

Bialgebras and Realizations

R. L. Grossman R. G. Larson

3 January 2003

In this paper we consider when a linear functional on a bialgebra is realized by the action of the bialgebra on a finite object. This depends on whether the action of the bialgebra on the functional is finite. We consider two specific cases: the Myhill–Nerode Theorem, which gives a condition for a language to be accepted by a finite automaton, and Fliess’ Theorem, which gives a condition for the input/output maps of a control system to be realized by action on a finite dimensional state space.

If H is a bialgebra, then the linear dual H^* is an algebra with

$$pq(h) = \sum_{(h)} p(h_{(1)})q(h_{(2)})$$

for $h \in H$, $p, q \in H^*$. The algebra H^* is a left and right module algebra over H via

$$\begin{aligned}(h \rightharpoonup p)(k) &= p(kh) \\ (p \leftarrow h)(k) &= p(hk).\end{aligned}$$

If A is a left or right H -module algebra, we say that H measures A to itself. If the bialgebra H measures the algebra A to itself, then the elements of $P(H)$ act as derivations of A .

The Myhill–Nerode Theorem says that a language is accepted by a finite automaton if a certain equivalence relation defined on the set of all words has only finitely many equivalence classes. In this situation the bialgebra H is the semigroup algebra of the semigroup of all words in the alphabet, and the functional $p \in H^*$ is the characteristic function of the language. We show that the language is accepted by a finite automaton if and only if $H \rightharpoonup p$ is finite dimensional. Our of the Myhill–Nerode Theorem is adapted from [4].

Fliess' Theorem says that if H is the universal enveloping algebra of a free Lie algebra and $p \in H^*$, then p is differentially produced by a finite rank augmented algebra R if and only if $P(H) \rightarrow p$ is finite dimensional. Our presentation of Fliess' Theorem is adapted from [3].

Our approach of studying realizations using bialgebras also has been used for the study of hybrid systems [3] and the study of data mining [5].

1 Myhill–Nerode Theorem

The Myhill–Nerode Theorem is traditionally stated as in Theorem 3.1 of [6]: If Σ is a finite alphabet, and $L \subseteq \Sigma^*$ is a language, define an equivalence relation on Σ^* by $w \sim w'$ if and only if $wz \in L$ exactly when $w'z \in L$ for all $z \in \Sigma^*$. The Myhill–Nerode Theorem states that L is accepted by a finite automaton if and only if the equivalence relation \sim partitions Σ^* into finitely many equivalence classes.

Let M be a finite automaton accepting the language $L \subseteq \Sigma^*$. That is, M has a finite set of states S , an initial state $s_0 \in S$, and a set $F \subseteq S$ of accepting states. The word $w \in \Sigma^*$ is *accepted* by M if and only if $s_0 \cdot w \in F$.

Σ^* is a semigroup with operation concatenation and with identity the empty string ϵ . The bialgebra version of the Myhill–Nerode Theorem is as follows.

Theorem 1.1 (Myhill–Nerode) *Let G be a semigroup with unit, and let $H = kG$. Let $p \in H^*$. Then the following are equivalent:*

- 1) $\dim(H \rightarrow p)$ is finite and there exists a non zero polynomial $Q(X) \in k[X]$ such that $Q(p) = 0$;
- 2) $\dim(H \rightarrow p \leftarrow H)$ is finite and there exists a non zero polynomial $Q(X) \in k[X]$ such that $Q(p) = 0$;
- 3) $\dim(p \leftarrow H)$ is finite and there exists a non zero polynomial $Q(X) \in k[X]$ such that $Q(p) = 0$;
- 4) there exists a finite dimensional commutative left H -module algebra R with augmentation α and $f \in R$ such that $p(h) = \alpha(h \cdot f)$ for all $h \in H$;
- 5) there exists an augmented commutative left H -module algebra $R \subseteq H^*$ which is isomorphic to the algebra of k -valued functions on some finite set S and $f \in R$ such that $p(h) = \alpha(h \rightarrow f)$ for all $h \in H$.

PROOF. It is immediate that (2) implies (1).

We prove that (3) implies (2). Let $I = \{h \in H \mid (p \leftarrow H) \leftarrow h = 0\}$. Then I is a two sided ideal in H . Since $\dim(p \leftarrow H)$ is finite, and H/I is isomorphic to a subalgebra of $\text{End}_k(p \leftarrow H)$, it follows that $\dim(H/I)$ is finite. Since I is a two sided ideal and $p(I) = p \leftarrow I(1) = 0$, it follows that $H \rightarrow p \leftarrow H \subseteq I^\perp \cong (H/I)^*$ is finite dimensional.

We prove that (4) implies (3). We first show that $p \leftarrow H$ is finite dimensional. Let r_1, \dots, r_n be a basis for R . Then there exist $x_1, \dots, x_n \in H^*$ such that

$$h \cdot f = \sum_{i=1}^n x_i(h)r_i, \quad \text{for all } h \in H.$$

Now

$$\begin{aligned} (p \leftarrow l)(h) &= p(lh) \\ &= \alpha(lh \cdot f) \\ &= \alpha(l \cdot h \cdot f) \\ &= \sum_{i=1}^n x_i(h)\alpha(l \cdot r_i), \end{aligned}$$

for all $h, k \in H$. Therefore $p \leftarrow H \subseteq \sum kx_i$ is finite dimensional.

We next show that there exists a polynomial $Q(X)$ such that $Q(p) = 0$. Since R is finite dimensional and $f \in R$, there exists a polynomial $Q(X)$ such that $Q(f) = 0$. Let $w \in \Sigma^*$. Then $r \mapsto w \cdot r$ is an algebra endomorphism. Therefore $Q(w \cdot f) = w \cdot Q(f) = 0$. Since $p(w) = \alpha(w \cdot f)$ and $\alpha : R \rightarrow k$ is an algebra homomorphism, it follows that

$$Q(p(w)) = Q(\alpha(w \cdot f)) = \alpha(Q(w \cdot f)) = 0.$$

Since H^* can be identified with the algebra of k -valued functions on Σ^* , it follows that $Q(p) = 0$.

It is immediate that (5) implies (4).

We finally prove that (1) implies (5). Since $q \mapsto (w \rightarrow q)$ is an algebra endomorphism of H^* , and since p satisfies $Q(p) = 0$, it follows that $Q(w \rightarrow p) = 0$. Therefore $H \rightarrow p \subseteq H^*$ is finite dimensional and spanned by algebraic elements, so generates a finite dimensional commutative algebra $R \subseteq H^*$ which is a left H -module algebra. Since H^* is the algebra of functions on Σ^* it contains no non zero nilpotent elements. Therefore R is semisimple. Therefore R is a direct sum of finitely many field extensions of k . Since H^*

is the direct product of copies of k , all of these field extensions must be k . Therefore R is isomorphic to the set of functions from S , the set of maximal ideals of R , to k . Let $f = p \in R$. Then it immediate that $p(h) = \alpha(f \dashv h)$ for all $h \in H$, where $\alpha(q) = q(1)$ for all $q \in H^*$. This completes the proof of the theorem.

We now discuss the connection between Theorem 1.1 and the traditional form of the Myhill–Nerode Theorem. In the traditional case, the function p is the characteristic function of the language L being considered, and takes only the values 0 and 1 on elements of Σ^* , and so always satisfies the polynomial $Q(X) = X^2 - X$. We will use this fact freely in the following discussion.

Condition (5) of Theorem 1.1 is equivalent to the assertion that the language L is accepted by a finite automaton. The set S of maximal ideals of R is the set of states of the automaton. Σ^* acts on S as follows: if $w \in \Sigma^*$, since $r \mapsto w \cdot r$ is an algebra homomorphism, it induces a map $S \rightarrow S$ on the set of maximal ideals of R . The augmentation $\alpha : R \rightarrow k$ gives a maximal ideal which is the initial state. The function $f \in R$ is the characteristic function of some subset of S which is the set of accepting states.

We now consider Condition (1) of Theorem 1.1. Define the equivalence relation \sim on Σ^* by $w \sim w'$ if and only if $q(w) = q(w')$ for all $q \in H \dashv p$. In other words, $w \sim w'$ if and only if $p(wz) = p(w'z)$ for all $z \in \Sigma^*$, if and only if $wz \in L$ exactly when $w'z \in L$ for all $z \in \Sigma^*$. The subalgebra of H^* generated by $H \dashv p$, which is finite dimensional if and only if $H \dashv p$ is finite dimensional, is the algebra of all functions on the equivalence classes of this equivalence relation. Therefore Condition (1) of Theorem 1.1 is equivalent to the assertion that this equivalence relation has finite index.

The Myhill–Nerode Theorem is a realization theorem, in that it describes when a formal language is realized as the language recognized by a finite automaton.

2 Fliess' Theorem

In this section we prove a realization theorem for input-output maps of control systems. We prove the algebraic parts of the classical results of Fliess [1], [2]

We use the following definition. If H is a bialgebra, we say that $p \in H^*$ is *differentially produced by the algebra R with the augmentation ϵ* if

1. there is right H -module algebra structure on R ;
2. there exists $f \in R$ satisfying $p(h) = \epsilon(f \cdot h)$.

If H is the universal enveloping algebra of a Lie algebra, we will characterize those $p \in H^*$ which are differentially produced by finite rank algebras.

Let H denote the free associative algebra in the symbols E_1, \dots, E_M over the field k .

If the coalgebra structure on H is defined by

$$\Delta(E_i) = 1 \otimes E_i + E_i \otimes 1$$

then H is the universal enveloping algebra of the free Lie algebra on E_1, \dots, E_M . H^* is isomorphic to a formal power series algebra in infinitely many variables.

Differentially produced functionals arise naturally when studying control systems with inputs and outputs. For example, let R denote the field of rational functions in the variables x_1, \dots, x_N with coefficients from the field k , and let E_1, \dots, E_M denote M derivations of R . The control system

$$\begin{aligned} \dot{z}(t) &= \sum_{i=1}^M u_i(t) E_i(zx(t)), \\ z(0) &= z^0 \in k^N \end{aligned} \tag{1}$$

together with an observation function $f \in R$

$$f : k^N \longrightarrow k \tag{2}$$

naturally specifies an input-output map, which is defined by sending the input functions

$$t \rightarrow u_1(t), \dots, t \rightarrow u_M(t)$$

to the output function

$$t \rightarrow f(z(t)).$$

The properties of the input-output map are captured by the formal series $\sum_{\mu} c_{\mu} \mu$, where $c_{\mu} = E_{\mu_k} \cdots E_{\mu_1} f(x(0))$.

This series is often called the generating series, while the data consisting of a control system with inputs, together with an observation, are called a state space realization of the input-output map.

If $p \in H^*$ is the formal series associated with such an input-output map, then it is differentially produced. Conversely, we can ask which formal series

$p \in H^*$ have the property that there is a control system and an observation function which realizes it as above; that is, which formal series p are differentially produced?

We say that $p \in H^*$ has *finite Lie rank* if $\dim P(H) \rightarrow p$ is finite.

Theorem 2.1 (Fliess) *Let H be a primitively generated bialgebra over a field of characteristic 0. Let $p \in H^*$. Then the following are equivalent:*

- 1) p has finite Lie rank;
- 2) p is differentially produced by some augmented k -algebra R for which $\dim(\text{Ker } \epsilon)/(\text{Ker } \epsilon)^2$ is finite;
- 3) p is differentially produced by a subalgebra of H^* which is isomorphic to $k[[x_1, \dots, x_N]]$, the algebra of formal power series in N variables.

PROOF. We first prove that (2.1) implies (2.1). Given a fixed $p \in H^*$, we define three basic objects:

$$\begin{aligned} L &= \{h \in P(H) \mid h \rightarrow p = 0\} \\ J &= HL \\ J^\perp &= \{q \in H^* \mid q(j) = 0 \text{ for all } j \in J\}. \end{aligned}$$

Since $L \subseteq P(H)$, it follows that J is a coideal, that is, $\Delta(J) \subseteq J \otimes H + H \otimes J$. Therefore $J^\perp \cong (H/J)^*$ is a subalgebra of H^* . We will show that J^\perp is isomorphic to a formal power series algebra, and will construct derivations of this ring which will be used to realize the input-output map defined by p .

Lemma 2.2 *If $\dim P(H) \rightarrow p = N$, then J^\perp is a subalgebra of H^* satisfying*

$$J^\perp \cong k[[x_1, \dots, x_N]].$$

PROOF. The sub Lie algebra L has finite codimension N . Choose a basis $\{e_1, e_2, \dots\}$ of $P(H)$ such that $\{e_{N+1}, e_{N+2}, \dots\}$ is a basis of L . Note that if \bar{e}_i is the image of e_i under the quotient map $P(H) \rightarrow P(H)/L$, then $\{\bar{e}_1, \dots, \bar{e}_N\}$ is a basis for $P(H)/L$.

By the Poincaré–Birkhoff–Witt Theorem, H has a basis of the form

$$\{e_{i_1}^{\alpha_{i_1}} \cdots e_{i_k}^{\alpha_{i_k}} \mid i_1 < \cdots < i_k \text{ and } 0 < \alpha_{i_r}\}.$$

Since L is a sub Lie algebra of $P(H)$, and the basis $\{e_i\}$ of $P(H)$ has been chosen so that $e_i \in L$ for $i > N$, it follows that the operation of putting monomials in standard form which is used in the proof of the Poincaré–Birkhoff–Witt Theorem will map elements of $J = HL$ to linear combinations of monomials of the form

$$e^\alpha = e_{i_1}^{\alpha_{i_1}} \cdots e_{i_k}^{\alpha_{i_k}}$$

with at least one $i_r > N$. Therefore J has a basis of such monomials. It follows that

$$\{\bar{e}_1^{\alpha_1} \cdots \bar{e}_N^{\alpha_N} \mid \alpha_1, \dots, \alpha_N \geq 0\}$$

is a basis for H/J . It now follows that the elements of the form

$$x_\alpha = \frac{x^\alpha}{\alpha!} = \frac{x_{i_1}^{\alpha_{i_1}} \cdots x_{i_k}^{\alpha_{i_k}}}{\alpha_{i_1}! \cdots \alpha_{i_k}!}$$

with all $1 \leq i_r \leq N$ are in $J^\perp \subseteq H^*$. Note that these elements satisfy

$$x_\alpha(e^\beta) = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, J^\perp consists precisely of the completion in the finite topology of the span of such elements. In other words,

$$J^\perp \cong k[[x_1, \dots, x_N]],$$

completing the proof.

We will use the following notation and facts from the proof of Lemma 2.2: Suppose that $\{e_1, \dots, e_N, \dots\}$ is a basis for $P(H)$ such that $\{e_{N+1}, \dots\}$ is a basis for L . Let $\{e^\alpha\}$ be the corresponding Poincaré–Birkhoff–Witt basis. Denote J^\perp by R . Then $R \cong k[[x_1, \dots, x_N]]$, and $x_1^{\alpha_1} \cdots x_N^{\alpha_N} / \alpha_1! \cdots \alpha_N!$ equals the element of the dual (topological) basis of H^* to the Poincaré–Birkhoff–Witt basis $\{e^\alpha\}$ of H , corresponding to the basis element $e_1^{\alpha_1} \cdots e_N^{\alpha_N}$.

We now collect some properties of the ring of formal power series R which will be necessary for the proof of the theorem.

Lemma 2.3 *Assume $p \in H^*$ has finite Lie rank, and let $R \subseteq H^*$, $e_\alpha \in H$, and $x^\alpha \in R$ be as above. Define*

$$f = \sum_{\alpha=(\alpha_1, \dots, \alpha_N)} c_\alpha x^\alpha \in R,$$

where $c_\alpha = \frac{p(e^\alpha)}{\alpha!}$. Then

1. H measures R to itself via \leftarrow ;
2. $p(h) = \epsilon(f \leftarrow h)$ for all $h \in H$.

PROOF. We begin with the proof of (1). Since H measures H^* to itself and $R \subseteq H^*$, we need show only that $R \leftarrow H \subseteq R$. Take $r \in R, h \in H$ and $j \in J$. We have $(r \leftarrow h)(j) = r(hj)$. Since J is a left ideal, $hj \in J$, so $r(hj) = 0$, so $r \leftarrow h \in J^\perp = R$.

We now prove (2). Let $e^\alpha = e_{i_1}^{\alpha_{i_1}} \cdots e_{i_k}^{\alpha_{i_k}}$ be a Poincaré–Birkhoff–Witt basis element of H . Since $e^\alpha \in J$ unless $\{i_1, \dots, i_k\} \subseteq \{1, \dots, N\}$, $p(e^\alpha) = 0$ unless $\{i_1, \dots, i_k\} \subseteq \{1, \dots, N\}$. Also $\epsilon(f \leftarrow e^\alpha) = f \leftarrow e^\alpha(1) = f(e^\alpha) = 0$ unless $\{i_1, \dots, i_k\} \subseteq \{1, \dots, N\}$. Now suppose $\{i_1, \dots, i_k\} \subseteq \{1, \dots, N\}$. We have in this case that $p(e^\alpha) = \alpha! c_\alpha = f(e^\alpha) = f \leftarrow e^\alpha(1) = \epsilon(f \leftarrow e^\alpha)$. Since $\{e^\alpha\}$ is a basis for H , this completes the proof of the lemma.

Corollary 2.4 *Under the assumptions of Lemma 2.3, $f = p$.*

Lemmas 2.2 and 2.3 yield that (2.1) implies (2.1) in Theorem 2.1. It is immediate that (2.1) implies (2.1).

We now complete the proof of Theorem 2.1 by proving that (2.1) implies (2.1).

Let x_1, \dots, x_N be chosen so that $\{\bar{x}_1, \dots, \bar{x}_N\}$ is a basis for $(\text{Ker } \epsilon)/(\text{Ker } \epsilon)^2$. If $f \in R$ and $h \in H$, then

$$f \cdot h = q_0(h)1 + \sum_{i=1}^N q_i(h)x_i + g(h),$$

where $q_i \in H^*$ and $g(h) \in (\text{Ker } \epsilon)^2$. Let $l \in P(H)$. Since H measures R to itself and $\Delta(l) = 1 \otimes l + l \otimes 1$, the map $f \mapsto f \cdot l$ is a derivation of R . Now let $f \in R$ be the element such that

$$p(h) = \epsilon(f \cdot h).$$

Then

$$\begin{aligned} f \cdot hl &= (f \cdot h) \cdot l \\ &= q_0(h)1 \cdot l + \sum_{i=1}^N q_i(h)x_i \cdot l + g(h) \cdot l. \end{aligned}$$

Since the map $f \mapsto f \cdot l$ is a derivation, $1 \cdot l = 0$; since $g(h) \in (\text{Ker } \epsilon)^2$, $g(h) \cdot l \in \text{Ker } \epsilon$. It follows that

$$\begin{aligned} l \mapsto p(h) &= p(hl) \\ &= \epsilon(f \cdot hl) \\ &= \sum_{i=1}^N q_i(h) \epsilon(x_i \cdot l). \end{aligned}$$

Therefore $P(H) \mapsto p \subseteq \sum_{i=1}^N kq_i$, so p has finite Lie rank. This completes the proof of Theorem 2.1

References

- [1] M. Fliess, Réalisation locale des systèmes non linéaires, algèbres de Lie filtrées transitives et séries génératrices non commutatives, *Invent. Math.*, **71** (1983) 521–537.
- [2] M. Fliess, Nonlinear realization theory and abstract transitive Lie algebras, *Bull. Amer. Math. Soc.*, (NS) **2** (1980), 444–446.
- [3] R. L. Grossman and R. G. Larson, The realization of input-output maps using bialgebras, *Forum Mathematicum* **4** (1992) 109–121.
- [4] R. L. Grossman and R. G. Larson, An algebraic approach to hybrid systems, *Theoretical Computer Science*, **138** (1995), 101–112.
- [5] R. L. Grossman and R. G. Larson, *An Algebraic Approach to Data Mining: Some Examples*, Proceedings of the 2002 IEEE International Conference on Data Mining (ICDM 2002), December 2002, Maebashi City, Japan.
- [6] J. E. Hopcroft and J. D. Ullman, *Formal Languages and their Relation to Automata*, Addison-Wesley, Reading, 1969.
- [7] M. E. Sweedler, *Hopf algebras*, W. A. Benjamin, New York, 1969.