

## **Phase Retrieval for Probability Distributions on Quantum Groups and Braided Groups**

**Uwe Franz,<sup>1,2</sup> Daniel Neuenschwander,<sup>3,4</sup> and René Schott<sup>1</sup>**

*Received December 15, 1997; revised July 10, 1998*

---

For nilpotent quantum groups [as introduced by Franz *et al.*<sup>(7)</sup>], we show that (in sharp contrast to the classical case) the symmetrization  $\mu * \bar{\mu}$  of a probability distribution  $\mu$  and the first moments of  $\mu$  together determine uniquely the original distribution  $\mu$ .

---

**KEY WORDS:** Probability distributions; nilpotent groups.

### **1. INTRODUCTION**

The starting-point of our investigations is the following question: Under which conditions is a probability measure (on the real line e.g.) uniquely determined (up to a shift) already by the absolute value of its Fourier transform? In other words: When is it possible to retrieve the phase (up to a constant) from the absolute value of the Fourier transform? This problem has its origin in crystallography and there exists a vast literature on it (there was even a Nobel prize given for this subject), see e.g., Carnal and Fel'dman<sup>(4,5)</sup> and the references cited there. Let  $\mu$  be the law of a random variable  $X$  (on the real line) and  $\varphi(u)$  ( $u \in \mathbb{R}$ ) its Fourier transform. Then  $|\varphi(u)|^2 = \varphi(u) \cdot \overline{\varphi(u)}$  can be interpreted as the Fourier transform of the symmetrization  $\mu * \bar{\mu}$  (where  $\bar{\mu}$  denotes the adjoint measure, i.e., the law of the random variable  $-X$ ). So this question can be reformulated in purely probabilistic terms: Under which conditions is a probability

---

<sup>1</sup> Université Henri Poincaré-Nancy I, Institut E. Cartan, LORIA, B.P. 239, F-54506 Vandoeuvre-lès-Nancy, France.

<sup>2</sup> Université Louis Pasteur, IRMA, 7, rue René Descartes, 67084 Strasbourg Cedex, France.

<sup>3</sup> Université de Lausanne, Ecole des Hautes Etudes Commerciales, Institut de Sciences Actuarielles, CH-1015 Lausanne, Switzerland.

<sup>4</sup> To whom correspondence should be addressed.

measure  $\mu$  uniquely determined by its symmetrization  $\mu * \bar{\mu}$  and the first moment of  $\mu$ ? If one formulates the question like this, it makes sense not only on vector spaces, but also on more general convolution structures. Carnal and Fel'dman<sup>(4,5)</sup> treated this problem on Abelian groups, but (up to now) no investigations in the noncommutative case seem to exist.

In this note, we will consider the problem on nilpotent quantum groups and nilpotent braided groups [as introduced by Franz *et al.*<sup>(7)</sup>]: Given the symmetrization  $\mu * \bar{\mu}$  and the first moments of the probability measure  $\mu$  on  $G$ , when is it possible to retrieve the original distribution  $\mu$  from these data? The somewhat surprising answer will be that in this framework, the afore-mentioned retrieval is always possible (provided that the quantum or braided group is “sufficiently” noncommutative, e.g., if  $q$  is not a root of unity). By definition distributions on quantum groups have all moments and are uniquely determined by them. So it will suffice to show that the moments of the symmetrization and the first moments of  $\mu$  together allow to calculate all moments of  $\mu$  recursively. Observe that one can not expect to be able to remove the condition of knowledge of the first moments of  $\mu$ , since already on the classical real line, in the best possible case  $\mu$  can be determined by its symmetrization only up to a shift. The situation on nilpotent quantum groups and nilpotent braided groups is in sharp contrast to the classical case of simply connected nilpotent Lie groups, where the moments can not be retrieved, see Section 2.

Probability theory on quantum groups and braided groups, in particular increment processes, has previously been studied, e.g. Accardi *et al.*,<sup>(1)</sup> Majid,<sup>(12)</sup> and Schürmann<sup>(13)</sup>].

## 2. CLASSICAL SIMPLY CONNECTED NILPOTENT LIE GROUPS

A simply connected nilpotent Lie group is a Lie group  $G$  with Lie algebra  $\mathcal{G}$  such that  $\exp: \mathcal{G} \rightarrow G$  is a diffeomorphism and that the descending central series is finite, i.e., there is some  $r \in \mathbb{N}$  such that

$$\mathcal{G}_0 \supseteq \mathcal{G}_1 \supseteq \dots \supseteq \mathcal{G}_r = \{0\}$$

where

$$\mathcal{G}_0 := \mathcal{G}, \quad \mathcal{G}_{k+1} := [\mathcal{G}, \mathcal{G}_k] \quad (0 \leq k \leq r-1)$$

$G$  is then called step  $r$ -nilpotent. So  $G$  may be interpreted as  $\mathbb{R}^d$  equipped with a Lie bracket  $[\cdot, \cdot]: \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}^d$  which is bilinear, skew-symmetric, and satisfies the Jacobi identity

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$

The most prominent examples are the so-called Heisenberg groups  $HW^d$ , given by  $\mathbb{R}^{2d+1}$  and the Lie bracket

$$[x, y] := (0, 0, \langle x', y' \rangle - \langle x'', y'' \rangle)$$

$$(x = (x', x'', x'''), y = (y', y'', y''')) \in \mathbb{R}^d \times \mathbb{R}^d \times \mathbb{R} \cong \mathbb{R}^{2d+1}$$

Consider an adapted vector space decomposition of  $G = \mathcal{G}$  [see Guivarc'h *et al.*<sup>(8)</sup>], i.e.,

$$G \cong \mathcal{G} \cong \mathbb{R}^d \cong \bigoplus_{i=1}^r V_i$$

such that

$$\bigoplus_{i=k}^r V_i = \mathcal{G}_{k-1}$$

Then on the “first layer”  $V_1$ , the group multiplication always reduces to euclidian addition  $+$ . But on the real line, a straightforward calculation of the third and the fourth moment of the symmetrization shows that the afore-mentioned moment retrieval is not possible. On the line:

$$E(X - X')^4 = 2E(X^4) - 8E(X^3)E(X) + 6E(X^2)^2,$$

$$E(X - X')^3 = 0$$

At this point, it would be interesting to characterize classes of probability measures for which the phase retrieval is nevertheless possible on nilpotent (and even more general) Lie groups.

### 3. QUANTUM GROUPS AND BRAIDED GROUPS

First, we briefly recall some definitions concerning quantum groups and braided groups, see also Majid<sup>(12)</sup> and references therein.

A quantum group is a Hopf algebra, i.e., an associative unital algebra  $(\mathcal{B}, m, \mathbb{1})$  with two homomorphisms  $\Delta: \mathcal{B} \rightarrow \mathcal{B} \otimes \mathcal{B}$ ,  $\varepsilon: \mathcal{B} \rightarrow \mathbb{C}$ , and an anti-homomorphism  $S: \mathcal{B} \rightarrow \mathcal{B}$  that satisfy

$$(\Delta \otimes \text{id}) \circ \Delta = (\text{id} \otimes \Delta) \circ \Delta$$

$$(\varepsilon \otimes \text{id}) \circ \Delta = (\text{id} \otimes \varepsilon) \circ \Delta$$

$$m \circ (\text{id} \otimes S) \circ \Delta = m \circ (S \otimes \text{id}) \circ \Delta = \mathbb{1} \circ \varepsilon$$

These maps are called coproduct, counit, and antipode, respectively. Here the tensor product  $\mathcal{B} \otimes \mathcal{B}$  is considered as an algebra with the multiplication defined by  $m_{\otimes}((a \otimes b) \otimes (c \otimes d)) = ac \otimes bd$ , i.e.,  $m_{\otimes} = (m \otimes m) \circ (\text{id} \otimes \tau \otimes \text{id})$ , where  $\tau: \mathcal{B} \otimes \mathcal{B} \rightarrow \mathcal{B} \otimes \mathcal{B}$  is the flip automorphism,  $\tau(a \otimes b) = b \otimes a$ . Placing ourselves in a braided category and substituting  $\tau$  by the braiding  $\Psi$  we are naturally led to braided Hopf algebras or braided groups. These axioms remain unchanged, but now  $m, \mathbb{1}, \Delta, \varepsilon$ , and  $S$  have to satisfy certain compatibility conditions with respect to the braiding  $\Psi$ . The comultiplication  $\Delta$  has to be an algebra homomorphism from  $\mathcal{B}$  to  $\mathcal{B} \tilde{\otimes} \mathcal{B}$ , i.e., the algebra structure in the tensor product is defined by  $m_{\Psi} = (m \otimes m) \circ (\text{id} \otimes \Psi \otimes \text{id})$ , or  $m_{\Psi}((a \otimes b) \otimes (c \otimes d)) = a\Psi(b \otimes c)d$ . And the antipode is no longer an anti-homomorphism, but satisfies  $S \circ m = m \circ \Psi \circ (S \otimes S)$ .

On Fourier transforms in the theory of quantum and braided groups see Kempf and Majid,<sup>(9)</sup> and Koornwinder.<sup>(10)</sup>

In the spirit of noncommutative geometry and quantum probability one treats these algebras as analogues of the coordinate ring of some noncommutative or quantum space, and the coproduct takes the roles of a group structure of the underlying space. Random variables are replaced by (\*-)homomorphisms  $j: \mathcal{B} \rightarrow \mathcal{A}$  into an (involutive) associative unital algebra  $\mathcal{A}$  (called quantum probability space) with a normalized positive functional  $\Phi$ , and their distribution is the functional  $\varphi_j = \Phi \circ j$ .

On quantum groups and braided groups the antipode plays the role of the inverse, so that the symmetrization of a functional  $\phi: \mathcal{B} \rightarrow \mathbb{C}$  is defined by

$$\phi * \bar{\phi} = (\phi \otimes (\phi \circ S)) \circ \Delta$$

We will not impose positivity or consider \*-structures here, if a functional is already characterized by its first moments and its symmetrization without the positivity condition, then this remains true, if we restrict to positive functionals.

**Example 1.** *The braided line  $\mathbb{R}_q$ .* Let  $q \in \mathbb{C} \setminus \{0\}$ ,  $q$  not a root of unity. As an algebra  $\mathbb{R}_q$  is isomorphic to the ring of polynomials in one variable  $\mathbb{R}[x]$ . The braiding used here is defined by  $\Psi(x^n \otimes x^m) = q^{nm}x^m \otimes x^n$ . On the generator the coproduct, counit, and antipode are defined by

$$\Delta(x) = x + x', \quad \varepsilon(x) = 0, \quad S(x) = -x$$

where we used  $x = x \otimes 1, x' = 1 \otimes x$ . From this one computes  $\Delta(x^n) = \sum_{\nu=0}^n \begin{bmatrix} n \\ \nu \end{bmatrix}_q x^\nu (x')^{n-\nu}$  and  $S(x^n) = (-1)^n q^{n(n-1)/2} x^n$ . Recall that the  $q$ -numbers  $q_n$ , the  $q$ -factorial  $q_n!$  and the  $q$ -binomial coefficients  $\begin{bmatrix} n \\ \nu \end{bmatrix}_q$  are defined as  $q_n = \sum_{\nu=0}^{n-1} q^\nu = (q^n - 1)/(q - 1), q_n! = \prod_{\nu=1}^n q_\nu, \begin{bmatrix} n \\ \nu \end{bmatrix}_q = q_n! / (q_\nu! q_{n-\nu}!)$ .

A probabilistic interpretation of the  $q$ -convolution of measures on the real line defined by  $(\mu * \nu)(f) = (\mu \otimes \nu)(\Delta f)$  for appropriate functions  $f$  has been given by Feinsilver.<sup>(6)</sup> We recall his nice result:

**Proposition 1.** Let  $Y = \sum_0^\infty Z_j$ , where  $Z_j$  are independent, exponentially distributed, with respective means  $q^j$ .

The  $q$ -convolution of  $X_1$  and  $X_2$ , independent random variables, corresponds to the random variable  $Y_1 X_1 + Y_2 X_2$ , where  $Y_1, Y_2$  are independent copies of  $Y$ , independent of the  $X$ 's as well.

### 3.1. The Phase Problem on the Braided Line

We consider first the braided line, because it turns out to be typical, but at the same time simpler since it has only one generator.

**Proposition 2.** Let  $q \in \mathbb{C} \setminus \{0\}$ ,  $q$  not a root of unity. A normalized functional  $\phi$  on  $\mathbb{R}_q$  is uniquely determined by its symmetrization  $\phi * \bar{\phi}$  and its first moment  $\phi(x)$ .

*Proof.* We have  $\Delta(x^n) = \sum_{\nu=0}^n \begin{bmatrix} n \\ \nu \end{bmatrix}_q x^\nu (x')^{n-\nu}$ , and  $S(x^n) = (-1)^n \times q^{n(n-1)/2} x^n$ , and thus

$$\begin{aligned} \phi * \bar{\phi}(x^n) &= \phi \otimes (\phi \circ S) \circ \Delta(x^n) \\ &= \sum_{\nu=0}^n \begin{bmatrix} n \\ \nu \end{bmatrix}_q (-1)^{n-\nu} q^{(n-\nu)(n-\nu-1)/2} \phi(x^\nu) \phi(x^{n-\nu}) \end{aligned}$$

If  $q$  is not a root of unity this gives a recurrence relation that allows to calculate all moments of  $\phi$  except the first from those of the symmetrization  $\phi * \bar{\phi}$ ,

$$\begin{aligned} \phi(x^n) &= \frac{1}{1 + (-1)^n q^{n(n-1)/2}} \\ &\times \left\{ (\phi * \bar{\phi})(x^n) - \sum_{\nu=1}^{n-1} \begin{bmatrix} n \\ \nu \end{bmatrix}_q q^{(n-\nu)(n-\nu-1)/2} \phi(x^\nu) \phi(x^{n-\nu}) \right\} \quad \square \end{aligned}$$

### 3.2. The Phase Problem on Nilpotent Quantum Groups or Nilpotent Braided Groups

Looking at the classical case and at the braided line, we see that it is sufficient for retrieving a certain moment  $\phi(x_n)$  if  $S(x_n) \neq -x_n$ , (if we suppose that all other moments are already known). In the classical case this

is true for even moments, thus symmetrical measures can be retrieved, if they are uniquely determined by their moments, [see Carnal and Dozzi,<sup>(3)</sup> Prop. 2.2]. On the braided line this is true for all powers of the generator  $x$  except the first, thus all moments except the first can be retrieved (Prop. 2). In general, on a class of quantum groups or braided groups called strongly nilpotent or  $S$ -nilpotent, it is sufficient, if the coefficient of  $x_n$  in the expansion of  $S(x_n)$  is not equal to  $-1$ .

To formulate this rigorously, we need the following definition.

**Definition 1.** A quantum group or braided group  $\mathcal{B}$  is called *S-nilpotent* or *strongly nilpotent*, if there exists a basis  $\{\mathbb{1}, a_i; i \in \mathcal{I}\}$ , indexed by a well-ordered set  $\mathcal{I}$ , such that

$$A(a_i) - a_i \otimes \mathbb{1} - \mathbb{1} \otimes a_i \in \mathcal{B}_{<i} \otimes \mathcal{B}_{<i}, \quad (3.1)$$

$$S(a_i) \in \mathcal{B}_{\leq i}, \quad (3.2)$$

for all  $i \in \mathcal{I}$ , where  $\mathcal{B}_{<i} = \text{span}\{\mathbb{1}, a_{i'}; i' < i\}$ ,  $\mathcal{B}_{\leq i} = \text{span}\{\mathbb{1}, a_{i'}; i' \leq i\}$ . Bases that satisfy these conditions will be called *adapted*.

**Remark 1.** If we require only condition (3.1), then we have the notion of nilpotency introduced by Franz *et al.*<sup>(7)</sup> It was motivated by the fact that the Hopf algebra of polynomials on a connected, simply connected nilpotent Lie group can be characterized in this way. But in that case we have  $S(x_1^{k_1} \dots x_n^{k_n}) = (-1)^{k_1 + \dots + k_n} x_1^{k_1} \dots x_n^{k_n}$ , so condition (3.2) is also satisfied.

On noncommutative nilpotent quantum groups and nilpotent braided groups there exist bases that satisfy (3.1), but not (3.2). Take for example the free algebra  $\mathbb{C} \langle\langle x, y \rangle\rangle$  with two primitive generators, then the basis of monomials  $\{\mathbb{1}, x, y, x^2, y^2, xy, yx, x^3, \dots\}$  (take any order such that  $a < b$  if the total degree of  $a$  is less than that of  $b$ ) satisfies (3.1), but not (3.2), since  $S(xy) = yx$  and  $S(yx) = xy$ . But we have  $S^2 = \text{id}$ , so we can choose a basis that diagonalizes  $S$  for each of the subspaces with total degree  $n$ , and the union of these bases,  $\{\mathbb{1}, x, y, x^2, y^2, xy + yx, xy - yx, x^3, \dots\}$ , satisfies both (3.1) and (3.2). We do not know if their exist quantum groups or braided groups that are nilpotent, but not  $S$ -nilpotent.

**Theorem 1.** Let  $\mathcal{B}$  be an  $S$ -nilpotent quantum group or  $S$ -nilpotent braided group, with the adapted basis  $\{a_i; i \in \mathcal{I}\}$  and let  $\mathcal{K} \subseteq \mathcal{I}$ . Suppose furthermore that the coefficient  $s_{i,k}$  of  $S(a_i)$  in the expansion  $S(a_i) = \sum_{k \leq i} s_{i,k} a_k$  is not equal to  $-1$  for all  $i \in \mathcal{I} \setminus \mathcal{K}$ . Then a normalized functional  $\phi: \mathcal{B} \rightarrow \mathbb{C}$  is uniquely determined by its symmetrization  $\phi * \bar{\phi}$  and its moments on  $\{a_k; k \in \mathcal{K}\}$ .

*Proof.* We can give an explicit procedure to calculate the moments of  $\phi$ . Let  $i$  be the smallest index in  $\mathcal{I}$  for which we do not yet know  $\phi(a_i)$ . Then

$$(\text{id} \otimes S) \circ \Delta(a_i) = 1 + s_{i,i} + \sum_{i', i'' < i} C_{i', i''}^{(i)} a_{i'} \otimes a_{i''}$$

and thus, since  $s_{i,i} \neq -1$ ,

$$\phi(a_i) = \frac{1}{1 + s_{i,i}} \left\{ \phi * \bar{\phi}(a_i) - \sum_{i', i'' < i} C_{i', i''}^{(i)} \phi(a_{i'}) \phi(a_{i''}) \right\} \quad \square$$

For example on  $\mathbb{R}$  the basis could be chosen as  $\{x^n; n \in \mathbb{N}\}$ , and the set of moments that have to be known to recover the measure is  $\mathcal{K} = \{2n + 1; n \in \mathbb{N}\}$ . On the braided line we have only  $\mathcal{K} = \{1\}$ .

### 3.3. On the Braided Plane

The braided plane  $\mathbb{C}_q^{2|0}$  [see e.g., Majid<sup>(11)</sup>] is the braided Hopf algebra with two generators  $x, y$  and defining relations

$$\begin{aligned} yx &= qxy, \\ x'x &= q^2xx', & x'y &= qyx', \\ y'x &= qxy' + (q^2 - 1)yx', & y'y &= q^2yy', \\ \Delta x &= x + x', & \Delta y &= y + y', \\ \varepsilon(x) &= \varepsilon(y) = 0, & S(x) &= -x, & S(y) &= -y \end{aligned}$$

The braided plane  $\mathbb{C}_q^{2|0}$  is  $S$ -nilpotent, and an adapted basis is given by  $\{x^n y^m; n, m \in \mathbb{N}\}$ , where  $\mathcal{I} = \{(n, m); n, m \in \mathbb{N}\}$  is taken with the order defined by  $(n_1, m_1) \leq (n_2, m_2)$  if and only if  $n_1 \leq n_2$  and  $m_1 \leq m_2$ .

To see that this basis is really adapted, one proves by induction

$$\begin{aligned} \Delta(x^n y^m) &= \sum_{\nu=0}^n \sum_{\mu=0}^m \begin{bmatrix} n \\ \nu \end{bmatrix}_{q^2} \begin{bmatrix} m \\ \mu \end{bmatrix}_{q^2} q^{\mu(n-\nu)} x^\nu y^\mu \otimes x^{n-\nu} y^{m-\mu} \\ S(x^n y^m) &= (-1)^{n+m} q^{(n+m)(n+m+1)} x^n y^m \end{aligned} \quad (3.3)$$

**Proposition 3.** Let  $q \in \mathbb{C} \setminus \{0\}$ ,  $q$  not a root of unity. A normalized functional  $\phi$  on the braided plane  $\mathbb{C}_q^{2|0}$  is uniquely determined by its first moments  $\phi(x)$ ,  $\phi(y)$ , and its symmetrization  $\phi * \bar{\phi}$ .

*Proof.* This follows immediately from Theorem 1 with Eq. (3.3), if we take  $\mathcal{K} = \{(0, 1), (1, 0)\}$ .  $\square$

### 3.4. On the Braided Heisenberg–Weyl Group

Our last example will be braided Heisenberg–Weyl group  $HW_q$  [cf. Franz *et al.*<sup>(7)</sup>]. For other quantum or braided analogues of the Heisenberg–Weyl groups see Baskerville and Majid<sup>(2)</sup> and the references cited there.

The braided Heisenberg–Weyl group  $HW_q$  is, as an algebra, generated by two generators  $a, c$  with the cubic relations

$$aac + qcaa = (1 + q)aca, \quad acc + qcca = (1 + q)cac \quad (3.4)$$

where  $q \in \mathbb{C} \setminus \{0\}$ ,  $q$  not a root of unity. We define the braiding by

$$a'a = qaa', \quad a'c = ca', \quad c'a = \frac{1}{q}ac', \quad c'c = qcc'$$

and the coproduct and antipode by  $\Delta a = a + a'$ ,  $\Delta c = c + c'$ , and  $S(a) = -a$ ,  $S(c) = -c$ , (extend the coproduct as an algebra homomorphism and the antipode by  $S \circ m = m \circ \Psi \circ (S \otimes S)$ ).

The relation to the classical Heisenberg–Weyl algebra and the oscillator algebra becomes clear, if a third generator defined by  $b = ac - qca$  is introduced (the defining relations imply that  $b$  is central).

We shall now derive some properties of the coproduct and the antipode of  $HW_q$ , in order to show that  $HW_q$  is  $S$ -nilpotent, and to determine which moments are necessary to characterize a functional on  $HW_q$  by its symmetrization.

This algebra is graded with  $\deg(a) = (1, 0)$ ,  $\deg(c) = (0, 1)$ , since the relations (3.4) are homogeneous. Let  $HW_q^{(n, m)}$  be the subspace of elements of degree  $(n, m)$ . The braiding of two homogeneous elements is given by

$$u'v = q^{(n_1 - m_1)n_2 + m_1m_2}vu', \quad \text{for } u \in HW_q^{(n_1, m_1)}, \quad v \in HW_q^{(n_2, m_2)} \quad (3.5)$$

This, together with the definition of the coproduct on the generators, implies that Eq. (3.1) holds for any basis of homogeneous elements ordered by their degree.

Equation (3.2) can also be satisfied, because

$$S^2|_{HW_q^{(n, m)}} = q^{n(n-1) + m(m-1) - nm} \text{id}_{HW_q^{(n, m)}} \quad (3.6)$$

and thus there exists a basis of homogenous elements that diagonalizes  $S$ . This basis, if ordered by the degree, is obviously adapted, and  $HW_q$  is thus  $S$ -nilpotent.

Equation (3.6) can be shown by complete induction. It is true for  $HW_q^{(0,0)} = \mathbb{C}\mathbb{1}$ , since  $S^2(\mathbb{1}) = \mathbb{1}$ . Let now  $u \in HW_q^{(n,m)}$ , then with Eq. (3.5)

$$\begin{aligned} S^2(au) &= \Psi^2(a \otimes S^2(u)) = q^{2n-m} a S^2(u) \\ S^2(cu) &= \Phi^2(c \otimes S^2(u)) = q^{2m-n} c S^2(u) \end{aligned}$$

**Proposition 4.** Let  $q \in \mathbb{C} \setminus \{0\}$ ,  $q$  not a root of unity. Then a normalized functional  $\phi$  on  $HW_q$  is uniquely determined by the moments  $\phi(a)$ ,  $\phi(c)$ ,  $\phi(aca)$ ,  $\phi(cac)$ ,  $\phi(aacc - q^2ccaa)$ ,  $\phi(acac - qcaca)$ , and its symmetrization  $\phi * \bar{\phi}$ .

*Proof.* After the preceding discussion we know that there exists an adapted basis of eigenvectors of  $S$ , so that, by Theorem 1, all that remains to be done is to determine the eigenspace  $E_{-1}$  of the eigenvalue  $-1$ . By Eq. (3.6) the only possible eigenvalues of  $S|_{HW_q^{(n,m)}}$  are  $\pm q^{\lfloor n(n-1) + m(m-1) - nm \rfloor / 2}$ . But  $n(n-1) + m(m-1) - nm \neq 0$  for all  $(n, m)$  except  $(0, 0)$ ,  $(1, 0)$ ,  $(0, 1)$ ,  $(2, 1)$ ,  $(1, 2)$ ,  $(2, 2)$ , so that  $E_{-1} \subseteq HW_q^{(0,0)} \oplus HW_q^{(1,0)} \oplus HW_q^{(0,1)} \oplus HW_q^{(2,1)} \oplus HW_q^{(1,2)} \oplus HW_q^{(2,2)} =: A$ . A simple calculation (note  $E_{-1} = (\text{id} - S)(A)$ , since  $S$  is involutive on  $A$ ) gives

$$E_{-1} = \text{span}\{a, c, aca, cac, aacc - q^2ccaa, acac - qcaca\}$$

and this proves the proposition.  $\square$

## ACKNOWLEDGMENTS

The authors are grateful to an anonymous referee for several suggestions.

## REFERENCES

1. Accardi, L., Schürmann, M., and Waldenfels, W. v. (1988). Quantum independent increment processes on superalgebras. *Math. Z.* **198**, 451–477.
2. Baskerville, W. K., and Majid, S. (1993). The braided Heisenberg groups. *J. Math. Phys.* **34**, 3588–3606.
3. Carnal, H., and Dozzi, M. (1989). On a decomposition problem for multivariate probability measures. *J. Multivariate Anal.* **31**, 165–177.
4. Carnal, H., and Fel'dman, G. M. (1995). Phase retrieval for probability measures on Abelian groups. *J. Theor. Prob.* **8** (3), 717–725.
5. Carnal, H., and Fel'dman, G. M. (1997). Phase retrieval for probability measures on Abelian groups II. *J. Theor. Prob.* **10** (4), 1065–1074.
6. Feinsilver, Ph. (1987). Generalized convolutions and probability theory based on the  $q$ -Heisenberg algebra. *Proc. First World Congr. Bernoulli Soc.*, VNU Science Press, pp. 729–741.

7. Franz, U., Neuenschwander, D., and Schott, R. (1997). Gauss laws in the sense of Bernstein and uniqueness of embedding into convolution semigroups on quantum groups and braided groups, *Prob. Th. Rel. Fields* **109**, 101–127.
8. Guivarc'h, Y., Keane, M., and Roynette, B. (1977). Marches aléatoires sur les groupes de Lie, *Lecture Notes in Math.*, Vol. 624, Springer-Verlag, Berlin.
9. Kempf, A., and Majid, S. (1994). Algebraic  $q$ -integration and Fourier theory on quantum and braided spaces. *J. Math. Phys.* **35**, 6801–6837.
10. Koornwinder, T. H. (1995). Minicourse “special functions and  $q$ -commuting variables.” *Workshop on “Special functions,  $q$ -series and related topics”*, Fields Institute, Toronto, Canada.
11. Majid, S. (1993). Braided momentum in the  $q$ -Poincaré group. *J. Math. Phys.* **34**, 2045–2058.
12. Majid, S. (1995). *Foundations of Quantum Group Theory*, Cambridge University Press.
13. Schürmann, M. (1993). *White Noise on Bialgebras*, *Lecture Notes in Math.*, Vol. 1544, Springer-Verlag, Berlin.