Discrete Mathematics 43 (1983) 273–279
North-Holland Publishing Company

A COMBINATORIAL PROOF OF THE CAYLEY–HAMILTON THEOREM

Howard STRAUBING

Department of Mathematics, Reed College, Portland, OR 97202, USA

Received 4 February 1982

An elementary combinatorial proof of the Cayley–Hamilton theorem is given. At the conclusion of the proof I discuss a connection with a combinatorial theory developed by Foata and Cartier.

Let A be an $n \times n$ matrix over a commutative ring R and let $P_A(x) = \det(xI - A)$ be its characteristic polynomial. The Cayley–Hamilton theorem asserts that $p_A(A)$ is the zero matrix. In this note I give a combinatorial proof of the theorem. At the conclusion of the proof a connection with the Foata–Cartier theory of the 'flow monoid' [1] is noted—this yields a slight generalization of the Cayley–Hamilton theorem to matrices over non-commutative rings.

1. Partial permutations

A *partial permutation* of $\{1, \ldots, n\}$ is a bijection σ of a subset of $\{1, \ldots, n\}$ onto itself. The domain of σ is denoted $\operatorname{dom} \sigma$. The cardinality of $\operatorname{dom} \sigma$ is called the degree of σ and is denoted $|\sigma|$. A partial permutation whose domain is all of $\{1, \ldots, n\}$ is called a *complete* permutation. If σ is a partial permutation of $\{1, \ldots, n\}$, then the *completion* of σ, denoted $\hat{\sigma}$, is the complete permutation of $\{1, \ldots, n\}$ defined by

$$\hat{\sigma}(i) = \begin{cases} \sigma(i) & \text{if } i \in \operatorname{dom} \sigma, \\ i & \text{if } i \in \{1, \ldots, n\} \backslash \operatorname{dom} \sigma. \end{cases}$$

The *signature* of a partial permutation σ, denoted $\operatorname{sgn} \sigma$, is defined by

$$\operatorname{sgn} \sigma = (-1)^{\hat{\sigma}}(-1)^{|\sigma|}$$

where $(-1)^{\hat{\sigma}}$ denotes the signature *in the usual sense* of the permutation $\hat{\sigma}$. (*Note.* If n is odd and σ is complete, then $\operatorname{sgn} \sigma \neq (-1)^{\sigma}$.)

Every partial permutation has a unique representation as a set of disjoint cycles. For example, the partial permutations

$$\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

0012-365X/83/0000–0000/$03.00

have, respectively, the cycle representations

$$\{(2,3)\}, \qquad \{(1),(2,3)\} \qquad \{(1,3,2),(4)\}.$$

The unique partial permutation of degree zero has the empty set as its cycle representation.

If σ is a cyclic partial permutation of degree k, then $\operatorname{sgn}\sigma = (-1)^k(-1)^{k+1} = -1$. It follows that for any partial permutation σ, $\operatorname{sgn}\sigma = (-1)^r$, where r is the number of cycles appearing in the cycle representation of σ.

2. Positive and negative parts of the characteristic polynomial

Let R be a commutative ring and let $A = (a_{ij})$ be an $n \times n$ matrix over R. The characteristic polynomial of A is given by

$$p_A(x) = \det(xI - A) = \sum_{\sigma} (-1)^{\sigma} \prod_{i=1}^{n} b_{i,\sigma(i)}$$

where

$$b_{ij} = \begin{cases} -a_{ij} & \text{if } i \neq j, \\ x - a_{ij} & \text{if } i = j \end{cases}$$

and where the summation is over all *complete* permutations of $\{1, \ldots, n\}$. It follows that the coefficient of x^{n-q} in $p_A(x)$ is

$$\sum_{|\sigma|=q} (-1)^q (-1)^{\hat{\sigma}} \prod_{i \in \operatorname{dom}\sigma} a_{i,\sigma(i)} = \sum_{|\sigma|=q} \operatorname{sgn}\sigma \prod_{i \in \operatorname{dom}\sigma} a_{i,\sigma(i)}$$

where now the summation is over all partial permutations of degree q. (If σ is the partial permutation of degree zero, then $\prod_{i \in \operatorname{dom}\sigma} a_{i,\sigma(i)}$ is taken to be 1.)

Thus $p_A(x) = p_A^+(x) - p_A^-(x)$ where

$$p_A^+(x) = \sum_{q=0}^{n} \Bigg(\sum_{\substack{|\sigma|=q \\ \operatorname{sgn}\sigma = 1}} \prod_{i \in \operatorname{dom}\sigma} a_{i,\sigma(i)} \Bigg) x^{n-q}$$

and

$$p_A^-(x) = \sum_{q=0}^{n} \Bigg(\sum_{\substack{|\sigma|=q \\ \operatorname{sgn}\sigma = -1}} \prod_{i \in \operatorname{dom}\sigma} a_{i,\sigma(i)} \Bigg) x^{n-q}.$$

The Cayley–Hamilton Theorem is

Theorem. $p_A^+(A) = p_A^-(A)$.

3. Proof of the Theorem

A *path* π in $\{1, \ldots, n\}$ is a sequence of ordered pairs $((i_0, i_1), (i_1, i_2), \ldots, (i_{q-1}, i_q))$ where each i_k belongs to $\{1, \ldots, n\}$. The number q is called the *length* of π and is denoted $|\pi|$. The i_j are called the *vertices* of π and the pairs (i_j, i_{j+1}) are the *edges* of π. The vertices i_0 and i_q are called the *start* of π and the *finish* of π and are denoted $\alpha(\pi)$ and $\omega(\pi)$ respectively. The *value* of π is the element $\mu(\pi) = \prod_{k=0}^{q-1} a_{i_k i_{k+1}}$ of R. I make the convention that for each $i \in \{1, \ldots, n\}$ there is a unique path π_i such that $|\pi_i| = 0$, $\alpha(\pi_i) = \omega(\pi_i) = i$ and $\mu(\pi_i) = 1$.

If σ is a partial permutation, then the *value* of σ is defined by

$$\mu(\sigma) = \prod_{i \in \operatorname{dom} \sigma} a_{i,\sigma(i)}.$$

By the convention made in the previous section, the value of the partial permutation of degree zero is 1.

Let $1 \leqslant i, j \leqslant n$ and let T_{ij}^+ be the set of all pairs (σ, π) where σ is a partial permutation and π is a path which satisfy

$$|\sigma| + |\pi| = n, \quad \alpha(\pi) = i, \quad \omega(\pi) = j, \quad \operatorname{sgn} \sigma = 1.$$

The set T_{ij}^- is defined identically, except that the condition '$\operatorname{sgn} \sigma = 1$' is replaced by '$\operatorname{sgn} \sigma = -1$'. T_{ij} denotes the union $T_{ij}^+ \cup T_{ij}^-$. Now for $k \geqslant 0$,

$$(A^k)_{ij} = \sum_{\substack{|\pi| = k,\ \alpha(\pi) = i,\\ \omega(\pi) = j}} \mu(\pi).$$

(The convention regarding paths of length zero makes this formula valid for $k = 0$ as well.) It follows that

$$p^+(A)_{ij} = \sum_{(\sigma,\pi) \in T_{ij}} \mu(\sigma)\mu(\pi), \qquad p^-(A)_{ij} = \sum_{(\sigma,\pi) \in T_{ij}^-} \mu(\sigma)\mu(\pi).$$

The theorem asserts that these two sums are equal for all $i, j \in \{1, \ldots, n\}$. This follows at once from

Lemma. *For each* $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ *there is a bijection* $\eta_{ij} : T_{ij}^+ \to T_{ij}^-$ *such that* $\eta_{ij}(\sigma, \pi) = (\sigma', \pi')$ *implies* $\mu(\sigma)\mu(\pi) = \mu(\sigma')\mu(\pi')$.

To prove the Lemma I represent each pair $(\sigma, \pi) \in T_{ij}$ by a directed graph with vertices $\{1, \ldots, n\}$ and two classes of edges:

$$U = \{(i, \sigma(i)) \mid i \in \operatorname{dom} \sigma\} \quad \text{and} \quad V = \{(k, l) \mid (k, l) \text{ is an edge of } \pi\}.$$

This graph will, in general, contain multiple edges, since π may traverse the same edge more than once (i.e., V is a *multiset*) or the same edge may appear in both U and V. $\mu(\sigma)\mu(\pi)$ is the product, with multiplicities taken into account, of all the a_{kl}, where (k, l) is an edge of the graph associated to (σ, π).

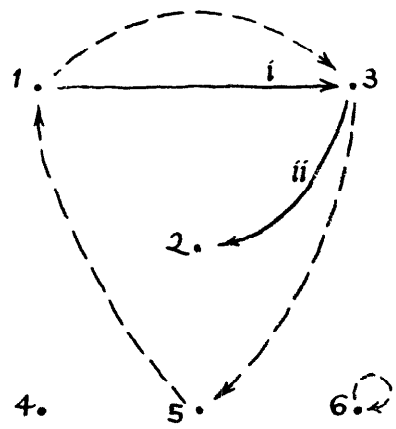

Fig. 1. $n = 6$, $\sigma = \begin{pmatrix} 1 & 3 & 5 & 6 \\ 3 & 5 & 1 & 6 \end{pmatrix}$ $\pi = ((1, 3), (3, 2))$.

Two examples are illustrated below (see Figs. 1 and 2). I have denoted the edges in U by dashed lines, and those in V by solid lines. The order of traversal of the edges of the path π is indicated by the small Roman numerals.

Let $\pi = ((i_0, i_1), \ldots, (i_{q-1}, i_q))$. There is a smallest integer $v \geq 0$ such that either $i_u = i_v$ for some u less than v or $i_v \in \operatorname{dom} \sigma$. Indeed, if there is no pair of distinct indices u and v such that $i_u = i_v$, then π has $|\pi| + 1$ distinct vertices; the edges $(i, \sigma(i))$ of U account for $|\sigma|$ different vertices, and $|\sigma| + |\pi| + 1 = n + 1$, thus there must be a vertex of π in $\operatorname{dom} \sigma$. Furthermore, this smallest v cannot have both properties, for if $i_v \in \operatorname{dom} \sigma$ and $i_u = i_v$ for some u with $u < v$, then we have an index u smaller than v with $i_u \in \operatorname{dom} \sigma$. In Fig. 1 above, $v = 0$, since $i_0 = 1 \in \operatorname{dom} \sigma$. In Fig. 2 $v = 3$, since $i_2 = i_3 = 2$, whereas $i_4 = 4$ is the only vertex of π in $\operatorname{dom} \sigma$. If $i_v \in \operatorname{dom} \sigma$, then I define $\eta_{ij}(\sigma, \pi) = (\sigma', \pi')$ where σ' is formed by removing the cycle containing i_v from σ, and where π' is formed by inserting this cycle into π. If, on the other hand, $i_u = i_v$ for some $u < v$, then the loop $((i_u, i_{u+1}), \ldots, (i_{v-1}, i_v))$ is removed from π and adjoined as a new cycle to σ. (Observe that none of the vertices in this loop already belongs to $\operatorname{dom} \sigma$.) In this instance I define $\eta_{ij}(\sigma, \pi) = (\sigma', \pi')$, where σ' is the resulting longer partial permutation and π' is the resulting shorter path. The results of applying η_{ij} in Figs. 1 and 2 are illustrated below (see Figs. 3 and 4).

Since the number of cycles in σ' differs by 1 from the number of cycles in σ, $\operatorname{sgn} \sigma = -\operatorname{sgn} \sigma'$ and thus η_{ij} maps T_{ij}^+ into T_{ij} and vice versa. A moment's reflection shows that the composition $\eta_{ij} \circ \eta_{ij}$ is the identity on T_{ij}, consequently

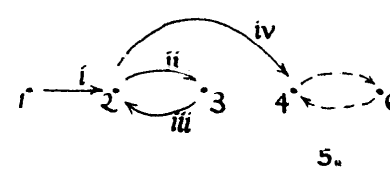

Fig. 2. $n = 6$, $\sigma = \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix}$, $\pi = ((1, 2), (2, 3), (3, 2), (2, 4))$.

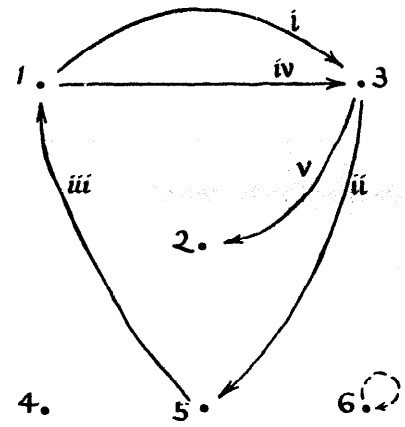

Fig. 3. $\sigma' = \begin{pmatrix} 6 \\ 6 \end{pmatrix}$, $\pi' = ((1,3),(3,5),(5,1),(1,3),(3,2))$.

the restriction of η_{ij} to T_{ij}^{+} is a bijection of T_{ij}^{+} onto T_{ij}^{-}. Finally, $\mu(\sigma)\mu(\pi) = \mu(\sigma')\mu(\pi')$—indeed, nothing has changed in the graph of (σ, π) except the colors of the edges. This completes the proof.

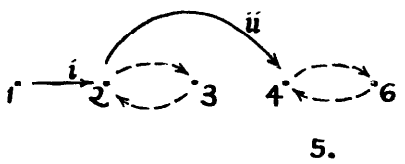

Fig. 4. $\sigma' = \begin{pmatrix} 2 & 3 & 4 & 6 \\ 3 & 2 & 6 & 4 \end{pmatrix}$, $\pi' = ((1,2),(2,4))$.

4. Connection with the Foata–Cartier theory

The proof just given can be presented in the framework of a combinatorial theory developed by D. Foata and P. Cartier (Cartier and Foata [1], Foata [2]. See also the exposition in Lallement [3].) When things are done in this fashion the argument loses some of its elementary quality. However the result obtained is slightly stronger, and certain conventions which appear rather arbitrary in the original proof become quite natural. In this section I outline this method of proof.

The set $X = \{1, \ldots, n\} \times \{1, \ldots, n\}$ is regarded as a finite alphabet (I will write the pairs in X vertically, as $\binom{i}{j}$ rather than as (i, j).) The free monoid X^* generated by X is the set of all finite sequences of elements of X (i.e., *words* in the letters of X) including an empty word, denoted 1, which is the identity element of X^*. The monoid-ring $\mathbb{Z}\langle X^* \rangle$ consists of all polynomials with integer coefficients in the letters of X, these now regarded as noncommuting variables. Any map $\mu : X \to M$, where M is a monoid, extends to a unique morphism of monoids $\mu : X^* \to M$, thence to a unique ring morphism $\mu : \mathbb{Z}\langle X^* \rangle \to \mathbb{Z}\langle M \rangle$.

A partial permutation

$$\begin{pmatrix} i_1 & \cdots & i_k \\ \sigma(i_1) & \cdots & \sigma(i_k) \end{pmatrix}$$

where $i_1 < \cdots < i_k$ is identified with the word

$$\binom{i_1}{\sigma(i_1)} \cdots \binom{i_k}{\sigma(i_k)}$$

and a path $\pi = ((i_0, i_1), \ldots, (i_{q-1}, i_q))$ with the word

$$\binom{i_0}{i_1} \cdots \binom{i_{q-1}}{i_q}.$$

In the proof I was, in effect, considering the elements $r_{ij} = \sum_{(\sigma, \pi) \in T_{ij}} (\operatorname{sgn} \sigma)\, \sigma\pi$ of $\mathbb{Z}\langle X^* \rangle$. (Observe what happens to the 'empty paths' π_i in this summation. If $i = j$, then r_{ij} includes the terms $(\operatorname{sgn} \sigma)\sigma$ where $|\sigma| = n$, because the empty word 1 is regarded as a path from i to j, and thus $(\sigma, 1) \in T_{ij}$. However, if $i \neq j$ these terms do not appear.) Let μ be the morphism of X^* onto the free commutative monoid M in the n^2 variables $\{a_{ij} \mid 1 \leq i, j \leq n\}$ defined by $\mu\binom{i}{j} = a_{ij}$. μ extends to a ring morphism from $\mathbb{Z}\langle X^* \rangle$ into $\mathbb{Z}\langle M \rangle$ (which is just the ring of polynomials in the commuting variables $\{a_{ij}\}$). One part of the proof of the theorem consisted of verifying that $\mu(r_{ij}) = p_A(A)_{ij}$ while the combinatorial lemma showed that $\mu(r_{ij}) = 0$.

Cartier and Foata introduced the *flow monoid* $F(X)$, which is the quotient of X^* by the commutativity relations

$$\binom{i}{j}\binom{i'}{j'} = \binom{i'}{j'}\binom{i}{j} \quad \text{whenever } i \neq i'.$$

It can be easily verified that when $\eta_{ij}(\sigma, \pi) = (\sigma', \pi')$, then the words $\sigma\pi$ and $\sigma'\pi'$ have the same image in $F(X)$ under the projection morphism $\lambda : X^* \to F(X)$. Thus, under the induced morphism $\lambda : \mathbb{Z}\langle X^* \rangle \to \mathbb{Z}\langle F(X) \rangle$, $\lambda(r_{ij}) = 0$. (The fact that $\mu(r_{ij}) = 0$ is a consequence of this, since the morphism μ factors through $F(X)$—that is, $\mu = \nu \circ \lambda$ for some morphism $\nu : \mathbb{Z}\langle F(X) \rangle \to \mathbb{Z}\langle M \rangle$) This observation leads to a slight generalization of the Cayley–Hamilton theorem: the theorem holds for a matrix $A = (a_{ij})$ over an arbitrary ring provided that entries from distinct rows of A commute with one another.

Acknowledgement

This work was done while I was a visiting member of the faculty of the Institut de Programmation, Université de Paris VI. I am grateful for the support and leisure I was provided.

References

[1] P. Cartier and D. Foata, Problèmes Combinatoires de Commutation et Réarrangement, Lecture Notes in Mathematics 85 (Springer-Verlag, Berlin, 1969).

[2] D. Foata, Chapter 10 in: Lothaire, ed., Combinatorics on Words (Addison-Wesley, Reading, MA, 1982).

[3] G. Lallement, Semigroups and Combinatorial Applications, (Wiley Interscience, New York, 1979).