) will be preserved by \( g \). We can suppose that \( \lambda \) itself is not least, else we are done.

Given a cyclic permutation \( g_1 \) of \( n \) and an element \( i \in n \), each element of \( n \) may be written in the form \( g_1(t) \); for this element, we write shortly \( t' \). Partitions preserved by \( g_1 \) are the same as congruences of the algebra \( (n; g_1) \). Each such non-trivial and proper congruence is uniquely determined by a divisor \( d(1 < d < n) \) of \( n \) (and hence it may be denoted by \( \pi_d \) in the following way: \( t' = t''(\pi_d) \) if and only if \( t' = t''(m) \) (mod \( d \)).

Let \( \pi \) be a block of \( \lambda \) with minimal number of elements, and \( i \in \pi \). Then \( \pi = n/2 \). On the other hand, the number of non-trivial proper divisors of \( n \) is less than \( n/2 \); hence we can define \( g_1 \) so that for each non-trivial proper divisor \( d \) of \( n \), \( d' \neq d' \). Now if, for some \( s, n \leq k \), from \( t' = t''(\pi_d) \) it follows \( t' = t''(\pi_d) \), i.e., \( t' \in \pi_d \), a contradiction.

**Proof of (b).** Let \( f \) be \( k \)-ary, \( k \leq n \). As \( f \) is not gluing, the system of equations

\[
\begin{align*}
&f_0(x) = k, \\
&f_i(x) = i
\end{align*}
\]

has at most one solution \( x^k \) in \( n \). Clearly, each element of \( n \) may be written in form
3. Co-operations and selective operations. Given arbitrary non-empty sets $P$ and $M$, a natural number $k$, and mappings $f_0: P \rightarrow k$, $f_1: P \rightarrow P$, we define a $k$-ary operation $f$ on $M^k$ by agreeing that, for every $p \in P$, the $p$-component of the result of $f$ is the $f_1$-component of the $f_0$th operand. Operations obtained in this way are called regular selective operations (see [1]). The mappings $f_0$ and $f_1$ are referred to as the first and second selectors of $f$. Observe that they can be considered as the labelling and the mapping of a co-operation (of the same arity as $f$) on $P$. Moreover, for any nontrivial $M$ and non-empty $P$, there is a bijection between the regular selective operations on $M^k$ and the co-operations on $P$ assigning to a selective operation $f$ a co-operation whose labelling and mapping are the first and second selectors of $f$, respectively. This bijection is a clone isomorphism, i.e., it sends a projection into the coprojection with appropriate indices, and a superposition of operations into the superposition of co-operations being the images thereof. This follows immediately from (2) in [1] and (1) in this paper. Hence the study of clones (including lattices of clones) of regular selective operations on a finite power of a set reduces to the study of clones of co-operations on a finite set.

E.g., Corollary 2.1. implies that the basic operations of a $k$-dimensional die $D$ (see [3]) generate the clone of all selective operations on the base set $M^k$ of $D$. Hence it follows that the variety of $k$-dimensional dice is equivalent to the $k$th power-variety of sets, an observation due to Taylor [15] (see also [14]).

Further, we can reformulate Corollary 3.1., using the following consequence of Corollary 2.2.: a co-operation $f$ on $n$ is Sheffer iff $\mathcal{F}_n \subseteq [f]$, and translating it into the language of selective operations, we obtain the following fact: For $p$ prime, all binary selective operations on $M^k (|M| = p)$ are term functions of the given binary selective operation $f$ and only if $f$ is essentially binary and the second selector of $f$ is a cyclic permutation of $p$. Formulated in different terms, this is the main result in [9].

Finally, Fig. 4 may be considered as the lattice of clones of selective operations on $M^k (|M| > 1)$.

References


