Jan. 30, 1998

INVERSES OF WORDS

Dominique Foata and Guo-Niu Han

Abstract. The inverse of a permutation is one of the basic operations in the symmetric group. In this paper we propose an extension of this operation to words (with repetitions) by constructing an explicit one-to-one transformation on words. We also show that there exists another transformation having one more property that would be the definitive bijection for deriving the inverse of a word. The open problem is to imagine its construction.

1. Introduction

Back in the Fall of 1997 we received a letter from Don Knuth [Kn97] saying the following: "While proofreading the new edition of my book *Sorting and Searching*, I ran across a remark in the last paragraph of the answer to exercise 5.1.2-14 that I had forgotten (page 583 of the first edition). Basically it asks for a bijective way to define the inverse of a multiset permutation (word). Has anybody come up with a satisfactory solution of that problem?"

Well, the immediate reaction was to go back to the theory of partially commutative monoids, where the notion of *cycle* (see [CF69]) had been introduced and try to use the result on unique decomposition of words. As we shall see, we can come up with a satisfactory answer that is developed in the next two sections. However an easy calculation on q-multinomial coefficients shows that there exists another transformation on words having one more property that would make it the definitive bijection to define the inverse of a word. In the last section we give the list of the properties of that ideal transformation and invite the reader to imagine its construction.

Let us first recall the basic properties of the inverse of a permutation. If $\sigma = \sigma(1)\sigma(2)\ldots\sigma(n)$ is a permutation of order n, its *inverse* σ^{-1} is defined by $\sigma^{-1}(\sigma(i)) = i$ for all i and its *number of inversions* "inv" by

$$\operatorname{inv}\sigma = \#\{(i,j) : 1 \le i < j \le n,\ \sigma(i) > \sigma(j)\}.$$

For the material on Young tableaux and the Robinson-Schensted correspondence the reader is referred to the book by Knuth [Kn73, pp. 52].

That famous correspondence maps each permutation σ onto an ordered pair of standard Young tableaux (P, Q) of the same shape. We shall denote it by $\sigma \mapsto (P, Q)$.

Let us enumerate some basic properties of the inverse.

(P1) The map $\sigma \mapsto \sigma^{-1}$ is involutive.

(P2) Each pair $(i, \sigma(i))$ is mapped onto the pair $(\sigma(i), i)$.

(P3) The number of inversions "inv" is preserved under the transformation $\sigma \mapsto \sigma^{-1}$, i.e., $\operatorname{inv} \sigma^{-1} = \operatorname{inv} \sigma$.

(P4) If $\sigma \mapsto (P, Q)$, then $\sigma^{-1} \mapsto (Q, P)$.

Our two results are the following.

1) In section 2 we construct an explicit transformation $w \mapsto w^*$ that extends the inverse mapping $\sigma \mapsto \sigma^{-1}$ to words. Furthermore, the properties (P1), (P2), (P3), once suitably reinterpreted for dealing with words, also hold (section 3).

2) In section 4 we prove the *existence* of a transformation that has all the properties (P1), (P2), (P3), (P4) adapted to words. However the explict construction of such a transformation is still an open problem.

2. The transformation

For convenience, let X be the alphabet $\{1, 2, \ldots, r\}$. If $\mathbf{c} = (c_1, c_2, \ldots, c_r)$ is a sequence of r nonnegative integers, then $1^{c_1} 2^{c_2} \ldots r^{c_r} = y_1 y_2 \ldots y_m$ is a nondecreasing word of length m with $m = c_1 + c_2 + \cdots + c_r$ and $y_1 = \cdots = y_{c_1} = 1$, $y_{c_1+1} = \cdots = y_{c_1+c_2} = 2, \ldots, y_{c_1+\cdots+c_{r-1}+1} = \cdots = y_m = r$. Denote by $R(\mathbf{c})$ be the set of all rearrangements of the word $y_1 y_2 \ldots y_m$.

A *circuit* is defined to be an ordered pair $\begin{pmatrix} u \\ v \end{pmatrix}$, where the words $u = y_1 y_2 \ldots y_m$ and $v = x_1 x_2 \ldots x_m$ are rearrangements of each other.

We use the following commutation rule for two adjacent biletters

$$(\spadesuit) \qquad \begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} \quad \text{if and only if } a \neq c$$

to change a circuit to another. Two circuits $\begin{pmatrix} u \\ v \end{pmatrix}$ and $\begin{pmatrix} u_1 \\ v_1 \end{pmatrix}$ are said to be *equivalent*, if we can go from one to the other by a finite sequence of adjacent transpositions of bi-letters as defined in ($\spadesuit$).

Construction of the transformation $w \mapsto w^*$. Let w be a word in $R(\mathbf{c})$. We first form the circuit $\Gamma(w) = \begin{pmatrix} \overline{w} \\ w \end{pmatrix}$, where $\overline{w}$ is the nondecreasing rearrangement of w. Using the same example as in [Lo83 p. 199] namely $w = 31514226672615$, we get

$$\Gamma(w) = \begin{pmatrix} \overline{w} \\ w \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 4 & 5 & 5 & 6 & 6 & 6 & 7 \\ 3 & 1 & 5 & 1 & 4 & 2 & 2 & 6 & 6 & 7 & 2 & 6 & 1 & 5 \end{pmatrix}.$$

Next we form the *dominated circuit factorization* of the circuit $\Gamma(w)$ as described in [Lo83 p. 199]

$$\Gamma(w) = \begin{pmatrix} 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 2 & 2 & 6 \\ 6 & 4 & 2 & 2 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix} \begin{pmatrix} 5 & 1 & 6 \\ 6 & 5 & 1 \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix}.$$

Now such a circuit can be decomposed into a product of *cycles*. The theory is not made in [Lo83], but is made in [CF69] (see page 42, Proposition 4.1). It is also discussed in [Kn73, theorem C, p. 28]. With the previous example

$$\Gamma(w) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 4 & 2 & 6 \\ 6 & 4 & 2 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix} \begin{pmatrix} 5 & 1 & 6 \\ 6 & 5 & 1 \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix}.$$

As shown in [CF69, p. 42] or [Kn73, p. 28] the above factorization ("decomposition") is *unique* in the sense that if two such factorizations are equal to the same $\Gamma(w)$ we can go from the first one to the second by a finite sequence of elementary transformations consisting of permuting two consecutive cycles having no letter in common.
Having such a product we can take the inverse of each cycle consisting of permuting the top and the bottom rows within each cycle. Call it $\tau\,\Gamma(w)$:

$$\tau\,\Gamma(w) = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 6 & 4 & 2 \\ 4 & 2 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix} \begin{pmatrix} 6 & 5 & 1 \\ 5 & 1 & 6 \end{pmatrix} \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix}.$$

Next using the commutation rule (♠) we rearrange the above product $\tau\,\Gamma(w)$ in such a way that the top row is nondecreasing. We get a circuit that corresponds to a rearrangement w^* of w:

$$\Gamma(w^*) = \begin{pmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 4 & 5 & 5 & 6 & 6 & 6 & 7 \\ 2 & 1 & 6 & 3 & 6 & 2 & 1 & 2 & 1 & 7 & 4 & 6 & 5 & 5 \end{pmatrix}.$$

The word w^* is defined as the bottom row of the previous two-matrix, that is

$$w^* = 21636212174655.$$

The above construction can be described as the sequence:

$$(\clubsuit) \qquad w \mapsto \Gamma(w) = \begin{pmatrix} \overline{w} \\ w \end{pmatrix} \mapsto \begin{pmatrix} u \\ v \end{pmatrix} \overset{\tau}{\mapsto} \begin{pmatrix} v \\ u \end{pmatrix} \mapsto \Gamma(w^*) = \begin{pmatrix} \overline{w} \\ w^* \end{pmatrix} \mapsto w^*.$$

Note that the unique decompositions $\binom{u}{v}$ and $\binom{v}{u}$ are equivalent to the two circuits $\Gamma(w)$ and $\Gamma(w^*)$, respectively.

Remark. In a subsequent letter [Kn98] Knuth told us that he had thought of the same construction for $w \mapsto w^*$.

3. Properties

Let $w = x_1 x_2 \ldots x_m$ belong to $R(\mathbf{c})$. When dealing with words (with repetitions) two kinds of inversions can be introduced, the *internal* and the *external* inversions. An *internal inversion* of a word $w = x_1 x_2 \ldots x_m$ in $R(\mathbf{c})$ is an inversion that occurs *inside* any one of the r factors $x_1 \ldots x_{c_1}$, $x_{c_1+1} \ldots x_{c_1+c_2}$, $\ldots$, $x_{c_1+\cdots+c_{r-1}+1} \ldots x_m$ of the word w. An *external inversion* is an inversion of two letters belonging to two different factors. Let $\operatorname{intinv} w$ (resp. $\operatorname{extinv} w$) denote the number of internal (resp. external) inversions of the word w. Of course, $\operatorname{intinv} + \operatorname{extinv} = \operatorname{inv}$, the usual number of inversions. If w has no repetitions (if it is a permutation), then $\operatorname{intinv} w = 0$ while $\operatorname{extinv} w = \operatorname{inv} w$.

Let $\binom{u}{v}$ be a circuit. Remember that $u = y_1 y_2 \ldots y_m$ and $v = x_1 x_2 \ldots x_m$ are rearrangements of each other and v is *not* necessarily nondecreasing. The *number of external inversions* $\operatorname{extinv} \binom{u}{v}$ of the circuit $\binom{u}{v}$ is defined to be the number of pairs (i, j) such that $1 \le i < j \le m$ and either $y_i < y_j$ and $x_i > x_j$, or $y_i > y_j$ and $x_i < x_j$.

Proposition 1. *Let $\overline{w}$ be the nondecreasing rearrangement of a word w and let u, v, u_1, v_1 be four rearrangements of w. Then*

(E1) $\operatorname{extinv} \binom{\overline{w}}{w} = \operatorname{extinv} w$;

(E2) $\operatorname{extinv} \binom{u}{v} = \operatorname{extinv} \binom{v}{u}$;

(E3) If two circuits $\binom{u}{v}$ and $\binom{u_1}{v_1}$ are equivalent, then

$$\operatorname{extinv} \binom{u}{v} = \operatorname{extinv} \binom{u_1}{v_1}.$$

Proof: When the top word in a biword is the nondecreasing rearrangement of the bottom word w, the definitions of "extinv" for the circuit $\binom{\overline{w}}{w}$ and for the word w coincide. Property (E2) is the extension to words of the invariance of the inversion number when a permutation is mapped onto its inverse. Property (E3) is true for two circuits differing by a transposition of two adjacent letters satisfying (♠) and then holds for two equivalent circuits. □

Theorem 2. *The transformation $w \mapsto w^*$ is a bijection of $R(\mathbf{c})$ onto itself having the following properties*

(W0) If $w = \sigma$ is a permutation, then $w^* = \sigma^{-1}$;

(W1) $w \mapsto w^*$ is an involution;

(W2) For each biletter $\binom{y}{x}$, the number of occurrences of the biletter $\binom{y}{x}$ in $\binom{\overline{w}}{w}$ is equal to the number of occurrences of the biletter $\binom{x}{y}$ in $\binom{\overline{w}}{w^*}$.

(W3) $\operatorname{extinv} w = \operatorname{extinv} w^*$;

Proof: Properties (W0), (W1), (W2) follows immediately from the construction of $w \mapsto w^*$ described in (♣). Property (W3) is a consequence of both (♣) and Proposition 1. $\square$

Example. With w and w^* derived in section 2 we have $\operatorname{extinv} w^* = \operatorname{extinv} w = 27$. Here $\operatorname{intinv} w^* = \operatorname{intinv} w = 4$ and $\operatorname{inv} w^* = \operatorname{inv} w = 31$, but this is a simple coincidence (see the example at the end of section 4.)

4. Another analogue?

For each word w and each element $i = 1, 2, \ldots, r$ in the alphabet let $|w|_i$ denote the number of letters of w equal to i. Let $A = (a(i,j))$ be an $r \times r$ matrix with nonnegative coefficients such that the sum of the entries in the first row and also in the first column is c_1, ... , the sum of the entries in the r-th row and also in the r-th column is c_r. Let $w = x_1 x_2 \ldots x_m$ belong to $R(\mathbf{c})$. It is said to be *of A-type*, if the following conditions hold:

$$|x_1 \ldots x_{c_1}|_1 = a(1,1),\ \ldots\ , |x_1 \ldots x_{c_1}|_r = a(1,r);$$
$$|x_{c_1+1} \ldots x_{c_1+c_2}|_1 = a(2,1),\ \ldots\ , |x_{c_1+1} \ldots x_{c_1+c_2}|_r = a(2,r);$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$|x_{c_1+\cdots+c_{r-1}+1} \ldots x_m|_1 = a(r,1),\ \ldots\ , |x_{c_1+\cdots+c_{r-1}+1} \ldots x_m|_r = a(r,r).$$

When $c_1 = c_2 = \cdots = c_r = 1$, each word w in $R(\mathbf{c})$ may be identified with a permutation of $1, 2, \ldots, r$. If it is of type A, then A is the permutation matrix corresponding to w. The inverse of w is of type A^T (the transpose of A).

Proposition 3. *Let $R(\mathbf{c}, A)$ be the set of the words in $R(\mathbf{c})$ which are of A-type. Then the generating polynomials for $R(\mathbf{c}, A)$ and for $R(\mathbf{c}, A^T)$ by the number of internal inversions are identical. Moreover,*

$$\sum_{w \in R(\mathbf{c},A)} q^{\operatorname{intinv} w} = \begin{bmatrix} c_1 \\ a(1,1) \ldots a(1,r) \end{bmatrix}_q \cdots \begin{bmatrix} c_r \\ a(r,1) \ldots a(r,r) \end{bmatrix}_q$$

$$= \begin{bmatrix} c_1 \\ a(1,1)\dots a(r,1) \end{bmatrix}_q \cdots \begin{bmatrix} c_r \\ a(1,r)\dots a(r,r) \end{bmatrix}_q$$
$$= \sum_{w\in R(\mathbf{c},A^T)} q^{\mathrm{intinv}\, w}$$

Proof. As is well-known (see, e.g., [An76, p. 41]) the generating polynomial for the rearrangements of the word $1^{a(1,1)}\dots r^{a(1,r)}$ by the number of inversions is equal to multinomial coefficient $\left[{c_1 \atop a(1,1)\dots a(1,r)}\right]_q$. ∎

Remarks.

1) Proposition 3 implies that there exists a bijection of $R(\mathbf{c},A)$ onto $R(\mathbf{c},A^T)$ that preserves the number of internal inversions. As will be explained, *constructing such a bijection* is the crucial problem still unsolved.

2) Our transformation $w\mapsto w^*$ gives a bijective proof of Proposition 3 in the case $q=1$.

Say that a word $w=x_1x_2\dots x_m$ in $R(\mathbf{c},A)$ is *minimal*, it it has *no* internal inversions. This means that all the factors $x_1\dots x_{c_1}$, $x_{c_1+1}\dots x_{c_1+c_2}$, … , $x_{c_1+\dots c_{r-1}+1}\dots x_m$ are nondecreasing. In each A-type class there is one and only one minimal word. Write it as the bottom word in the following two-row matrix:

$$\begin{pmatrix} 1 & \dots & 1 & 2 & \dots & 2 & \dots & r & \dots & r \\ x_1 & \dots & x_{c_1} & x_{c_1+1} & \dots & x_{c_1+c_2} & \dots & x_{c_1+\dots+c_{r-1}+1} & \dots & x_m \end{pmatrix}.$$

Interchange the two rows; then rearrange the vertical bi-letters $\binom{a'}{a}$ of the resulting two-row matrix in such a way that the top row becomes $1^{c_1}2^{c_2}\dots r^{c_r}$, using the commutation rule (♠). Let w' be the bottom word in the final two-row matrix. This implies the following proposition.

Proposition 4. *The mapping $w\mapsto w'$ is an involution of the set of the minimal words in $R(\mathbf{c})$ that sends each minimal word of A-type onto a minimal word of A^T-type. Moreover*

$$\mathrm{extinv}\, w' = \mathrm{extinv}\, w.$$

Example. The word $w=3,1,2,2$ is minimal and of type $A=\begin{pmatrix}0&0&1\\1&1&0\\0&1&0\end{pmatrix}$. It is mapped onto

$$\begin{pmatrix}1&2&2&3\\3&1&2&2\end{pmatrix}\mapsto\begin{pmatrix}3&1&2&2\\1&2&2&3\end{pmatrix}=\begin{pmatrix}1&2&2&3\\2&2&3&1\end{pmatrix}\mapsto 2,2,3,1=w',$$

which is minimal and of type $A^T=\begin{pmatrix}0&1&0\\0&1&1\\1&0&0\end{pmatrix}$. Moreover $\mathrm{extinv}\, w' = \mathrm{extinv}\, w = 3$.

In [Kn70] Knuth derived an extension of the Robinson-Schensted correspondence. When that extension is applied to a *minimal* word w, it can be viewed as a one-to-one mapping of each circuit $\begin{pmatrix}\overline{w}\\ w\end{pmatrix}$ onto an ordered pair of semi-standard Young tableaux (P, Q) of the same shape and the same evaluation. Again denote that one-to-one mapping by $w \mapsto (P, Q)$. Knuth also proved the following property:

$$\textit{If } w \mapsto (P, Q), \textit{ then } w' \mapsto (Q, P).$$

As all words belonging to the same class $R(\mathbf{c}, A)$ have the same number of external inversions, the previous two propositions imply the following theorem.

Theorem 5. *There exists a bijection $w \mapsto w'$ of $R(\mathbf{c})$ having the following properties*

(N0) If $w = \sigma$ is a permutation, then $w' = \sigma^{-1}$;

(N1) $w \mapsto w'$ is an involution;

(N2) For each biletter $\begin{pmatrix}y\\ x\end{pmatrix}$, the number of occurrences of the biletter $\begin{pmatrix}y\\ x\end{pmatrix}$ in $\begin{pmatrix}\overline{w}\\ w\end{pmatrix}$ is equal to the number of occurrences of the biletter $\begin{pmatrix}x\\ y\end{pmatrix}$ in $\begin{pmatrix}\overline{w}\\ w'\end{pmatrix}$.

(N2') if w is of A-type, then w' is of A^T-type;

(N3) $\operatorname{extinv} w = \operatorname{extinv} w'$;

(N4) If w is a minimal word and w is mapped onto (P, Q) by the Robinson-Schensted correspondence, then $w' \mapsto (Q, P)$;

(N4') $\operatorname{intinv} w = \operatorname{intinv} w'$;

(N4") $\operatorname{inv} w = \operatorname{inv} w'$;

Take the minimal word $w = 3122$. We have $w^* = 2321$, which is not a minimal word. We know that our transformation $w \mapsto w^*$ in section 2 does not verify all the properties of theorem 5. Finding such a transformation is the open problem that we propose to the reader.

REFERENCES

[An76] George E. Andrews, "The Theory of Partitions," London, Addison-Wesley, 1976 (*Encyclopedia of Math. and Its Appl.*, **2**).

[CF69] P. Cartier and D. Foata, "Problèmes combinatoires de permutations et réarrangements," Berlin, Springer-Verlag, 1969 (*Lecture Notes in Math.,* **85**).

[Kn70] D.E. Knuth, Permutations, matrices, and generalized Young tableaux, *Pacific J. Math.* **34** (1970), 709-727.

[Kn73] D.E. Knuth, "The Art of Computer Programming, vol. 3, Sorting and Searching," Addison-Wesley, Reading, 1973.

[Kn97] D.E. Knuth, Private communication, Oct. 1997.

[Kn98] D.E. Knuth, Private communication, Jan. 1998.

[Lo83] M. Lothaire, "Combinatorics on words," Reading, Addison-Wesley, 1983 (*Encyclopedia of Math. and its Appl.*, **17**).

Dominique Foata
Département de mathématique
Université Louis Pasteur
7, rue René-Descartes
F-67084 Strasbourg
foata@math.u-strasbg.fr

Guo-Niu Han
I.R.M.A. et C.N.R.S.
Université Louis Pasteur
7, rue René-Descartes
F-67084 Strasbourg
guoniu@math.u-strasbg.fr