

Coproducts and Decomposable Machines

MICHAEL A. ARBIB*

*Department of Computer and Information Science, University of Massachusetts,
Amherst, Massachusetts 01002*

January 25, 1972; revised August 19, 1972

The crucial discovery reported here is that the free monoid U^* on the input set U does not yield a sufficiently rich set of inputs when algebraic structure is placed on the machine. For group machines, the appropriate structure is the coproduct U^{\otimes} of an infinite sequence of copies of U . U^{\otimes} reduces to a reasonable facsimile of U^* in the Abelian case. A structure theorem for monoids of linear systems reveals the R monoid of Give'on and Zalcstein as appropriate only when no distinct powers of the state-transition matrix have the same action.

1. DECOMPOSABLE \mathcal{K} -MACHINES

We consider a *linear* system to be one for which U , Y , and X are all R -modules for a fixed ring R with identity and for which $\delta: X \times U \rightarrow X$ and $\beta: X \rightarrow Y$ are R -linear, i.e., there exist R -linear maps $F: X \rightarrow X$, $G: U \rightarrow X$ and $H: X \rightarrow Y$ such that the next-state map δ and output map β are given by

$$\begin{aligned}\delta(x, u) &= Fx + Gu, \\ \beta(x) &= Hx,\end{aligned}\tag{1}$$

for all x in X and u in U .

The zero-state response of the linear system (F, G, H) is given by the map $f: U^* \rightarrow Y$ defined by

$$f(u_k, \dots, u_1) = \sum_{j=1}^k HF^{j-1}Gu_j \text{ with each } u_j \in U.\tag{2}$$

By sacrificing the monoid structure on U^* we can turn the underlying set into

* Preparation of this paper was supported in part by the Department of the Army under Grant No. DAHC 04-70-C-0043.

an R -module¹ U^{\S} by identifying each $\omega = (u_k, \dots, u_1)$ with the left-infinite sequence $\hat{\omega} = (\dots, 0, \dots, 0, u_k, \dots, u_1)$ and defining addition, and multiplication by scalars, componentwise. The formula (2) then allows us to re-view f as an R -linear function $f^{\S}: U^{\S} \rightarrow Y$.

Now let us summarize what happens when we apply the Nerode construction [2, Section 3.4] to f^{\S} instead of f .²

We define $U^{\S} \times U^* \rightarrow U^{\S}$: $(\omega, \omega_1) \mapsto \omega\omega_1$ as the obvious extension of concatenation $U^* \times U^* \rightarrow U^*$:

$$(\dots, 0, \dots, 0, u_k, \dots, u_1)(v_l, \dots, v_1) = (\dots, 0, \dots, 0, u_k, \dots, u_k, \dots, u_1, v_l, \dots, v_1).$$

The relation \dot{E}_f^{\S} on U^{\S} is then defined by decreeing that, for each ω_1, ω_2 in U^{\S} , we have

$$\omega_1 E_f^{\S} \omega_2 \Leftrightarrow f^{\S}(\omega_1\omega) = f^{\S}(\omega_2\omega) \quad \text{for all } \omega \text{ in } U^*.$$

It is easily verified, from the linearity of f^{\S} , that

$$\omega_1 E_f^{\S} \omega_2 \Leftrightarrow f^{\S}(\omega_1 0^n) = f^{\S}(\omega_2 0^n) \quad \text{for each } n \in N, \tag{3}$$

where 0^n is the all zero sequence of length n in U^* . From this it follows that $X_f^{\S} = U^{\S}/E_f^{\S}$ inherits the R -module structure of U^{\S} with $r_1[\omega_1]_{\S} + r_2[\omega_2]_{\S} = [r_1\omega_1 + r_2\omega_2]_{\S}$. Further, the next-state map

$$\delta_f^{\S}: X_f^{\S} \times U \rightarrow X_f^{\S}: ([\omega]_{\S}, u) \mapsto [\omega u]_{\S} = [\omega \cdot 0]_{\S} + [\hat{u}]_{\S}$$

and the output map

$$\beta_f: X_f^{\S} \rightarrow Y: [\omega]_{\S} \rightarrow f^{\S}(\omega)$$

are well defined and R -linear, so that we obtain a linear machine $M(f^{\S})$ with

$$F_f[\omega]_{\S} + G_f u = [\omega u]_{\S}$$

and

$$H_f[\omega]_{\S} = f^{\S}(\omega).$$

¹ It must be confessed that we did not use the distinct notation U^{\S} in [1] until Section 5 and did not distinguish $\hat{\omega}$ from ω at all. Thus, although verbal warnings should have served to give sufficient contextual cues, a reader of Section 4 [1] might be forgiven if he thought we were imputing the R -module structure to U^* on occasions when only the monoid structure was available. I suspect that this is at the root of the erroneous statement [3, p. 555] that "Arbib and Zeiger . . . present a heuristic discussion of dynamics which cannot be made rigorous . . .".

² The emphasis in [1] was not so much on the fact that the Nerode construction went through for linear systems but rather on the fact that it could be seen to yield a whole family of identification algorithms. These results need not detain us here.

It is clear that, by throwing away the action of scalars, this construction yields [4] a procedure for obtaining the minimal realizations of Abelian group machines.

So far we have considered two special subclasses of machines.

Linear machines: U , X and Y are R -modules, and there exist linear maps $F: X \rightarrow X$, $G: U \rightarrow X$ and $H: X \rightarrow Y$ such that

$$\delta(x, u) = Fx + Gu; \quad \beta(x) = Hx.$$

Abelian group machines: U , X and Y are Abelian groups and there exist homomorphisms $F: X \rightarrow X$, $G: U \rightarrow X$ and $H: X \rightarrow Y$ such that

$$\delta(x, u) = Fx + Gu; \quad \beta(x) = Hx.$$

More generally given any category³ \mathcal{K} of sets with structure including a distinguished binary operation \cdot on each structured set (we refer to a set with such a structure as a \mathcal{K} -object and call a structure-preserving map between two \mathcal{K} -objects a \mathcal{K} -morphism), we may now define the following.

Decomposable \mathcal{K} -machines: U , X and Y are \mathcal{K} -objects, and there exist \mathcal{K} -morphisms $F: X \rightarrow X$, $G: U \rightarrow X$ and $H: X \rightarrow Y$ such that

$$\delta(x, u) = Fx \cdot Gu; \quad \beta(x) = Hx.$$

Our success with linear machines and Abelian group machines may then suggest the following.

FALSE CONJECTURE. *Let $M = (U, X, Y, \delta, \beta)$ be a decomposable \mathcal{K} -machine with $f: U^* \rightarrow Y$ an associated response function. Then U^* may be given the structure of a \mathcal{K} -object U^{\natural} in such a way that the $f^{\natural}: U^{\natural} \rightarrow Y$ obtained from f is a \mathcal{K} -morphism. Conversely, given a \mathcal{K} -morphism $f^{\natural}: U^{\natural} \rightarrow Y$, we may apply the Nerode construction to the corresponding $f: U^* \rightarrow Y$ to obtain the minimal \mathcal{K} -machine with f as associated response function.*

Indeed, we have seen that this holds when we take \mathcal{K} to be sets, R -modules, or Abelian groups. However, it does *not* hold for groups. We devote the rest of this section to the appropriate counterexamples and then give the correct theory for groups in Section 2.

³ This paper is carefully written to avoid any use of the terminology of category theory. However, a forthcoming paper by Manes and Arbib [5] will exploit category theory to build upon the insights of the present paper. For the present, a category \mathcal{K} may be thought of as a collection of sets with structure together with a collection of structure preserving mappings between these sets.

By a *group machine*,⁴ we shall mean a machine for which U , X , and Y are groups, and

$$\delta(x, u) = Fx \cdot Gu \quad \text{and} \quad \beta(x) = Hx,$$

for suitable homomorphisms $F: X \rightarrow X$, $G: U \rightarrow X$ and $H: X \rightarrow Y$.

We may impose a group structure on U^* by identifying a sequence with any sequence obtained from it by preloading with a sequence of identity elements, and then by using componentwise multiplication. However, even in very simple cases, the identity-state response function is not a group homomorphism.

EXAMPLE. Let $X = U = Y$ be any finite non-Abelian group. Let F , G , and H be the identity maps. The identity-state response function of the resultant group machine is then given by

$$f(u_n, u_{n-1}, \dots, u_1) = u_n u_{n-1} \cdots u_1.$$

However, this is not a group homomorphism since the multiplication suggested for U^* yields

$$(u_2, u_1) = (u_2, 1) \cdot (1, u_1) = (1, u_1) \cdot (u_2, 1).$$

But if f were a homomorphism we would then have both

$$f(u_2, u_1) = f(u_2, 1) \cdot f(1, u_1) = u_2 u_1,$$

and

$$f(u_2, u_1) = f(1, u_1) \cdot f(u_2, 1) = u_2 u_1,$$

for all u_1, u_2 in U , contradicting the assumption that U is non-Abelian.

However, the situation is even worse. It will be recalled that $M(f)$ is reachable. However, the following crucial example, due to Brockett and Willsky [5], shows that if we restrict the state-space of a group machine to contain only states reachable from the identity, the resulting space may only be a subset, and not a subgroup, of the original group.

EXAMPLE. Consider the machine with $U = Y = \mathbf{Z}_2$ and $X = \mathbf{D}_4$, the dihedral group with elements $\{e, y, x, xy, x^2, x^2y, x^3, x^3y\}$ where e is the identity, $x^4 = y^2 = e$, and $xyx = y$ (so that, for example, $xy^2 = xy \cdot xyx = xyx \cdot yx = yyx = x$).

⁴ This notion has, of course, been introduced by many authors. For example, it is what Brockett and Willsky [6] have called a *homomorphic sequential group machine*.

Define our machine by

$$F(x) = e, \quad F(y) = xy \quad (\text{so that } F(e) = e, F(xy) = xy, \text{ etc}),$$

$$G(0) = e, \quad G(1) = y,$$

and

$$H(x) = 0, \quad H(y) = 1.$$

Then the only states reachable from the identity are those of

$$\mathcal{R} = \{e, y, xy, x\}$$

and this is clearly not a subgroup of \mathbf{D}_4 .

While Brockett and Willsky [6] sought conditions under which the Nerode realization yields a group machine and conditions under which \mathcal{R} is a group, we shall instead take the previous examples as suggesting that U^* must be replaced by some larger structure if we are to salvage our conjecture.

2. THE MINIMAL GROUP MACHINE

Given a group U , the appropriate generalization of U^* is, as we shall see, the coproduct U^\natural of denumerably many copies of U . If, for each $n \in \mathbf{N}$ we take U_n to be a distinct group isomorphic to U_n [e.g. $U_n = \{(u, n) \mid u \in U\}$ with $(u, n)(u', n) = (uu', n)$] then the elements of U^\natural are of the form

$$(u_{i_1}, i_1)(u_{i_2}, i_2) \cdots (u_{i_n}, i_n) \text{ with each } u \in U, i \in \mathbf{N}$$

(we use Λ to denote the empty string) subject to the usual restrictions, and with multiplication simply concatenation, with the usual simplifying operations (see [7, Chapter 17] where the coproduct is called a *free product*).

For each n we may then define the *injection*

$$i_n: U_n \rightarrow U^\natural,$$

which sends an element of U_n to the length one string of U^\natural comprising that single element. i_n is clearly a homomorphism.

Note that if we work in the category of *Abelian groups*, this does indeed reduce to the additive structure of the U^\natural of Section 1, and Manes and Arbib [5] have introduced decomposable machines as the appropriate general categorical explication of this situation. U^\natural is then revealed as a simple-recursive object with basis U , which is often constructed as a countably-infinite coproduct of copies of U . However, we shall

content ourselves in the rest of this paper by studying the role of the above U^{\S} in realization theory for group machines.

Given a group machine $M = (U, X, Y, F, G, H)$, then for each n , we define the homomorphism

$$r_n: U_n \rightarrow X: (u, n) \mapsto F^nGu.$$

The reason that coproducts were invented is that this yields a unique homomorphism

$$r^{\S}: U^{\S} \rightarrow X,$$

for which $r_n = r^{\S} \circ i_n$ for every $n \in \mathbf{N}$. We call r^{\S} the *reachability map* of M .

Now since U^{\S} is a group and r^{\S} is a homomorphism, it follows that $r^{\S}(U^{\S})$ is a subgroup of X . Note, however, that since U^* , considered as sequences of the form $(u_{i_1}, i_1)(u_{i_2}, i_2) \cdots (u_{i_n}, i_n)$ for which $i_1 > i_2 > \cdots > i_n$, is not a subgroup of U^{\S} it follows that there is no guarantee that $r^{\S}(U^*)$ is a subgroup of X , as indeed we saw in the last example. This injection of U^* into U^{\S} does *not* respect the multiplicative structure placed on U^* at the end of Section 1.

EXAMPLE. Consider the last example in which $U = Y = \mathbf{Z}_2$, $X = \mathbf{D}_4$, $G(0) = e$, $G(1) = y$, $F(x) = e$ and $F(y) = xy$. Then $r^{\S}(U^{\S}) = \mathbf{D}_4$, since for example

$$\begin{aligned} x^2y &= x \cdot x \cdot xy = r^{\S}((1, 1)(1, 0)) r^{\S}((1, 1)(1, 0)) r^{\S}((1, 1)) \\ &= r^{\S}((1, 1)(1, 0)(1, 1)(1, 0)(1, 1)). \end{aligned}$$

Next we define the *identity-state response function* of the machine to be

$$f^{\S} = Hr^{\S}: U^{\S} \rightarrow Y,$$

which is the unique homomorphism for which $f^{\S} \circ i_n = HF^nG$.

EXAMPLE. Consider the first example in which $U = X = Y$ is a non-Abelian group, and F, G , and H are identity maps. Then

$$(u_1, 1)(u_2, 0) \quad \text{and} \quad (u_2, 0)(u_1, 1)$$

are different elements of U^{\S} , and we have

$$\begin{aligned} f^{\S}((u_1, 1)(u_2, 0)) &= f^{\S}(u_1, 1) f^{\S}(u_2, 0) = HFGu_1 \cdot HGu_2 = H(FGu_1 \cdot Gu_2), \\ f^{\S}((u_2, 0)(u_1, 1)) &= f^{\S}(u_2, 0) f^{\S}(u_1, 1) = HGu_2 \cdot HFGu_1 = H(Gu_2 \cdot FGu_1). \end{aligned}$$

Now for R -modules we reduced the Nerode equivalence to the simultaneous satisfaction of the equivalences

$$f^{\S}(w_1 0^n) = f^{\S}(w_2 0^n)$$

for each $n \in \mathbf{N}$. We now set up the corresponding sequence of equivalences for the group case.

For each n , we define the successor homomorphism

$$s_n: U_n \rightarrow U^{\S}: (u, n) \mapsto (u, n + 1).$$

This then yields the unique *successor* homomorphism

$$s: U \rightarrow U^{\S}$$

for which $s_n = s \circ i_n$ for every $n \in \mathbf{N}$.

Given any homomorphism $f^{\S}: U^{\S} \rightarrow Y$ we then define the congruence $E_{f^{\S}}$ on U^{\S} by

$$w_1 E_{f^{\S}} w_2 \Leftrightarrow f^{\S} s^n(w_1) = f^{\S} s^n(w_2) \quad \text{for all } n \in \mathbf{N}.$$

Let X_f be the factor group $U^{\S}/E_{f^{\S}}$, and let $\eta_f: U^{\S} \rightarrow U^{\S}/E_{f^{\S}}$ be the canonical epimorphism. Then we may define three homomorphisms as follows:

$$F_f: X_f \rightarrow X_f: [w] \mapsto [sw],$$

$$G_f: U \rightarrow X_f: u \mapsto [i_0 u],$$

$$H_f: X_f \rightarrow Y: [w] \mapsto f^{\S}(w).$$

It is a routine calculation to check that these three definitions do indeed yield well defined homomorphisms, and that the identity-state response of the group machine,

$$M(f^{\S}) \stackrel{\text{def}}{=} (X_f, U, Y, F_f, G_f, H_f),$$

is indeed f^{\S} .

We say that a group machine $(U, X_1, Y, F_1, G_1, H_1)$ is a *reduction* of the group machine $(U, X_2, Y, F_2, G_2, H_2)$ if there exists a subgroup X_3 of X_2 , and an epimorphism $h: X_3 \rightarrow X_1$ such that

$$G_2(U) \subset X_3; \quad hG_2 = G_1; \quad hF_2 = F_1h \text{ on } X_3; \quad \text{and} \quad H_1h = H_2 \text{ on } X_3.$$

THEOREM 1. $M(f^{\S})$ is minimal in the sense that it is a reduction of any group machine with identity-state response f^{\S} .

Proof. Let $M = (U, X, Y, F, G, H)$ be any machine with identity-state response f^s ; and let its reachability map be r^s . Let R be the subgroup $r^s(U^s)$ of X . We claim that

$$r^s(w_1) = r^s(w_2) \Rightarrow [w_1] = [w_2].$$

But it is clear that

$$r^s(s^n w_1) = F^n r^s(w_1) \quad \text{and that} \quad f^s(s^n w_1) = HF^n r^s(w_1).$$

Thus,

$$\begin{aligned} r^s(w_1) = r^s(w_2) &\Rightarrow f^s(s^n w_1) = f^s(s^n w_2) \quad \text{for all } n \in \mathbf{N} \\ &\Rightarrow [w_1] = [w_2]. \end{aligned}$$

This allows us to define a map $h: R \rightarrow X_f: r^s(w) \mapsto [w]$, and h is clearly a homomorphism since

$$r^s(w_1) \cdot r^s(w_2) = r^s(w_1 w_2) \mapsto [w_1 w_2] = [w_1] \cdot [w_2]$$

Finally, it is clear that $G(U) \subset G(U^s) = R$; $hG = G_f$; and that on R we have $hF = F_f h$ and $H_f h = H$. Thus, $M(f^s)$ is a reduction of M , as was to be shown. ■

In some sense, all this is trivial. The crucial point is that we had to discover the use of the *coproduct* to gain this triviality—the false conjecture of Section 1 provided a real obstacle to a general theory until this discovery was made. It is clear that Theorem 1 can be generalized to other classes of \mathcal{X} -machines. However, the appropriate setting for the general result requires too much category theory, and we must refer the reader to the forthcoming study by Manes and Arbib for further information. Instead, we close this section by defining a sequential machine which simulates the response of a group machine to all of U^s .

Given U , we define the set \tilde{U} to be $U \cup \{r\}$ where r is a new symbol, indicating a reset.

We then define a map $e: U^s \rightarrow \tilde{U}^*$ inductively by taking $e i_n: U_n \rightarrow \tilde{U}^*: (u, n) \mapsto u$, and then setting

$$e[zw \cdot (u, n) \cdot (u', n')] = \begin{cases} e[zw \cdot (u, n)] \cdot u' & \text{if } n > n' \\ e[zw \cdot (u, n)] \cdot r \cdot u' & \text{if } n < n'. \end{cases}$$

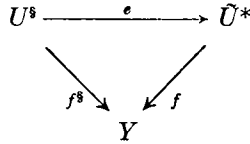
Then given the group machine $M = (U, X, Y, F, G, H)$ we define its *cumulator* \tilde{M} to be the machine

$$\tilde{M} = (\tilde{U}, X \times X, Y, \tilde{\delta}, \tilde{\beta})$$

for which

$$\begin{aligned} \tilde{\delta}((x_1, x_2), u) &= \begin{cases} (x_1 x_2, 1) & \text{if } u = r \\ (x_1, Fx_2 \cdot Gu) & \text{if } u \neq r \end{cases} \\ \tilde{\beta}(x_1, x_2) &= H(x_1 x_2). \end{aligned}$$

If $\tilde{f}: \tilde{U}^* \rightarrow Y$ is the (1, 1)-state response of \tilde{M} while f^\S is the identity-state response of M it is then straightforward to verify that the following diagram commutes



3. MONOIDS OF LINEAR SYSTEMS

Returning now to the minimal linear system $M(f^\S)$ which introduced Section 1, we note that the action of U upon X_f^\S may be extended to U^* simply by taking

$$X_f^\S \times U^* \rightarrow X_f^\S: ([\omega]_\S, \omega') \mapsto [\omega\omega']_\S.$$

What is the monoid of the minimal linear system $M(f^\S)$? We follow the usual procedure of starting with U^* and identifying strings which move the states in the same way to yield the monoid of a system. In the present case this yields the following development.

The monoid S_f^\S of $M(f^\S)$ is the factor monoid U^*/\equiv , where \equiv is the congruence on U^* defined for each ω_1, ω_2 in U^* by

$$\omega_1 \equiv \omega_2 \Leftrightarrow [\omega\omega_1]_\S = [\omega\omega_2]_\S \quad \text{for all } \omega \text{ in } U^\S.$$

If we define the relation \sim_f on N by

$$n_1 \sim_f n_2 \Leftrightarrow 0^{n_1} \equiv 0^{n_2}, \tag{4}$$

it is a straightforward exercise to obtain the lemma [1].

LEMMA. For all ω_1, ω_2 in U^* , we have

$$\omega_1 \equiv \omega_2 \Leftrightarrow [\hat{\omega}_1 E_f^\S \hat{\omega}_2 \text{ and } |\omega_1| \sim_f |\omega_2|].$$

In other words, to find whether two input strings move the states in the same way, we require that they correspond to the same state of the minimal realization, and then our only additional requirement is a length condition which has nothing to do with the internal structure of the strings. Actually, this is hardly surprising, for the state-transition of (1) is given by

$$(x, u_k \cdots u_1) \mapsto F^k x + \sum_{j=1}^k F^{j-1} G u_j,$$

in which the first-term depends only on the length of the string, while the second term is the state to which $(u_k \cdots u_1)$ sends (F, G, H) from the zero-state.

Let $N_f = N/\sim_f$. Clearly N_f inherits from N the structure of a monoid under addition, and is isomorphic to the cyclic submonoid of S_f^s generated by the action of the unit-length zero sequence 0. Call this action F_f^s . If all powers of F_f^s are distinct, N_f is isomorphic to N . If, on the other hand r and $r + m$ are the smallest distinct integers for which $(F_f^s)^r = (F_f^s)^{r+m}$, then N_f has $r + m$ elements, and is a finite cyclic monoid of index r and period m .

Let us now use this characterization of N_f , and the lemma, to characterise the structure of S_f^s .

THEOREM 2. *The monoid S_f^s of the linear system $M(f^s)$ may be expressed as the disjoint union*

$$\bigcup_{n \in N_f} S_n,$$

where $S_n = \{[\hat{\omega}]_s : |\omega| \sim_f n\}$ and where the multiplication is given by the functions (for each $m, n \in N_f$, with $m + n$ being defined in N_f)

$$S_m \times S_n \rightarrow S_{m+n}: ([\hat{\omega}_1]_s, [\hat{\omega}_2]_s) \mapsto [(\omega_1 \omega_2)^{\wedge}]_s,$$

where $|\omega_1| \sim_f m$ and $|\omega_2| \sim_f n$.

Now each S_n can be turned into an R -module by regarding it as a submodule of X_f^s . However, in the context of S_f^s , it does not make sense to add elements of S_m and S_n for distinct m and n since the crucial length index is then destroyed. We, thus, deduce that *in case all powers of F_f^s are distinct* S_f^s has the R monoid structure defined by Give'on and Zalcstein [1].

REFERENCES

1. M. A. ARBIB AND M. P. ZEIGER, On the relevance of abstract algebra to control theory, *Automatica* 5 (1969), 589-606.
2. M. A. ARBIB, "Theories of Abstract Automata," Prentice-Hall, Englewood Cliffs, NJ, 1969.
3. Y. GIVE'ON AND Y. ZALCSTEIN, Algebraic structures in linear systems theory, *J. Comput. System Sci.* 4 (1970), 539-556.
4. M. A. ARBIB, Decomposition of automata and biological systems, in "System Structure" (A. S. Morse, Ed.), pp. 1-56, IEEE Control Society, New York, 1971.
5. M. A. ARBIB AND E. G. MANES, Decomposable machines and simple recursion, in press.
6. R. W. BROCKETT AND A. S. WILLSKY, Finite-state homomorphic sequential machines, *IEEE Transactions Automatic Control*, AC-17 (1972), 483-490. (See also the related note by Arbib in the same issue, pp. 554-555.)
7. M. HALL, JR., "The Theory of Groups," The Macmillan Company, New York, 1959.