ADVANCES IN MATHEMATICS 31, 330–349 (1979)

A Noncommutative Version of the Matrix Inversion Formula

DOMINIQUE FOATA*

Département de Mathématique, Université de Strasbourg, 7 rue René-Descartes, 67084 Strasbourg, France

The cofactor expression $(-1)^{i+j}\det(I-B)_{ji}/\det(I-B)$ for the (i,j)-entry in the inverse of a matrix $(I-B)$ is proved to be equal to the corresponding entry of the series $\sum_{m\geqslant 0} B^m$, by using purely combinatorial methods: circuit monoid techniques and monomial rearrangements. Moreover, the identity is shown to hold in a non-commutative formal power series algebra.

1. INTRODUCTION

Let $B=(b(i,j))$ be a square matrix of order $n\geqslant 1$ with complex entries and denote by I the identity matrix. Let also $(I-B)_{ji}$ be the matrix obtained from $(I-B)$ by deleting the j-th row and i-th column. If $\det(I-B)\neq 0$, let

$$(I-B)_{ij}^{-\mathrm{cof}}=(-1)^{i+j}\frac{1}{\det(I-B)}\det(I-B)_{ji}\,. \tag{1.1}$$

Of course, (1.1) is the traditional *cofactor formula* for the inverse of $(I-B)$. On the other hand, for each $m\geqslant 0$ let $(B^m)_{ij}$ be the (i,j)-entry of the matrix B^m and define

$$(I-B)_{ij}^{-\mathrm{inv}}=\sum_{m\geqslant 0}(B^m)_{ij}\,. \tag{1.2}$$

Because of the identity

$$(I-B)^{-1}=\sum_{m\geqslant 0}B^m, \tag{1.3}$$

formula (1.2) provides another expression for the inverse of $(I-B)$. In other words,

$$(I-B)_{ij}^{-\mathrm{cof}}=(I-B)_{ij}^{-\mathrm{inv}}. \tag{1.4}$$

The purpose of this paper is to establish a non-commutative version of (1.4) by using combinatorial methods. What is meant by "non-commutative" is the

[*] Supported in part by NSF Grant MCS 77-02113, while the author was on leave at the Department of Mathematics, University of California at San Diego, La Jolla, California 92093.

0001-8708/79/030330–20$05.00/0

following. The n^2 entries $b(i,j)$ $(1 \leqslant i,j \leqslant n)$ of the matrix B are *indeterminates* subject to the following commutation rule: $b(i,j)$ and $b(i',j')$ commute whenever i and i' are distinct (i.e. whenever the indeterminates are not in the same row in B). Two monomials in the $b(i,j)$'s are regarded to be equal if either one can be obtained from the other by a finite sequence of transformations consisting of permuting two successive variables $b(i,j)$ in agreement with the above commutation rule. There is no difficulty in defining the $\mathbb{Z}$-algebra of formal power series in the variables $b(i,j)$'s (still subject to the above commutation rule). Denote it by $\mathbb{Z}[[\mathbf{B}]]$. By using the classical expansion of the determinant of a matrix $A = (a(i,j))$, namely

$$\det A = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{1 \leqslant i \leqslant n} a(i, \sigma i),$$

both determinants $\det(I - B)$ and $\det(I - B)_{ji}$ are well-defined elements of $\mathbb{Z}[[\mathbf{B}]]$. Accordingly, $(I - B)_{ij}^{-\mathrm{cof}}$ defined by (1.1) is also a series in that algebra, as well as $(I - B)_{ij}^{-\mathrm{inv}}$ defined by (1.2). The purpose of this paper is to show that (1.4) holds in $\mathbb{Z}[[\mathbf{B}]]$.

Now by "combinatorial" it is meant that the two series $(I - B)_{ij}^{-\mathrm{cof}}$ and $(I - B)_{ij}^{-\mathrm{inv}}$ must appear as generating functions for sequences of finite structures and the two structure sequences be mapped to one another by an appropriate one-to-one correspondence. Let us illustrate the first point with the series $(I - B)_{ij}^{-\mathrm{inv}}$ after introducing a few basic notations.

In the whole paper n is a fixed positive integer (the order of the matrix B) and the interval $[n] = \{1, 2,..., n\}$, referred to as the *color set*, is denoted by X. A *color word* is a finite sequence $w = x_1 x_2 \cdots x_m$ of elements of X. The integer m is the *length* of w. For each $m \geqslant 0$ the set of all color words of length m is denoted by X^m. Let i and j be two elements of X. Then $X^m(i)$ (resp. $X^m(ij)$) stands for the set of all color words $w = x_1 x_2 \cdots x_m$ of length m starting with $x_1 = i$ (resp. starting with $x_1 = i$ and ending with $x_m = j$). Those words are called *i-linked* (resp. *ij-linked*). Finally, for each non-empty color word $w = x_1 x_2 \cdots x_m$ let

$$\beta(w) = b(x_1, x_2)\, b(x_2, x_3) \cdots b(x_{m-1}, x_m)\, b(x_m, x_1). \tag{1.5}$$

If the last letter of w is regarded as being adjacent with the first one, it is said that $\beta(w)$ records the colors of w *by adjacency*. If with every element s of a finite set S is associated a *monomial* $\alpha(s)$, the following notation will be used throughout

$$\alpha\{S\} = \sum \{\alpha(s) : s \in S\}. \tag{1.6}$$

Now for each $m \geqslant 1$ the (i,j)-entry in the matrix B^m reads

$$(B^m)_{ij} = \sum_{1 \leqslant x_2, \ldots, x_m \leqslant n} b(i, x_2)\, b(x_2, x_3) \cdots b(x_m, j) \tag{1.7}$$

when the $b(k, l)$'s belong to a ring. When the $b(k, l)$'s are subject to the above commutation rule take (1.7) as a definition. Thus $(B^m)_{ij}$ is an element of $\mathbb{Z}[[\mathbf{B}]]$ that, in view of (1.5) and (1.6), may be rewritten as

$$(B^m)_{ii} = \beta\{X^m(i)\} \qquad (m \geqslant 1) \tag{1.8}$$

and for $i \neq j$

$$(B^m)_{ij}\, b(j, i) = \beta\{X^{m+1}(ij)\} \qquad (m \geqslant 1). \tag{1.9}$$

(Note the discrepancy between the case $i = j$ and $i \neq j$.) Therefore (1.2) has the alternate form

$$(I - B)_{ii}^{-\mathrm{inv}} = 1 + \sum_{m \geqslant 1} \beta\{X^m(i)\} \tag{1.10}$$

and for $i \neq j$

$$(I - B)_{ij}^{-\mathrm{inv}}\, b(j, i) = \sum_{m \geqslant 2} \beta\{X^m(ij)\}. \tag{1.11}$$

Thus $(I - B)_{ii}^{-\mathrm{inv}}$ (resp. $(I - B)_{ij}^{-\mathrm{inv}}\, b(j, i)$) is the *generating function* for the sequence $(X^m(i))_{m\geqslant 1}$ (resp. $(X^m(ij))_{m\geqslant 2}$) by β.

Of course, this is the straightforward part of the proof. To do the same for $(I - B)_{ij}^{-\mathrm{cof}}$ requires a more elaborate construction. The series is the product of $1/\det(I - B)$ with a polynomial (the order of the factors matters). As $1/\det(I - B)$ is the generating function for the so-called *circuits* by some function β_{cir} (as was proved in [1]), it is natural to try to find a combinatorial interpretation also in terms of circuits. Without going into the details at this stage let us simply say that for each $m \geqslant 1$ and i, j in X a subclass $\Gamma_m(i)$ (resp. $\Gamma_m(ij)$) of so-called *i-linked* (resp. *ij-linked*) *circuits* can be found with the property that

$$(I - B)_{ii}^{-\mathrm{cof}} = 1 + \sum_{m \geqslant 1} \beta_{\mathrm{cir}}\{\Gamma_m(i)\} \tag{1.12}$$

and for $i \neq j$.

$$(I - B)_{ij}{}^{\mathrm{cof}}\, b(j, i) = \sum_{m \geqslant 1} \beta_{\mathrm{cir}}\{\Gamma_m(ij)\}. \tag{1.13}$$

What remains to be done is to construct for each $m \geqslant 1$ a bijection $w \rightarrow \gamma$ of $X^m(i)$ into $\Gamma_m(i)$ (resp. $X^m(ij)$ onto $\Gamma_m(ij)$) with the property that

$$\beta(w) = \beta_{\mathrm{cir}}(\gamma). \tag{1.14}$$

This will be done with the help of two operators, the *disentangling* operator δ that breaks each color word into basic circuits called *cycles*, and the *entangling* operator ϵ that amalgamates several cycles together to make up a color word.

The paper depends heavily on the theory of circuit monoids developed in [1]. However, with the exceptions of the proof of the unicity of the V-factorization and the determination of the Möbius function of the commutation-rule monoid it is self-contained. The properties on the commutation-rule monoids are recalled in the next section, and those on the circuit monoids in section 5. Identities (1.12) and (1.13) will be derived in section 5 from a basic formula on so-called z-tight words, the latter one presented in section 3. As several formulas involving determinants will be obtained, it will be convenient to isolate them. This is done in section 4. The one-to-one correspondence between color words and linked circuits could have been derived from the main theorem on rearrangements ([1] p. 49). The construction of the correspondence given here has the advantage of being self-contained.

The author wishes to thank Professors Bender and Williamson for helpful conversations, and also for the part they played in securing adequate support.

2. Commutation Rule Monoids

Let Z be a non-empty set. The *free monoid* Z^* generated by Z is the set of all finite *words* $w = z_1 z_2 \cdots z_m$ with $z_1, z_2, ..., z_m$ in Z. The operation in the free monoid is the *juxtaposition product*, the empty word e being the identity element. Let C be a subset of $Z \times Z$ with the property that whenever (z, z') is in C, then $z \neq z'$ and $(z', z) \in C$. The elements z and z' will be said to *commute*. Two words w and w' are said to be *C-adjacent* if there exist two words u, v and a pair (z, z') in C with $w = uzz'v$ and $w' = uz'zv$. Furthermore, two words w and w' are *C-equivalent* if $w = w'$ or if there exists a sequence of words $w_0, w_1, ..., w_p$ with $w_0 = w$, $w_p = w'$, and w_{i-1} and w_i C-equivalent for $1 \leqslant i \leqslant p$. The quotient monoid of Z^* derived by the C-equivalence is called the *C-commutation rule monoid*. It will be denoted by $L(Z; C)$. The C-equivalence class of a one-letter word z will also be denoted by z and that of the empty word by 1. Finally there exists an involution ι of $L(Z; C)$ that is characterized by the formulas

$$\iota(1) = 1, \qquad \iota(z) = z, \qquad \iota(uv) = \iota(v)\,\iota(u) \tag{2.1}$$

for every letter z in Z and u, v in $L(Z; C)$.

The *V-factorization* introduced next provides a system of unique representatives for each C-equivalence class. A subset F of Z is a *commutative part* if it is finite, non-empty and if any two of its elements always commute (i.e. for every z and z' in F with $z \neq z'$, then $(z, z') \in C$). There will be no confusion in using the same letter F for the product

$$F = \prod_{z \in F} z$$

in the monoid $L(Z; C)$. A letter z is said to be *tied* with a subset F of Z if, either $z \in F$, or F contains a letter that does not commute with z. If F and F' are two subsets of Z, then F is *contiguous* to F' if every element of F' is tied with F.

Finally, a sequence $(F_1, F_2, ..., F_r)$ of commutative parts of Z is a *V-factorization* of an element u of $L(Z; C)$ if the following two conditions hold

(i) for $1 \leqslant i \leqslant r - 1$ the part F_i is contiguous to F_{i+1};

(ii) $u = F_1 F_2 \cdots F_r$.

For instance, let $Z = \{1, 2, 3, 4, 5\}$ and C be the subset of the star signs in Figure 1.

	1	2	3	4	5
1		*	*		
2	*		*		*
3	*	*			
4					*
5		*		*	

FIGURE 1

The subsets $F_1 = \{1, 2, 3\}$ and $F_2 = \{2, 5\}$ are commutative parts, and F_2 is contiguous to F_1 for $2 \in F_1$ and 5 does not commute with 3. Furthermore, the element $u = 1\,2\,2\,3\,5\,4\,1\,3$ in $L(Z; C)$ admits the V-factorization

$$(1\,2\,3,\ 2\,5,\ 4,\ 1\,3).$$

Another example of commutation-rule monoid is the monoid **B** generated by the variables $b(i, j)$ $(1 \leqslant i, j \leqslant n)$ with

$$C = \{(b(i, j), b(i', j')) : i \neq i'\}.$$

For the proofs of the next theorem and its two corollaries the reader is referred to ([1] pp. 11–15).

THEOREM 1.2. *Every element u of $L(Z; C)$ admits a unique V-factorization.*

COROLLARY 2.2. *The multiplication in $L(Z; C)$ is simplifiable.*

COROLLARY 2.3. *Let u be an element of $L(Z: C)$ different from 1. Let $(F_1, F_2, ..., F_r)$ be its V-facorization and F be a commutative part of Z. Then, there exists v in $L(Z; C)$ with*

$$u = Fv$$

if and only if $F \subset F_1$.

Next consider the large algebra over $\mathbb{Z}$ of the monoid $L(Z; C)$. The elements of this algebra are formal sums

$$\sum_{u} a(u)u$$

where u runs over all of $L(Z; C)$ and $a(u)$ is an integer. The product of two formal sums is defined by

$$\sum_{u} a(u)u \cdot \sum_{v} b(v)v = \sum_{w} c(w)w$$

with

$$c(w) = \sum_{u \cdot v = w} a(u)\, b(v).$$

There are indeed finitely many pairs (u, v) of $L(Z; C) \times L(Z; C)$ whose product is equal to w. The monoid $L(Z; C)$ has a *Möbius function* μ, that is to say, there exists a function μ with the property that

$$\left(\sum_{v} \mu(u)u\right)^{-1} = \sum_{v} v. \tag{2.2}$$

Note that the right-hand side is the formal sum extended over $L(Z; C)$ whose coefficients are all equal to 1. It is called the *generating function* for $L(Z; C)$.

With $| F |$ denoting the cardinality of the finite set F it was proved in ([1] p. 21, théorème 2.4) that the Möbius function μ of $L(Z; C)$ could be defined by

$$\begin{aligned} \mu(u) &= 0 \text{ if } u \text{ is neither 1, nor a commutative part;} \\ &= (-1)^{|F|} \text{ if } u \text{ is a commutative part } F. \\ &= 1 \text{ if } u = 1. \end{aligned}$$

Accordingly, identity (2.2) may be rewritten as

$$\left(1 + \sum_{F \text{ comm.}} (-1)^{|F|} F\right)^{-1} = \sum_{u \in L(Z; C)} u. \tag{2.4}$$

3. Tight Words

For each z in Z an element u of $L(Z; C)$ is said to be *z-tight* if its V-factorization is of the form

$$(\{z\}, F_2, \ldots, F_r).$$

This means that each word in the C-equivalence class of u starts with z. In particular, each element in F_2 is either equal to z, or does not commute with z. Next denote by μ_z the function on $L(Z; C)$ defined by

$$\begin{aligned}\mu_z(u) &= \mu(u) = (-1)^{|F|} \text{ if } u \text{ is a commutative part } F \text{ and } z \in F;\\ &= 0 \text{ otherwise.}\end{aligned} \tag{3.1}$$

THEOREM 3.1. *The generating function for the z-tight elements of $L(Z; C)$ is given by*

$$\sum_{v\ z\text{-tight}} v = \Big(\sum_u \mu_z(u)u\Big)(-1)\Big(\sum_v \mu(v)v\Big)^{-1}, \tag{3.2}$$

also written

$$\sum_{v\ z\text{-tight}} v = \Big(\sum_{\substack{F\,\text{comm.}\\ F\ni z}} (-1)^{|F|+1}F\Big)\Big(1 + \sum_{F\,\text{comm.}} (-1)^{|F|}F\Big)^{-1}.$$

Note that the order of the factors in the right-hand side of the above identity is essential, as $L(Z; C)$ is not necessarily commutative.

Proof. As

$$\Big(\sum_v \mu(v)v\Big)^{-1} = \sum_v v,$$

only the following identity

$$\sum_{u\ z\text{-tight}} u = \sum_{\substack{F\,\text{comm},\\ F\ni z}} (-1)^{|F|+1}F \cdot \sum_v v$$

is to be verified.

Let $(F_1, F_2, ..., F_r)$ be the V-factorization of an element u in $L(Z; C)$. The coefficient of u in the product of the two series in the right-hand side member is equal to

$$\sum (-1)^{|F|+1},$$

the summation being over all pairs (F, v) with the following properties

(i) F is a commutative part;

(ii) v is in $L(Z; C)$;

(iii) $F \cdot v = u$;

(iv) F contains z.

But corollary 1.3 says that conditions (i), (ii), (iii) hold if and only if $F \subset F_1$. Hence the above coefficient is equal to

$$\sum_{\{z\}\subset F\subset F_1} (-1)^{|F|+1}.$$

In particular, the coefficient is zero if z is not in F_1. If $F_1 = \{z\}$, the only term is the summation is $\{z\}$, so that the coefficient is 1. If $F_1 = \{z\} \cup G_1$ with G_1 non-empty and not containing z, the coefficient is equal to

$$\sum_{G \subset G_1} (-1)^{|G|}.$$

With $|G| = k \geqslant 1$

$$\sum_{G \subset G_1} (-1)^{|G|} = \sum_{0 \leqslant i \leqslant k} (-1)^k \binom{k}{i} = (1-1)^k = 0,$$

Q.E.D.

Remember the involution ι of $L(Z; C)$ defined in (2.1). An element u of $L(Z; C)$ is said to be *z-end tight* if $\iota(u)$ is z-linked, i.e. if all the words in the C-equivalence class of u *end* with z.

COROLLARY 3.2. *The generating function for the z-end tight elements of $L(Z; C)$ is equal to*

$$\sum_{v\ z\text{-end tight}} v = \left(\sum_v \mu(v)v\right)^{-1} (-1) \sum_u \mu_z(u)u. \tag{3.3}$$

Proof. Extend ι to an antihomorphism of the large algebra of $L(Z; C)$ into itself and apply ι to both members of (3.2),

Q.E.D.

4. Some Determinantal Calculations

Before applying the commutation-rule monoid techniques to circuit monoids we isolate in this preliminary section some basic formulas involving determinants.

If $A = (a(i,j))_{(1 \leqslant i,j \leqslant n)}$ is a square matrix, and Y and Y' two subsets of $X = [n]$, the submatrix $(a_{ij})_{(i \in Y, j \in Y')}$ is denoted by $A_{YY'}$.

The next formula is well-known when B is a matrix with entries in a commutative ring. When B is the matrix $(b(i,j))_{(1 \leqslant i,j \leqslant n)}$ whose entries are the basis elements of the monoid $\mathbf{B}$ (see §2), the formula also holds (this time in $\mathbb{Z}[[\mathbf{B}]]$)

$$\det(I - B) = \sum_{Y \subset X} (-1)^{|Y|} \det B_{YY}. \tag{4.1}$$

(By convention, the determinant of the empty matrix is 1.) For each subset Y of X let S_Y denote the permutation group of Y. Then

$$\det B_{YY} = \sum_{\sigma \in S_Y} \epsilon(\sigma) \prod_{k \in Y} b(k, \sigma k). \tag{4.2}$$

Furthermore, if $r(\sigma)$ denotes the ***number of disjoint cycles*** of the permutation σ, let

$$\mu(\sigma) = (-1)^{r(\sigma)}. \tag{4.3}$$

As it will become apparent, there is no ambiguity in using the same letter μ in (2.3) and (4.3). A simple calculation shows that

$$\mu(\sigma) = (-1)^{|Y|}\,\epsilon(\sigma). \tag{4.4}$$

Finally, if Y is non-empty, let

$$\beta_{\text{cir}}(\sigma) = \prod_{k\in Y} b(k, \sigma k) \tag{4.5}$$

and $\beta_{\text{cir}}(\sigma) = 1$ if Y is empty. By (4.2), (4.4) and (4.5) we have

$$(-1)^{|Y|} \det B_{YY} = \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma), \tag{4.6}$$

so that

$$\det(I - B) = \sum_{Y\subset X} \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma). \tag{4.7}$$

In the same manner, formula (4.1) with $(I - B)_{ii}$ (the matrix obtained from $(I - B)$ by deleting the i-th row and i-th column) instead of $(I - B)$ reads

$$\det(I - B)_{ii} = \sum_{Y\subset X\setminus\{i\}} (-1)^{|Y|} \det B_{YY}\,.$$

Hence, by (4.6)

$$\begin{aligned}\det(I - B) - \det(I - B)_{ii} &= \sum_{\{i\}\subset Y\subset X} (-1)^{|Y|} \det B_{YY} \\ &= \sum_{\{i\}\subset Y\subset X} \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma).\end{aligned}$$

Next the cofactor formula (1.1) yields

$$1 - (I - B)_{ii}^{-\text{cof}} = \frac{1}{\det(I - B)}\,(\det(I - B) - \det(I - B)_{ii}),$$

that is

$$1 - (I - B)_{ii}^{-\text{cof}} = \frac{1}{\det(I - B)} \sum_{\{i\}\subset Y\subset X} \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma). \tag{4.8}$$

There is an analogous formula for $(I - B)_{ij}^{-\text{cof}}$ when $i \neq j$. The expansion of $\det(I - B)$ by its j-th row is

$$\det(I - B) = (1 - b(j, j)) \det(I - B)_{jj} + \sum_{k\neq j} (-1)^{j+k}(-b(j, k)) \det(I - B)_{jk}\,. \tag{4.9}$$

In formula (4.5) for $\beta_{\text{cir}}(\sigma)$ to be divisible by $b(j, i)$ it is necessary that $j \in Y$ $i \in Y$ and $\sigma(j) = i$. Hence, the sum of the terms in the (4.7)-expansion of $\det(I - B)$ that are divisible by $b(j, i)$ is equal to

$$\sum_{\{i,j\} \subset Y \subset X} \sum_{\sigma \in S_Y} \mu(\sigma)\, \beta_{\text{cir}}(\sigma)\, \chi(\sigma(j) = i)$$

(making use of the χ-notation dear to Professor Garsia: for each statement E the expression $\chi(E)$ is 1 or 0 depending on whether E is true or false). Comparing the latest expression with (4.9) yields

$$(-1)^{i+j+1}\, b(j, i) \det(I - B)_{ji} = \sum_{\{i,j\} \subset Y \subset X} \sum_{\sigma \in S_Y} \mu(\sigma)\, \beta_{\text{cir}}(\sigma)\, \chi(\sigma(j) = i).$$

Note that $b(j, i)$ commutes with $\det(I - B)_{ji}$. Thus, for $i \neq j$

$$-(I - B)_{ij}^{-\text{cof}}\, b(j, i) = \frac{1}{\det(I - B)} \sum_{\{i,j\} \subset Y \subset X} \sum_{\sigma \in S_Y} \mu(\sigma)\, \beta_{\text{cir}}(\sigma)\, \chi(\sigma(j) = i). \tag{4.10}$$

5. The Circuit Monoid

Again the reader is referred to chapter 4 of [1] for the contents of this section. However all the basic material needed in the rest of the paper is here recorded. The *circuit monoid* is a commutation-rule monoid $L(Z; C)$ with Z and C defined as follows. For every non-empty subset Y of $X(=[n])$ let Z_Y denote the set of all cyclic permutations of Y. Then Z is the disjoint union

$$Z = \bigcup_{\phi \neq Y \subset X} Z_Y.$$

The elements of Z are called *cycles*. A cycle z is of *length m* if $z \in Z_Y$ for some Y with $|Y| = m$. A color word $w = x_1 x_2 \cdots x_m$ is *multilinear* if no letter is repeated in w. Let $w = x_1 x_2 \cdots x_m$ be a non-empty multilinear color word (so $1 \leqslant m \leqslant n$). Then, the cycle z that maps x_1 to $z(x_1) = x_2$, x_2 to $z(x_2) = x_3, \ldots, x_{m-1}$ to $z(x_{m-1}) = x_m$ and x_m to $z(x_m) = x_1$ is denoted by

$$z = \zeta(w). \tag{5.1}$$

Thus, two multilinear words that differ by a cyclic rearrangement of their letters give rise to the same cycle. Now two color words w and w' are *disjoint* if they have no letter in common. If they are both multilinear, the *cycles* $\zeta(w)$ and $\zeta(w')$ are also said to be *disjoint*. Finally, the commutation set C consists of all pairs of *disjoint cycles*. The commutation-rule monoid $L(Z; C)$ so constructed is called the *circuit monoid* and denoted by $\Gamma(X)$. Its elements are the circuits. A *circuit* is then a product

$$\gamma = \zeta(w_1)\,\zeta(w_2)\cdots\zeta(w_r) \tag{5.2}$$

of cycles *not necessarily disjoint*. By definition the *length* of γ is the sum of the lengths of the cycles $\zeta(w_1)$, $\zeta(w_2),\ldots,\zeta(w_r)$ (i.e. the length of the color word $w_1w_2\cdots w_r$. By construction the number $r(\gamma)=r$ of cycles in the product depends only on γ. Whenever $\zeta(w_1)$, $\zeta(w_2),\ldots,\zeta(w_r)$ commute, the product (5.2) may be identified with a permutation σ of a subset Y of X. Actually, Y is the set of all the (distinct) letters of the juxtaposition product $w_1w_2\cdots w_r$, and σ is the product of the *disjoint* cycles $\zeta(w_1)\,\zeta(w_2)\cdots\zeta(w_r)$. The commutative parts of Z are then the *permutations of non-empty subsets of* X.

It follows from (2.3) that the Möbius function μ of $\Gamma(X)$ is defined by

$$\mu(\gamma)=0 \text{ if } \gamma \text{ is not a permutation of a subset of } X, \text{ and} \tag{5.3}$$

$$\mu(\gamma)=(-1)^{r(\gamma)} \tag{5.4}$$

if γ is a permutation of a subset of X (including the empty set).

Thus, definitions of $\mu(\gamma)$ given in (4.3) and (5.4) coincide whenever γ is a permutation.

Identity (2.2) written for the circuit monoid $\Gamma(X)$ reads

$$(\textstyle\sum\mu(\gamma)\,\gamma)^{-1}=\sum\gamma, \tag{5.5}$$

the two series extended over all circuits and μ given by (5.3) and (5.4). Using the notations of the previous section (5.4) is rewritten

$$\Bigl(\sum_{Y\subset X}\sum_{\sigma\in S_Y}\mu(\sigma)\sigma\Bigr)^{-1}=\sum_{\gamma\in\Gamma(X)}\gamma.$$

In (1.5) the monomial $\beta(w)$ was defined for every color word w. Next, if $z=\zeta(w)$ is a cycle with $w=x_1x_2\cdots w_m$, let

$$\beta_{\text{cir}}(z)=\beta(w)=b(x_1,x_2)\,b(x_2,x_3)\cdots b(x_{m-1},x_m)\,b(x_m,x_1). \tag{5.7}$$

In other words, if Y is the set of all distinct letters $\{x_1,x_2,\ldots,x_m\}$ of w, then

$$\beta_{\text{cir}}(z)=\prod_{k\in Y}b(k,z(k)). \tag{5.8}$$

Note again that all the variables $b(i,j)$ commute in the above product, so that the unordered product writing makes sense.

If the two cycles z and z' *commute* (i.e. if they are *disjoint*), then

$$\beta_{\text{cir}}(z)\,\beta_{\text{cir}}(z')=\beta_{\text{cir}}(z')\,\beta_{\text{cir}}(z).$$

Consequently, β_{cir} can be extended to a homomorphism of $\Gamma(X)$ into the monoid $\mathbf{B}$ by letting

$$\begin{aligned}\beta_{\mathrm{cir}}(\gamma) &= 1 \text{ if } \gamma \text{ is the empty circuit}\\ &= \beta_{\mathrm{cir}}(z_1)\,\beta_{\mathrm{cir}}(z_2)\cdots\beta_{\mathrm{cir}}(z_r)\end{aligned}$$

if γ is the product of the cycles $z_1 z_2 \cdots z_r$.

Let σ be a permutation of a non-empty set Y of X. Then σ is the product of some disjoint cycles $z_1 z_2 \cdots z_r$. Hence

$$\begin{aligned}\beta_{\mathrm{cir}}(\sigma) &= \prod_{1\leqslant i\leqslant r} \beta_{\mathrm{cir}}(z_i)\\ &= \prod_{1\leqslant i\leqslant r}\prod_{k\in Y_i} b(k, z_i(k))\end{aligned}$$

for some partition $\{Y_1, Y_2, \ldots, Y_r\}$ of Y. Therefore

$$\beta_{\mathrm{cir}}(\sigma) = \prod_{1\leqslant i\leqslant r}\prod_{k\in Y_i} b(k, \sigma k) = \prod_{k\in Y} b(k, \sigma k).$$

Thus, the definitions of β_{cir} given in (4.5) and (5.9) coincide when restricted to permutations.

PROPOSITION 5.1. *In the algebra* $\mathbb{Z}[[\mathbf{B}]]$ *the following identity holds*

$$(\det(I - B))^{-1} = \sum_{\gamma\in\Gamma(X)} \beta_{\mathrm{cir}}(\gamma) = \sum_{m\geqslant 0} \beta_{\mathrm{cir}}\{\Gamma_m\}. \tag{5.10}$$

Proof. Extend β_{cir} to a homomorphism of the large algebra of $\Gamma(X)$ into $\mathbb{Z}[[\mathbf{B}]]$ by

$$\beta_{\mathrm{cir}} \sum a(\gamma)\gamma = \sum a(\gamma)\,\beta_{\mathrm{cir}}(\gamma).$$

As the *degree* of the monomial $\beta_{\mathrm{cir}}(\gamma)$ is equal to the *length* of γ, this homomorphism is continuous. When applied to identity (5.5), it yields

$$\left(\sum_{Y\subset X}\sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\mathrm{cir}}(\sigma)\right)^{-1} = \sum_{\gamma\in\Gamma(X)} \beta_{\mathrm{cir}}(\gamma),$$

which is the identity to be proved by taking (4.7) into account,

Q.E.D.

6. LINKED CIRCUITS

The results of section 3 on tight elements are now applied to the circuit monoid. Let i, j be two distinct elements of X. A circuit γ is *i-linked* (resp. *ij-linked*) if γ is z-end tight with z a cycle containing i (resp. a cycle containing

i and j and $z(j) = i$). In an equivalent manner, a circuit γ is *i-linked* (resp. *ij-linked*) if *all* the factorizations $z_1 z_2 \cdots z_s$ of γ as products of cycles have the following properties

(i) i is a letter of z_s (resp. i and j are letters of z_s and $z_s(j) = i$);

(ii) z_{s-1} and z_s are not disjoint.

In the following example the circuit

$$\gamma = \zeta(28)\,\zeta(39)\,\zeta(1352) = \zeta(39)\,\zeta(28)\,\zeta(1352)$$

is i-linked for each $i = 1, 3, 5, 2$ and ij-linked for the pairs (3, 1), (5, 3), (2, 5), (1, 2).

For each $m \geqslant 1$ let $\Gamma_m(i)$ (resp. $\Gamma_m(ij)$) be the set of all i-linked (resp. ij-linked) circuits of length m. Also let $\Gamma(i)$ (resp. $\Gamma(ij)$) be the union of the $\Gamma_m(i)$'s (resp. $\Gamma_m(ij)$'s) for $m \geqslant 1$. Note that $\Gamma_m(ij)$ is empty for $m = 1 (i \neq j)$.

Proposition 6.1. *The following identity holds in* $\mathbb{Z}[[\mathbf{B}]]$

$$(I - B)_{ii}^{-\mathrm{cof}} - 1 = \sum_{\gamma \in \Gamma(i)} \beta_{\mathrm{cir}}(\gamma) = \sum_{m \geqslant 1} \beta_{\mathrm{cir}}\{\Gamma_m(i)\}.$$

Proof. Clearly

$$\sum_{\gamma \in \Gamma(i)} \gamma = \sum_{z \ni i} \sum_{\gamma\ z\text{-end tight}} \gamma,$$

the first summation on the right-hand side being over all cycles z containing i. But from corollary 3.2

$$\sum_{\gamma\ z\text{-end tight}} \gamma = \left(\sum \mu(\gamma)\gamma\right)^{-1} (-1) \sum \mu_z(\gamma)\gamma.$$

It follows from (3.1) and (5.3) that $\mu_z(\gamma) = (-1)^r$ if γ is a product of r disjoint cycles including z (write $\gamma \ni z$). Otherwise $\mu_z(\gamma) = 0$. Therefore

$$\sum_{\gamma\ z\text{-end tight}} \gamma = \left(\sum \mu(\gamma)\gamma\right)^{-1} (-1) \sum_{\gamma \ni z} \mu(\gamma)\gamma.$$

But a permutation γ contains the cycle z and z contains i if and only if γ is a permutation of a subset Y of X with $i \in Y$. Thus

$$\begin{aligned}\sum_{\gamma \in \Gamma(i)} \gamma &= \sum_{z \ni i} \sum_{\gamma\ z\text{-end tight}} \gamma \\ &= -\left(\sum \mu(\gamma)\gamma\right)^{-1} \sum_{z \ni i} \sum_{\gamma \ni z} \mu(\sigma)\sigma \\ &= -\left(\sum \mu(\gamma)\gamma\right)^{-1} \sum_{\{i\} \subset Y \subset X} \sum_{\sigma \in S_Y} \mu(\sigma)\sigma.\end{aligned}$$

Now applying the homomorphism β_{cir} to both members yields

$$\sum_{\gamma\in\Gamma(i)} \beta_{\text{cir}}(\gamma) = -\Big(\sum \mu(\gamma)\,\beta_{\text{cir}}(\gamma)\Big)^{-1} \sum_{\{i\}\subset Y\subset X}\ \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma),$$

that is,

$$\sum_{\gamma\in\Gamma(i)} \beta_{\text{cir}}(\gamma) = -\frac{1}{\det(I-B)} \sum_{\{i\}\subset Y\subset X}\ \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma)$$

by (5.3), (5.10) and (4.7). The right-hand side member is equal to $(I-B)_{ii}^{-\text{cof}} - 1$ by (4.8),

Q.E.D.

The analogous result for the ij-linked circuits in stated next.

Proposition 6.2. *The following identity holds*

$$(I-B)_{ij}^{-\text{cof}}\, b(j,i) = \sum_{\gamma\in\Gamma(ij)} \beta_{\text{cir}}(\gamma) = \sum_{m\geqslant 2} \beta_{\text{cir}}\{\Gamma_m(ij)\}. \tag{6.2}$$

Proof. In the same manner

$$\begin{aligned}\sum_{\gamma\in\Gamma(ij)} \gamma &= \sum_{z\ni j,\, z(j)=i}\ \sum_{\gamma\ z\text{-end tight}} \gamma\\ &= -\Big(\sum \mu(\gamma)\gamma\Big)^{-1} \sum_{z\ni j,\, z(j)=i}\ \sum_{\gamma\ni z} \mu(\gamma)\gamma\\ &= -\Big(\sum \mu(\gamma)\gamma\Big)^{-1} \sum_{\{i,j\}\subset Y\subset X}\ \sum_{\sigma\in S_Y} \mu(\sigma)\,\sigma\,\chi(\sigma(j)=i).\end{aligned}$$

The image under β_{cir} reads

$$\begin{aligned}\sum_{\gamma\in\Gamma(ij)} \beta_{\text{cir}}(\gamma) &= -\frac{1}{\det(I-B)} \sum_{\{i,j\}\subset Y\subset X}\ \sum_{\sigma\in S_Y} \mu(\sigma)\,\beta_{\text{cir}}(\sigma)\,\chi(\sigma(j)=i)\\ &= (I-B)_{ij}^{-\text{cof}}\, b(j,i)\end{aligned}$$

by (4.10),

Q.E.D.

7. The Correspondence

The identities (1.10), (1.11), (1.12) and (1.13) being now established, there remains to construct for each $m \geqslant 1$ a bijection $w \to \gamma$ of $X^m(i)$ (resp. $X^m(ij)$) to $\Gamma_m(i)$ (resp. $\Gamma_m(ij)$) with the property that $\beta(w) = \beta_{\text{cir}}(\gamma)$. Roughly speaking, the bijection $w \rightarrow \gamma$ described in theorem 7.2 below consists of removing multilinear factors from w, making up cycles out of them and taking the product of those cycles in $\Gamma(X)$. More precisely, the construction goes as follows.

Let $w = x_1 x_2 \cdots x_m$ be a non-empty color word. A non-empty factor $d = x_k x_{k+1} \cdots x_l$ $(1 \leqslant k < l \leqslant m)$ is said to be *prime* if the following properties hold

(i) d multilinear;

(ii) either $1 = k < l = m$ and w itself is multilinear, or $l + 1 \leqslant m$ and $x_k = x_{l+1}$;

(iii) the words $w_1 = x_1 x_2 \cdots x_{k-1}$ and $d = x_k x_{k+1} \cdots x_l$ are disjoint.

For instance, the two squared factors in the following example are prime factors of w.

$$w = 1 \; \boxed{3\;4} \; 3\;4\;6 \; \boxed{9\;5\;2} \; 9\;6\;3\;8\;1\;5\;7\;5\;2\;8\;2.$$

LEMMA 7.1. *Any two prime factors of a word w do not overlap.*

Proof. Let $d = x_k x_{k+1} \cdots x_l$ and $d' = x_{k'} x_{k'+1} \cdots x_{l'}$ be two prime factors of w with $k \leqslant k'$ and $(k, l) \neq (k', l')$. If d and d' overlapped, one of the following conditions would hold

(i) $k = k' < l' < l$; (ii) $k = k' < l < l'$; (iii) $k < k' < l' < l$; (iv) $k < k' < l' = l$; (v) $k < k' < l < l'$.

Cases (i), (iii) and (iv) (resp. case (ii)) cannot hold because d (resp. d') is multilinear. In case (v) the letter x_k occurs in $x_1 x_2 \cdots x_{k'-1}$ and x_{l+1} in $d' = x_{k'} x_{k'+1} \cdots x_{l'}$. As $x_k = x_{l+1}$, axiom (iii) of the prime factor definition would be violated for d', Q.E.D.

Axiom (iii) above together with the lemma imply that any two prime factors of a word w are *disjoint*. Let $P(w)$ be the set of all prime factors of w. The product

$$\Pi(w) = \prod_{d \in P(w)} \zeta(d) \tag{7.1}$$

in the circuit monoid $\Gamma(X)$, is a *commutative part*. Each element $\zeta(d)$ in this product will be referred to as a *prime cycle* of w.

It also follows from lemma 7.1 that, if $P(w)$ has p elements, w factorizes as

$$w = v_1 d_1 v_2 d_2 \cdots v_p d_p v_{p+1} \tag{7.2}$$

where

(i) $d_1, d_2, \ldots, d_p$ are the p elements of $P(w)$;

(ii) v_1 is multilinear;

(iii) $v_1, v_2, \ldots, v_{p+1}$ are non-empty words with the possible exception of v_1 and v_{p+1}.

With these notations let $R(w)$ be the juxtaposition product

$$R(w) = v_1 v_2 v_3 \cdots v_p v_{p+1}\,, \tag{7.3}$$

that is, the word obtained from w by deleting all its prime factors. Of course, $R(w)$ is empty if and only if w is multilinear, and in this case $\Pi(w) = \zeta(w)$. The map R can be iterated and for each color word w it makes sense to define $h = h(w)$ as the *smallest* non-negative integer with the property that $R^h(w)$ *is empty*. The product

$$\delta^*(w) = \Pi(w) \cdot \Pi R(w) \cdot \cdots \cdot \Pi R^{h-1}(w) \tag{7.4}$$

in $\Gamma(X)$ will then be a circuit of the same length as w.

THEOREM 7.2. *Let i, j be two distinct elements of X and $m \geqslant 1$. Then δ^* defined by* (7.4) *is a bijection of $X^m(i)$* (resp. $X^m(ij)$) *onto $\Gamma_m i)$* (resp. $\Gamma_m(ij)$) *with the property that*

$$\beta(w) = \beta_{\mathrm{cir}}\delta^*(w). \tag{7.5}$$

With the same example as above

$$w = 1\ \boxed{3\ 4}\ 3\ 4\ 6\ \boxed{9\ 5\ 2}\ 9\ 6\ 3\ 8\ 1\ 5\ 7\ 5\ 2\ 8\ 2;$$

$$\Pi(w) = \zeta(34)\,\zeta(952); \quad R(w) = 1\ 3\ 4\ \boxed{6\ 9}\ 6\ 3\ 8\ 1\ \boxed{5\ 7}\ 5\ 2\ 8\ 2$$

$$\Pi R(w) = \zeta(69)\,\zeta(57); \quad R^2(w) = 1\ \boxed{3\ 4\ 6}\ 3\ 8\ 1\ 5\ 2\ 8\ 2$$

$$\Pi R^2(w) = \zeta(346); \quad R^3(w) = \boxed{1\ 3\ 8}\ 1\ 5\ 2\ 8\ 2;$$

$$\Pi R^3(w) = \zeta(138); \quad R^4(w) = 1\ 5\ \boxed{2\ 8}\ 2;$$

$$\Pi R^4(w) = \zeta(28); \quad R^5(w) = \boxed{1\ 5\ 2};$$

$$\Pi R^5(w) = \zeta(152); \quad R^6(w) = e.$$

Thus

$$\delta^*(w) = \zeta(34)\,\zeta(952) \mid \zeta(69)\,\zeta(57) \mid \zeta(346) \mid \zeta(138) \mid \zeta(28) \mid \zeta(152).$$

The vertical bars indicate the V-factorization of $\delta^*(w)$. Note that $w \in X^{20}(1, 2)$ and $\delta^*(w)$ is a 1, 2-linked circuit of length 20. It can be verified that

$$\beta(w) = b(1, 3)\, b(3, 4) \cdots b(8, 2)\, b(2, 1) \qquad \text{and}$$

$$\beta_{\mathrm{cir}}\delta^*(w) = b(3, 4)\, b(4, 3)\, b(9, 5) \cdots b(5, 2)\, b(2, 1)$$

are two identical elements of **B**.

The proof of theorem 7.2 requires several lemmas. The construction of the inverse bijection ϵ^* of δ^* will also be given.

LEMMA 7.3. *Let w be a non-empty non-multilinear color word. Then, every prime factor of $R(w)$ has a letter in common with some prime factor of w.*

Proof. Keep the above notations (7.2) and (7.3). Let d be a prime factor of $R(w)$. As the first letters of d_i and v_{i+1} are equal for $i = 1, 2, \ldots, p$ (axiom (ii)), d cannot be a right factor of v_i, that is, a factorization such as $v_i = w_i d$ cannot hold. If $v_i = w_i d w_i'$ with w_i' nonempty, then $i \geqslant 2$ because v_1 is multilinear. In the case $i \geqslant 2$ the factor d is disjoint with each of the words $v_1, \ldots, v_{i-1}, w_i$ (axiom (iii)). If it were also disjoint with all the words $d_1, \ldots, d_{i-1}$, then d would belong to $P(w)$. Finally, if d overlaps with the end of a factor v_i and the beginning of $v_{i+1} (1 \leqslant i \leqslant p)$, then d has a letter in common with d_{i-1}, Q.E.D.

With the notion of contiguity introduced in section 5 another way of stating lemma 7.3 is to say that either $R(w)$ is empty, or the commutative part $\Pi(w)$ is contiguous to the commutative part $\Pi R(w)$.

Let $E(X^m(i))$ (resp. $E(X^m(ij))$) be the set of all pairs (F, w) with the following properties

(i) F is a commutative part of $\Gamma(X)$;

(ii) w is a color word;

(iii) either w is empty and F consists of a single i-(resp. ij-) linked cycle, or w is an i-(resp. ij-) linked color word and F is contiguous to $\Pi(w)$;

(iv) the sum of the lengths of F and w is m.

The *disentangling* operator δ is defined by

$$\delta(w) = (\Pi(w), R(w)) \tag{7.6}$$

with $\Pi(w)$ and $R(w)$ shown in (7.1) and (7.3).

From the remark stated just after lemma 7.3, it follows that δ maps $X^m(i)$ (resp. $X^m(ij)$) into $E(X^m(i))$ (resp. $E(X^m(ij))$). The inverse operator is defined next.

Let $z = \zeta(y_1 y_2 \cdots y_q)$ be a cycle and $w = x_1 x_2 \cdots x_{m'}$ be a non-empty color word. Assume that z and w are non-disjoint. Denote by s the least integer with the property that $x_s = y_t$ for some $t = 1, 2, \ldots, q$. Then $\epsilon_z(w)$ is defined to be the color word

$$\epsilon_z(w) = x_1 \cdots x_{s-1} y_t y_{t+1} \cdots y_q y_1 \cdots y_{t-1} x_s \cdots x_{m'} . \tag{7.7}$$

For instance, if $z = \zeta(295)$ and $w = 1\ 3\ 4\ 6\ 9\ 6\ 3\ 8\ 1\ 5\ 7\ 2\ 8\ 2$, then

$$\epsilon_z(w) = 1\ 3\ 4\ 6\ \boxed{9\ 5\ 2}\ 9\ 6\ 3\ 8\ 1\ 5\ 7\ 2\ 8\ 2.$$

(The inserted factor has been squared.)

Now let F be a commutative part $F = z_1 z_2 \cdots z_r$ and assume that *none* of the cycles $z_k (1 \leqslant k \leqslant r)$ is disjoint with w. Define the *entangling* operator ϵ to be

$$\epsilon(F, w) = \epsilon_{z_1} \epsilon_{z_2} \cdots \epsilon_{z_r}(w). \tag{7.8}$$

As the cycles $z_1, z_2, \ldots, z_r$ are disjoint, the r factors that are successively inserted into w do not overlap. On the other hand, $\epsilon(F, w)$ does not depend on the order in which the operators $\epsilon_{z_1}, \epsilon_{z_2}, \ldots, \epsilon_{z_r}$ are applied to w, so that notation (7.8) makes sense. Finally, the r factors inserted are *prime* factors of $\epsilon(F, w)$. They are also the *only ones*, because if $\zeta(d)$ was a prime cycle of $\epsilon(F, w)$ not in F, a fortiori $\zeta(d)$ would be a prime cycle of w. Hence, a prime cycle of w and F would be disjoint, i.e. F would not be contiguous to $\Pi(w)$. Thus

$$\Pi\epsilon(F, w) = F. \tag{7.9}$$

For instance, take $F = \zeta(34)\, \zeta(295)$ and

$$w = 1\ 3\ 4\ \boxed{6\ 9}\ 6\ 3\ 8\ 1\ \boxed{5\ 7}\ 5\ 2\ 8\ 2.$$

Then

$$\epsilon(F, w) = 1\ \boxed{3\ 4}\ 3\ 4\ 6\ \boxed{9\ 5\ 2}\ 9\ 6\ 3\ 8\ 1\ 5\ 7\ 5\ 2\ 8\ 2.$$

The squared factors are indeed the only prime factors of $\epsilon(F, w)$.

If (F, w) belongs to $E(X^m(i))$ (resp. $E(X^m ij)))$) and if w is non-empty, the color word $\epsilon(F, w)$ is well-defined. If w is empty, let $\epsilon(F, w)$ be the unique color word v in $X^m(i)$ (resp. $X^m(ij)$) with

$$\zeta(v) = F.$$

For instance, with $i = 1, j = 2$, $\epsilon(\zeta(521), e) = 152$.

Lemma 7.4. *The entangling operator ϵ is a bijection of $E(X^m(i))$* (resp. *$E(X^m(ij))$*) *onto $X^m(i)$* (resp. *$X^m(ij)$*). *The disentangling operator δ is the inverse of ϵ.*

Proof. Let (F, w) be in $E(X^m(i))$ (resp. $E(X^m(ij))$). If w is empty, we already know that $\epsilon(F, w)$ is in $X^m(i)$ (resp. $X^m(ij)$). If w is nonempty, let $w = x_1 x_2 \cdots x_{m'}$ with $x_1 = i$ (resp. $x_1 = i$, $x_{m'} = j$). With the notations of (7.7), either $x_s = y_t \neq i$ and $s \geqslant 2$, or $x_s = y_t = i$ and $s = 1$. In both cases the word $\epsilon_z(w)$ written in (7.7) starts with i (resp. starts with i and ends with j). Thus, by induction on the number of cycles in F, the word $\epsilon(F, w)$ is in $X^m(i)$ (resp. $X^m(ij)$).

Next from (7.6) and (7.9)

$$\delta\epsilon(F, w) = (\Pi\epsilon(F, w), R\,\epsilon(F, w)) = (F, w).$$

The other identity

$$\epsilon\delta(w) = \epsilon(\Pi(w), R(w)) = w$$

is obvious by (7.2), (7.3) and (7.7),

Q.E.D.

Let w be an i-(resp. ij-) linked color word of length m. The definition of $\delta^*(w)$ given in (7.4) may be restated as follows. Let

$$\delta(w) = (F_1, w_1), \delta(w_1) = (F_2, w_2), \ldots, \delta(w_{h-1}) = (F_h, w_h) \tag{7.10}$$

with $w_h = e$. Then

$$\delta^*(w) = F_1 F_2 \cdots F_h . \tag{7.11}$$

As each pair (F_k, w_k) belongs to $E(X^{m'}(i))$ (resp. $E(X^{m'}(ij))$) for some m', each F_k is contiguous to F_{k+1} for $k = 1, 2, \ldots, h-1$. Hence, $(F_1, F_2, \ldots, F_h)$ is the V-factorization of the circuit $\delta^*(w)$. On the other hand, as w_h is empty, the commutative part F_h consists of a single i-(resp. ij-) linked cycle. Therefore $\delta^*(w)$ is an i-(resp. ij-) *linked circuit.*

Conversely, let $(F_1, F_2, \ldots, F_h)$ be the V-factorization of an i-(resp. ij-) linked circuit γ. It follows from lemma 7.4 that it makes sense to define a sequence of color words $(w_{h-1}, w_{h-2}, \ldots, w_1, w)$ by

$$\begin{aligned} w_{h-1} &= \epsilon(F_h, e), & w_{h-2} &= \epsilon(F_{h-1}, w_{h-1}), \ldots, \\ w_1 &= \epsilon(F_2, w_2), & w &= \epsilon(F_1, w_1). \end{aligned} \tag{7.12}$$

Then, let

$$w = \epsilon^*(\gamma). \tag{7.13}$$

As F_h consists of a single i-(resp. ij-) linked cycle, the *color word* w is i-(resp. ij-) *linked.*

Lemma 7.4 also implies that $\delta^*\epsilon^*$ and $\epsilon^*\delta^*$ are identity maps.

There remains to prove (7.5). Take again the notations of lemma 7.1. If $d = x_k x_{k+1} \cdots x_l$ is a prime factor of $w = x_1 x_2 \cdots x_m$, then

$$\begin{aligned} \beta(w) = b(x_1, x_2) \cdots b(x_{k-1}, x_k)\, b(x_k, x_{k+1}) \cdots b(x_l, x_{l+1}) \\ \times b(x_{l+1}, x_{l+2}) \cdots b(x_{m-1}, x_m)\, b(x_m, x_1). \end{aligned}$$

As $x_k = x_{l+1}$, and $x_1 \cdots x_{k-1}$ and d are disjoint, this can be rewritten

$$\beta(w) = \beta(d)\, \beta(x_1 \cdots x_{k-1} x_{l+1} \cdots x_m).$$

By induction on the number of prime factors

$$\beta(w) = \prod_{d \in P(w)} \beta(d) \cdot \beta R(w)$$
$$= \beta_{\mathrm{cir}} \Pi(w) \cdot \beta R(w).$$

Next by induction on h

$$\beta(w) = \beta_{\mathrm{cir}} \Pi(w) \cdot \beta_{\mathrm{cir}} \Pi R(w) \cdot \cdots \cdot \beta_{\mathrm{cir}} \Pi R^{h-1}(w)$$
$$= \beta_{\mathrm{cir}} \delta^*(w).$$

This completes the proof of the theorem 7.2.

Reference

1. P. Cartier and D. Foata, Problèmes combinatoires de commutation et réarrangements, Lecture Notes in Mathematics, No. 85, Springer-Verlag, Berlin/Heidelberg/New York, 1969.