BRAIDS, Q-BINOMIALS AND QUANTUM GROUPS

MARCELO AGUIAR

Abstract. The classical identities between the $q$-binomial coefficients and factorials can be generalized to a context where numbers are replaced by braids. More precisely, for every pair $i, n$ of natural numbers, there is defined an element $b_i^{(n)}$ of the braid group algebra $kB_n$, and these satisfy analogs of the classical identities for the binomial coefficients. By choosing representations of the braid groups, one obtains numerical or matrix realizations of these identities, in particular one recovers the $q$-identities in this way. These binomial braids $b_i^{(n)}$ play a crucial role in a simple definition of a family of quantum groups, including the quantum groups $U_q^+(C)$ of Drinfeld and Jimbo.

1. Introduction

The classical identities between the $q$-binomial coefficients and factorials can be generalized to a context where numbers are replaced by braids, or more precisely, elements of the braid group algebras $kB_n$. Thus, for every pair $i, n$ of natural numbers there is defined an element $b_i^{(n)} \in kB_n$ (section 3), and these satisfy analogs of the classical identities for the binomial coefficients (sections 4 through 8). Moreover, by choosing representations of the braid groups one obtains concrete realizations of these identities; the simplest such choices yield the identities for the classical and $q$-binomial coefficients, other choices yield new identities that involve matrices rather than numbers.

The following chart describes the action of the braids introduced in this paper when $X$ is certain one-dimensional representation defined by $q \in k^*$ (section 2.5). The definition of the $q$-analogs will be reviewed before each corresponding braid analog is introduced.

<table>
<thead>
<tr>
<th>Braid</th>
<th>name</th>
<th>defined in section</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_i^{(n)}$</td>
<td>generator</td>
<td>2.1</td>
<td>$q$</td>
</tr>
<tr>
<td>$s_{i,j}^{(n)}$</td>
<td></td>
<td>2.1</td>
<td>$q^{j-i}$</td>
</tr>
<tr>
<td>$e^{(n)}$</td>
<td>twistor</td>
<td>2.2</td>
<td>$q^{(z)}$</td>
</tr>
<tr>
<td>$\beta_{m,n}$</td>
<td>braiding</td>
<td>2.4</td>
<td>$q^{mn}$</td>
</tr>
<tr>
<td>$s_i^{(n)}$</td>
<td></td>
<td>3</td>
<td>$q^{|I|}$</td>
</tr>
<tr>
<td>$b_i^{(n)}$</td>
<td>binomial</td>
<td>3</td>
<td>$[n \atop i]$</td>
</tr>
<tr>
<td>$[n]_q$</td>
<td>natural</td>
<td>5</td>
<td>$[n]$</td>
</tr>
<tr>
<td>$s_{s}^{(n)}$</td>
<td></td>
<td>5</td>
<td>$q^{\text{inv}(\sigma)}$</td>
</tr>
<tr>
<td>$f^{(n)}$</td>
<td>factorial</td>
<td>5</td>
<td>$[n]!$</td>
</tr>
<tr>
<td>$s_f^{(n)}$</td>
<td></td>
<td>7.1</td>
<td>$q^{\text{inv}(f)}$</td>
</tr>
<tr>
<td>$m^{(n)}$</td>
<td>multinomial</td>
<td>7.1</td>
<td>$[n \atop \eta]$</td>
</tr>
<tr>
<td>$\mu^{(n)}$</td>
<td>Möbius</td>
<td>6.2</td>
<td>$(-1)^nq^{(z)}$</td>
</tr>
<tr>
<td>$C^{(n)}$</td>
<td>Catalan</td>
<td>8</td>
<td>$C_n$</td>
</tr>
<tr>
<td>$G^{(n)}$</td>
<td>Galois</td>
<td>8</td>
<td>$G_n$</td>
</tr>
<tr>
<td>$F^{(n)}$</td>
<td>Galoiss</td>
<td>8</td>
<td>$F_n$</td>
</tr>
</tbody>
</table>

Date: January 1997.
1991 Mathematics Subject Classification. Primary:05A30; Secondary:17B37.
Key words and phrases. Braids, $q$-analogues, quantum groups.
These binomial braids \( b_{i}^{(n)} \) play a crucial role in the generalization of the definition of the quantum group \( U_{q}^{+}(C) \) of Drinfeld [Dr] and Jimbo [J] presented in [A] and briefly discussed here in section 9.

At the level of braids, the proofs of the combinatorial identities follow a constant pattern: first there is the set-theoretic part, which involves dealing with the same bijections that are used for the case of the classical \( (q = 1) \) identities, then there is the geometric part that consists in proving that two braids, labeled by corresponding elements under the bijection considered, are in fact equal.

The classical \( q \)-identities that we generalize are taken mostly from papers by Goldman and Rota [GR]; in particular these include Pascal’s, Vandermonde’s and Cauchy’s identities, the factorial formula, Rota’s binomial theorem, Möbius inversion, several identities involving multinomial braids and definitions and formulas for the Galois, Fibonacci and Catalan braids.

It is also possible to define the braid analog of a partition of a set, and then Stirling and Bell braids. These will be studied elsewhere.

2. Braid groups and the braid category

2.1. Basics. The group \( B_{n} \) of braids in \( n \) strands has generators \( s_{1}^{(n)}, \ldots, s_{n-1}^{(n)} \) subject to the relations

\[
\begin{align*}
\text{(A1)} & \quad s_{i}^{(n)} s_{j}^{(n)} = s_{j}^{(n)} s_{i}^{(n)} & \text{if } |i - j| \geq 2, \\
\text{(A2)} & \quad s_{i}^{(n)} s_{i+1} s_{i}^{(n)} = s_{i+1} s_{i}^{(n)} s_{i+1} & \text{if } 1 \leq i \leq n - 2.
\end{align*}
\]

The generator \( s_{i}^{(n)} \) is represented by the following picture, and the product \( st \) of two braids \( s \) and \( t \) in \( B_{n} \) is obtained by putting the picture of \( s \) on top of that of \( t \). The identity of \( B_{n} \) is represented by the picture with \( n \) vertical strands; the inverse of \( s \) is obtained by reflecting its picture across a horizontal line, without leaving the plane of the picture.

\[
s_{i}^{(n)} = \begin{array}{cccccccc}
1 & 2 & \cdots & i - 1 & i & i + 1 & \cdots & n \\
1 & 2 & \cdots & i & i - 1 & \cdots & n - 1 & n
\end{array}
\]

The collection \( \mathcal{B} = \coprod_{n \geq 0} B_{n} \) of all braid groups forms a category, where the objects are the natural numbers, \( B_{n} \) is the set of endomorphisms of \( n \), and there are no morphisms between distinct objects. This category is monoidal; the tensor product \( s \otimes t \in B_{n+m} \) of two braids \( s \in B_{n} \) and \( t \in B_{m} \) is obtained by putting \( t \) to the right of \( s \), i.e. \( s_{i}^{(n)} \otimes s_{j}^{(m)} = s_{i}^{(n+m)} s_{n+j}^{(m)} \). Moreover, this monoidal category is braided, in the sense that there is a natural map \( \beta_{n,m} : n \otimes m \rightarrow m \otimes n \), i.e. a braid \( \beta_{n,m} \in B_{n+m} \), satisfying some axioms (2.4 below). For more details on this, the reader is referred to [K], X.6 and XIII.2.

We develop some basic notation. For each pair \( (i, j) \) with \( 1 \leq i \leq j \leq n \), define

\[
s^{(n)}(i, j) = \begin{cases} 
1 & \text{if } i = j, \\
\frac{s_{i}^{(n)} \cdot s_{i+1}^{(n)} \cdots s_{j-1}^{(n)}}{s_{i}^{(n)} \cdot s_{i+1}^{(n)} \cdots s_{j-1}^{(n)}} & \text{if } i < j.
\end{cases}
\]

We provide a first set of lemmas.
Lemma.

(1) \( s^{(n)}(i, k) = s^{(n)}(i, j)s^{(n)}(j, k) \) when \( 1 \leq i \leq j \leq k \leq n \)

(2) \( s^{(m+n)}_i = s^{(m)}_i \otimes 1^{(n)} \) when \( 1 \leq i \leq m - 1, \ n \geq 0 \)

(3) \( s^{(m+n)}_{i+n} = 1^{(n)} \otimes s^{(m)}_i \) when \( 1 \leq i \leq j \leq m, \ n \geq 0 \)

(4) \( s^{(m+n)}_{i+l} = 1^{(l)} \otimes s^{(m)}_i \otimes 1^{(n-l)} \) when \( 1 \leq i \leq m - 1, \ 0 \leq l \leq n \)

(5) \( s^{(n)}(i, j)s^{(n)}_k = s^{(n)}_{h+1}s^{(n)}(i, j) \) when \( 1 \leq i \leq h \leq j - 2 \)

\[ s^{(n)}(i, j)s^{(n)}(h, k) = s^{(n)}(h+1, k+1)s^{(n)}(i, j) \] when \( 1 \leq i \leq h \leq k \leq j - 1 \).

Proof. Equation (1) is a direct consequence of the notation, the first parts of (2) and (3) hold simply by definition of the tensor product, and the second parts follow by repeated use of the first ones. Now,

\[ s^{(m+n)}_i = s^{(m)}_i \otimes 1^{(n)} = 1^{(l)} \otimes s^{(m)}_i \otimes 1^{(n-l)}, \]

proving the first part of (4). Similarly the second part follows from the second parts of (2) and (3).

Finally, if \( 1 \leq i \leq h \leq j - 2 \), we can write

\[ s^{(n)}(i, j)s^{(n)}_h = s^{(n)}(i, h)s^{(n)}_h s^{(n)}_{h+1}s^{(n)}(h+2, j) = s^{(n)}(i, h)s^{(n)}_h s^{(n)}_{h+1}s^{(n)}(h+2, j). \]

Repeating use of (1) and (5) shows that \( c^{(n)}s^{(n)} = s^{(n)}_{n-1}c^{(n)} \), hence \( \sim \) is the inner automorphism defined by conjugation by \( c^{(n)} \). It follows that \( c^{(n)} \) is in the center of the braid group, since \( \tilde{s} = s \) for any \( s \). Moreover, it can be shown that \( c^{(n)} \) generates \( Z(B_n) \); we won’t make use of this fact.

Let us prove that, for any \( s \in B_n \) and \( t \in B_m \),

\[ \tilde{s} \otimes t = \tilde{t} \otimes \tilde{s}, \]

where \( \tilde{s} \) is obtained by rotating in 3-space that of \( s \) 180 degrees around a vertical line. Consider the twistor braid,

\[ c^{(n)} = s^{(n)}(1, n)s^{(n)}(1, n-1) \cdots s^{(n)}(1, 2)s^{(n)}(1, 1). \]

For instance

\[ c^{(4)} = \]

\[ \begin{array}{cccc}
1 & 2 & \cdots & 3 \cdots 4 \\
\end{array} \]

Repeated use of (1) and (5) shows that \( c^{(n)} s^{(n)} = s^{(n)}_{n-1} c^{(n)} \), hence \( \sim \) is the inner automorphism defined by conjugation by \( c^{(n)} \). It follows that \( c^{(n)} \) is in the center of the braid group, since \( \tilde{s} = s \) for any \( s \). Moreover, it can be shown that \( c^{(n)} \) generates \( Z(B_n) \); we won’t make use of this fact.
Proof. Notice that if the statement holds for \( s \otimes t \) and \( s' \otimes t' \), then so it does for \( ss' \otimes tt' \). Hence it suffices to prove it for \( s = s_i^{(n)} \) and \( t = s_j^{(m)} \). Now,

\[
\begin{align*}
\tilde{s_i^{(n)}} \otimes \tilde{s_j^{(m)}} &= s_i^{(n+m)} s_{n+j}^{(n+m)} \\
&\iff s_i^{(n+m)} s_{n+m-i}^{(n+m)} = s_i^{(n+m)} s_{n+m-i}^{(n+m)} (A1) \\
& \quad \text{(since } n + m - i \geq m + 1) \\
& = \tilde{s_i^{(n)}} \otimes \tilde{s_j^{(m)}}.
\end{align*}
\]

2.3. Horizontal symmetry. There is a map \( * : B_n \to B_n \) defined by the conditions that \( s_i^{(n)*} = s_i^{(n)} \) and \( (st)^* = t*s* \). The picture for \( s* \) is obtained by rotating that of \( s \) in 3-space 180 degrees around a horizontal line.

It is clear that the three operators \( *, \tilde{,}^{−1} : B_n \to B_n \) commute pairwise, and also that

\[
\begin{align*}
&s^{**} = s & \forall s \in B_n, \\
&(s \otimes t)^* = s^* \otimes t^* & \forall * \in B_n, t \in B_m, \\
&s^{(n)}(i, j)^* = s^{(n)}(n + 1 - j, n + 1 - i) & \forall i, j, n, \\
&c^{(n)*} = c^{(n)} & \forall n.
\end{align*}
\]

From (8) it follows easily that

\[
c^{(n)} = s^{(n)}(n, n)s^{(n)}(n - 1, n)\ldots s^{(n)}(2, n)s^{(n)}(1, n)
\]

and from here that

\[
c^{(n)^2} = s^{(n)}(1, n)^n.
\]

2.4. Properties of the braiding. The braiding \( \beta_{m,n} \) is most easily defined in terms of its picture:

\[
\beta_{m,n} =
\]

It is viewed as a natural map \( \beta_{m,n} : m \otimes n \to n \otimes m \) in the category \( \mathcal{B} \) of braids, and as such it satisfies some important properties. We will list some of them below without proof, since we won’t use them, although they are very easily obtained through the use of pictures, see [K] XIII.2. However, it will be convenient for us to have an explicit description of \( \beta_{m,n} \) in terms of the canonical generators. For this, we first define some special “powers” for braids as follows.

Let \( m \geq 1 \). For \( s \in B_m \) and \( n \geq 0 \), define

\[
s^{(n)} = \begin{cases}
1 & \text{if } n = 0, \\
1^{(n-1)} \otimes s \cdot 1^{(n-2)} \otimes 1 \cdot \ldots \cdot 1 \otimes 1^{(n-2)} \cdot s \otimes 1^{(n-1)} & \text{if } n \geq 2.
\end{cases}
\]
Thus $s^{(n)} \in B_{m+n-1}$ for all $m \geq 1$, $n \geq 0$ (and it is not defined if $m = 0$). Notice that $s^{(n+1)} = 1 \otimes s^{(n)} \cdot s \otimes 1$, from which it follows easily by induction that

$$s^{(p+q)} = 1^{(q)} \otimes s^{(p)} \cdot s^{(q)} \otimes 1^{(p)} \quad \forall \ p, q \geq 0,$$

$$(10) \quad 1^{(k)} \otimes s^{(n)} \otimes 1^{(h)} = [1^{(k)} \otimes s \otimes 1^{(h)}]^{(n)} \quad \forall \ n, k, h \geq 0.$$  

We then define

$$(11) \quad \beta_{m,n} = s^{(m+1)}(1, m + 1)^{(n)} \in B_{m+n}.$$  

It is easy to see that this corresponds to the picture above. These are some of the properties that $\beta$ satisfies:

$$\beta_{m,n} \cdot s^{\otimes t} = t^{\otimes s} \cdot \beta_{m,n} \quad \forall \ s \in B_m, \ t \in B_n, \ (\text{naturalness of the braiding}),$$

$$c^{(n+m)} = c^{(n)} \otimes c^{(m)} \cdot \beta_{m,n} \quad \forall \ m, n \geq 0,$$

$$\beta_{m,n} = \beta_{n,m} = \beta^*_{m,n} \quad \forall \ m, n \geq 0,$$

$$\beta_{p,q,r} = 1^{(q)} \otimes \beta_{p,r} \cdot \beta_{p,q} \otimes 1^{(r)} \quad \forall \ p, q, r \geq 0,$$

$$\beta_{p+q,r} = \beta_{p+q,r} \otimes 1^{(q)} \cdot 1^{(p)} \otimes \beta_{q,r} \quad \forall \ p, q, r \geq 0.$$  

2.5. Representations. Throughout the paper $k$ will denote a fixed field (although any commutative ring would do just as well).

The identities we will obtain between elements of the braid group algebras $kB_n$ can be converted into matrix or numerical identities by choosing $k$-linear representations of the braid groups $B_n$.

More precisely we will be interested in monoidal representations of the braid category $\mathcal{B}$, that is a vector space $X$, such that the braid group $B_n$ acts on the tensor power $X^{\otimes n}$, with the property that

$$s^{\otimes t} \cdot x \otimes y = (s \cdot x) \otimes (t \cdot y) \quad \forall \ s \in B_m, \ t \in B_n, \ x \in X^{\otimes n}, \ y \in X^{\otimes m}.$$  

Since $s_i^{(n)} = 1^{(i-1)} \otimes s_1^{(2)} \otimes 1^{(n-1)}$, this condition implies that the action of $B_n$ on $X^{\otimes n}$ is uniquely determined by the action of $s_1^{(2)}$ on $X \otimes X$. Moreover, a linear operator $R : X \otimes X \rightarrow X \otimes X$ defines a monoidal representation of $\mathcal{B}$ if and only if it is invertible and satisfies the Yang-Baxter equation:

$$(R \otimes \text{id}_X) \circ (\text{id}_X \otimes R) \circ (R \otimes \text{id}_X) = (\text{id}_X \otimes R) \circ (R \otimes \text{id}_X) \circ (\text{id}_X \otimes R).$$

This is a consequence of (A2).

If $X$ is one-dimensional, then any invertible operator $R : X \rightarrow X$ satisfies this equation. $R$ is necessarily given by multiplication by some non-zero scalar $q \in k$. Hence, in this case, $s_i^{(n)}$ acts by multiplication by $q$ for every $n \geq 2$, $1 \leq i \leq n-1$. It is the simplest choice that will produce the classical $q$-identities from the identities for braids. In particular the trivial one-dimensional representation yields the case $q = 1$. Higher dimensional representations will be discussed in sections 9 and 10.

The chart in section 1 describes the action of the braids introduced in this paper when $X$ is the one-dimensional representation defined by $q \in k^*$ as above.

Let us also remark that since the non-commutativity of the braid groups necessarily disappears when acting on a one-dimensional representation, the actions of $s, s$ and $s^*$ coincide for any braid $s$ in this case.

3. Binomial braids

For each pair $(n,i)$ with $i \leq n$ let $S_i(n)$ denote the set of subsets of $\{1,2,\ldots,n\}$ with cardinality $i$. Recall that the $q$-binomial coefficients can be defined as

$$\binom{n}{i} = \sum_{I \in S_i(n)} q^{||I||} \text{ where } ||I|| = \sum_{j \in I} j \sum_{j=1}^i.$$
The braid analog of this definition is as follows. 
First, for each $I \in S_i(n)$, write $I = \{j_1, j_2, \ldots, j_i\}$ with $j_1 < j_2 < \ldots < j_i$, then define $s_I^{(n)} \in B_n$ as

$$s_I^{(n)} = s^{(n)}(i, j_1) \cdots s^{(n)}(j_2, j_1) s^{(n)}(1, j_1);$$

if $i = 0$ we let $s_0^{(n)} = 1$.

For instance if $I = \{m + 1, m + 2, \ldots, m + n\} \in S_n(m + n)$ then $s_I^{(m+n)} = \beta_{m,n}$.

Then the binomial braid $b_i^{(n)} \in kB_n$ is defined as

$$b_i^{(n)} = \sum_{I \in S_i(n)} s_I^{(n)}.$$ 

Thus $b_0^{(n)} = b_1^{(n)} = 1 \forall n$, while for instance

$$b_1^{(2)} = 1 + s_1^{(2)}, \quad b_1^{(3)} = 1 + s_1^{(3)} + s_1^{(3)} s_2^{(3)}, \quad b_2^{(3)} = 1 + s_2^{(3)} + s_2^{(3)} s_1^{(3)}.$$ 

We see that $b_i^{(n)} \neq b_{n-i}^{(n)}$ in general. However:

**Proposition.** For all $n \geq i \geq 0$,

$$b_i^{(n)} = b_{n-i}^{(n)}.$$  

(12)

**Proof.** Consider the bijection $S_i(n) \to S_{n-i}(n)$ that sends $I$ to $\tilde{I}^c$, where $\tilde{I} = \{n + 1 - i / i \in I\}$. It is enough to show that, for every $I \in S_i(n)$,

$$(*) \quad s_I^{(n)} = s_{\tilde{I}^c}^{(n)}.$$ 

First, we show that if $(*)$ holds when $n \in I$, then it holds for every $I$. In fact, given $I \in S_i(n)$, let $m = \max I$, and let $I'$ be the same set $I$ but viewed as an element of $S_i(m)$. Then we have that

$$s_I^{(n)}(2) = s_{I'}^{(m)} \otimes 1^{(n-m)},$$

hence, by (6), and assuming $(*)$ for $I'$,

$$s_I^{(n)} = 1^{(n-m)} \otimes s_{I'}^{(m)}(2) = 1^{(n-m)} \otimes s_{I_{1_{I'}}}^{(m)}(2) = s_{I_{1_{I'}}}^{(m)}(2) = s_{I_{1_{I'}}}^{(m)}(3) = s_{n+1-I_{1_{I'}}}^{(n)} = s_{\tilde{I}^c}^{(n)},$$

so $(*)$ holds for $I$ as well.

To finish the proof we show $(*)$ by induction on $i$. For $i = 0$ it is clear. Assume $i \geq 1$. As just explained, we can also assume that $n \in I$. Therefore, we can decompose $I = I_1 \cup \{n\}$ with $I_1 \in S_{i-1}(n-1)$; then we have $\tilde{I} = \tilde{I}_1 \cup \{1\}$ and $\tilde{I}_1^c = \tilde{I}^c \cup \{1\}$.

Write $\tilde{I}^c = \{h_1 < h_2 < \ldots < h_{n-i}\}$, so that $\tilde{I}_1^c = \{1 < h_1 < h_2 < \ldots < h_{n-i}\}$. We have

$$s_I^{(n)} = s^{(n)}(i, n) s_{I_1}^{(n)} s_{I_{1+1}}^{(n)} \cdots s_{I_{n-1}}^{(n)} s_{I_n}^{(n)},$$

hence, by induction hypothesis,

$$s_I^{(n)} = s_{n-I_{1_{I_{1+1}}}}^{(n)} \cdots s_1^{(n)} s_{I_{1_{I_{1+1}}}}^{(n)}$$

$$= s_{n-I_{1_{I_{1+1}}}}^{(n)} s_{n-I_{1_{I_{1+1}}}}^{(n)}(n-i+1, h_{n-i}) \cdots s^{(n)}(3, h_2) s^{(n)}(2, h_1) s^{(n)}(1, 1).$$
Now using (A1),\( s^{(n)}(n-i+1, h_{n-i}) \), can be moved to the left past all the factors \( s^{(n)}_{1}, \ldots, s^{(n)}_{n-i-1} \). Then, it combines with \( s^{(n)}_{n-i} \) to form \( s^{(n)}(n-i, h_{n-i}) \). Similarly the other factors of the form \( s^{(n)}(k+1, h_{k}) \) can be moved to the left until they reach \( s^{(n)}_{k} \) to form \( s^{(n)}(k, h_{k}) \). At the end of the process we have
\[
\tilde{s}^{(n)}_{I} = s^{(n)}(n-i, h_{n-i}) \ldots s^{(n)}(2, h_{2}) s^{(n)}(1, h_{1}) = \tilde{s}^{(n)}_{i}.
\]
This finishes the induction and the proof.

\[\square\]

4. IDENTITIES OF PASCAL AND VANDERMONDE

For the \( q \)-binomial coefficients Pascal’s identity says that
\[
\begin{bmatrix} n \end{bmatrix}_{i} = q^{-i} \begin{bmatrix} n - 1 \end{bmatrix}_{i-1} + \begin{bmatrix} n - 1 \end{bmatrix}_{i} = \begin{bmatrix} n - 1 \end{bmatrix}_{i-1} + q^{\begin{bmatrix} n - 1 \end{bmatrix}_{i}}.
\]
Its generalization to braids is as follows.

Proposition. For any \( i = 1, \ldots, n - 1 \),
\[
(b^{(n)})_{i} = s^{(n)}(i, n) \cdot b^{(n-1)}_{i-1} \otimes 1 + b^{(n-1)}_{i-1} \otimes 1 = 1 \otimes b^{(n-1)}_{i-1} + s^{(n)}(n-i, n) \cdot \tilde{1} \otimes b^{(n-1)}_{i-1}.
\]

Proof. Consider the bijection \( S_{i-1}(n-1) \cup S_{i-1}(n-1) \rightarrow S_{i}(n) \) that sends \( I \in S_{i-1}(n-1) \) to \( I \cup \{n\} \in S_{i}(n) \) and \( J \in S_{i}(n-1) \) to \( J \in S_{i}(n) \). From (2) and the definition of \( s_{I} \) we see that
\[
s^{(n)}_{J} = s^{(n)}_{J} \otimes 1 \text{ and } s^{(n)}_{I \cup \{n\}} = s^{(n)}(i, n) \cdot s^{(n-1)}_{I} \otimes 1;
\]
summing over all such \( I \) and \( J \) we obtain the first equality. The other one follows by applying \( \tilde{\ } \), using (6) and replacing \( n - i \) by \( i \).

Vandermonde’s identity says that
\[
\begin{bmatrix} m + n \end{bmatrix}_{p} = \sum_{k=0}^{p} q^{(m-k)(p-k)} \begin{bmatrix} m \end{bmatrix}_{k} \begin{bmatrix} n \end{bmatrix}_{p-k}.
\]
Its generalization to braids reads:

Proposition. For any \( m, n, p \) with \( 0 \leq p \leq m, n \),
\[
b^{(m+n)}_{p} = \sum_{k=0}^{p} q^{(k)} \otimes \beta^{m-k, p-k} \otimes 1^{(n-p-k)} \cdot b^{(m)}_{k} \otimes b^{(n)}_{p-k}.
\]

Proof. Consider the bijection
\[
\bigcup_{k=0}^{p} S_{k}(m) \times S_{p-k}(n) \rightarrow S_{p}(m + n), \quad (I, J) \mapsto I \cup (m + J).
\]
It suffices to show that, for each \( I \in S_{k}(m) \) and \( J \in S_{p-k}(n) \),
\[
(s^{(m+n)}_{I \cup (m+J)})_{k} = q^{(k)} \otimes \beta^{m-k, p-k} \otimes 1^{(n-p-k)} \cdot s^{(m)}_{I} \otimes s^{(n)}_{J}.
\]
Let \( h = p - k \). If \( h = 0 \) then (*) reduces to \( s^{(m+n)}_{I} = s^{(m)}_{I} \otimes 1^{(n)} \), which holds by (2).
Assume \( h \geq 1 \). Write \( I = \{i_1 < \ldots < i_k\} \) and \( J = \{j_1 < \ldots < j_h\} \) so that \( I \cup (m + J) = \{i_1 < \ldots < i_k < m + j_1 < \ldots < m + j_h\} \). Then
\[
 s_{I \cup (m + J)}^{(m+n)} = s^{(m+n)}(k + h, m + j_h)s^{(m+n)}(k + h - 1, m + j_{h-1}) \ldots s^{(m+n)}(k + 1, m + j_1) \cdot \\
 \cdot s^{(m+n)}(k, i_k)s^{(m+n)}(k - 1, i_{k-1}) \ldots s^{(m+n)}(1, i_1) \\
 = (1) \cdot (2) [s^{(m+n)}(k + h, m + h)s^{(m+n)}(m + h, m + j_h)] \\
 \cdot [s^{(m+n)}(k + h - 1, m + h - 1)s^{(m+n)}(m + h - 1, m + j_{h-1})] \ldots \\
 \ldots [s^{(m+n)}(k + 1, m + 1)s^{(m+n)}(m + 1, m + j_1)] \\
 \cdot [s^{(m)}(k, i_k) \otimes 1^{(n)}] [s^{(m)}(k - 1, i_{k-1}) \otimes 1^{(n)}] \ldots [s^{(m)}(1, i_1) \otimes 1^{(n)}] \\
\]

Now notice that each of the factors
\[
s^{(m+n)}(k + h - 1, m + h - 1), \ s^{(m+n)}(k + h - 2, m + h - 2), \ldots, s^{(m+n)}(k + 1, m + 1)
\]
can be moved to the left past all the factors
\[
s^{(m+n)}(m + h, m + j_h), \ s^{(m+n)}(m + h - 1, m + j_{h-1}), \ldots, s^{(m+n)}(m + 2, m + j_2),
\]
simply because of (A1): \( s^{(m+n)}(k + h - 1, m + h - 1) \) only involves strands \( m + h - 1 \) and lower, while \( s^{(m+n)}(m + h, m + j_h) \) only involves strands \( m + h \) and higher; similarly for the others. After performing this commutation we get that
\[
 s_{I \cup (m + J)}^{(m+n)} = s^{(m+n)}(k + h, m + h)s^{(m+n)}(k + h - 1, m + h - 1) \ldots s^{(m+n)}(k + 1, m + 1) \cdot \\
 \cdot s^{(m+n)}(m + h, m + j_h)s^{(m+n)}(m + h - 1, m + j_{h-1}) \ldots s^{(m+n)}(m + j_1) \cdot \\
 \cdot s_I^{(m)} \otimes 1^{(n)} \\
 = (2) \cdot (3) [s^{(m+n-h+1)}(k + 1, m + 1)] [s^{(m+n-h+1)}(k + 1, m + 1) \otimes 1^{(n)}] \ldots \\
 \ldots [s^{(m-n+h+1)}(k + 1, m + 1) \otimes 1^{(n-h)}] \cdot [s^{(m)} \otimes s^{(n)}(h, j_h)] [s^{(m)} \otimes s^{(n)}(h - 1, j_{h-1})] \ldots [s^{(m)} \otimes s^{(n)}(1, j_1)] \\
 \cdot s_I^{(m)} \otimes 1^{(n)} \\
 = (9) [s^{(m+n-h+1)}(k + 1, m + 1) \otimes h] \cdot s^{(m)} \otimes s_I^{(n)} \\
 = (2) \cdot (3) [s^{(m-k+1)}(1, m - k + 1) \otimes 1^{(n-h)}]^{(h)} \cdot s_I^{(m)} \otimes s_f^{(n)} \\
 = (10) [s^{(m-k+1)}(1, m - k + 1) \otimes 1^{(n-h)}]^{(h)} \cdot s_I^{(m)} \otimes s_f^{(n)} \\
 = (11) [s^{(m-k+1)}(1, m - k + 1) \otimes 1^{(n-h)}]^{(h)} \cdot s_I^{(m)} \otimes s_f^{(n)}.
\]
Thus (*) holds and the proof is complete.

5. **Natural and factorial braids**

5.1. **Definition.** The \( q \)-analog of a natural number \( n \) is
\[
 [n] = 1 + q + q^2 + \ldots + q^{n-1}.
\]
For $n \geq 1$, the natural braid $[n] \in kB_n$ is defined as

$$[n] = \sum_{i=1}^{n} s^{(n)}(1, i) = 1 + s_1^{(n)} s_2^{(n)} + \ldots + s_1^{(n)} s_2^{(n)} \ldots s_{n-1}^{(n)};$$

we also set $[0] = 0 \in kB_0$.

Notice that $[n] = b_1^{(n)}$. Hence, as a particular case of Vandermonde’s formula (14) we have:

$$[m + n] = [m] \otimes 1^{(n)}(1, m + 1) \cdot 1^{(m)} \otimes [n];$$

since $\beta_{m, 1} = s_1^{(m+1)}(1, m + 1)$.

While $[1] = \tilde{[1]} = [1]^*$ and $[2] = \tilde{[2]} = [2]^*$, we have

$$[3] = 1 + s_1^{(3)} + s_1^{(3)} s_2^{(3)}; \quad \tilde{[3]} = 1 + s_2^{(3)} + s_2^{(3)} s_1^{(3)}$$

and $[3]^* = 1 + s_1^{(3)} + s_2^{(3)} s_1^{(3)}$;

thus $b_1^{(n)}$ is not another binomial braid in general. However, it will turn out (17) that the factorial braids are symmetric with respect to both $\tilde{\cdot}$ and $^*$.

The $q$-analog of the factorial number $n!$ is

$$[n]! = \sum_{\sigma \in S_n} q^{\text{inv} (\sigma)};$$

where the inversion index of a permutation $\sigma \in S_n$ is defined as

$$\text{inv} (\sigma) = \# \{(i, j) / i < j \text{ but } \sigma (i) > \sigma (j)\}.$$
We next show that the factorial and natural braids are related by means of a product formula, generalizing \([n]! = [n][n-1] \cdots [2][1]\) for \(q\)-numbers. Variations of this will follow after we study the effect of \(-\) and \(*\) on the \(s^{(n)}_\sigma\)’s.

**Proposition.** For every \(n \geq 1\),

\[
(15) \quad f^{(n)} = 1^{(n-1)} \otimes [1] \cdot 1^{(n-2)} \otimes [2] \cdots 1 \otimes [n-1] \cdot [n].
\]

**Proof.** We need to show that \(f^{(n)} = 1 \otimes f^{(n-1)} \cdot [n] \forall n \geq 1\).

Consider the bijection \(S_{n-1} \times \{1, 2, \ldots, n\} \to S_n, (\sigma, i) \mapsto (1 \otimes \sigma)(1, 2, \ldots, i)\). (From \(\tau := (1 \otimes \sigma)(1, 2, \ldots, i)\) we recover \(i\) as \(\tau^{-1}(1)\) and then \(1 \otimes \sigma\) as \(\tau \cdot (1, 2, \ldots, i)^{-1}\); here \(1 \otimes \sigma\) is such that \((1 \otimes \sigma)(j) = \sigma(j-1)+1\).

It suffices to show that

\[
s^{(n)}_\sigma = 1 \otimes s^{(n-1)}_\sigma \cdot s^{(n)}(1, i).
\]

Since \(\tau = (\sigma_{(1)+1} \cdots \sigma_{(i-1)+1} 1 \cdots \sigma_{(n-1)+1})\), we have that \(r_j(\tau) = \begin{cases} r_{j-1}(\sigma) & \text{if } j = i+1, \ldots, n, \\ 0 & \text{if } j = i, \\ r_j(\sigma) + 1 & \text{if } j = 1, \ldots, i-1. \end{cases}\)

Hence

\[
s^{(n)}_\sigma = s^{(n)}(\tau(n) - r_n(\tau), n) \cdots s^{(n)}(\tau(i+1) - r_{i+1}(\tau), i+1) \cdot s^{(n)}(\tau(i) - r_i(\tau), i) \cdot \\
s^{(n)}(\tau(i-1) - r_{i-1}(\tau), i-1) \cdots s^{(n)}(\tau(1) - r_1(\tau), 1)
\]

\[
= s^{(n)}(\sigma(n-1) + 1 - r_{n-1}(\sigma), n) \cdots s^{(n)}(\sigma(i) + 1 - r_i(\sigma), i+1) \cdot s^{(n)}(1, i) \cdot \\
s^{(n)}(\sigma(i-1) + 1 - r_{i-1}(\sigma), i-1) \cdots s^{(n)}(1 - r_1(\sigma), 1) = s^{(n)}(\sigma(n-1) + 1 - r_{n-1}(\sigma), n) \cdots s^{(n)}(\sigma(i) + 1 - r_i(\sigma), i+1) \cdot \\
s^{(n)}(\sigma(i-1) + 1 - r_{i-1}(\sigma), i-1) \cdots s^{(n)}(1 - r_1(\sigma), 1) = 1 \otimes s^{(n-1)}_\sigma \cdot s^{(n)}(1, i)
\]

and the proof is complete. \(\square\)

### 5.2. Symmetries of the factorial braids

To obtain the announced symmetry of the \(f^{(n)}\)’s, we first describe a multiplicativity property of the map \(\xi : S_n \to B_n, \sigma \mapsto s^{(n)}_\sigma\). From its definition it is clear that \(\xi\) is a section of the canonical projection \(B_n \to S_n\), and that \(\xi((i, i+1)) = s^{(n)}_i\).

**Lemma.** Let \(\sigma = \sigma_{i_1} \cdots \sigma_{i_l} \in S_n\) be a reduced expression for \(\sigma\) as a product of elementary transpositions \(\sigma_{ij} = (i_j, i_{j+1})\). Then \(s^{(n)}_\sigma = s^{(n)}_{i_1} \cdots s^{(n)}_{i_l}\).

**Proof.** We are given that \(\text{length}(\sigma) = l\), where the length of a permutation is the minimum number of elementary transpositions required to write it as a product of such. We will make use of the well-known fact that \(\text{inv} = \text{length}\).

Clearly, it suffices to show that if \(\sigma = \tau \cdot (i, i+1)\) and \(\text{length}(\sigma) = \text{length}(\tau) + 1\) then \(s^{(n)}_\sigma = s^{(n)}_\tau \cdot s^{(n)}_{i}\).

In this case, \(\tau = (1 \cdots \tau(i-1) \tau(i+1) \tau(i) \tau(i+2) \cdots \tau(n))\).

Hence \(r_j(\sigma) = r_j(\tau) \forall j \neq i, i+1\). We claim that \(\tau(i) < \tau(i+1)\). For if not, we would have \(r_i(\sigma) = r_{i+1}(\tau)\) and \(r_{i+1}(\sigma) = r_i(\tau) - 1\), from which \(\text{length}(\sigma) = \text{inv}(\sigma) = \sum_{j=1}^n r_j(\sigma) = \text{length}(\tau) - 1\), again against our hypothesis. Thus \(\tau(i) < \tau(i+1)\), and

\[\text{Lusztig} [1, 2, 1.2] \text{ has considered sections of this sort for arbitrary Weyl groups } W. \text{ From lemma (5.2) it follows that } \xi \text{ coincides with Lusztig’s section for } W = S_n.\]
then \( r_i(\sigma) = r_{i+1}(\tau) + 1 \) and \( r_{i+1}(\sigma) = r_i(\tau) \). Hence,
\[
s^{(n)}_\sigma = s^{(n)}(\sigma(n) - r_n(\sigma), n) \cdot \ldots \cdot s^{(n)}(\sigma(1) - r_1(\sigma), 1)
= s^{(n)}(\tau(n) - r_n(\tau), n) \cdot \ldots \cdot s^{(n)}(\tau(i + 2) - r_{i+2}(\tau), i + 2) \cdot s^{(n)}(\tau(i) - r_i(\sigma), i + 1) \\
\cdot s^{(n)}(\tau(i + 1) - r_i(\tau, i - 1)) \cdot s^{(n)}(\tau(i - 1) - r_{i-1}(\tau), i - 1) \cdot \ldots \cdot s^{(n)}(\tau(1) - r_1(\tau), 1)
\]
(5)
\[
\bar{s}^{(n)}_\sigma = s^{(n)}_\sigma \cdot s^{(n)*}_\sigma = s^{(n)}_{\sigma^{-1}}, \quad \text{where } \bar{\sigma}(j) = n + 1 - \sigma(n + 1 - j)
\]
(16)
\[
f^{(n)} = f^{(n)}_\sigma = f^{(n)*}_{\sigma^{-1}}.
\]
(17)
\[
f^{(n)} = 1^{(n-1)} \otimes [1] \cdot 1^{(n-2)} \otimes [2] \cdots \cdot 1^{(n)} \otimes [n]
= [1] \otimes 1^{(n-1)} \cdot [2] \otimes 1^{(n-2)} \cdots \cdot [n-1] \otimes 1 \cdot [n]
= [n]^* \cdot [n-1]^* \cdots \cdot [2]^* \otimes 1^{(n-2)} \cdot [1]^* \otimes 1^{(n-1)}.
\]
(18)
Proof. To prove (16), it suffices by the lemma to check these equalities on the elementary transpositions, since both \( \bar{\sigma} \) and \( \sigma^{-1} \) preserve the length of a permutation. But in this case they hold by definition of \( \bar{\sigma} \) and \( \sigma^{-1} \) for braids. Then (17) follows by summing over all \( \sigma \in S_n \), and the product formulas (18) follow from (15) and (17).

5.3. Other expressions for \( s^{(n)}_\sigma \). For any \( \sigma \in S_n \) and \( i = 1, \ldots, n \) let
\[
e_i(\sigma) = \# \{ j \leq i / \sigma(j) \leq \sigma(i) \}.
\]
There is a simpler expression for \( s^{(n)}_\sigma \) in terms of the \( e_i \)'s.

Proposition. For any \( \sigma \in S_n \) and \( i = 1, \ldots, n \), \( \sigma(i) = r_i(\sigma) + e_i(\sigma) \). Hence
\[
s^{(n)}_\sigma = s^{(n)}(e_n(\sigma), n) \cdot \ldots \cdot s^{(n)}(e_2(\sigma), 2) \cdot s^{(n)}(e_1(\sigma), 1).
\]
(19)
Proof.
\[
r_i(\sigma) + e_i(\sigma) = \# \{ j > i / \sigma(j) < \sigma(i) \} + \# \{ j \leq i / \sigma(j) \leq \sigma(i) \}
= \# \{ j > i / \sigma(j) \leq \sigma(i) \} + \# \{ j \leq i / \sigma(j) \leq \sigma(i) \}
= \# \{ j / \sigma(j) \leq \sigma(i) \} = \# \{ j / \sigma(j) \in \{ 1, 2, \ldots, \sigma(i) \} \}
= \sigma(i).
\]

For completeness, we provide another expression for \( s^{(n)}_\sigma \), this time in terms of some partial inversion indices that are obtained by reading \( \sigma \) from right to left. For any \( i = 1, \ldots, n \) let
\[
l_i(\sigma) = \# \{ j < i / \sigma(j) > \sigma(i) \}.
\]
Proposition. For any $\sigma \in S_n$, 
\[
s_{\sigma}^{(n)} = s^{(n)}(n, \sigma^{-1}(n) + l_n(\sigma^{-1})) \cdot \ldots \cdot s^{(n)}(2, \sigma^{-1}(2) + l_2(\sigma^{-1})) \cdot s^{(n)}(1, \sigma^{-1}(1) + l_1(\sigma^{-1})).
\]

Proof. Notice that $r_i(\sigma) = l_{n+1-i}(\overline{\sigma})$ for all $i = 1, \ldots, n$. Hence 
\[
s_{\sigma}^{(n)} = s^{(n)}(\sigma(n) - r_n(\sigma), n) \cdot \ldots \cdot s^{(n)}(\sigma(1) - r_1(\sigma), 1) = s^{(n)}(\sigma(n) - l_1(\overline{\sigma}), n) \cdot \ldots \cdot s^{(n)}(\sigma(1) - l_n(\overline{\sigma}), 1)
\]
\[
\Rightarrow s_{\sigma}^{(n)} = s^{(n)}(1) \cdot \overline{\sigma}^{-1}(n) \cdot \ldots \cdot s^{(n)}(\sigma(n) - l_1(\overline{\sigma}), n) \cdot (n)
\]
\[
(7) = s^{(n)}(n, n + 1 - \sigma(1) + l_n(\overline{\sigma})) \cdot \ldots \cdot s^{(n)}(1, n + 1 - \sigma(n) + l_1(\overline{\sigma}))
\]
\[
= s^{(n)}(n, \overline{\sigma}(n) + l_n(\overline{\sigma})) \cdot \ldots \cdot s^{(n)}(1, \overline{\sigma}(1) + l_1(\overline{\sigma}))
\]
\[
\Rightarrow s_{\sigma}^{(n)} = s^{(n)}(n, \overline{\sigma}(n) + l_n(\overline{\sigma})) \cdot \ldots \cdot s^{(n)}(1, \overline{\sigma}(1) + l_1(\overline{\sigma})).
\]

Replacing $\sigma$ by $\overline{\sigma}^{-1}$ yields the result. \qed

5.4. Factorial formulas for the binomial coefficients. Next, we present the analog of the well-known formula \[
\left[ \begin{array}{c} n-i \\ j-i \end{array} \right] = \left[ \begin{array}{c} n \\ j \end{array} \right] \] for $q$-binomials, from which the factorial formula will be deduced. We choose to provide a bijection proof, even though a proof based on Pascal’s identity is possible and shorter, in particular because it yields the stronger result $(*)$ below.

Proposition. Whenever $0 \leq i \leq j \leq n$,
\[
1^{(i)} \otimes b_{j-i}^{(n-i)} \cdot b_i^{(n)} = b_j^{(n-j)} \otimes 1^{(n-j)} \cdot b_i^{(n)}
\]

Proof. Consider the map $S_j(n) \times S_i(j) \to S_{j-i}(n-i) \times S_i(n)$, $(A, B) \mapsto (X, Y)$, defined as follows. First consider the unique order-preserving bijection $k : \{1, \ldots, j\} \to A$ and let $Y = k(B) \in S_i(n)$, then consider the unique order-preserving bijection $f : \{1, \ldots, n\} \setminus Y \to \{1, \ldots, n-i\}$ and let $X := f(A \setminus Y) \in S_{j-i}(n-i)$.

Given $(X, Y) \in S_{j-i}(n-i) \times S_i(n)$ one recovers $A = Y \cup f^{-1}(X)$ and $B = k^{-1}(Y)$; thus, $(A, B) \mapsto (X, Y)$ is a bijection, so to obtain the result it suffices to prove that
\[
(*)
\]
\[
1^{(i)} \otimes s_X^{(n-i)} \cdot s_Y^{(n)} = s_B^{(j)} \otimes 1^{(n-j)} \cdot s_A^{(n)}.
\]

We start by examining the right hand side. Write $A = \{h_1 < \ldots < h_{i+1}\} \subseteq \{1, \ldots, n\}$ and $B = \{h_1 < \ldots < h_j\} \subseteq \{1, \ldots, j\}$. Notice that then $Y := \{h_{i+1}, \ldots, h_i\} \subseteq \{1, \ldots, n\}$.

For each $r = 0, \ldots, i$ let $s_{A_r}^{(n)} := \prod_{h_r < z < h_{r+1}} s^{(n)}(z, k_z)$. (This and all products below are taken in the decreasing order: the index $z$ decreases from left to right. If the interval $(h_r, h_{r+1})$ is empty then we take $s_{A_r}^{(n)} = 1$; also, we set $h_0 = 0$ and $h_{i+1} = j + 1$.) Then, by definition,
\[
s_{A_r}^{(n)} = \prod_{0 < z < j+1} s^{(n)}(z, k_z) = s_{A_0}^{(n)} \cdot s_{A_1}^{(n)} \cdot s_{A_2}^{(n)} \cdot s_{A_3}^{(n)}(h_1, k_{h_1}) \cdot \ldots \cdot s_{A_i}^{(n)}(h_i, k_{h_i}).
\]

Hence
\[
s_B^{(j)} \otimes 1^{(n-j)} \cdot s_A^{(n)} = s_A^{(n)}(i, h_1) \cdot \ldots \cdot s_A^{(n)}(2, h_2) \cdot s_A^{(n)}(1, h_1) \cdot s_A^{(n)} \cdot s_A^{(n)}(h_2, k_{h_2}) \cdot s_A^{(n)} \cdot s_A^{(n)}(h_1, k_{h_1}) = s_A^{(n)} \cdot s_A^{(n)}(h_1, k_{h_1}) \cdot \ldots \cdot s_A^{(n)}(h_2, k_{h_2}) \cdot s_A^{(n)}(h_1, k_{h_1}).
\]

In this expression, $s^{(n)}(1, h_1)$ commutes with all the factors to its right until $s_A^{(n)}$, including it, since these only involve strands $h_1 + 1$ and higher. When placed there, it joins $s^{(n)}(h_1, k_{h_1})$ to form $s^{(n)}(1, k_{h_1})$, ...
by (1). Similarly \( s^{(n)}(2, h_2) \) commutes past \( s_{A_2}^{(n)} \) where it joins \( s^{(n)}(h_2, k_{h_2}) \) to become \( s^{(n)}(2, k_{h_2}) \), and finally \( s^{(n)}(i, h_i) \) and \( s^{(n)}(h_i, k_{h_i}) \) become \( s^{(n)}(i, k_{h_i}) \). After this transformation we get

\[
s_B^{(j)} \otimes s_A^{(n-j)} \cdot s_A^{(n)} = s_A^{(n)} \cdot s_A^{(n)}(i, k_{h_i}) \cdot \ldots \cdot s_A^{(n)}(2, k_{h_2}) \cdot s_A^{(n)}(1, k_{h_1}) \cdot s_A^{(n)}(1, k_{h_1}) \cdot s_A^{(n)}(1, k_{h_1}) \cdot s_A^{(n)}(1, k_{h_1}).
\]

Now notice that each factor in \( s_{A_0}^{(n)} \) is of the form \( s^{(n)}(z, k_z) \) with \( 1 \leq z < h_1 \), hence by (5) and (3)

\[
s^{(n)}(1, k_{h_1}) \cdot s^{(n)}(1, k_{h_1}) = 1 \otimes s_{A_0}^{(n-1)} \cdot s^{(n)}(1, k_{h_1}).
\]

Similarly we can now commute \( s_{A_1}^{(n)} \cdot 1 \otimes s_{A_0}^{(n-1)} \) past \( s^{(n)}(2, h_2) \), using (5) and (3); this factor becomes \( 1 \otimes s_{A_1}^{(n)} \cdot 1 \otimes s_{A_0}^{(n-1)} \) when placed to the left of \( s^{(n)}(2, h_2) \). After doing this for each \( r = 0, \ldots, i - 1 \) we get

\[
s_B^{(j)} \otimes 1^{(n-j)} \cdot s_A^{(n)} = s_A^{(n)} \cdot 1 \otimes s_{A_1}^{(n-1)} \cdot \ldots \cdot 1 \otimes 2 \otimes s_{A_2}^{(n)} \cdot 1 \otimes 1 \otimes s_{A_0}^{(n)} \cdot 1 \otimes 1 \otimes s_{A_0}^{(n)} \cdot s^{(n)}(1, k_{h_1}) \cdot s^{(n)}(2, k_{h_2}) \cdot s^{(n)}(1, k_{h_1}) \cdot s^{(n)}(1, k_{h_1}) \cdot s^{(n)}(1, k_{h_1})
\]

Thus, to obtain (*), we need to show that

\[
(**) \quad 1^{(i)} \otimes s_{X_r}^{(n-i)} = \prod_{r=0}^{i} 1^{(i-r)} \otimes s_{A_r}^{(n-i+r)}
\]

To this end, we describe \( f \) and \( X \) explicitly. By definition, \( f : \{1, \ldots, n\} \setminus \{k_{h_1}, \ldots, k_{h_i}\} \to \{1, \ldots, n-i\} \) is translation by \(-r\) on each open interval \( (k_{r \cdot}, k_{r+1}) \), for \( r = 0, \ldots, i \) (where we set \( k_0 = 0 \) and \( k_{j+1} = n + 1 \)). Then, since

\[
A \setminus Y = k(\{1, \ldots, j\} \setminus \{h_1, \ldots, h_i\}) = \bigcup_{r=0}^{i} k((h_r, h_{r+1}))
\]

we have that

\[
X = f(A \setminus Y) = \bigcup_{r=0}^{i} k((h_r, h_{r+1})) - r.
\]

Thus, letting \( s_{X_r}^{(n-i)} \) denotes \( s_{X_r}^{(n-i)}(z-r, k_z-r) \), we have that

\[
s_{X_r}^{(n-i)} = \prod_{r=0}^{i} s_{X_r}^{(n-i)}.
\]

But notice that

\[
1^{(i)} \otimes s_{X_r}^{(n-i)} = \prod_{h_r < z < h_{r+1}} 1^{(i)} \otimes s_{X_r}^{(n-i)}(z-r, k_z-r) \overset{(3)}{=} \prod_{h_r < z < h_{r+1}} s(n)(z+i-r, k_z+i-r)
\]

hence

\[
1^{(i)} \otimes s_{X_r}^{(n-i)} = \prod_{r=0}^{i} 1^{(i)} \otimes s_{X_r}^{(n-i)} = \prod_{r=0}^{i} 1^{(i-r)} \otimes s_{A_r}^{(n-i+r)}
\]

so (***) holds and the proof is complete.

We can now derive the braid analog of the usual expression for the binomial coefficients in terms of factorials.
We will write \( p \) elementwise inside \( kB \times \) where section.

Multiplying both sides by \( 1 \) this (choosing \( \tilde{\cdot} \) the variables commute among themselves and with the coefficients. The embeddings \( kB \) of this yields

\[
\text{Formula (20) with } i = 1 \text{ says } 1 \otimes b_j^{(n-1)} \cdot [n] = [j] \otimes 1^{(n-j)} \cdot b_j^{(n)}.
\]

Repeated use of this yields

\[
1^{(j-1) \otimes [n-j+1]} \cdot 1^{(j-2) \otimes [n-j+2]} \cdots \cdot 1 \otimes [n-1] : [n] = 1^{(j-1) \otimes [1]} 1^{(n-j)} \cdot 1^{(j-2) \otimes 2} 1^{(n-j)} \cdots \cdot 1^{(j-1)} 1^{(n-j)} \cdot [j] \otimes 1^{(n-j)} \cdot b_j^{(n)} = f(j) \otimes 1^{(n-j)} \cdot b_j^{(n)}
\]

(15)

Multiplying both sides by \( 1^{(j) \otimes f^{(n-j)}} \) and using (15) we get the result. \( \square \)

It seems that in the course of the proof of (21) we obtained a stronger “simplified” formula; in fact this is equivalent to (21) since the braid group algebras do not possess zero divisors.

Recall that the natural braids \( [j] \) are not \( \sim \)-symmetric. However, an amusing consequence of (20) is this (choosing \( n = j + 1, i = 1 \)):

\[
1 \otimes [j] \cdot [j + 1] = [j] \otimes 1 \cdot [j + 1].
\]

Thus this element is fixed by \( \sim \).

6. Rota’s binomial theorem, Cauchy’s identities and Möbius inversion

6.1. The binomial theorem. The following remarkable \( q \)-binomial theorem is proven in [GR1]: if \( P_k(x, y) = (x - y)(x - qy) \cdots (x - q^{k-1}y) \) then

\[
P_n(x, z) = \sum_{k=0}^{n} \binom{n}{k} P_k(x, y) P_{n-k}(y, z),
\]

this is an identity in the ordinary polynomial ring \( k[x, y, z] \). When \( q = 1 \) this reduces to the familiar

\[
(x - z)^n = \sum_{k=0}^{n} \binom{n}{k} (x - y)^k (y - z)^{n-k}.
\]

We will generalize this result to the context of braids, and derive from it the other results of the section.

We consider ordinary polynomial rings \( kB_n[x_1, \ldots, x_r] \) over the non-commutative ring \( kB_n \); thus, the variables commute among themselves and with the coefficients. The embeddings

\[
B_k \to B_n, \; s \mapsto s \otimes 1^{(n-k)} \quad \text{and} \quad B_{n-k} \to B_n, \; t \mapsto 1^{(k)} \otimes t
\]

eextend to embeddings

\[
kB_k[x_1, \ldots, x_r] \to kB_n[x_1, \ldots, x_r], \; p \mapsto p \otimes 1^{(n-k)} \quad \text{and} \quad kB_{n-k}[x_1, \ldots, x_r] \to kB_n[x_1, \ldots, x_r], \; q \mapsto 1^{(k)} \otimes q
\]

where \( x_i \) is sent to \( x_i \) in both cases. The images of \( kB_k[x_1, \ldots, x_r] \) and \( kB_{n-k}[x_1, \ldots, x_r] \) commute elementwise inside \( kB_n[x_1, \ldots, x_r] \), so there is an induced map

\[
kB_k[x_1, \ldots, x_r] \otimes kB_{n-k}[x_1, \ldots, x_r] \to kB_n[x_1, \ldots, x_r], \; p \otimes q \mapsto p \otimes 1^{(n-k)} \cdot 1^{(k)} \otimes q.
\]

We will write \( p \otimes q \) for \( p \otimes 1^{(n-k)} \cdot 1^{(k)} \otimes q \).

\footnote{In fact, \( B_n \) is right-ordered by a recent result of Dehornoy [Deh], hence \( kB_n \) does not possess zero divisors nor non-trivial units by the results in chapter 13.1 of Passman’s book [Pas]. We thank Dale Rolfsen for making us aware of this.}
For any \( k \geq 1 \) let
\[
P_k(x, y) = [x - s^{(k)}(1, k)y] \cdot [x - s^{(k)}(1, k - 1)y] \cdot \ldots \cdot [x - s^{(k)}(1, 1)y] \in kB_k[x, y]
\]
and set \( P_0(x, y) = 1 \in kB_0 \).

Then, with the above convention, the binomial theorem is the following identity in \( kB_n[x, y, z] \):

**Proposition.** For any \( n \geq 0 \),
\[
P_n(x, z) = \sum_{k=0}^{n-1} P_k(y, z) \otimes P_{n-k}(x, y) \cdot t^{(n)}_k.
\]

**Proof.** We do induction on \( n \). For \( n = 0, 1 \) the statement is trivial. Assuming it true for \( n - 1 \) with \( n \geq 2 \), we have
\[
P_n(x, z) = [x - s^{(n)}(1, n)z] \cdot [P_{n-1}(x, z) \otimes 1] = [x - s^{(n)}(1, n)z] \cdot \sum_{k=0}^{n-1} [P_k(y, z) \otimes P_{n-1-k}(x, y) \otimes 1] \cdot [b^{(n-1)}_k \otimes 1]
\]
\[
= \sum_{k=0}^{n-1} [x - s^{(n)}(k + 1, n)y + s^{(n)}(k + 1, n)y - s^{(n)}(1, n)z] \cdot [P_k(y, z) \otimes P_{n-1-k}(x, y) \otimes 1] \cdot [b^{(n-1)}_k \otimes 1] +
\]
\[
= \sum_{k=0}^{n-1} [y - s^{(n)}(1, k + 1)z] \cdot [P_k(y, z) \otimes 1^{(n-k)}] \cdot s^{(n)}(k + 1, n) \cdot [1^{(k)} \otimes P_{n-1-k}(x, y) \otimes 1] \cdot [b^{(n-1)}_k \otimes 1] +
\]
\[
= \sum_{k=0}^{n-1} [y - s^{(n)}(k + 1, 1)z] \cdot [P_k(y, z) \otimes 1^{(n-k-1)}] \cdot s^{(n)}(k + 1, n) \cdot [1^{(k+1)} \otimes P_{n-1-k}(x, y) \otimes 1] \cdot [b^{(n-1)}_k \otimes 1] +
\]
\[
= \sum_{k=0}^{n-1} [P_k(y, z) \otimes 1^{(n-k)}] \cdot [1^{(k)} \otimes P_{n-1-k}(x, y)] \cdot [b^{(n-1)}_k \otimes 1] +
\]
\[
= \sum_{k=0}^{n-1} [P_{k+1}(y, z) \otimes 1^{(n-k-1)}] \cdot s^{(n)}(k + 1, n) \cdot [1^{(k)} \otimes P_{n-1-k}(x, y) \otimes 1] \cdot [b^{(n-1)}_k \otimes 1].
\]

Now we use (5) to commute \( s^{(n)}(k + 1, n) \) past \( P_{n-1-k}(x, y) \) as follows:
\[
s^{(n)}(k + 1, n) \cdot [1^{(k)} \otimes P_{n-1-k}(x, y) \otimes 1] = s^{(n)}(k + 1, n) \cdot \left[1^{(k)} \otimes [x - s^{(n-1-k)}(1, n - 1 - k)y] \cdot \ldots \cdot [x - s^{(n-1-k)}(1, 1)y] \otimes 1\right]
\]
\[
= [x - s^{(n)}(k + 1, n)y] \cdot \ldots \cdot [x - s^{(n)}(k + 1, k + 1)y] \cdot s^{(n)}(k + 1, n)
\]
\[
= 1^{(k+1)} \otimes [x - s^{(n-1-k)}(1, n - k - 1)y] \cdot \ldots \cdot [x - s^{(n-1-k)}(1, 1)y] \cdot s^{(n)}(k + 1, n)
\]
\[
= 1^{(k+1)} \otimes P_{n-1-k}(x, y) \cdot s^{(n)}(k + 1, n).
\]
Substituting this in the above expression for $P_n$ we get

$$P_n(x, z) = \sum_{k=0}^{n-1} [P_k(y, z) \otimes 1^{(n-k)}] \cdot [1^{(k)} \otimes P_{n-k}(x, y)] \cdot [b_k^{(n-1)} \otimes 1] +$$

$$+ \sum_{k=0}^{n-1} [P_{k+1}(y, z) \otimes 1^{(n-k-1)}] \cdot [1^{(k+1)} \otimes P_{n-1-k}(x, y)] \cdot s^{(n)}(k+1, n) \cdot [b_k^{(n-1)} \otimes 1]$$

$$= \sum_{k=0}^{n-1} [P_k(y, z) \otimes P_{n-k}(x, y)] \cdot [b_k^{(n-1)} \otimes 1] + \sum_{k=0}^{n} [P_k(y, z) \otimes P_{n-k}(x, y)] \cdot s^{(n)}(k+1, n) \cdot [b_k^{(n-1)} \otimes 1]$$

$$= \sum_{k=0}^{n} [P_k(y, z) \otimes P_{n-k}(x, y)] \cdot [b_k^{(n-1)} \otimes 1 + s^{(n)}(k+1, n) \cdot b_k^{(n-1)} \otimes 1] = \sum_{k=0}^{n} [P_k(y, z) \otimes P_{n-k}(x, y)] \cdot b_k^{(n)} \cdot 1^{(k)}.$$ 

\[\square\]

6.2. Cauchy’s identities. These identities are attributed to Cauchy in [GR1]:

$$(x - 1)(x - q) \ldots (x - q^{n-1}) = \sum_{k=0}^{n} \left[ \begin{array}{c} n \\ k \end{array} \right] (-1)^k q^k \cdot x^{n-k},$$

$$x^n = \sum_{k=0}^{n} \left[ \begin{array}{c} n \\ k \end{array} \right] (x - 1)(x - q) \ldots (x - q^{k-1}).$$

Just as in the $q$-case, its generalizations to braids are easily obtained from the binomial theorem. In this context, it is natural to introduce the Möbius braid $\mu^{(k)} \in kB_k$ as

$$\mu^{(k)} = (-1)^k c^{(k)}$$

where $c^{(k)} = s^{(k)}(1, k)s^{(k)}(1, k - 1) \ldots s^{(k)}(1, 1) \in kB_k$ is the twistor braid of section 2.2.

**Corollary.** For any $n \geq 0$,

$$(23) \quad [x - s^{(n)}(1, n)] \cdot [x - s^{(n)}(1, n-1)] \cdot \ldots \cdot [x - s^{(n)}(1, 1)] = \sum_{k=0}^{n} \mu^{(k)} \otimes 1^{(n-k)} \cdot b_k^{(n)} \cdot x^{n-k}$$

$$(24) \quad x^n = \sum_{k=0}^{n} [x - s^{(n)}(k+1, n)] \cdot [x - s^{(n)}(k+1, n-1)] \cdot \ldots \cdot [x - s^{(n)}(k+1, k+1)] \cdot b_k^{(n)}.$$ 

**Proof.** Setting $y = 0$ and $z = 1$ in (22) we obtain (23); setting $y = 1$ and $z = 0$ we obtain (24). These evaluations are well-defined morphisms of algebras because the evaluating points commute with the coefficients. \[\square\]

Möbius inversion formula will be deduced from the following two consequences of Cauchy’s identities. Setting $x = 1$ in (23) we obtain

$$(25) \quad \sum_{k=0}^{n} \mu^{(k)} \otimes 1^{(n-k)} \cdot b_k^{(n)} = 0 \forall n > 0,$$

and setting $x = 0$ in (24) (or applying $\sim$ to (25))

$$(26) \quad \sum_{k=0}^{n} 1^{(k)} \otimes \mu^{(n-k)} \cdot b_k^{(n)} = 0 \forall n > 0.$$
Both of these reduce in the \(q\)-case to the well-known

\[
\sum_{k=0}^{n} (-1)^k q^{\binom{i}{j}} \left[\begin{array}{c} n \\ k \end{array}\right] = 0 \quad \forall \ n > 0.
\]

Some other interesting consequences of Cauchy’s identities are obtained through other evaluations; these all reduce to the same identity in the \(q\)-case, but are distinct at the level of braids. To briefly discuss this situation, consider the polynomial ring \(B[x]\) over a non-commutative ring \(B\). For each \(b \in B\) there are two natural evaluation maps \(B[x] \to B\), according to whether we write the variable to the right or left of the coefficients. More precisely, these are defined as

\[
e_\ell^b : B[x] \to B \\
e_r^b : B[x] \to B
\]

These maps are not multiplicative in general; however, if \(h\), \(f\) and \(g\) are polynomials such that \(h = fg\) and \(b\) commutes with the coefficients of \(g\), then \(e_\ell^b(h) = e_\ell^b(f)e_\ell^b(g)\). Similarly, if \(b\) commutes with the coefficients of \(f\) then \(e_r^b(h) = e_r^b(f)e_r^b(g)\).

Consider \(B = kB_1\), \(f(x) = [x - s^{(n)}(1, n)] \cdot [x - s^{(n)}(1, n - 1)] \cdot \ldots \cdot [x - s^{(n)}(1, 3)]\) and \(g(x) = [x - s^{(n)}(1, 2)] [x - s^{(n)}(1, 1)]\). Writing \(x\) to the right of the coefficients and evaluating (23) at \(b = s^{(n)}(1, 2) = s^{(n)}_1\) we obtain

\[
\sum_{k=0}^{n} \mu^{(k)} \odot 1^{(n-k)} \cdot b_k^{(n)} \cdot (s^{(n)}_1)^{n-k} = 0.
\]

Similarly, letting \(f(x) = x - s^{(n)}(1, n)\), \(g(x) = [x - s^{(n)}(1, n - 1)] \cdot \ldots \cdot [x - s^{(n)}(1, 1)]\), writing \(x\) to the left and evaluating (23) at \(b = s^{(n)}(1, n)\) we obtain

\[
\sum_{k=0}^{n} [s^{(n)}(1, n)]^{n-k} \cdot \mu^{(k)} \odot 1^{(n-k)} \cdot b_k^{(n)} = 0.
\]

6.3. **Möbius inversion.** A particular case of the general theory of Möbius inversion [R] is the following \(q\)-numerical inversion formula: for any scalars \(a_0, \ldots, a_m, b_0, \ldots, b_m\),

\[
b_i = \sum_{j=0}^{i} \left[\begin{array}{c} i \\ j \end{array}\right] a_{i-j} \forall \ i = 0, \ldots, m \iff a_i = \sum_{j=0}^{i} (-1)^{j}q^{\binom{l}{j}} \left[\begin{array}{c} i \\ j \end{array}\right] b_{i-j} \forall \ i = 0, \ldots, m.
\]

Its generalization is:

**Proposition.** Let \(x^{(i)}\) and \(y^{(i)}\) \(\in kB_i\) be given braids for \(i = 0, \ldots, m\). Then

\[
x^{(i)} = \sum_{j=0}^{i} \mu^{(j)} \odot x^{(i-j)} \cdot b_j^{(i)} \forall \ i = 0, \ldots, m \iff y^{(i)} = \sum_{j=0}^{i} \mu^{(j)} \odot x^{(i-j)} \cdot b_j^{(i)} \forall \ i = 0, \ldots, m.
\]
We usually write
\( f(2) = \sum_{j=0}^{i} \mu^{(j)} \otimes x^{(i-j)} \cdot b_j^{(i)}(\text{hyp.}) = \sum_{j=0}^{i} \mu^{(j)} \otimes \left[ \sum_{h=0}^{i-j} 1^{(h)} \otimes y^{(i-j-h)} \cdot b_h^{(i-j)} \right] \cdot b_j^{(i)} \)

\( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ \mu^{(j)} \otimes 1^{(h)} \otimes y^{(i-j-h)} \right] \cdot \left[ 1^{(j)} \otimes b_h^{(i-j)} \right] \cdot b_j^{(i)} \)

(20) \( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ \mu^{(j)} \otimes 1^{(i-j)} \right] \cdot \left[ b_j^{(h+j)} \otimes 1^{(i-j-h)} \right] \cdot b_h^{(i)} \)

\( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ \mu^{(j)} \otimes 1^{(i-j)} \right] \cdot \left[ b_j^{(h+j)} \otimes y^{(i-j-h)} \right] \cdot b_h^{(i)} \)

\( (k := h + j) \sum_{k=0}^{i} \sum_{j=0}^{k} \left[ \mu^{(j)} \otimes 1^{(i-j)} \right] \cdot \left[ b_j^{(k)} \otimes y^{(i-k)} \right] \cdot b_k^{(i)} = y^{(i)}, \)

since by (23) all terms corresponding to \( k \neq 0 \) in the above sum vanish.

(\( \Leftarrow \))

\( \sum_{j=0}^{i} 1^{(j)} \otimes y^{(i-j)} \cdot b_j^{(i)}(\text{hyp.}) = \sum_{j=0}^{i} 1^{(j)} \otimes \left[ \sum_{h=0}^{i-j} \mu^{(h)} \otimes x^{(i-j-h)} \cdot b_h^{(i-j)} \right] \cdot b_j^{(i)} \)

\( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ 1^{(j)} \otimes \mu^{(h)} \otimes x^{(i-j-h)} \right] \cdot \left[ 1^{(j)} \otimes b_h^{(i-j)} \right] \cdot b_j^{(i)} \)

(20) \( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ 1^{(j)} \otimes \mu^{(h)} \otimes x^{(i-j-h)} \right] \cdot \left[ b_j^{(h+j)} \otimes 1^{(i-j-h)} \right] \cdot b_h^{(i)} \)

\( = \sum_{j=0}^{i} \sum_{h=0}^{i-j} \left[ 1^{(j)} \otimes \mu^{(h)} \otimes x^{(i-j-h)} \right] \cdot \left[ b_j^{(h+j)} \otimes x^{(i-j-h)} \right] \cdot b_h^{(i)} \)

\( (k := h + j) \sum_{k=0}^{i} \sum_{j=0}^{k} \left[ 1^{(j)} \otimes \mu^{(k-j)} \otimes b_j^{(k)} \otimes x^{(i-k)} \right] \cdot b_k^{(i)} = x^{(i)}, \)

since by (24) all terms corresponding to \( k \neq 0 \) in the above sum vanish.

\( \square \)

7. Multinominal Braids

7.1. Definition. For each \( n \) and \( r \in \mathbb{N} \) let \( \mathcal{F}(n, r) \) denote the set of all functions \( \{1, \ldots, n\} \rightarrow \{1, \ldots, r\} \), and \( \mathcal{C}(n, r) = \{ (\eta_1, \ldots, \eta_r) \in \mathbb{N}^r / \eta_1 + \ldots + \eta_r = n \} \). A sequence \( \eta \in \mathcal{C}(n, r) \) is sometimes called a weak composition of \( n \) into \( r \) parts. For any \( \eta \in \mathcal{C}(n, r) \) let

\( S(\eta) = \{ f \in \mathcal{F}(n, r) / \# f^{-1}(1) = \eta_1, \# f^{-1}(2) = \eta_2, \ldots, \# f^{-1}(r) = \eta_r \}. \)

We usually write \( f = (1 \ 2 \ 3 \ 4 \ 5) \) to abbreviate that \( f : \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3\} \) is \( f(1) = f(5) = 2, \ f(2) = f(3) = 1, \ f(4) = 3. \) One may think of the elements of \( S(\eta) \) as permutations of the elements of \( \{1, 2, \ldots, r\} \) with repetitions as specified by \( \eta \). For this reason the elements of \( S(\eta) \) are called permutations of the multiset \( \{1^{n_1}, 2^{n_2}, \ldots, r^{n_r}\} \).

There are canonical identifications \( S(1, 1, \ldots, 1) = S_r \) (r ones) and (when \( r = 2 \) ) \( S(i, n-i) = S_r(n), \)

\( f \mapsto \{ j \in \{1, 2, \ldots, n\} / f(j) = 1 \}. \)
Given \( \eta \in \mathbb{C}(n, r) \), the corresponding \( q \)-multinomial coefficient is defined as
\[
\binom{n}{\eta} = \sum_{f \in \mathcal{S}(\eta)} q^{\text{inv}(f)},
\]
where the \textit{inversion index} \( \text{inv}(f) \) is
\[
\text{inv}(f) = \# \{(i, j) \mid 1 \leq i < j \leq n, \ f(i) > f(j)\}.
\]

To define its braid analog we proceed as follows. First, for any \( f \in \mathcal{F}(n, r) \) and \( i \in \{1, 2, \ldots, n\} \), set
\[
e_i(f) = \# \{j \leq i / f(j) \leq f(i)\}.
\]

Next, define \( s_f^{(n)} \in B_n \) as
\[
s_f^{(n)} = s^{(n)}(e_n(f), n) \cdot \cdots \cdot s^{(n)}(e_2(f), 2) \cdot s^{(n)}(e_1(f), 1).
\]

Then, for any \( \eta \in \mathbb{C}(n, r) \), define the multinomial braid \( m^{(\eta)} \in kB_n \) as
\[
m^{(\eta)} = \sum_{f \in \mathcal{S}(\eta)} s_f^{(n)};
\]
and \( m^{(0, \ldots, 0)} = 1 \in kB_0 \).

A few remarks are in order. First, notice that for \( \sigma \in S_r = \mathbb{S}(1, 1, \ldots, 1) \) (\( r \) ones), the definition of \( s_\sigma^{(n)} \) given here coincides with that of section 5, because of equation (19). Hence \( m^{(1, 1, \ldots, 1)} = f^{(r)} \), the factorial braid.

Second, suppose \( r = 2 \), and let \( I \in \mathbb{S}(n) \) correspond to \( f \in \mathcal{S}(n, n - i) \) under the bijection described above: if \( I = \{j_1 < j_2 < \ldots < j_i\} \) then \( f = \left( \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \ \frac{1}{2} \ 2 \right) \).

Thus, \( e_j(f) = \begin{cases} j & \text{if } j \notin I, \\ h & \text{if } j = j_h \in I, \end{cases} \)
from where \( s_f^{(n)} = s^{(n)}(i, j_i) \cdot \cdots \cdot s^{(n)}(2, j_2) \cdot s^{(n)}(1, j_1) = s_I^{(n)} \), and hence \( m^{(i, n-i)} = b_I^{(n)} \). Thus multinomial braids reduce to binomial braids when \( r = 2 \).

Finally, let us check that in the one-dimensional representation defined by \( q \) (section 2.5), \( s_f^{(n)} \) acts as multiplication by \( q^{\text{inv}(f)} \), and hence \( m^{(\eta)} \) as \( \binom{n}{\eta} \).

To this end, we introduce the \( \eta \)-shuffle \( \sigma_f \in S_n \) corresponding to \( f \in \mathcal{S}(\eta) \) as follows: on \( f^{-1}(1) \), \( \sigma_f \) is the unique increasing bijection onto \( \{1, \ldots, \eta\} \), similarly on \( f^{-1}(2) \) onto \( \{\eta_1 + 1, \ldots, \eta_1 + \eta_2\} \), and on \( f^{-1}(r) \) onto \( \{\eta_1 + \ldots + \eta_{r-1} + 1, \ldots, \eta_1 + \ldots + \eta_r\} \).

We also introduce the partial inversion index \( r_i(f) = \# \{j > i / f(j) < f(i)\} \), extending the one already defined for permutations in section 5. Notice that \( \text{inv}(f) = \sum_{i=1}^n r_i(f) \).

\textbf{Lemma.} For any \( f \in \mathcal{S}(\eta) \) and \( i \in \{1, 2, \ldots, n\} \), \( e_i(f) = e_i(\sigma_f) \) and \( r_i(f) = r_i(\sigma_f) \).

\textbf{Proof.} From the definition of \( \sigma_f \) we see that:

For \( j \leq i \), \( \sigma_f(j) \leq \sigma_f(i) \iff f(j) \leq f(i) \). From here, \( e_i(f) = e_i(\sigma_f) \).

For \( j > i \), \( \sigma_f(j) < \sigma_f(i) \iff f(j) < f(i) \). From here, \( r_i(f) = r_i(\sigma_f) \).

Now we can show that \( s_f^{(n)} \) acts as \( q^{\text{inv}(f)} \), i.e. that the number of elementary generators in \( s^{(n)}(e_n(f), n) \cdot \cdots \cdot s^{(n)}(e_2(f), 2) \cdot s^{(n)}(e_1(f), 1) \) is \( \text{inv}(f) \). Recall (section 5.3) that for any \( \sigma \in S_n \) we have \( \sigma(i) = r_i(\sigma) + e_i(\sigma) \). Hence, \( \sigma_f(i) = r_i(\sigma_f) + e_i(\sigma_f) = r_i(f) + e_i(f) \), from where
\[
\# \text{generators in } s_f^{(n)} = \sum_{i=1}^n i - e_i(f) = \sum_{i=1}^n \sigma_f(i) - e_i(f) = \sum_{i=1}^n r_i(f) = \text{inv}(f),
\]
as needed.
From the lemma we also deduce that \( s_f(n) = s_{\bar{\tau}}(n) \), just comparing their definitions. This shows that our multinomial braids coincide with those braids already considered by Schauenburg in [S, definition 2.6]. Some of the identities we prove here ([(13), (21), and a particular case of (29)]) are stated in that paper, although the connection to combinatorics is not pointed out.

7.2. Symmetry of the multinomial braids. Here we generalize the facts (12) and (17) that \( \overline{b_i(n)} = b_{n-i}(n) \) and \( \overline{f(n)} = f(n) \). For any \( \eta = (\eta_1, \eta_2, \ldots, \eta_r) \), let \( \bar{\eta} = (\eta_r, \ldots, \eta_2, \eta_1) \).

Proposition. For any \( \eta \in \Sigma(n,r) \), \( m(\eta) = m(\bar{\eta}) \).

Proof. Consider the bijection \( F(n,r) \to F(n,r) \), \( f \to \bar{f} \), where \( \bar{f}(i) = r + 1 - f(n+1-i) \). This clearly restricts to a bijection \( S(\eta) \to S(\bar{\eta}) \), so it is enough to show that

\[
\overline{s_f(n)} = s_{\bar{\tau}}(n) \forall f \in S(\eta)
\]

to obtain the result.

We have that

\[
\bar{f}^{-1}(h) = n + 1 - f^{-1}(r + 1 - h), \forall h = 1, \ldots, r,
\]

from where

\[
\sigma_{\bar{f}}(i) = n + 1 - \sigma_f(n + 1 - i) = \overline{\sigma_f(i)} \forall i = 1, \ldots, n,
\]

and thus

\[
\overline{s_f(n)} = s_{\bar{\tau}}(n) = s_{\sigma_{\bar{f}}}(n) = s_{\sigma_f}(n) = s_f(n)
\]

as needed.

7.3. Pascal’s identity for multinomial braids. Let \( \Sigma^+(n,r) \) denote the set of strict compositions of \( n \) into \( r \) parts, i.e. those sequences \((\eta_1, \ldots, \eta_r)\) such that \( \eta_1 + \ldots + \eta_r = n \) and \( \eta_i \in \mathbb{Z}^+ \) \( \forall i = 1, \ldots, r \).

Pascal’s identity (13) is actually a particular case of the following identity for multinomial braids.

Proposition. For any \( \eta \in \Sigma^+(n,r) \),

\[
m^{(\eta_1, \eta_2, \ldots, \eta_r)} = s^{(n)}(\eta_1, n) \cdot m^{(\eta_1-1, \eta_2, \ldots, \eta_r)} \odot 1 + s^{(n)}(\eta_1 + \eta_2, n) \cdot m^{(\eta_1, \eta_2-1, \ldots, \eta_r)} \odot 1 + \ldots + s^{(n)}(\eta_1 + \eta_2 + \ldots + \eta_r, n) \cdot m^{(\eta_1, \eta_2, \ldots, \eta_r-1)} \odot 1.
\]

Proof. Consider the bijection

\[
\prod_{i=1}^r S(\eta_1, \ldots, \eta_i - 1, \ldots, \eta_r) \to S(\eta_1, \eta_2, \ldots, \eta_r)
\]

that sends \( f \in S(\eta_1, \ldots, \eta_i - 1, \ldots, \eta_r) \) to \( g \in S(\eta_1, \eta_2, \ldots, \eta_r) \) defined by

\[
g(j) = \begin{cases} f(j) & \text{if } j \in \{1, 2, \ldots, n-1\}, \\ i & \text{if } j = n. \end{cases}
\]
Hence \( s^{(n)}_g = s^{(n)}(\eta_1 + \eta_2 + \ldots + \eta_i, n) \cdot s^{(f)}_{n-1} \odot 1 \). The result follows by summing over all such \( f' \)s. 

7.4. Multinomials in terms of binomials and factorials. In this section we relate the multinomial braids to the binomials and factorials, obtaining identities that generalize (20) and (21).

**Proposition.** Let \((\eta_1, \ldots, \eta_r) \in \mathcal{E}(n, r) \), \( s \leq r \), and \( n_1 = \eta_1 + \ldots + \eta_s \), \( n_2 = \eta_{s+1} + \ldots + \eta_r \). Then

\[
\begin{align*}
\text{multinomial } m^{(n_1, \ldots, n_r)} & = m^{(n_1, \ldots, n_s)} \odot m^{(n_{s+1}, \ldots, n_r)} \odot m^{(n_1, n_2)}.
\end{align*}
\]

**Proof.** Consider the bijection

\[
\begin{align*}
S(\eta_1, \ldots, \eta_r) & \rightarrow S(\eta_1, \ldots, \eta_s) \times S(\eta_{s+1}, \ldots, \eta_r) \times S(n_1, n_2) \\
\text{or } & (f_1, f_2, I)
\end{align*}
\]

defined as follows:

\[
\begin{align*}
I & = \{ j \in \{1, \ldots, n\} \mid f(j) \leq s \} = \{ j_1 < j_2 < \ldots < j_{n_1} \} \in S_{n_1}(n), \\
I^c & = \{ k \in \{1, \ldots, n\} \mid f(k) > s \} = \{ k_1 < k_2 < \ldots < k_{n_2} \} \in S_{n_2}(n), \\
f_1 & = (f_{(1)} f_{(2)} \ldots f_{(n_1)}) \in S(\eta_1, \ldots, \eta_s), \\
f_2 & = (f_{(k_{-s})} f_{(k_{-s+1})} \ldots f_{(n_2)_{-s}}) \in S(\eta_s+1, \ldots, \eta_r).
\end{align*}
\]

(Informally, \( f_1 = f|_{i}, f_2 = f|_{r-i} \).

It is enough to show that

\[
\begin{align*}
s^{(n)}_f = s^{(f_1)}_{n_1} \odot s^{(f_2)}_{n_2} \odot s^{(I)}.
\end{align*}
\]

We start by noting that for any \( j \in \{1, \ldots, n\}, \)

\[
\begin{align*}
e_j(f) & = \# \{ h \in \{1, \ldots, n\} \mid h \leq j \text{ and } f(h) \leq f(j) \} \\
& = \# \{ h \in I \mid h \leq j \text{ and } f(h) \leq f(j) \} + \# \{ h \in I^c \mid h \leq j \text{ and } f(h) \leq f(j) \}.
\end{align*}
\]

Thus, if \( j = j_1 \in I, \)

\[
\begin{align*}
(*) \quad e_j(f) & = \# \{ h \in I \mid h \leq j \text{ and } f(h) \leq f(j) \} = e_i(f_1), \\
while \text{ if } j = k_i \in I^c, \\
(\ast) \quad e_j(f) & = \# \{ h \in I \mid h \leq j \} + \# \{ h \in I^c \mid h \leq j \text{ and } f(h) \leq f(j) \} \\
& = \# \{1, 2, \ldots, k_i\} - \# \{ h \in I^c \mid h \leq k_i \} + e_i(f_2)
\end{align*}
\]

(\ast\ast)

\[
\begin{align*}
& = k_i - i + e_i(f_2).
\end{align*}
\]

Now,

\[
\begin{align*}
(2) & = 1^{(n)} \odot s^{(f_2)}_{n_2} \odot s^{(n)}(e_{n_1}(f_1), n_1) \odot \ldots \odot s^{(n)}(e_{1}(f_1), 2) \odot s^{(n)}(e_{1}(f_1), 1) s^{(n)}(n_1, j_{n_1}) \odot \ldots \odot s^{(n)}(2, j_2) \odot s^{(n)}(1, j_1) \\
(\text{A1}) & = 1^{(n)} \odot s^{(f_2)}_{n_2} \odot s^{(n)}(e_{n_1}(f_1), j_{n_1}) \odot \ldots \odot s^{(n)}(e_{2}(f_1), j_2) \odot s^{(n)}(e_{1}(f_1), j_1) \\
(3) & = s^{(n)}(n_1 + e_{n_2}(f_2), n_1 + n_2) \cdot s^{(n)}(n_1 + e_{2}(f_2), n_1 + 2) \cdot \ldots \cdot s^{(n)}(n_1 + e_{1}(f_2), n_1 + 1) \cdot s^{(n)}(e_{n_1}(f_1), j_{n_1}) \odot \ldots \odot s^{(n)}(e_{2}(f_1), j_2) \odot s^{(n)}(e_{1}(f_1), j_1).
\end{align*}
\]
At this point there are two cases to distinguish, according to whether $k_1 = n_1 + 1$ or $k_1 \leq n_1$ (notice that necessarily $k_1 \leq n_1 + 1$, since $k_1$ is the first element of $I^n$).

If $k_1 = n_1 + 1$ then necessarily $j_i = i$ and $k_i = n_1 + i \forall i$, so

$$s^{(n)}(n_1 + e_1(f_2), n_1 + i) = s^{(n)}(k_i - i + e_1(f_2), n_1 + i) \overset{(**)}{=} s^{(n)}(e_{k_i}(f), n_1 + i) = s^{(n)}(e_{n_1+i}(f), n_1 + i)$$

and

$$s^{(n)}(e_i(f_1), j_i) \overset{(*)}{=} s^{(n)}(e_{j_i}(f_1), j_i) = s^{(n)}(e_i(f), i).$$

Thus, in this case, all the factors in the above expression for $s^{(f_1)}_{n_1} \otimes s^{(f_2)}_{n_2} \cdot s^{(n)}_f$ are already in the “right order”:

$$s^{(f_1)}_{n_1} \otimes s^{(f_2)}_{n_2} \cdot s^{(n)}_f = s^{(n)}(e_{n_1+n_2}(f), n_1 + n_2) \cdot \ldots \cdot s^{(n)}(e_{n_1+1}(f), n_1 + 1) \cdot s^{(n)}(e_{n_1}(f), n_1) \cdot \ldots \cdot s^{(n)}(e_1(f), 1) = s^{(n)}_f,$$

as needed.

The other case occurs when $k_1 \leq n_1$. In this case $j_{k_1}$ is well-defined. We will move $s^{(n)}(n_1 + e_1(f_2), n_1 + 1)$ to its right past the factors $x_i := s^{(n)}(e_i(f_1), j_i)$ from $i = n_1$ down to $i = k_1$, using (5). We illustrate this process as follows:

$$s^{(n)}(n_1 + e_1(f_2), n_1 + 1) \xrightarrow{\text{past } x_{n_1}} s^{(n)}(n_1 + 1 + e_1(f_2), n_1) \xrightarrow{\text{past } x_{n_1-1}} \ldots \xrightarrow{\text{past } x_{i+1}} s^{(n)}(i + e_1(f_2), i + 1) \xrightarrow{\text{past } x_i} \ldots \xrightarrow{\text{past } x_{k_1}} s^{(n)}(k_1 - 1 + e_1(f_2), k_1) \overset{(**)}{=} s^{(n)}(e_{k_1}(f), k_1).$$

Before proceeding, we must check that the hypothesis of (5) hold, in order to validate this commutation. In this situation those hypothesis are

$$e_i(f_1) \leq i - 1 + e_1(f_2) \text{ and } i \leq j_i - 1, \forall i \in \{k_1, \ldots, n_1\}.$$ 

The first inequality holds because, for any $f$ and $g$, $e_i(f) \leq i$ and $e_1(g) \geq 1$. And the second one does too, for if not, we would have that $j_i \leq i$ and hence $\{j_1, j_2, \ldots, j_i\} = \{1, 2, \ldots, i\}$. But since $k_1 \leq i$, this would imply that $k_1 \in I$, a contradiction. Thus the commutation process described above is valid.

Returning to the main argument, we next proceed similarly with the remaining factors $s^{(n)}(n_1 + e_2(f_2), n_1+2), \ldots, s^{(n)}(n_1 + e_{n_2}(f_2), n_1+n_2)$, moving them to the right until they become $s^{(n)}(e_{k_2}(f), k_2)$, $\ldots, s^{(n)}(e_{k_{n_2}}(f), k_{n_2})$. After this has been done we are left with all the factors in the “right order”:

$$s^{(f_1)}_{n_1} \otimes s^{(f_2)}_{n_2} \cdot s^{(n)}_f = s^{(n)}(e_{n_1+n_2}(f), n_1 + n_2) \cdot \ldots \cdot s^{(n)}(e_{n_1+1}(f), n_1 + 1) \cdot s^{(n)}(e_{n_1}(f), n_1) \cdot \ldots \cdot s^{(n)}(e_1(f), 1) = s^{(n)}_f.$$ 

This completes the proof. 

From (29) we can easily deduce expressions for the multinomial braids in terms of binomials or factorials, that generalize well-known $q$-formulas.
Corollary.

\[(30)\]

\[
m^{(n_1,\ldots,n_r)} = 1^{(n_1+\ldots+n_{r-1})} \otimes 1^{(n_1+\ldots+n_{r-2})} \otimes 1^{(n_1+\ldots+n_{r-1})} \cdot 1^{(n_{r-1}+n_r)} \cdot b_0^{(n_1+\ldots+n_r)}. \]

\[(31)\]

\[
m^{(n_1,\ldots,n_r)} = b_0^{(n_1)} \otimes 1^{(n_2+\ldots+n_r)} \cdot b_0^{(n_1+n_2)} \otimes 1^{(n_3+\ldots+n_r)} \cdot b_0^{(n_1+n_2+n_3)} \otimes 1^{(n_4+\ldots+n_r)} \cdots \cdot b_0^{(n_1+\ldots+n_{r-1})} \otimes 1^{(n_r)} \cdot b_0^{(n_1+\ldots+n_{r-1})}.
\]

\[(32)\]

\[
f^{(n_1)} \otimes \cdots \otimes f^{(n_r)} \cdot m^{(n_1,\ldots,n_r)} = f^{(n_1+\ldots+n_r)}
\]

Proof. Choosing \( s = 1 \) in equation (29) we get

\[
m^{(n_1,\ldots,n_r)} = 1^{(n_1)} \otimes m^{(n_2,\ldots,n_r)} \cdot b_0^{(n_1+\ldots+n_r)}.
\]

From here (30) follows immediately by induction on \( r \).

Similarly, (31) follows by induction on \( r \) from

\[
m^{(n_1,\ldots,n_r)} = m^{(n_1,\ldots,n_{r-1})} \otimes 1^{(n_r)} \cdot b_0^{(n_1+\ldots+n_{r-1})},
\]

which is the case \( s = r - 1 \) of (29).

The remaining identity can also be obtained by induction on \( r \), as follows:

\[
f^{(n_1)} \otimes \cdots \otimes f^{(n_r)} \cdot m^{(n_1,\ldots,n_r)} = \left[ f^{(n_1)} \otimes \cdots \otimes f^{(n_r)} \cdot m^{(n_1,\ldots,n_r)} \right] \otimes \left[ f^{(n_2+\ldots+n_r)} \otimes \cdots \otimes f^{(n_r)} \cdot m^{(n_1+\ldots+n_r)} \right] = m^{(n_1,n_2)} \]

\[(\text{ind.hyp.}) \]

\[
f^{(n_1)} \otimes f^{(n_2)} \cdot m^{(n_1,n_2)} = f^{(n)}.
\]

\[
7.5. \textbf{Witt’s identity.} \text{ The following identity for q-multinomials is a particular case of an identity that holds for all finite reflection groups, sometimes known as Witt’s identity:}
\]

\[
\sum_{r=0}^{n} (-1)^r \sum_{\eta \in \mathcal{C}^+(n,r)} \binom{n}{\eta} = (-1)^n q^{\binom{n}{2}}
\]

(this is [H, proposition 1.11] for the case of the reflection group \( S_n \).

Recall that \( \mathcal{C}^+(n,r) \) denotes the set of strict compositions of \( n \) into \( r \) parts. We should agree that

\[
\mathcal{C}^+(n,0) = \begin{cases} 0 & \text{if } n > 0, \\ \{0\} & \text{if } n = 0 \end{cases}, \text{ and that } m^{(0)} = 1 \in B_0.
\]

Witt’s identity can be generalized to braids as follows.

Proposition. For every \( n \geq 0 \),

\[
\sum_{r=0}^{n} (-1)^r \sum_{\eta \in \mathcal{C}^+(n,r)} m^{(n)} = \mu^{(n)}.
\]

Proof. We do induction on \( n \). For \( n = 0 \) the statement is obvious. Assume \( n \geq 1 \). Consider the decomposition

\[
\prod_{k=0}^{n-1} \mathcal{C}^+(k,r-1) \rightarrow \mathcal{C}^+(n,r), (\eta_1,\ldots,\eta_{r-1}) \mapsto (\eta_1,\ldots,\eta_{r-1},n-k).
\]

Recall that, by (31), for any \( \eta \in \mathcal{C}^+(k,r-1) \) we have

\[
m^{(n,n-k)} = m^{(\eta)} \otimes 1^{(n-k)} \cdot b_0^{(n)}.
\]
that when are studied in [GR2], where they are called the Galois numbers. They satisfy the following recurrence,

One may define Galois braids \( G \) as follows:

Thus,

These Galois braids \( g \) satisfy the simpler formula:

8. Galois, Fibonacci and Catalan Braids

The \( q \)-numbers

are studied in [GR2], where they are called the Galois numbers. They satisfy the following recurrence, that when \( q = 1 \) simply says that \( G_n = 2^n \):

One may define Galois braids \( G^{(n)} \in kB_n \) as

then one easily obtains the following generalization of the recurrence above:

Alternatively, one can define Galois braids \( g^{(n)} \in kB_n \) as follows:

these braids satisfy the simpler formula:

in fact, this is just the binomial theorem (22) at \( x = 1, y = 0, z = -1 \).

These Galois braids \( g^{(n)} \) specialize to Galois numbers

and the formula above becomes

\[ g_n = (1 + q^{n-1}) \cdot (1 + q^{n-2}) \cdot \ldots \cdot (1 + q) \cdot (1 + 1). \]
The Fibonacci numbers $F_n$ count the number of subsets of $\{1, 2, \ldots, n\}$ without consecutive elements; one has $F_n = F_{n-1} + F_{n-2}$. It is easy to obtain $q$-versions of these numbers. More general braid analogs can be defined as follows. Let $F(n, k)$ denote the set of subsets of $\{1, 2, \ldots, n\}$ with $k$ elements no two of which are consecutive, and set

$$F_k^{(n)} = \sum_{I \in F(n, k)} s_I^{(n)} \in kB_n.$$  

As for the Galois braids, we have two options for defining the Fibonacci braids in terms of the $F_k^{(n)}$, according to whether we weight by the twistors $c^{(k)}$ or not. As before, weighting leads to simpler identities. So we define the Fibonacci braids $F^{(n)} \in kB_n$ as

$$F^{(n)} = \sum_{k=0}^{n} c^{(k)} \otimes 1^{(n-k)} \cdot F_k^{(n)}.$$  

The same bijection considered in the proof of Pascal’s identity (13) shows that

$$F_k^{(n)} = F_k^{(n-1)} \otimes 1 + s^{(n)}(k, n) \cdot F_{k-1}^{(n-2)} \otimes 1^{(2)};$$

from here it follows easily that

$$F^{(n)} = F^{(n-1)} \otimes 1 + s^{(n)}(1, n) \cdot F^{(n-2)} \otimes 1^{(2)}.$$  

Thus these braids specialize to $q$-numbers $F_n$ that satisfy

$$F_n = F_{n-1} + q^{n-1}F_{n-2}.$$  

The Catalan numbers $C_n$ count the number of subsets $I$ of $\{1, 2, \ldots, 2n\}$ satisfying the following two conditions:

$$\#I = n \text{ and for every } j = 1, 2, \ldots, 2n, \#I \cap \{1, 2, \ldots, j\} \geq \#I^c \cap \{1, 2, \ldots, j\}.$$  

Let $C(n)$ denote the family of those subsets, and set

$$C^{(n)} = \sum_{I \in C(n)} s_I^{(2n)} \in kB_{2n}.$$  

It is easy to see from (*) in the proof of (12) that

$$C^{(n)} = \widetilde{C^{(n)}}.$$  

Similarly, from (*) in the proof of (14) one deduces that

$$C^{(n+1)} = \sum_{k=0}^{n} 1^{(k+1)} \otimes 1^{(k+1)} \otimes 1^{(n-k)} \cdot 1 \otimes C^{(k)} \otimes 1 \otimes C^{(n-k)}.$$  

Thus these braids specialize to $q$-numbers $C_n$ that satisfy

$$C_{n+1} = \sum_{k=0}^{n} q^{(k+1)(n-k)} C_k C_{n-k}.$$  

These are the $q$-Catalan numbers of Carlitz and Riordan [CR].
9. Binomial braids and quantum groups

In section 2.5 we explained how Yang-Baxter operators yield monoidal representations of the braid category $\mathcal{B}$. In this regard we should add that Majid began the study of combinatorial identities between operators on tensor powers of a vector space $X$ corresponding to a Yang-Baxter operator on $X \otimes X$: in thm. 10.4.12 of [Ma] the case $i = 1$ of (20) is obtained.

So far in this paper we have considered only one-dimensional representations, corresponding to the Yang-Baxter operator that simply multiplies by $q$. Other Yang-Baxter operators are obtained through the theory of quantum groups. Every module over a quasitriangular Hopf algebra comes equipped with a canonical Yang-Baxter operator on $X \otimes X$. The converse essentially holds: every Yang-Baxter operator on a vector space $X$ gives rise to a coquasitriangular bialgebra that coacts on $X$ (if the bialgebra is finite-dimensional then $X$ can be seen as a module over the dual bialgebra, which is quasitriangular).

An equivalent way to describe monoidal representations of the braid category is by means of the following fact: $\mathcal{B}$ is the free braided monoidal strict category on one object (the object $1 \in \mathbb{N}$). This says that given any object $X$ of a braided monoidal category $\mathcal{C}$, there is a unique functor $F : \mathcal{B} \rightarrow \mathcal{C}$ that preserves the monoidal structures and the braidings and such that $F(1) = X$. If $\mathcal{C}$ carries in addition a $k$-linear structure (compatible with the rest of the structure), then $F$ extends to $F : k\mathcal{B} \rightarrow \mathcal{C}$. Usually $\mathcal{C}$ consists of vector $k$-spaces with some additional structure, and thus $F : k\mathcal{B} \rightarrow \mathcal{C}$ yields linear representations of the various braid groups. This is the case for instance when $\mathcal{C}$ is the category of modules over a quasitriangular Hopf algebra as above. Another family of examples arises from the category $\mathcal{D}_G$ of crossed $G$-modules, for any group $G$. An object of $\mathcal{D}_G$ is a $k$-space $X$ equipped with a linear action of $G$ and a linear $G$-grading, i.e. a decomposition $X = \bigoplus_{g \in G} X_g$ into subspaces, such that the action of $h \in G$ carries $X_g$ to $X_{gh^{-1}}$. In this context, one usually writes $|x| = g$ when $x \in X_g$, so that the condition just mentioned becomes $|h \cdot x| = h|x| |h^{-1}$. This category is braided monoidal under the usual tensor product of $k$-spaces, where $X \otimes Y$ is equipped with the $G$-action $g \cdot (x, y) = (g \cdot x, g \cdot y)$ and the $G$-grading $|(x, y)| = |x| |y|$, and the braiding is

$$\beta_{X,Y} : X \otimes Y \rightarrow Y \otimes X, \quad \beta_{X,Y}(x, y) = (|x| \cdot y) \otimes x.$$ 

This construction can in fact be carried out for any Hopf algebra $H$ in place of $G$. If $H$ is finite-dimensional, then $\mathcal{D}_H$ is the category of modules over the Drinfeld double $D(H)$ of $H$, which is a quasitriangular Hopf algebra.

We have described in [A] a general procedure for constructing a quantum group out of this data (that is, a group $G$, or more generally a Hopf algebra, and a crossed module $X$). In this procedure the action of the binomial braids $b^{(a)}$ on the various tensor powers $X^\otimes n$ plays a crucial role. Drinfeld and Jimbo’s quantized enveloping algebra $U_q^+(C)$ associated to a symmetrizable generalized Cartan matrix $C$ arises from this construction with $G = \mathbb{Z}^r$, the free abelian group of rank $r$, where $r$ is the size of $C$, and the following crossed $\mathbb{Z}^r$-module $X$: let $A = [a_{hk}]$ be the symmetrized matrix corresponding to $C$, an integer square matrix of size $r$, let $X$ be the vector space with basis $\{x_1, \ldots, x_r\}$ and define

$$|x_k| = (a_{1k}, \ldots, a_{rk}) \in \mathbb{Z}^r, \quad (n_1, \ldots, n_r) \cdot x_h = q^{n_h} x_h \quad \forall (n_1, \ldots, n_r) \in \mathbb{Z}^r,$$

where $q \in k^*$ is any fixed scalar, not a root of unity.

We will now briefly describe this procedure, without proofs. For the general case of a crossed module over a Hopf algebra, the construction involves the notions of internal categories and admissible sections developed in [A]. A small linear category $\mathcal{M}$ is an example of an internal category. Let us concentrate on this special case that requires less strange terminology, and that covers the main example $U_q^+(C)$.

The idea is to attach a small linear category $\mathcal{U}_q^+(X)$ to the given group $G$ and crossed module $X$, and then obtain the quantum group as the matrix ring of the category, as defined by Mitchell in [Mi]. The coalgebra structure on the quantum group is seen to come from a deltagroup structure on the
category. This is the crucial point where the binomial braids enter, so we had better explain it in some detail.

For small linear categories (and more generally for internal categories) there is an alternative notion of morphisms, besides that of ordinary functors. We have called them cofunctors, because a different special case (Lie groupoids) has received that name in the literature [HM]. A cofunctor induces a morphism of algebras between the corresponding matrix rings (on the other hand, a functor does not, unless it is bijective on objects -this was the case considered in [Mi]). A small deltacategory $\mathcal{U}$ is a small linear category equipped with a coassociative cofunctor $\Delta : \mathcal{U} \to \mathcal{U} \otimes \mathcal{U}$. (More precisely, it is a comonoid in the monoidal category of small linear categories and cofunctors). The matrix ring of such a category is then a bialgebra. The main point of these considerations is that most quantum groups arise as matrix rings of naturally defined deltacategories.

Let us describe the deltacategory $\mathcal{U}^+_G(X)$. First we consider the graph whose vertex set is $G$ and whose set of arrows is $\prod_{g \in G} X_g \times G$, where each $(x, h)$ is an arrow from $h$ to $h|x|$. Then we pass to the free linear category $\Sigma_{G}(X)$ on this graph. It turns out that $\Sigma_{G}(X)$ possesses a deltacategory structure, defined on the generating arrows as follows:

$$\Delta(x, gh) = e_g \hat{\otimes} (x, h) + (h \cdot x, g) \hat{\otimes} e_h.$$ 

Here $e_g$ denotes the identity arrow of the object $g \in G$.

It follows from coassociativity that the general expression for $\Delta$ is

$$\Delta(x, gh) = \sum_{i=0}^{n} (h \cdot (b_i^{(n)} x)_i, g) \otimes ((b_i^{(n)} x)'_i, h) \text{ for } x \in X \otimes^{\infty}.$$

Here $b_i^{(n)}$ is of course the binomial braid, acting on $X \otimes^n$ as explained above; we have also used the notation $y = y(i) \otimes y(i)'$ for the canonical identification $X \otimes^n \cong X \otimes X \otimes^{n-1}$. This is in fact how we ran into these braids in the first place. One immediately sees from this expression for $\Delta$ that there is a natural set of relations on $\Sigma_{G}(X)$ that are preserved by $\Delta$. Namely, if for each $n \geq 2$ we let

$$I^{(n)} := \bigoplus_{n=2}^{\infty} I^{(n)} \text{ and } I := \bigoplus_{n=2}^{\infty} I^{(n)},$$

then the ideal of $\Sigma_{G}(X)$ spanned by $I \times G$ is preserved by $\Delta$. Hence, the quotient category $\mathcal{U}^+_G(X) := \Sigma_{G}(X)/I \times G$ inherits a deltacategory structure.

One can show that when $G = \mathbb{Z}^r$ and $X$ is defined from a symmetrizable generalized Cartan matrix $C$ as above, then the matrix ring of $\mathcal{U}^+_G(X)$ is the quantum group $U^+_G(C)$.

Some other simple choices of $G$ and $X$ yield well-known quantum groups, for instance $G = \mathbb{Z}_2$ and $X$ the non-trivial one dimensional representation of $G$ yield Sweedler’s Hopf algebra $H_4$; $G = \mathbb{Z}_n$ and $X$ a one dimensional representation of $G$ yield Taft’s Hopf algebras.

But notice that this construction is more general: one can use any integral matrix for $C$, and of course other groups or even Hopf algebras, and obtain other (new) quantum groups.

These assertions will be complemented with more details and proofs in [A].

10. ADDITIONAL REMARKS

Further interesting combinatorial phenomena arises from the study of the behavior of the various braid analogs on higher dimensional representations $X$ of the braid groups. In particular, the determinants of $b_i^{(n)}$ and $f^{(n)}$ on $X \otimes^n$ seem to factor in some rather remarkable ways, intimately related to the combinatorics of the braid arrangement $A_{r-1} = \{ H_{hk} / 1 \leq h < k \leq r \}$, where $H_{hk} = \{(x_1, \ldots, x_r) \in \mathbb{R}^r / x_h = x_k \}$.

For instance, consider the representation constructed from a symmetric matrix $A = [a_{hk}]$ of size $r$ as in section 9. Thus, $B_n$ acts on $X \otimes^n \forall n \geq 0$, where $X$ is a vector space with basis $\{x_1, \ldots, x_r\}$.
The subspace $X_r$ of $X^\otimes r$ spanned by those tensors of the form $x_{\sigma(1)} \otimes x_{\sigma(2)} \ldots \otimes x_{\sigma(r)}$, where $\sigma$ runs over $S_r$, is invariant under the action of $B_r$. The matrix of $f^{(r)} : X_r \to X_r$ with respect to this basis turns out to be the same matrix that Varchenko associates to the weighted hyperplane arrangement $A_{r-1}$ (weighted by the $a_{hk}$'s) [V]. A factorization formula for the determinant of the matrix of an arbitrary weighted real hyperplane arrangement is obtained in that work. For the special case of the braid arrangement, further factorization formulas seem to hold, not only for the determinant of the factorial braid, but also for the binomials, and on other invariant subspaces of $X^\otimes n$ as well.

In particular, on the subspace $X_{h,k}$ of $X^{\otimes (n+1)}$ spanned by $x_h \otimes x_k \otimes x_1 \otimes \ldots \otimes x_n$ and its permutations, one can show that

$$\det\left( a_1^{(n+1)}|_{X_{h,k}} \right) = (1 - q^{a[n]})(1 - q^{a[n-1]}) \ldots (1 - q^{a[1]})|n|!q^{a_{kk}},$$

where

$$a[i] = (i - 1)a_{kk} + a_{hk} + a_{kh}.$$

These questions will be the subject of further work.

Bibliography

[Mi]: B. Mitchell, Rings with several objects, Advances in Math. 8 (1972), 1-161.

The following articles can be found in Gian-Carlo Rota on Combinatorics: Introductory papers and commentaries, edited by Joseph P.S. Kung, Birkhäuser (1995).