hexagon:2611.00831v1

EASINESS OVER CHARACTERISTIC ZERO FIELDS

C. OPUS AND T. BANICA

ABSTRACT. The easy quantum groups have intertwiners T_π, depending on set-theoretic partitions π, with integer entries, and so are defined over $\mathbb{Q}$. We study them over an arbitrary field F of characteristic 0. Easiness itself does not depend on F, and the field comes into play via the F-forms: those of O_N^+, coming from the central simple algebras with orthogonal involution and from the quadratic forms up to similarity, and a family of F-forms of S_N^+, coming from the finite étale algebras. We also discuss the quantum symmetries of the free quadrics, described by bilinear forms. We also discuss free probability over F, and the p-adic case.

CONTENTS

Introduction 1
1. Hopf algebras over fields 3
2. Easiness and base change 5
3. Forms and congruence classes 9
4. Free quadrics, deformations 12
5. Galois forms of permutations 14
6. Laws over arbitrary fields 17
7. Analysis over the p-adics 19
8. Questions and perspectives 21
References 22

INTRODUCTION

The easy quantum groups from [10] are the compact quantum groups $G \subset O_N^+$ whose intertwiner spaces are spanned by the maps T_π associated to the partitions π in a category D. The basic examples are the permutation and orthogonal groups S_N, O_N, their free versions S_N^+, O_N^+, coming from the noncrossing partitions, and the bistochastic and hyperoctahedral versions. The point that we would like to start from is that the maps T_π have entries 0 and 1. Thus these quantum groups are defined by relations with integer coefficients, and so they make sense over any ring, and in particular over any field F of characteristic 0.

The question is then what happens over such fields. Over $\mathbb{C}$ we have the usual theory, coming from Woronowicz [53, 54], over $\mathbb{R}$ we have the real forms, which are of interest in connection with the noncompact quantum groups, over the number fields we have Galois symmetries, and over the p-adic fields we have a second, nonarchimedean analysis. Our purpose here is to explain what survives, what changes, and what new phenomena appear, in this setting. Let us mention that a good part of the algebraic theory, notably for S_N^+ and O_N^+, was developed over arbitrary fields by Bichon [14, 16], and our work here can be regarded as a continuation of his. Our first result, which is quite expected, is that easiness itself does not depend on the field:

2020 *Mathematics Subject Classification.* 16T05 (11E04, 11S80, 46L54).
Key words and phrases. Easy quantum group, Galois form, free quadric, p-adic measure.

Theorem A. *Let D be a category of partitions, $N \geq 1$, and F a field of characteristic 0. The Hopf algebra $\mathcal{O}(G)_F$ presented by the relations $T_\pi \in Hom(u^{\otimes k}, u^{\otimes l})$ with $\pi \in D(k,l)$ is the base change of its rational version, its intertwiner spaces are spanned by the maps T_π, and it has a Haar functional h_F, which is F-valued and restricts to the Haar functional $h_{\mathbb{Q}}$ of $\mathcal{O}(G)_{\mathbb{Q}}$, given by the Weingarten formula when the Gram matrix G_{kN} is invertible. The moments of the main character are $h_F(\chi^k) = rank(G_{kN}) \in \mathbb{N}$, with no invertibility assumption.*

Thus, the absolute objects are the same over all fields. However, a Hopf algebra over F can have several F-forms, which become isomorphic over the algebraic closure $\bar{F}$, and this is where the field comes into play. For the free orthogonal quantum groups, the F-forms come from the Hopf algebras $B(E)$ of Dubois-Violette and Launer [28], associated to the bilinear forms E, studied by Bichon in [14], and from the central simple algebras with involution, in the sense of [35]. We have here:

Theorem B. *For $N \geq 2$, the F-forms of O_N^+ correspond to the isomorphism classes of pairs (Z, σ) consisting of a central simple F-algebra Z of degree N and an orthogonal involution σ. The split F-forms, with $Z = M_N(F)$, are the Hopf algebras $B(E)$ with E symmetric, with $B(E) \simeq B(E')$ when $E' = cP^tEP$ with $c \in F^*$, $P \in GL_N(F)$, and only in this case. Over $\mathbb{R}$ this gives the quantum groups $O^+(p,q)$, up to $(p,q) \sim (q,p)$, plus one more real form for N even. Over $\mathbb{Q}$, for $N \geq 3$, we have $B_N^+ \simeq O_{N-1}^+$ precisely when N is an odd square, when $4|N$, or when $N \equiv 2$ modulo 4 is a sum of 2 squares.*

The Hopf algebras $B(E)$ with E neither symmetric nor antisymmetric are not of Kac type, and appear as quantum symmetry groups of the free quadrics, studied over $\mathbb{R}$ in [31]. Over an arbitrary field, a free quadric in N variables is given by a bilinear form $A \in GL_N(F)$, and the Hopf algebra of its quantum symmetry group is $B(A^{-1})$. In 2 variables, we obtain the following classification:

Theorem C. *Write $A = Q + \kappa J \in GL_2(F)$, with Q symmetric and J the standard symplectic matrix, and assume $d = \det Q \neq 0$. Then $r = \kappa^2/d \neq -1$, because $\det A = d(1+r)$, and $t = tr(A^{-1}A^t)$ is given by $t = 2(1-r)/(1+r)$. Over $\bar{F}$ the quantum symmetry group is monoidally equivalent to $SL_q(2)$, with $q^2+tq+1 = 0$. In the cosemisimple case, the isomorphism class over F of its Hopf algebra is determined by the similarity class of Q, and by $r \in F$. Also, in general, $S^2 = id$ happens precisely when $r = 0$.*

With $F = \mathbb{C}$ and $A = H$ a Hermitian matrix depending on real parameters λ, μ, the generators being self-adjoint, as in the real quadrics from [31], this recovers the deformation parameters of the elliptic and hyperbolic free conics from there, namely $q = (\lambda-1)/(\lambda+1)$, and $q = -e^{\pm 2i\theta}$.

Regarding now the quantum permutation group S_N^+ of Wang [51], it has a family of F-forms coming from the finite étale algebras. Given a finite étale algebra K of dimension N over F, we can consider the Hopf algebra A_K of the universal coaction on K preserving the multiplication, the unit, and the trace. This is an F-form of S_N^+, and we have the following result, which uses as well the quantum group $G_3 \subset S_9^+$ from [8], preserving the oriented area tensor on the 9 points of $\mathbb{F}_3^2$, and coming from the color sector of the Standard Model:

Theorem D. *For $N \geq 3$ with $N \neq 6$, the F-forms A_K of S_N^+ coming from the finite étale F-algebras K of dimension N are pairwise nonisomorphic, $A_K \simeq A_{K'}$ implying $K \simeq K'$, and over $\mathbb{R}$ this construction gives $[N/2]+1$ real forms, corresponding to $K = \mathbb{R}^r \times \mathbb{C}^s$. Also, the quantum group G_3, defined over $\mathbb{Q}(\omega)$, has a $\mathbb{Q}$-form, which is a quantum subgroup of S_K^+ with $K = \mathbb{Q}^3 \times \mathbb{Q}(\omega)^3$, the area tensor making K into a copy of $M_3(\mathbb{Q})$.*

In the second part of the paper we discuss analysis. We first explain how the moments, cumulants and free cumulants work over an arbitrary field F, with the Möbius functions being

integer-valued, and with the convolution semigroups being indexed by F, and we prove some limit theorems over the complete valued fields. Then we specialize to the p-adic case, where a law is a bounded measure on $\mathbf{Z}_p$ when its binomial moments are bounded, by the theorem of Mahler [38]. We prove that the Poisson law of parameter t is such a measure precisely when $v_p(t) \geq 1/(p-1)$, that the Gaussian laws of nonzero variance never are, and that the laws of the main characters of O_N^+ with $N \geq 2$ and of S_N^+ with $N \geq 4$, which are the semicircle and free Poisson laws, are not either. By contrast, the laws for S_N are bounded measures, with norms going to infinity with N, for any prime p.

These results, which make use of Kummer's theorem on the carries, of the congruences of Touchard and Barsky [11, 47] for the Bell numbers, and of the analytic theory of Amice [2], show that the p-adic analysis distinguishes between the classical and free worlds in a way which is quite different from what happens over $\mathbb{R}$, where the free laws are the nice ones, being compactly supported. All this suggests looking for a p-adic analogue of the free probability theory of Voiculescu [50], and we will discuss this question, among others, at the end.

The paper is organized as follows: 1-2 contain generalities and the proof of Theorem A, 3-5 deal with the forms, and contain the proofs of Theorems B, C, D, 6-7 deal with analysis, over arbitrary fields and over the p-adics, and 8 contains a list of questions.

Acknowledgments. We would like to thank Julien Bichon and Serban Belinschi for various discussions over the time, on these topics.

1. Hopf algebras over fields

Throughout this paper F is a field of characteristic 0, with algebraic closure $\bar{F}$, and absolute Galois group $\Gamma = Gal(\bar{F}/F)$. For a matrix $u = (u_{ij})$ with entries in an algebra we denote by $u^t = (u_{ji})$ its transpose, and by $u \dot{\otimes} v$ the matrix with entries $\sum_k u_{ik} \otimes v_{kj}$. For the general theory of Hopf algebras over fields we refer to [3, 46]. Much of the classification theory works over an algebraically closed field of characteristic 0, see for instance [5, 14, 41], and we will be careful about this point. We use the following Hopf algebra, which is that of Wang's free unitary group [51], with the involution forgotten:

Definition 1.1. *We let $\mathcal{O}(GL_N^+)_F$ be the universal F-algebra generated by the entries of 2 matrices u, v of size N, with the relations $uv^t = v^t u = 1$ and $vu^t = u^t v = 1$.*

In other words, u and u^t are both invertible, with $v^t = u^{-1}$. This algebra is a Hopf algebra, with comultiplication $\Delta(u) = u \dot{\otimes} u$, $\Delta(v) = v \dot{\otimes} v$, counit $\varepsilon(u) = \varepsilon(v) = 1$, and antipode $S(u) = v^t$, $S(v) = u^t$, which satisfies $S^2 = id$. The verifications here are routine, and only involve the defining relations, which have integer coefficients, so everything works over any field. We will need as well Hopf algebras which are not of Kac type, and we use the following general notion:

Definition 1.2. *A quantum group over F, of matrix type, is a pair (A, u), where A is a Hopf algebra over F and $u \in M_N(A)$ is an invertible matrix, with $\Delta(u) = u \dot{\otimes} u$, $\varepsilon(u) = 1$, such that A is generated as an algebra by the entries of u and u^{-1}. We write $A = \mathcal{O}(G)_F$, and we say that G is of Kac type when $S^2 = id$.*

This is the dual notion of the inner linear Hopf algebras from [4]. The generation by u and u^{-1}, and not by u alone, is needed, as shown by the group algebra $F[\mathbb{Z}]$, with $u = (z)$, which is not generated by z. In the Kac case $S(u^t) = (S(u))^t$ is the inverse of u^t, and so $\mathcal{O}(G)_F$ is a quotient of $\mathcal{O}(GL_N^+)_F$, by $v \to (u^{-1})^t$. This is the setting used in [8] and in the study of the real forms. The corepresentations of G are the matrices $r \in M_k(A)$ with $\Delta(r) = r \dot{\otimes} r$ and $\varepsilon(r) = 1$, and their intertwiners are given by:

$$Hom(r, s) = \left\{ T \in M_{l \times k}(F) \middle| Tr = sT \right\}$$

Given a field extension L/F, the base change $\mathcal{O}(G)_L = \mathcal{O}(G)_F \otimes_F L$ is a quantum group over L, with the same fundamental matrix. The intertwiner spaces behave as follows:

Proposition 1.3. *For any corepresentations r, s of G over F and any extension L/F we have $Hom_L(r,s) = Hom_F(r,s) \otimes_F L$. In particular, the dimensions of the intertwiner spaces do not depend on the field.*

Proof. The space $Hom_F(r,s)$ is the kernel of the F-linear map $M_{l\times k}(F) \to M_{l\times k}(A)$ given by $T \to Tr - sT$, and the space $Hom_L(r,s)$ is the kernel of its base change. Since L is flat over F, taking kernels commutes with the base change, and this gives the result. □

A Haar functional of $\mathcal{O}(G)_F$ is a linear form $h : \mathcal{O}(G)_F \to F$ with $h(1) = 1$ which is left and right invariant, $(id \otimes h)\Delta = (h \otimes id)\Delta = h(.)1$. By the theorem of Larson and Sweedler [46], such a functional exists if and only if $\mathcal{O}(G)_F$ is cosemisimple, and in this case it is unique. We have:

Proposition 1.4. *The Haar functional of $\mathcal{O}(G)_F$ exists if and only if the Haar functional of $\mathcal{O}(G)_L$ exists, for some, or any, extension L/F, and in this case $h_L = h_F \otimes id$. Moreover, if L/F is Galois, the Haar functional is Galois equivariant.*

Proof. If h_F exists, $h_F \otimes id$ is a Haar functional for $\mathcal{O}(G)_L$. Conversely, if $\mathcal{O}(G)_L$ is cosemisimple, the dual algebra of any finite dimensional subcoalgebra $C \subset \mathcal{O}(G)_F$ becomes semisimple after tensoring with L, and is therefore semisimple, its radical being nilpotent, and so extending to a nilpotent ideal. Thus $\mathcal{O}(G)_F$ is cosemisimple, and h_F exists, with $h_L = h_F \otimes id$ by uniqueness. Finally, for $\gamma \in Gal(L/F)$ acting on the second factor, $\gamma h_L \gamma^{-1}$ is a Haar functional, so it equals h_L. □

We now discuss the F-forms. If B is a Hopf algebra over L, an F-form of B is a Hopf algebra A over F with $A \otimes_F L \simeq B$. The forms are classified by Galois cohomology, in the usual way, see Serre [44] and Waterhouse [52], and are closely related to the Hopf-Galois objects, see Bichon [17]:

Proposition 1.5. *Let A be a Hopf algebra over F, and L/F a finite Galois extension, with group Γ_L. The F-forms of $A \otimes_F L$ which split over L, up to isomorphism, are in bijection with $H^1(\Gamma_L, Aut_L(A \otimes_F L))$, with Γ_L acting on the Hopf algebra automorphisms by conjugation. The same holds over $\bar{F}$, with continuous cohomology, when A is finitely generated.*

Proof. Given a form A' and an isomorphism $f : A' \otimes L \to A \otimes L$, the elements $c_\gamma = f\gamma f^{-1}\gamma^{-1}$, with γ acting on the second factors, are Hopf algebra automorphisms, forming a cocycle, whose class does not depend on f. Conversely, a cocycle defines a twisted semilinear action $\gamma \to c_\gamma\gamma$ on $A \otimes L$, and the fixed points form a Hopf algebra A' over F, with $A' \otimes L \simeq A \otimes L$, by the lemma of Speiser, which states that a vector space over L with a semilinear action of Γ_L is spanned by its fixed points. In the infinite case, the finite generation of A ensures that any isomorphism between $A' \otimes \bar{F}$ and $A \otimes \bar{F}$ is defined over a finite extension, so that the corresponding cocycle is continuous. □

Observe that the automorphisms here are the Hopf algebra automorphisms, which are not required to preserve a given fundamental matrix. Thus, if $A = \mathcal{O}(G)_F$ is of matrix type, an F-form of $A \otimes \bar{F}$ is a Hopf algebra over F which is generated by the entries of some fundamental matrix, but this matrix need not be a descended version of u, and can even have a different size. For instance the group μ_3 of cubic roots of unity is a $\mathbb{Q}$-form of the cyclic group $\mathbb{Z}_3$, because $\mu_3 \simeq \mathbb{Z}_3$ over $\mathbb{Q}(\omega)$. Here $\mathcal{O}(\mu_3)_{\mathbb{Q}} = \mathbb{Q}[z]/(z^3 - 1)$ is generated by the coefficient of the 1-dimensional corepresentation z, while $\mathcal{O}(\mathbb{Z}_3)_{\mathbb{Q}} = \mathbb{Q}^3$ has no such generator, its only 1-dimensional corepresentation being the trivial one.

Let us discuss now the involutions. Over $\mathbb{C}$, a Hopf $*$-algebra structure is an antilinear involution $*$ which is antimultiplicative and comultiplicative. Such an involution is not a Galois real form, because it reverses the products, and the composition $S\circ *$ is antilinear and multiplicative, but anti-comultiplicative. In the commutative case, however, $*$ itself is multiplicative, and defines a real form in the Galois sense, namely the real coordinate algebra of the descended group. Observe that the real points alone can miss functions, as shown by the group μ_3 of cubic roots of unity, which has 1 real point, and whose real coordinate algebra $\mathbb{R}[z]/(z^3-1)$ has dimension 3. In the noncommutative case the 2 notions are related as follows:

Proposition 1.6. *Let A be a Hopf algebra over $\mathbb{R}$, generated by the entries of u, and assume that there is an antimultiplicative coalgebra automorphism ι of A with $\iota(u_{ij})=u_{ij}$. Then $A\otimes\mathbb{C}$ is a Hopf $*$-algebra, with $(a\otimes z)^*=\iota(a)\otimes\bar{z}$, and $u_{ij}^*=u_{ij}$.*

Proof. The map $*$ is antilinear and antimultiplicative, it is an involution since ι^2 is multiplicative and fixes the generators, and it is comultiplicative, because ι and the conjugation both are. Finally, $u_{ij}^*=\iota(u_{ij})=u_{ij}$. □

For $\mathcal{O}(GL_N^+)$ the map ι reversing the order of the products exists, because the relations are exchanged by it, and this gives the real involution $u_{ij}^*=u_{ij}$, $v_{ij}^*=v_{ij}$, which corresponds to $GL_N^+(\mathbb{R})$. We will see that the same happens for the easy quantum groups, and for the Hopf algebras $B(E)$ with E real and symmetric, giving the quantum groups $O^+(p,q)$. Let us discuss now the role of the algebraic closure. Over a field F which is not algebraically closed, an irreducible corepresentation is not necessarily absolutely irreducible. For instance, the algebra of functions on $\mathbb{Z}_3$, over $\mathbb{Q}$, has a 2-dimensional irreducible corepresentation, which splits over $\mathbb{Q}(\omega)$. Also, the deformation parameters which appear in the monoidal equivalences, such as the parameter q of $SL_q(2)$ below, live in general only in $\bar{F}$. Our results will be of 2 types:

(1) Statements which are invariant under base change, such as the dimensions of the intertwiner spaces, the cosemisimplicity, or the existence of the Haar functional. These hold over any F, with the proofs typically done over $\bar{F}$, or over $\mathbb{C}$, and then descended.
(2) Statements about the F-forms, which only make sense when F is not algebraically closed, all the forms becoming isomorphic over $\bar{F}$. Here the proofs are done over $\bar{F}$, and then descended via Proposition 1.3 and Proposition 1.5.

The statements which genuinely need $\bar{F}$, such as the monoidal equivalences, will be formulated after base change. Also, we will always say absolutely irreducible when this is what is needed. Summarizing, we have the following result:

Theorem 1.7. *Given a quantum group G over F, and an extension L/F:*

(1) *$Hom_L(r,s)=Hom_F(r,s)\otimes L$, for any corepresentations r,s.*
(2) *G is cosemisimple over F if and only if it is so over L, with $h_L=h_F\otimes id$.*
(3) *The F-forms of $\mathcal{O}(G)_{\bar{F}}$ correspond to the classes in $H^1(\Gamma,Aut(\mathcal{O}(G)_{\bar{F}}))$, with continuous cohomology.*
(4) *Over $\mathbb{R}$, the real forms equipped with an anti-automorphism as above produce Hopf $*$-algebras over $\mathbb{C}$, with self-adjoint generators.*

Proof. This follows from Propositions 1.3, 1.4, 1.5, 1.6. □

2. Easiness and base change

We recall that $P(k,l)$ is the set of partitions between an upper row of k points and a lower row of l points, and that $NC(k,l)\subset P(k,l)$ is the subset of noncrossing partitions. Given

$\pi \in P(k,l)$ and an integer $N \geq 1$ we have a linear map $T_\pi : (F^N)^{\otimes k} \to (F^N)^{\otimes l}$, given by:

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

Here $\delta_\pi = 1$ when the indices fit, in the sense that any 2 indices in the same block of π are equal, and $\delta_\pi = 0$ otherwise. A category of partitions is a collection of subsets $D(k,l) \subset P(k,l)$, stable under horizontal concatenation, vertical composition and upside-down turning, and containing the identity and the semicircle $\cap \in P(0,2)$. Such a category is automatically stable under rotation. The main examples are the categories P, NC, P_2, NC_2 of all partitions, noncrossing partitions, pairings and noncrossing pairings, and their versions P_{12}, NC_{12} with singletons and pairs, and P_{even}, NC_{even} with blocks of even size. See [10].

Definition 2.1. *Given a category of partitions D and $N \geq 1$, we let $\mathcal{O}(G_N(D))_F$ be the quotient of $\mathcal{O}(GL_N^+)_F$ by the relations $T_\pi \in Hom(u^{\otimes k}, u^{\otimes l})$, for any $\pi \in D(k,l)$.*

We denote by $G = G_N(D)$ the corresponding quantum group. Here $u^{\otimes k}$ is the matrix with entries $u_{i_1 j_1} \ldots u_{i_k j_k}$. Since $\cap \in D(0,2)$ and $\cup \in D(2,0)$, we have $uu^t = u^t u = 1$, so $v = u$ in the quotient, and u is orthogonal. With $D = P, P_2, P_{12}, P_{even}$ we obtain the groups S_N, O_N, B_N, H_N, and with $D = NC, NC_2, NC_{12}, NC_{even}$ we obtain their free versions $S_N^+, O_N^+, B_N^+, H_N^+$. We have:

Proposition 2.2. *$\mathcal{O}(G_N(D))_F$ is a Hopf algebra of Kac type, with $S(u_{ij}) = u_{ji}$. Over $\mathbb{C}$, it has an involution given by $u_{ij}^* = u_{ij}$, and is the CQG algebra of the easy quantum group $G_N(D)$ from [10].*

Proof. The relations coming from $\pi \in D(k,l)$ generate a biideal, because with $X = T_\pi u^{\otimes k} - u^{\otimes l} T_\pi$ we have $\Delta(X) = X \dot{\otimes} u^{\otimes k} + u^{\otimes l} \dot{\otimes} X$. Regarding the antipode, consider the antimultiplicative map given by $S(u_{ij}) = u_{ji}$. With $\tilde{\pi}$ being the rotation of π by 180°, applying S to the relation for π, which reverses the order of the products and transposes the indices, gives the relation $T_{\tilde{\pi}} u^{\otimes l} = u^{\otimes k} T_{\tilde{\pi}}$. Since $\tilde{\pi} \in D(l,k)$, S is well-defined on the quotient, and since $u^t u = uu^t = 1$ it satisfies the antipode axioms on the generators, and so everywhere. The same argument, with the conjugation added, shows that $u_{ij}^* = u_{ij}$ extends to an involution over $\mathbb{C}$, the maps T_π being real. We obtain in this way a Hopf $*$-algebra generated by the coefficients of an orthogonal matrix, which is a CQG algebra in the sense of [27], and the universal C^*-completion is the algebra $C(G_N(D))$ from [10], by universality. □

We will need the Gram matrix of a category of partitions, which is the matrix indexed by $D(k) = D(0,k)$ given by $G_{kN}(\pi, \sigma) = N^{|\pi \vee \sigma|}$, where $|.|$ is the number of blocks. This matrix has integer entries, and is the Gram matrix of the vectors $\xi_\pi = T_\pi(1) \in (F^N)^{\otimes k}$, with respect to the standard bilinear form. When G_{kN} is invertible, its inverse $W_{kN} = G_{kN}^{-1}$ is the Weingarten matrix. We can now state and prove our first main result:

Theorem 2.3. *Let D be a category of partitions, $N \geq 1$, and F a field of characteristic 0.*

1. *$\mathcal{O}(G_N(D))_F = \mathcal{O}(G_N(D))_{\mathbb{Q}} \otimes_{\mathbb{Q}} F$.*
2. *$Hom(u^{\otimes k}, u^{\otimes l}) = span_F(T_\pi | \pi \in D(k,l))$.*
3. *The Haar functional h_F exists, is F-valued, and restricts to the Haar functional $h_{\mathbb{Q}}$ of $\mathcal{O}(G_N(D))_{\mathbb{Q}}$, which is $\mathbb{Q}$-valued. When G_{kN} is invertible, we have*

$$h_F(u_{i_1 j_1} \ldots u_{i_k j_k}) = \sum_{\pi, \sigma \in D(k)} \delta_\pi(i) \delta_\sigma(j) W_{kN}(\pi, \sigma)$$

4. *The main character $\chi = \sum_i u_{ii}$ satisfies $h_F(\chi^k) = rank(G_{kN})$, with no invertibility assumption.*

Proof. (1) This is clear, because the defining relations have integer coefficients.

(2) Over $\mathbb{C}$ this is the main result of [10], coming from Woronowicz's Tannakian duality [54], applied to the CQG algebra from Proposition 2.2. By Proposition 1.3 we have $Hom_{\mathbb{C}} = Hom_{\mathbb{Q}} \otimes \mathbb{C}$, and since the maps T_π are rational, a rational matrix in their complex span is in their rational span. Thus $Hom_{\mathbb{Q}} = span_{\mathbb{Q}}(T_\pi)$, and Proposition 1.3 again gives the result over F.

(3) Over $\mathbb{C}$, the Haar state of Woronowicz satisfies $(id \otimes h)(u^{\otimes k}) = P_k$, the orthogonal projection onto the fixed point space $Fix(u^{\otimes k}) = span(\xi_\pi | \pi \in D(k))$. Since these vectors are rational, P_k is rational, being given by $P_k = X(X^tX)^{-1}X^t$, with X having as columns a maximal linearly independent family of vectors ξ_π, whose Gram matrix X^tX is positive definite over $\mathbb{Q}$. Thus h maps $\mathcal{O}(G)_{\mathbb{Q}}$ into $\mathbb{Q}$, and its restriction $h_{\mathbb{Q}}$ is a Haar functional over $\mathbb{Q}$, whose extension h_F to F is the Haar functional over F, by uniqueness, with the same formula for P_k. When G_{kN} is invertible, the ξ_π are linearly independent, and $P_k = \sum_{\pi\sigma} W_{kN}(\pi, \sigma)\xi_\pi\xi_\sigma^t$, which gives the formula.

(4) We have $h_F(\chi^k) = tr(P_k) = \dim Fix(u^{\otimes k})$, which is the rank of the Gram matrix. □

As a first comment, the proof of (2) uses the analysis over $\mathbb{C}$, and it would be interesting to have a direct algebraic proof over $\mathbb{Q}$, based for instance on a Tannakian duality theorem for Hopf algebras of Kac type over $\mathbb{Q}$. Observe also that no involution on F is needed in the above, the hermitian structure of $\mathbb{C}$ being only used in order to compute rational data, namely the spaces $span_{\mathbb{Q}}(T_\pi)$ and the projections P_k. Over a general field the standard bilinear form can be isotropic, as for instance $(1, i) \in \mathbb{C}^2$, which has square 0, so a projection onto a subspace, orthogonal with respect to this form, might not exist. This problem does not appear here, because the fixed point spaces are spanned by rational vectors, and the restriction of the standard form to them is positive definite over $\mathbb{Q}$, and so stays nondegenerate over any field of characteristic 0. Finally, the fact that the Haar functional is $\mathbb{Q}$-valued on the rational form follows as well from Proposition 1.4, applied with $L = \mathbb{C}$, for any Hopf algebra defined over $\mathbb{Q}$ which becomes cosemisimple over $\mathbb{C}$, the extra information in the easy case being the explicit formula for the projections P_k, in terms of the partition vectors.

When G_{kN} is invertible, the Weingarten matrix being the inverse of an integer matrix, its entries lie in $\mathbb{Z}[1/\det G_{kN}]$, and in general, with X as in the above proof, the denominators of P_k divide $\det(X^tX)$. Observe that the Gram matrix can be singular, even for small values of the parameters. For instance for S_1 and $k = 2$ we have $P(2) = \{\sqcap, ||\}$, the Gram matrix is the all-one 2×2 matrix, and we have $h_F(\chi^2) = 1$, which is its rank. Thus the determinants of the Gram matrices control the arithmetic of the Haar functional. These determinants are polynomials in N with integer coefficients, which can be computed in closed form, see [9]. In the classical case, we have the following result, where f^μ denotes the number of standard Young tableaux of shape μ, and where for $\lambda = (\lambda_1, \lambda_2, \ldots)$ we set $2\lambda = (2\lambda_1, 2\lambda_2, \ldots)$:

Proposition 2.4. *The Gram determinants of S_N and O_N are given by the following formulae:*

(1) *For S_N, with k points,* $\det G_{kN} = \prod_{\pi \in P(k)} N(N-1)\ldots(N-|\pi|+1)$.

(2) *For O_N, with $2k$ points,* $\det G_{2k,N} = \prod_{\lambda \vdash k} \left(\prod_{(i,j)\in\lambda}(N+2j-i-1)\right)^{f^{2\lambda}}$.

Proof. (1) For $\nu \in P(k)$, the number $N^{|\nu|}$ counts the maps $\{1, \ldots, k\} \to \{1, \ldots, N\}$ which are constant on the blocks of ν, and by grouping these maps according to their kernel $\tau \geq \nu$, we obtain $N^{|\nu|} = \sum_{\tau \geq \nu} N(N-1)\ldots(N-|\tau|+1)$. Since $\pi \vee \sigma \leq \tau$ means $\pi, \sigma \leq \tau$, we obtain $G_{kN} = ZDZ^t$, with $Z(\pi, \tau) = \delta_{\pi \leq \tau}$, which is unitriangular, and with D diagonal, $D(\tau, \tau) = N(N-1)\ldots(N-|\tau|+1)$. Thus $\det G_{kN} = \det D$, which is a well-known result of Lindström [37].

(2) Here the pairings of $2k$ points are the cosets of the hyperoctahedral group inside S_{2k}, and the Gram matrix is diagonalized by the zonal spherical functions, its eigenvalues being the products in the statement, with multiplicities $f^{2\lambda}$, see Collins and Matsumoto [21]. The program `gram.py` checks these formulae, up to $k = 5$, and up to $2k = 8$. □

In the free case the formulae involve the Chebyshev polynomials of the second kind, given by $U_0 = 1$, $U_1 = x$ and $U_{m+1} = xU_m - U_{m-1}$, and the following integers, with the convention that the binomial coefficients with negative lower index vanish:

$$a_{km} = \binom{2k}{k-m} - 2\binom{2k}{k-m-1} + \binom{2k}{k-m-2}$$

With these notations, and with C_k being the Catalan numbers, we have the following result, coming from the work of Di Francesco on the meander determinants [26]:

Proposition 2.5. *The Gram determinants of O_N^+ and S_N^+ are given by the following formulae:*

(1) *For O_N^+, with $2k$ points,* $\det G_{2k,N} = \prod_{m=1}^{k} U_m(N)^{a_{km}}$.
(2) *For S_N^+, with k points,* $\det G_{kN} = N^{C_k/2} \prod_{m=1}^{k} U_m(\sqrt{N})^{a_{km}}$.

Proof. (1) This is the formula of Di Francesco for the meander determinants [26]. Observe that some exponents a_{km} can be negative, the first example being $a_{8,1} = -208$, but the product is a polynomial in N, with integer coefficients.

(2) We use the fattening bijection $NC(k) \simeq NC_2(2k)$, $\pi \to \tilde{\pi}$. The number of loops of $\tilde{\pi}$ and $\tilde{\sigma}$ is $2|\pi \vee \sigma| - |\pi| - |\sigma| + k$. Thus, with T an indeterminate, $N = T^4$, and D the diagonal matrix with entries $T^{2|\pi|-k}$, which can be negative powers of T, we have $G_{kN} = DG'_{2k,T^2}D$ over the ring $\mathbb{Z}[T, T^{-1}]$, where G' is the Gram matrix of O^+. Since the average number of blocks of $\pi \in NC(k)$ is $(k+1)/2$, we have $\det D^2 = T^{2C_k} = N^{C_k/2}$, and taking determinants, (1) gives the result, as an identity of rational functions in T. The right-hand side, simplified as a rational function, is then a polynomial in $\mathbb{Z}[N]$, and we can specialize N to any element of F, including $N = 0$. The program `gram.py` checks these formulae, up to $2k = 12$, and up to $k = 6$, and checks that the product in (1) is a polynomial, up to $k = 8$. □

Since the zeros of U_m are the numbers $2\cos(j\pi/(m+1))$ with $1 \leq j \leq m$, the zeros of the Gram determinants are integers in the classical case, namely $0, 1, \ldots, k-1$ for S_N, and numbers in $[-2k+2, k-1]$ for O_N, and Beraha type numbers in the free case, namely $2\cos(j\pi/(m+1))$ for O_N^+, and 0 and $4\cos^2(j\pi/(m+1))$ for S_N^+. Here are the first few values, with k being the number of points, first in the permutation case:

G	k	$\det G_{kN}$
S_N	2	$N^2(N-1)$
S_N	3	$N^5(N-1)^4(N-2)$
S_N	4	$N^{15}(N-1)^{14}(N-2)^7(N-3)$
S_N^+	2	$N^2(N-1)$
S_N^+	3	$N^5(N-1)^4(N-2)$
S_N^+	4	$N^{14}(N-1)^{13}(N-2)^6(N^2-3N+1)$

Observe that the values for S_N and S_N^+ coincide at $k \leq 3$, because $P(k) = NC(k)$ in this case. The difference appears at $k = 4$, where the factor $N-3$ for S_N, coming from the partition into 4 singletons, is replaced for S_N^+ by the factor $N^2 - 3N + 1$, whose roots $4\cos^2(\pi/5)$ and

$4\cos^2(2\pi/5)$ are the first Beraha numbers which are not integers. In the orthogonal case, the first values are as follows:

G	k	$\det G_{kN}$
O_N	4	$N^3(N-1)^2(N+2)$
O_N	6	$N^{15}(N-1)^{14}(N-2)^5(N+2)^{10}(N+4)$
O_N	8	$N^{105}(N-1)^{104}(N-2)^{70}(N-3)^{14}(N+1)^{14}(N+2)^{91}(N+4)^{21}(N+6)$
O_N^+	4	$N^2(N^2-1)$
O_N^+	6	$N^5(N^2-1)^4(N^2-2)$
O_N^+	8	$N^{14}(N^2-1)^{13}(N^2-2)^6(N^4-3N^2+1)$

Here the factor $N^4-3N^2+1=(N^2-N-1)(N^2+N-1)$ for O_N^+ corresponds to the factor N^2-3N+1 for S_N^+, via $N\to\sqrt{N}$, in agreement with Proposition 2.5. For instance, for S_N^+ at $k=2$ we have, with the partitions ordered as $\{\sqcap,||\}$:

$$W_{2N}=\frac{1}{N^2(N-1)}\begin{pmatrix}N^2&-N\\-N&N\end{pmatrix}$$

We will come back to the arithmetic of these formulae in section 7, in the p-adic setting. The basic phenomenon is that, for $N\geq 3$, the Haar functional of S_N^+ is p-integral on the products of at most 4 coordinates when p does not divide $N(N-1)(N-2)(N^2-3N+1)$, the last factor being responsible for $p=5$, and for the primes $p\equiv\pm1$ modulo 5. Finally, let us mention that the Gram matrices are polynomial in N, and the Weingarten matrices are rational functions in N, so that they can be interpolated at arbitrary values $N=t\in F$, away from the zeros of the Gram determinants, in the spirit of Deligne's categories $Rep(S_t)$ [25]. The theorem below, which is Theorem A, summarizes:

Theorem 2.6. *Over any field F of characteristic 0, the easy quantum groups are cosemisimple, with intertwiners spanned by the maps T_π, and with F-valued Haar functional h_F, which restricts to a $\mathbb{Q}$-valued functional on the rational form, given by the Weingarten formula when the Gram matrix is invertible, with denominators dividing the Gram determinant. In addition, the law of the main character has integer moments, $h_F(\chi^k)=rank(G_{kN})$.*

Proof. This follows from Theorem 2.3, and from the above discussion. □

3. Forms and congruence classes

We discuss here the F-forms of O_N^+, in the Galois sense, that is, the Hopf algebras over F which become isomorphic to $\mathcal{O}(O_N^+)$ over $\bar{F}$. These will come from the bilinear forms $E\in GL_N(F)$, so the word "form" will have 2 meanings in what follows, and we will always write F-form for the first one, and bilinear or quadratic form for the second one. The relevant objects are the following Hopf algebras, introduced by Dubois-Violette and Launer [28]:

Definition 3.1. *Given $E\in GL_N(F)$, we let $B(E)$ be the universal F-algebra generated by the entries of a matrix u of size N, with the relations $E^{-1}u^tEu=1=uE^{-1}u^tE$.*

This is a Hopf algebra, with $\Delta(u)=u\dot{\otimes}u$, $\varepsilon(u)=1$, $S(u)=E^{-1}u^tE$, see [14, 28]. The first relation reads $u^tEu=E$, so $B(E)$ is the universal Hopf algebra preserving the bilinear form E. We have $S^2(u)=MuM^{-1}$, with $M=E^{-1}E^t$, and so $B(E)$ is of Kac type when E is symmetric or antisymmetric. At $E=1$ we obtain $\mathcal{O}(O_N^+)$. Observe also that, the relations having coefficients in F, we have $B(E)\otimes_F L=B(E)_L$ for any extension L/F, where $B(E)_L$

is the Hopf algebra over L associated to E, regarded as an element of $GL_N(L)$. The basic properties of these quantum groups are as follows:

Proposition 3.2. *Let $E \in GL_N(F)$, with $N \geq 2$.*

1. *$B(cP^tEP) \simeq B(E)$ for any $c \in F^*$ and $P \in GL_N(F)$, via $u \to PuP^{-1}$.*
2. *$B(E) \otimes \bar{F}$ is monoidally equivalent to $\mathcal{O}(SL_q(2))_{\bar{F}}$, with $q \in \bar{F}$ given by $q^2 + tq + 1 = 0$, where $t = tr(E^{-1}E^t) \in F$.*
3. *$B(E)$ is cosemisimple if and only if q is not a root of unity of order ≥ 3.*
4. *In the cosemisimple case, the irreducible corepresentations over $\bar{F}$ are $r_0 = 1, r_1 = u, r_2, \ldots$ with dimensions $d_0 = 1$, $d_1 = N$, $d_{k+1} = Nd_k - d_{k-1}$, and u is absolutely irreducible.*

Proof. (1) The matrix $w = PuP^{-1}$, with u the generator of $B(cP^tEP)$, satisfies

$$E^{-1}w^tEw = E^{-1}P^{-t}u^tP^tEPuP^{-1} = P(P^tEP)^{-1}u^t(P^tEP)uP^{-1} = 1$$

and similarly for the other relation, and the scalar c cancels. Thus we have a morphism $B(E) \to B(cP^tEP)$, and the inverse is constructed in the same way.

(2) This is the main result of Bichon [14], which is formulated over an algebraically closed field of arbitrary characteristic, and does not depend on cosemisimplicity. The monoidal equivalence maps u to the fundamental corepresentation. Since q is in general not in F, the equivalence must be formulated over $\bar{F}$.

(3) Over $\bar{F}$, which is of characteristic 0, the Hopf algebra $\mathcal{O}(SL_q(2))_{\bar{F}}$ is cosemisimple precisely when q is not a root of unity of order ≥ 3, and the monoidal equivalence in (2) preserves the cosemisimplicity, see [14]. The cosemisimplicity over F is then equivalent to that over $\bar{F}$, by Proposition 1.4.

(4) The fusion rules are those of $SL_q(2)$, and the dimensions follow from $r_1 \otimes r_k = r_{k-1} + r_{k+1}$, and from $\dim u = N$. □

At $E = 1$ we have $t = N$, so $q + q^{-1} = -N$, which is the well-known parameter of O_N^+, and for $N \geq 3$ we have $q \notin \mathbb{Q}$. For more on monoidal equivalence, see Bichon, De Rijdt and Vaes [18], and for the finite dimensional cosemisimple Hopf algebras having a self-dual 2-dimensional irreducible corepresentation, which are deformations of the binary polyhedral groups, see Bichon and Natale [20]. Now let us look for the isomorphisms between the Hopf algebras $B(E)$. We have:

Proposition 3.3. *Let $E, E' \in GL_N(F)$, $N \geq 2$, with $B(E)$ cosemisimple. Then $B(E) \simeq B(E')$ as Hopf algebras if and only if $E' = cP^tEP$, for some $c \in F^*$ and $P \in GL_N(F)$.*

Proof. One implication is Proposition 3.2 (1). Conversely, let $f : B(E) \to B(E')$ be an isomorphism. Then $f(u)$ is a corepresentation of dimension N of $B(E')$, whose coefficients generate $B(E')$. Over $\bar{F}$, by Proposition 3.2 (4) the irreducible corepresentations have dimensions $1 < N < d_2 < \ldots$, and $r_0 = 1$ is the only 1-dimensional one, so $f(u)$ is either equivalent to u', or to a sum of N copies of the trivial corepresentation. In the latter case $f(u) = 1$, which is impossible, so $f(u) \simeq u'$ over $\bar{F}$. Now by Proposition 1.3 we have $Hom_F(u', f(u)) \otimes \bar{F} = Hom_{\bar{F}}(u', f(u))$, which is 1-dimensional, spanned by an invertible matrix V_0. Thus $Hom_F(u', f(u))$ is 1-dimensional too, spanned by a matrix $V = \lambda V_0$ with $\lambda \in \bar{F}^*$, which is invertible, and from $Vu' = f(u)V$ we obtain $f(u) = Vu'V^{-1}$, with $V \in GL_N(F)$. Applying f to $u^tEu = E$ gives $u'^t(V^tEV)u' = V^tEV$, so V^tEV is an invariant bilinear form for u'. But these bilinear forms X, with $u'^tXu' = X$, correspond to the space $Hom(u' \otimes u', 1)$, which is 1-dimensional by the fusion rules $u' \otimes u' = 1 + r_2$, so $V^tEV = c^{-1}E'$, and so $E' = cV^tEV$, as claimed. □

For E symmetric we have $t = N$, and $B(E)$ is cosemisimple for any $N \geq 2$, because $q^2 + Nq + 1 = 0$ has no roots of unity of order ≥ 3 as solutions. Thus the isomorphism classes of the Hopf algebras $B(E)$ with E symmetric are the similarity classes of nondegenerate quadratic forms over F. These need not exhaust the F-forms of O_N^+, and in order to find the others we need the automorphism group:

Proposition 3.4. *For $N \geq 2$, the Hopf algebra automorphisms of $\mathcal{O}(O_N^+)_{\bar{F}}$ are the maps $u \to V^{-1}uV$, with V in the group of orthogonal similitudes $GO_N(\bar{F})$, and we have $Aut(\mathcal{O}(O_N^+)_{\bar{F}}) = PGO_N(\bar{F})$, as groups with Γ-action.*

Proof. As in the proof of Proposition 3.3, an automorphism f maps u to $V^{-1}uV$, and the relation $u^tu = 1$ is preserved precisely when VV^t is a scalar matrix. The scalar matrices V give the identity, and the Γ-action is the natural one, because u is defined over $\mathbb{Q}$. □

Now recall from [35] that the Galois cohomology set $H^1(F, PGO_N)$ classifies the pairs (Z, σ) consisting of a central simple F-algebra Z of degree N and an orthogonal involution σ, up to isomorphism. The split ones are the pairs $(M_N(F), \sigma_E)$, with $\sigma_E(X) = E^{-1}X^tE$ the adjoint involution of a symmetric bilinear form E, and two such pairs are isomorphic precisely when the bilinear forms are similar. Thus the underlying algebra is $M_N(F)$ for all the split pairs, which are distinguished by the involution. Also, for N odd every such pair is split. Thus, we have:

Proposition 3.5. *For $N \geq 2$, the F-forms of O_N^+ correspond to the isomorphism classes of pairs (Z, σ) consisting of a central simple F-algebra Z of degree N and an orthogonal involution σ. The split ones, with $Z = M_N(F)$, are the Hopf algebras $B(E)$, with E symmetric, up to similarity, and for N odd all F-forms are split.*

Proof. This follows from Proposition 1.5 and Proposition 3.4, and from the correspondence in [35]. The split pair $(M_N(F), \sigma_E)$ corresponds to the cocycle obtained from an isomorphism $B(E) \otimes \bar{F} \simeq \mathcal{O}(O_N^+)_{\bar{F}}$, given by $u \to V^{-1}uV$ with $V^tV = E$. □

Over $\mathbb{R}$, the central simple algebras are $M_N(\mathbb{R})$ and $M_{N/2}(\mathbb{H})$, with N even in the second case. The orthogonal involutions on $M_N(\mathbb{R})$ come from the quadratic forms of signature (p, q), up to $(p, q) \sim (q, p)$, and on $M_{N/2}(\mathbb{H})$ there is a unique orthogonal involution up to isomorphism, corresponding to the Lie group $SO^*(N)$. Thus O_N^+ has $[N/2] + 1$ real forms of type $O^+(p, q)$, and for N even one more, which can be regarded as a free version of $SO^*(N)$. The quantum groups $O^+(p, q)$ are free analogues of the groups $O(p, q)$, and the involution in Proposition 1.6, which exists because for E symmetric the relations of $B(E)$ are stable under the reversal of the products, is $u_{ij}^* = u_{ij}$.

Let us discuss now the rational case, with the free bistochastic quantum group $B_N^+ = G_N(NC_{12})$. Here $u\xi = \xi$, with ξ the all-one vector, and $u^t\xi = \xi$ as well. Let C be the Gram matrix of the vectors $f_k = e_k - e_{k+1}$, with $k = 1, \ldots, N-1$, which is the Cartan matrix of type A_{N-1}. We have:

Proposition 3.6. *Over any field F of characteristic 0, and for $N \geq 2$, we have $\mathcal{O}(B_N^+)_F \simeq B(C)$. The matrix C has determinant N, and is equivalent to the diagonal quadratic form $\langle 1 \cdot 2, 2 \cdot 3, \ldots, (N-1)N \rangle$, whose determinant $N((N-1)!)^2$ has the same square class.*

Proof. Since $\langle \xi, \xi \rangle = N$ is nonzero in F, the characteristic being 0, we have $F^N = F\xi \oplus \xi^\perp$, and in the basis $\xi, f_1, \ldots, f_{N-1}$, given by a matrix P, the Gram matrix is $P^tP = diag(N, C)$. Since u fixes ξ and is orthogonal, $P^{-1}uP = diag(1, w)$, with $w^tCw = C$ and $wC^{-1}w^t = C^{-1}$. Conversely, any such w produces via $u = P\,diag(1, w)P^{-1}$ an orthogonal matrix fixing ξ, and these 2 constructions are inverse to each other. As for the diagonalization, the vectors $g_k =$

$e_1+\ldots+e_k-ke_{k+1}$ are an orthogonal basis of $\xi^\perp$, with $\langle g_k,g_k\rangle=k(k+1)$, and the product of these numbers is $N\cdot((N-1)!)^2$. □

Now by the Hasse-Minkowski theorem [45], deciding whether C is similar to the identity quadratic form reduces to a computation with the Hilbert symbols. The program `forms.py` does these computations, and finds that $B_N^+\simeq O_{N-1}^+$ over $\mathbb{Q}$ for $N=4,8,9,10,12,16,18,20,24,25,\ldots$ In fact, we have the following clean statement, which is the end of the proof of Theorem B:

Theorem 3.7. *For $N\geq 2$, the F-forms of O_N^+ correspond to the isomorphism classes of pairs (Z,σ) consisting of a central simple algebra of degree N and an orthogonal involution, with $B(E)\simeq B(E')$ for E,E' symmetric precisely when they are similar, and over $\mathbb{R}$ we obtain the quantum groups $O^+(p,q)$, and one more real form when N is even. Over $\mathbb{Q}$, for $N\geq 3$, we have $B_N^+\simeq O_{N-1}^+$ if and only if:*

(1) *N is odd, and is a square,*
(2) *or N is a multiple of 4,*
(3) *or $N\equiv 2$ modulo 4, and N is a sum of 2 squares.*

Proof. The first assertions are Propositions 3.3 and 3.5, and the discussion after them. For the last one, we must decide when $C\simeq cI_{N-1}$ for some $c\in\mathbb{Q}^*$. Since $C\perp\langle N\rangle\simeq I_N$, by Witt cancellation this is equivalent to $I_N\simeq cI_{N-1}\perp\langle N\rangle$. If N is odd, $N-1$ is even, and the determinants show that N must be a square, and conversely in this case we can take $c=1$ and cancel $\langle N\rangle=\langle 1\rangle$. If N is even, the determinants give $c=N$ modulo squares, and the condition becomes $NI_N\simeq I_N$. When $4|N$ this holds, because N is a sum of 4 squares, by the theorem of Lagrange, and $\langle 1,1,1,1\rangle$ is the norm form of the quaternions, which is multiplicative, so that $N\langle 1,1,1,1\rangle\simeq\langle 1,1,1,1\rangle$, and we can write I_N as a sum of $N/4$ copies of $\langle 1,1,1,1\rangle$. When $N\equiv 2$ modulo 4 we write $I_N=I_{N-2}\perp I_2$, with $N-2$ a multiple of 4, and by cancellation the condition becomes $\langle N,N\rangle\simeq\langle 1,1\rangle$, which holds if and only if N is represented by $\langle 1,1\rangle$, that is, is a sum of 2 squares. The program `forms.py` checks this statement against a direct Hasse-Minkowski computation, for $N\leq 150$. □

For instance B_3^+ is a nontrivial $\mathbb{Q}$-form of O_2^+, coming from the norm form $\langle 2,6\rangle\sim\langle 1,3\rangle$ of the Eisenstein integers, and B_6^+ is a nontrivial $\mathbb{Q}$-form of O_5^+, while $B_4^+\simeq O_3^+$ over $\mathbb{Q}$, in agreement with the coincidence of root systems $A_3=D_3$. Over $\mathbb{R}$, of course, C is positive definite, and $B_N^+\simeq O_{N-1}^+$.

4. Free quadrics, deformations

We discuss now the free quadrics, over an arbitrary field F. Consider the free algebra $F\langle x_1,\ldots,x_N\rangle$, and a quadratic polynomial $f=\sum_{ij}A_{ij}x_ix_j-1$, with $A\in GL_N(F)$. Observe that A is not necessarily symmetric, because $x_ix_j\neq x_jx_i$. See [7] for more on such quantum algebra questions over general fields. The free quadric X_f is the abstract space whose coordinate algebra is $F\langle x_1,\ldots,x_N\rangle/(f)$. With $F=\mathbb{C}$, with $A=H$ a Hermitian matrix, having complex coefficients, and with the generators x_i being self-adjoint, these are the real free quadrics from [31].

Definition 4.1. *The quantum symmetry group $G^+(f)$ is the universal quantum group of matrix type over F coacting on $F\langle x_1,\ldots,x_N\rangle$ via $x_i\to\sum_j x_j\otimes u_{ji}$, in such a way that $f\to f\otimes 1$.*

In particular, the coaction maps the ideal (f) into $(f)\otimes\mathcal{O}(G^+(f))_F$, and so factorizes through the coordinate algebra of X_f. As in [31], we use the coaction convention $x_i\to\sum_j x_j\otimes u_{ji}$. We have:

Proposition 4.2. *We have $\mathcal{O}(G^+(f))_F = B(A^{-1})$, and for $N \geq 2$ the quantum group $G^+(f)$ becomes over $\bar{F}$ monoidally equivalent to $SL_q(2)$, with $q \in \bar{F}$ given by $q^2 + tq + 1 = 0$, where $t = tr(A^{-1}A^t) \in F$. Also, $S^2 = id$ precisely when A is symmetric or antisymmetric.*

Proof. With $X_i = \sum_j x_j \otimes u_{ji}$ we have $\sum_{ik} A_{ik}X_iX_k = \sum_{jl} x_jx_l \otimes (uAu^t)_{jl}$, and since the monomials x_jx_l are linearly independent, the invariance of f is equivalent to $uAu^t = A$. In a Hopf algebra u is invertible, and this relation is equivalent to $u^tA^{-1}u = A^{-1}$, and to $uAu^tA^{-1} = 1$, so we obtain the relations of $B(A^{-1})$. Regarding t, we have $tr(AA^{-t}) = tr(A^{-1}A^t)$, by transposition. The monoidal equivalence for $N \geq 2$ is Proposition 3.2 (2), while for $N = 1$ we obtain the relation $u^2 = 1$, and so the algebra of functions on $\mu_2 = \{\pm 1\}$. Finally, $S^2(u) = MuM^{-1}$ with $M = AA^{-t}$, and $S^2 = id$ means $M \in End_F(u)$. For $N = 1$ both conditions hold. For $N \geq 2$, since u is absolutely irreducible, the fundamental corepresentation of $SL_q(2)$ being simple for any q, we have $End_F(u) \otimes \bar{F} = End_{\bar{F}}(u) = \bar{F}1$, so $S^2 = id$ if and only if M is scalar, $A^t = \lambda A$, which forces $\lambda = \pm 1$. □

When $F = \mathbb{C}$ and $A = H = Q + iR$ is Hermitian, with Q real symmetric and R real antisymmetric, we have $A^t = \bar{H}$, and $t = tr(H^{-1}\bar{H})$ is real. Indeed, $M = H^{-1}\bar{H}$ satisfies $\bar{M} = M^{-1}$, and $M^t = H\bar{H}^{-1}$ is similar to M^{-1}, so $tr(M) = tr(M^{-1}) = \overline{tr(M)}$. Also, $S^2 = id$ precisely when $R = 0$ or $Q = 0$, so the free quadrics with both $Q \neq 0$ and $R \neq 0$ produce non-Kac quantum groups. In the case of conics, with $F = \mathbb{C}$, and with real parameters λ, μ, we have:

Proposition 4.3. *For the elliptic conic $E(q, 1)$ from [31], whose classical version is an ellipse, given by $H = \begin{pmatrix} 1 & i\lambda \\ -i\lambda & 1 \end{pmatrix}$ with $\lambda \in \mathbb{R} - \{\pm 1\}$, we have $t = 2(1 + \lambda^2)/(1 - \lambda^2)$, and the roots are $q = (\lambda - 1)/(\lambda + 1)$ and its inverse. For the hyperbolic conic $H(\theta, 1)$ from [31], whose classical version is a hyperbola, given by $H = \begin{pmatrix} 1 & i\mu \\ -i\mu & -1 \end{pmatrix}$ with $\mu = \tan\theta \in \mathbb{R}$, we have $t = 2\cos 2\theta$, and $q = -e^{\pm 2i\theta}$.*

Proof. For the first conic $\det H = 1 - \lambda^2 \neq 0$, and with $q = (\lambda - 1)/(\lambda + 1)$ we have $q + q^{-1} = -2(1 + \lambda^2)/(1 - \lambda^2)$, which is $-t$. For the second one $\det H = -(1 + \mu^2) \neq 0$, and $t = 2(1 - \mu^2)/(1 + \mu^2) = 2\cos 2\theta$, and $q + q^{-1} = -2\cos 2\theta$ gives $q = -e^{\pm 2i\theta}$. All this follows as well from Proposition 4.4 below, and the program `quadrics.py` checks it numerically. □

These are exactly the parameters of the elliptic and hyperbolic conics in [31]. More generally, for the elliptic quadric given by a block diagonal sum of elliptic conic blocks with parameters λ_k, plus a 1×1 block when N is odd, the trace is additive, and we obtain $q + q^{-1} = \sum_k (q_k + q_k^{-1}) - \delta$, with $\delta = 1$ for N odd, and $\delta = 0$ for N even. Also, for $H > 0$, writing $H = Z^*Z$ and $Y = Z^{-t}Z^*$, we have $Y\bar{Y} = 1$ and $tr(Y^*Y) = t$, which is the usual parametrization of the universal orthogonal quantum groups $A_o(Y)$ of Van Daele and Wang [48]. For the non-Kac universal quantum groups beyond this setting, namely the universal cosovereign Hopf algebras, see Bichon [15]. The program `quadrics.py` checks these formulae, on random examples.

Let us now classify the free conics, $N = 2$, over an arbitrary field F. Any $A \in M_2(F)$ decomposes as $A = Q + \kappa J$, with Q symmetric and $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and we set $d = \det Q$. We have:

Proposition 4.4. *Assume $d \neq 0$, and $r = \kappa^2/d \neq -1$. Then A is invertible, and we have $t = tr(A^{-1}A^t) = 2(1 - r)/(1 + r)$. The quantity r is invariant under $A \to cP^tAP$, and the pair formed by the similarity class of Q and by r is a complete invariant for this equivalence relation.*

Proof. We have $\det A = d+\kappa^2 = d(1+r)$. Since the adjugate of Q is symmetric and the adjugate of J is $-J$, we have $adj(A)A^t = (adj(Q)-\kappa J)(Q-\kappa J) = (d-\kappa^2)1-\kappa(adj(Q)J+JQ)$, and the last matrix is traceless, being a sum of products of a symmetric and an antisymmetric matrix. Thus $tr(A^{-1}A^t) = 2(d-\kappa^2)/(d+\kappa^2)$, as claimed. Now under $A \to cP^tAP$ we have $Q \to cP^tQP$ and, since $P^tJP = \det(P)J$, $\kappa \to c\det(P)\kappa$, so both d and κ^2 get multiplied by $c^2\det(P)^2$, and r is invariant. Conversely, if $Q' = cP^tQP$ and $r' = r$, then $\kappa' = \pm c\det(P)\kappa$, and in the case of the minus sign we can replace P by P_0P, with $P_0 \in O(Q)(F)$ a reflection, which has determinant -1, and which exists because Q, being nondegenerate, has a vector of nonzero norm. Indeed, we have $(P_0P)^tQ(P_0P) = P^tQP$, and the sign of $c\det(P)\kappa$ changes. The program `quadrics.py` checks these formulae, with exact rational arithmetic. □

When $d = 0$ and $\kappa \neq 0$ we have $t = -2$, so $q = 1$, but for $Q \neq 0$ the matrix $M = A^{-1}A^t$ is not scalar, so $S^2 \neq id$. In this degenerate case, when $Q \neq 0$, the matrix A is congruent to $\kappa J + a\,e_{22}$, the relation $\sum_{ij} A_{ij}x_ix_j = 0$ defines the Jordan plane, and we are in the setting of the Jordanian deformation of $SL(2)$, while when $Q = 0$ we have $A = \kappa J$, and the relation is $x_1x_2 - x_2x_1 = 0$. Over $\mathbb{R}$, the similarity classes of nondegenerate binary forms are the definite one and the indefinite one, and in the Hermitian setting of [31], where the linear changes of variables preserving the self-adjointness of the generators have real coefficients, we have $\kappa \in i\mathbb{R}$, so $r = -\lambda^2 \leq 0$ in the elliptic case, and $r = \mu^2 \geq 0$ in the hyperbolic case. We can now state and prove our classification result, which is Theorem C:

Theorem 4.5. *For the free conics $f = \sum_{ij} A_{ij}x_ix_j - 1$ over a field F of characteristic 0, with $A = Q + \kappa J$, $d = \det Q \neq 0$, and $r = \kappa^2/d \neq -1$, we have:*

1. *$\mathcal{O}(G^+(f))_F = B(A^{-1})$, and $G^+(f)$ becomes over $\bar{F}$ monoidally equivalent to $SL_q(2)$, with $q + q^{-1} = -2(1-r)/(1+r)$.*
2. *In the cosemisimple case, $G^+(f) \simeq G^+(f')$ if and only if Q, Q' are similar and $r = r'$.*
3. *$G^+(f)$ is of Kac type if and only if $r = 0$, that is, A is symmetric.*

Proof. (1) follows from Propositions 4.2 and 4.4. For (2), Proposition 3.3 applied to A^{-1} shows that the isomorphism classes correspond to the classes of A^{-1}, and so of A, under $A \to cP^tAP$, and Proposition 4.4 gives the invariants. As for (3), with $d \neq 0$, A cannot be antisymmetric, so Proposition 4.2 gives the result. □

This answers, at least at the level of the quantum symmetry groups, the question in [31] regarding the free conics over other fields, which correspond to the bilinear forms in 2 variables, up to congruence. Indeed, for the conics themselves, up to linear changes of the variables, the same argument without the scalar c shows that the invariants are the isometry class of Q, and $r \in F$. As an illustration, over $\mathbb{Q}$ the free circle $x_1^2 + x_2^2 = 1$ has as quantum symmetry group O_2^+, while the free conic $x_1^2 + 3x_2^2 = 1$ has as quantum symmetry group the nontrivial $\mathbb{Q}$-form B_3^+ of O_2^+, because $A^{-1} = diag(1, 1/3)$ is similar to the form $\langle 2, 6\rangle$ from Proposition 3.6, and not to the identity.

5. Galois forms of permutations

We discuss now the quantum permutation groups. Recall that a commutative F-algebra K of finite dimension N is finite étale when $K \otimes \bar{F} \simeq \bar{F}^N$, which in characteristic 0 means that K is a finite product of finite field extensions of F. In other words, K is the algebra of functions on a set of N points twisted by the Galois group, the points being the embeddings $K \to \bar{F}$, permuted by Γ. For instance $K = \mathbb{Q}(\sqrt{2})$, with basis $1, \sqrt{2}$, has no nontrivial idempotents, but over $\mathbb{Q}(\sqrt{2})$ it acquires the 2 orthogonal idempotents $(1 \pm \sqrt{2} \otimes \sqrt{2}^{-1})/2$, which are exchanged by the Galois automorphism. In dimension 2, the finite étale algebras are $F \times F$, and the quadratic

extensions $F(\sqrt{a})$, with $a \in F^*$ not a square. By the Galois theory of Grothendieck, the finite étale algebras of dimension N correspond to the actions of Γ on N points, up to isomorphism, see [52]. The trace $Tr = Tr_{K/F}$ becomes, over $\bar{F}$, the sum of the coordinates. Following Wang [51], and Bichon [16], who worked out the algebraic theory of S_N^+ over arbitrary fields, we use:

Definition 5.1. *Given a finite étale F-algebra K of dimension N, with a basis $e_1, \ldots, e_N$, we let A_K be the universal Hopf algebra quotient of $\mathcal{O}(GL_N^+)_F$ making the multiplication $m : K \otimes K \to K$, the unit $\eta : F \to K$ and the trace $Tr : K \to F$ colinear, for the coaction $e_j \to \sum_i e_i \otimes u_{ij}$. We denote by S_K^+ the corresponding quantum group, so that $A_K = \mathcal{O}(S_K^+)_F$.*

The colinearity of a map T means $T \in Hom(u^{\otimes k}, u^{\otimes l})$, and with the conventions above A_K is the universal Kac type Hopf algebra coacting on K, preserving m, η, Tr. For $K = F^N$ this is the quantum permutation algebra studied in [16], where it is shown in particular that, in characteristic 0, it corresponds to the largest linearly reductive algebraic quantum group acting on N points. A change of basis conjugates u, so A_K depends only on K. We have:

Proposition 5.2. *We have $A_K \otimes_F L = A_{K \otimes L}$ for any extension L/F, and $A_{F^N} = \mathcal{O}(S_N^+)_F$. Thus A_K is an F-form of S_N^+, which splits over any field splitting K.*

Proof. The first assertion is clear, because A_K is defined by relations with coefficients in F, namely the structure constants of m, η, Tr in the basis $e_1, \ldots, e_N$, which are also the structure constants of $K \otimes L$ in the basis $e_1 \otimes 1, \ldots, e_N \otimes 1$, and taking the universal Hopf quotient commutes with the base change. For $K = F^N$ with its idempotent basis, the colinearity of m, η, Tr means $u_{ij}u_{ik} = \delta_{jk}u_{ij}$, $\sum_j u_{ij} = 1$ and $\sum_i u_{ij} = 1$. These relations give $u_{ij}^2 = u_{ij}$, and $u^t u = 1$, so $u^t = u^{-1}$, and applying the antipode $S(u_{ij}) = u_{ji}$ to the first relation gives $u_{ki}u_{ji} = \delta_{jk}u_{ji}$. Thus u is a magic matrix, and we obtain $\mathcal{O}(S_N^+)_F$, and conversely the magic relations imply ours. □

The abelianization of A_K represents the functor $R \to Aut_R(K \otimes R)$, so it is the algebra of functions on the finite étale group scheme $Aut(K)$, whose $\bar{F}$-points form the group S_N, with the Galois action twisted by K. In concrete terms, Γ acts on the N-element set $Hom_F(K, \bar{F})$, via a morphism $\rho : \Gamma \to S_N$, well-defined up to conjugation, and:

Proposition 5.3. *The abelianization of A_K is $\mathcal{O}(Aut(K))$, and its F-points form the group $Aut_F(K)$, which is the centralizer of $\rho(\Gamma)$ in S_N.*

Proof. The first assertion follows from the universal property, and the second one from the Galois theory of étale algebras, in the version of Grothendieck, see [52]. □

The program `galois.py` computes these centralizers, and finds for instance $|Aut(K)| = 24, 4, 8, 1, 4, 2, 1$ for $K = \mathbb{Q}^4, \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2})^2, \mathbb{Q}(2^{1/3}), \mathbb{Q}(\zeta_5), \mathbb{Q}(2^{1/4}), \mathbb{Q}(2^{1/3}) \times \mathbb{Q}$. In the case $K = \mathbb{Q}(2^{1/4})$ the Galois group is the dihedral group D_4 acting on the 4 roots of $x^4 - 2$, and its centralizer is $\mathbb{Z}_2$, coming from $x \to -x$. Now, we have the following result:

Proposition 5.4. *For $N \geq 3$ with $N \neq 6$, and finite étale F-algebras K, K' of dimension N, we have $A_K \simeq A_{K'}$ if and only if $K \simeq K'$. Over $\mathbb{R}$ we obtain in this way $[N/2] + 1$ pairwise nonisomorphic real forms of S_N^+, corresponding to $K = \mathbb{R}^r \times \mathbb{C}^s$, with $r + 2s = N$.*

Proof. An isomorphism $A_K \simeq A_{K'}$ induces an isomorphism of abelianizations, so $Aut(K) \simeq Aut(K')$, as finite étale group schemes, and so as Γ-groups. That is, there is an automorphism φ of S_N with $\varphi(\rho(\gamma)x\rho(\gamma)^{-1}) = \rho'(\gamma)\varphi(x)\rho'(\gamma)^{-1}$. For $N \neq 6$, φ is inner, given by some $\tau \in S_N$, and then $\rho'(\gamma)^{-1}\tau\rho(\gamma)\tau^{-1}$ is central in S_N, and so trivial, for $N \geq 3$. Thus $\rho' = \tau\rho\tau^{-1}$, and the finite étale algebras, which correspond to the Γ-sets, are isomorphic. Over $\mathbb{R}$ the étale algebras are the products $\mathbb{R}^r \times \mathbb{C}^s$, and there are $[N/2] + 1$ of them. □

For $N=1,2,3$ we have $S_N^+=S_N$, and for $N=2$ all the quadratic étale algebras give the same Hopf algebra $\mathcal{O}(\mathbb{Z}_2)$, so the assumption $N\geq 3$ is needed. At $N=6$ the outer automorphism of S_6 might identify the F-forms coming from twin sextic algebras, and we do not know what happens. For instance over $\mathbb{R}$ the algebras $\mathbb{R}^4\times\mathbb{C}$ and $\mathbb{C}^3$ correspond to a transposition and to a product of 3 disjoint transpositions, which are exchanged by the outer automorphism, so their abelianizations are isomorphic, and the above proof does not apply. The question of the real forms of S_N^+ is of interest in connection with the noncompact quantum groups, the F-forms A_K with $s\geq 1$ being natural candidates for having noncompact involutions.

Let us discuss now the quantum group $G_3\subset S_9^+$ from [8]. Consider the 9 points of $\mathbb{F}_3^2$, and the oriented area tensor, with $\omega=e^{2\pi i/3}$:

$$b(\delta_a\otimes\delta_c)=\frac{1}{9}\sum_r\omega^{-\det(a-r,c-r)}\delta_r$$

Then G_3 is the quantum subgroup of S_9^+ making b colinear, which is a twist of PU_3, in the spirit of the twisting deformations of finite groups studied by Galindo and Natale [33], and is infinite, with classical version $\mathbb{F}_3^2\rtimes SL_2(3)$, of order 216, see [8]. Since b has coefficients in $\mathbb{Q}(\omega)$, G_3 is defined over $\mathbb{Q}(\omega)$. Consider the involution $s(x,y)=(x,-y)$ of $\mathbb{F}_3^2$, which reverses the orientation, $\det(sa,sc)=-\det(a,c)$. We have:

Proposition 5.5. *The semilinear map $\tau=\alpha_s c$ on $\mathcal{O}(S_9^+)_{\mathbb{Q}(\omega)}$, where c is the complex conjugation of the coefficients, and $\alpha_s(u_{ij})=u_{s(i)s(j)}$, preserves the Hopf ideal defining G_3. Thus G_3, which is defined over $\mathbb{Q}(\omega)$, descends to a $\mathbb{Q}$-form $G_3^{\mathbb{Q}}$, which is a quantum subgroup of S_K^+, with $K=\mathbb{Q}^3\times\mathbb{Q}(\omega)^3$.*

Proof. The complex conjugation transforms the relation for b into the relation for $\bar{b}$, and α_s transports it into the relation for $s\cdot\bar{b}$, where

$$(s\cdot\bar{b})(\delta_a\otimes\delta_c)=\frac{1}{9}\sum_r\omega^{\det(sa-sr,sc-sr)}\delta_r=\frac{1}{9}\sum_r\omega^{-\det(a-r,c-r)}\delta_r=b(\delta_a\otimes\delta_c)$$

after the substitution $r\to sr$. Thus τ, which is a semilinear Hopf algebra automorphism with $\tau^2=id$, preserves the ideal, and Galois descent for $Gal(\mathbb{Q}(\omega)/\mathbb{Q})=\mathbb{Z}_2$ gives the $\mathbb{Q}$-form. The fixed points of τ on $\mathcal{O}(S_9^+)_{\mathbb{Q}(\omega)}$ form A_K, where K is the fixed point algebra of $f\to\overline{f\circ s}$ on $\mathbb{Q}(\omega)^9$. Now s fixes the 3 points with $y=0$, giving 3 copies of $\mathbb{Q}$, and exchanges the 6 others in pairs, giving 3 copies of $\mathbb{Q}(\omega)$. □

The area tensor itself descends, because it commutes with τ, and so becomes a $\mathbb{Q}$-bilinear map $b_0:K\otimes K\to K$. In the Fourier basis $\psi_g(r)=\omega^{\det(g,r)}$ we have $b(\psi_g\otimes\psi_h)=\omega^{\det(g,h)}\psi_{g+h}$, so b is the product of a twisted group algebra of $\mathbb{Z}_3^2$, which is a copy of $M_3(\mathbb{Q}(\omega))$, and (K,b_0) is a central simple algebra of degree 3 over $\mathbb{Q}$, split by $\mathbb{Q}(\omega)$, and therefore split, because its index divides both 2 and 3. Alternatively, $(\psi_0+\psi_{(1,0)}+\psi_{(2,0)})/3$ is a nontrivial idempotent in it. The program `galois.py` checks all this. Summarizing, we have the following result, which includes Theorem D:

Theorem 5.6. *The quantum permutation group S_N^+ has F-forms A_K, indexed by the finite étale F-algebras K of dimension N, which are pairwise nonisomorphic for $N\geq 3$, $N\neq 6$. Also, $G_3\subset S_9^+$ has a $\mathbb{Q}$-form, which is the quantum subgroup of S_K^+ with $K=\mathbb{Q}^3\times\mathbb{Q}(\omega)^3$ making colinear, in addition to the multiplication of K, a second product b_0 on K, with $(K,b_0)\simeq M_3(\mathbb{Q})$. The rational points of its classical version form a group of order 6, isomorphic to S_3.*

Proof. The first assertions follow from Propositions 5.2, 5.4, 5.5 and the above discussion. As for the last one, the Galois action on the classical version $\mathbb{F}_3^2\rtimes SL_2(3)$ is by conjugation with

s, so the rational points are the affine maps $x \to Mx + v$ commuting with s. This forces $M = diag(a, a^{-1})$ with $a = \pm 1$, and $v = (v_1, 0)$, and we obtain a group of order 6, which is $\mathbb{Z}_3 \rtimes \mathbb{Z}_2 = S_3$. The program `galois.py` finds these 6 elements among the 216. □

Thus, the 9 points of the color sector, which in [8] appear as the 9 inflection points of a plane cubic, carry over $\mathbb{Q}$ 2 algebra structures, a commutative étale one, $\mathbb{Q}^3 \times \mathbb{Q}(\omega)^3$, and a matrix one, $M_3(\mathbb{Q})$, and the rational form of G_3 is the quantum symmetry group of this pair. This is quite reminiscent of the finite geometry of the Standard Model, where the algebras $\mathbb{C}$, $\mathbb{H}$ and $M_3(\mathbb{C})$ are considered over $\mathbb{R}$.

6. Laws over arbitrary fields

We discuss now probability over our field F, of characteristic 0. Since the moments of the laws of the main characters in Theorem A are integers, these laws make sense over any field, and the question is what can be done with them. We use the following simple notion:

Definition 6.1. *A law over F is a linear form $\mu : F[x] \to F$ with $\mu(1) = 1$. Its moments are $m_n = \mu(x^n)$, its classical cumulants κ_n are defined by $m_n = \sum_{\pi \in P(n)} \kappa_\pi$, and its free cumulants κ_n^+ by $m_n = \sum_{\pi \in NC(n)} \kappa_\pi^+$, where $\kappa_\pi = \prod_{b \in \pi} \kappa_{|b|}$.*

The point is that these definitions involve no analysis, and that the inversions are defined over $\mathbb{Z}$. Indeed, by Möbius inversion we have $\kappa_n = \sum_\pi \mu_P(\pi, 1_n) m_\pi$, where $\mu_P(\pi, 1_n) = (-1)^{|\pi|-1}(|\pi| - 1)!$, and similarly in the free case, with $\mu_{NC}(\pi, 1_n)$ being a product of signed Catalan numbers, via the Kreweras complement [36, 42]. Thus:

Proposition 6.2. *The moments, cumulants and free cumulants of a law are polynomials with integer coefficients in each other. In particular, for any $s \in F$ we have well-defined convolution powers μ^{*s} and $\mu^{\boxplus s}$, with cumulants $s\kappa_n$ and $s\kappa_n^+$, and well-defined convolutions $\mu * \nu$ and $\mu \boxplus \nu$.*

Proof. This follows from the above discussion. Over $\mathbb{R}$, and for compactly supported probability measures, these operations are the usual ones whenever the corresponding probability measures exist, because the moments determine the measures, and the cumulants linearize the classical and free convolutions, see [42]. Observe however that the convolution powers are in general just formal, and do not come from probability measures, even over $\mathbb{R}$. For instance with $s = -1$, and μ centered of variance 1, the law μ^{*s} has second moment -1. □

The free multiplicative convolution can be treated in the same way, the formulae involving again the Kreweras complement, with integer coefficients. For the convolution powers with respect to $\boxplus$, and their remarkable interplay with the Boolean ones, see Belinschi and Nica [12, 13]. For the various other algebraic approaches to free cumulants, see [29, 30, 32, 40], and for finite free probability, see [6, 39]. The basic examples are the Poisson laws p_t, with $\kappa_n = t$, the free Poisson laws π_t, with $\kappa_n^+ = t$, the Gaussian law g_t, with $\kappa_2 = t$ and $\kappa_n = 0$ otherwise, and the semicircle law γ_t, with $\kappa_2^+ = t$ and $\kappa_n^+ = 0$ otherwise. Their moments are as follows:

$$m_n(p_t) = \sum_{\pi \in P(n)} t^{|\pi|} \quad , \quad m_n(\pi_t) = \sum_{\pi \in NC(n)} t^{|\pi|} \quad , \quad m_n(g_1) = |P_2(n)| \quad , \quad m_n(\gamma_1) = |NC_2(n)|$$

In connection with the easy quantum groups, we have the following result:

Proposition 6.3. *Over any field F of characteristic 0, the law of the main character is the semicircle law γ_1 for O_N^+ with $N \geq 2$, and the free Poisson law π_1 for S_N^+ with $N \geq 4$. For S_N it is the law of the number of fixed points, $\mu_N = \sum_j c_j \delta_j$, with $c_N = 1/N!$ and $c_{N-1} = 0$.*

Proof. By Theorem 2.3, $h_F(\chi^k) = rank(G_{kN})$, and for O_N^+ with $N \geq 2$, and for S_N^+ with $N \geq 4$, the Gram matrices are invertible, their determinants vanishing only at numbers of the form $2\cos(j\pi/m)$, respectively 0 and $4\cos^2(j\pi/m)$, which are < 2, respectively < 4, so we obtain $|NC_2(k)|$ and $|NC(k)|$. For S_N, the Haar functional is the average over the group, and $\chi(\sigma)$ is the number of fixed points of σ. □

Let us discuss now the finite dimensionality. A law μ has finite Hankel rank r when the matrix $(m_{i+j})_{i,j\geq 0}$ has rank r. By the classical theorem of Kronecker, this happens precisely when the annihilating ideal $I_\mu = \{f \in F[x] | \mu(fg) = 0, \forall g\}$ is nonzero. In this case $I_\mu = (P)$, with P monic of degree r, and μ is a linear combination, with coefficients in $\bar{F}$, of the functionals $f \to f^{(j)}(a)$, with a a root of P, and j smaller than its multiplicity. Thus μ is finitely atomic over $\bar{F}$, $\mu = \sum_a c_a\delta_a$, precisely when P has simple roots, and when these roots are in F, the weights c_a are in F too, being solutions of a Vandermonde system. See [23] for the analytic, real and complex, versions of this, with flat data. We have:

Proposition 6.4. *If $\mathcal{O}(G)_F$ is finite dimensional and cosemisimple, so that its Haar functional h exists, normalized by $h(1) = 1$, the law of any element $a \in \mathcal{O}(G)_F$ with respect to h has finite Hankel rank. For S_N^+ with $N \geq 4$ the law of χ has infinite Hankel rank, because the Hankel determinants of the Catalan numbers are all equal to 1, while for S_N the law of χ has Hankel rank N, with atoms $0, 1, \ldots, N-2, N$.*

Proof. In the finite dimensional case a satisfies a polynomial relation $P(a) = 0$, and so $\mu(x^kP) = h(a^kP(a)) = 0$ for any k. Observe that the cosemisimplicity assumption is needed, in order to have a law, as shown by the 4-dimensional Hopf algebra of Sweedler [46], over $\mathbb{Q}$, whose integrals vanish on 1, so that no normalized Haar functional exists. The Hankel determinants of the Catalan numbers are well-known to be 1, see [1], and the program `gram.py` checks this, along with the assertions about S_N. □

This gives a purely algebraic proof, over any F, of the fact that $\mathcal{O}(S_N^+)_F$ is infinite dimensional for $N \geq 4$. Let us discuss now limits. Assume that F is complete with respect to an absolute value, archimedean or not. We say that a sequence of laws μ_ε converges to μ when the moments converge. The Bernoulli law $\beta_s = (1-s)\delta_0 + s\delta_1$ has all moments of order ≥ 1 equal to s, and so its cumulants of both types are of the form $\kappa_n(\beta_s) = s + s^2R_n(s)$, with $R_n \in \mathbb{Z}[s]$. With these observations in hand, we have the following result:

Theorem 6.5. *Assume that F is complete with respect to an absolute value, and let $t \in F$, and $\varepsilon, \delta \in F^*$, going to 0.*

1. *We have $\beta_{t\varepsilon}^{*1/\varepsilon} \to p_t$ and $\beta_{t\varepsilon}^{\boxplus 1/\varepsilon} \to \pi_t$.*
2. *If μ has $m_1 = 0$, $m_2 = 1$, and D_δ is the dilation, $m_n \to \delta^n m_n$, then $D_\delta(\mu)^{*1/\delta^2} \to g_1$ and $D_\delta(\mu)^{\boxplus 1/\delta^2} \to \gamma_1$.*
3. *In the nonarchimedean case, with $|t\varepsilon| \leq 1$, the cumulants in (1) satisfy the uniform estimate $|\kappa_n - t| \leq |t|^2|\varepsilon|$.*

Proof. (1) The cumulants of $\beta_{t\varepsilon}^{*1/\varepsilon}$ are $\kappa_n(\beta_{t\varepsilon})/\varepsilon = t + t^2\varepsilon R_n(t\varepsilon) \to t$, and similarly in the free case, and the moments are polynomials in the cumulants.

(2) The cumulants are $\delta^{n-2}\kappa_n(\mu)$, which converge to 1 for $n = 2$, and to 0 for $n \geq 3$, the first one being 0.

(3) This follows from the formula in (1), because R_n has integer coefficients, so $|R_n(t\varepsilon)| \leq 1$. □

In the p-adic case we can take $\varepsilon = p^m$ with $m \to \infty$, and the Poisson and central limits hold, in the p-adic sense, with p^{-m} convolution factors. Of course, these convolution powers are not integer ones, and this is where the integer-valued Möbius functions are needed.

7. Analysis over the p-adics

Let p be a prime, v_p the p-adic valuation, and $\mathbf{C}_p$ the completion of the algebraic closure of $\mathbf{Q}_p$. By the theorem of Mahler [38], any continuous function $f : \mathbf{Z}_p \to \mathbf{C}_p$ can be uniquely written as $f(x) = \sum_n a_n \binom{x}{n}$, with $a_n \to 0$, and $||f|| = \max |a_n|$. Thus the bounded measures on $\mathbf{Z}_p$, that is, the continuous linear forms on $C(\mathbf{Z}_p, \mathbf{C}_p)$, correspond to the bounded sequences, via $b_n = \mu\binom{x}{n}$, see [2, 43]. Since the binomial polynomials form a basis of $\mathbf{C}_p[x]$, we can formulate:

Definition 7.1. *A law μ over $\mathbf{C}_p$ is a bounded measure on $\mathbf{Z}_p$ when its binomial moments $b_n = \mu\binom{x}{n}$ are bounded, and its norm is then $||\mu|| = \sup_n |b_n|$.*

The binomial moments are related to the moments by $n!b_n = \sum_k s(n,k)m_k$, with $s(n,k)$ the Stirling numbers of the first kind, and at the level of generating series, with $L(z) = \log(1+z)$, we have the formal identity $\sum_n b_n z^n = \sum_k m_k L(z)^k/k!$, coming from $(1+z)^x = \exp(xL(z))$. This power series is the Amice transform of μ. We have the following necessary condition:

Proposition 7.2. *If μ is a bounded measure on $\mathbf{Z}_p$, with $||\mu|| \leq p^c$, then for any $r \geq 1$ and $n \geq r$ we have $v_p(m_{n+\varphi(p^r)} - m_n) \geq r - c$, where $\varphi(p^r) = (p-1)p^{r-1}$.*

Proof. For $x \in \mathbf{Z}_p$ we have $|x^n(x^{\varphi(p^r)} - 1)| \leq p^{-r}$, because when $p|x$ the factor x^n is divisible by p^r, and when x is a unit $x^{\varphi(p^r)} \equiv 1$ modulo p^r. Thus the continuous function $x^n(x^{\varphi(p^r)} - 1)$ has norm $\leq p^{-r}$, and its integral is bounded by p^{c-r}. □

Let us first discuss the classical laws. For the Poisson law p_t the binomial moments are $b_n = t^n/n!$, and the Amice transform is e^{tz}. We have:

Proposition 7.3. *The Poisson law p_t with $t \in \mathbf{C}_p$ is a bounded measure on $\mathbf{Z}_p$ if and only if $v_p(t) \geq 1/(p-1)$, with the case $t = 0$ included, and in this case $||p_t|| = 1$. For $v_p(t) > 1/(p-1)$ we have the Dobinski formula $p_t = e^{-t}\sum_k t^k \delta_k/k!$, with a convergent series.*

Proof. By Legendre's formula $v_p(n!) = (n - s_p(n))/(p-1)$, with s_p the sum of digits, we have $v_p(t^n/n!) = n(v_p(t) - 1/(p-1)) + s_p(n)/(p-1)$, which is bounded from below if and only if $v_p(t) \geq 1/(p-1)$, and is then ≥ 0, with $b_0 = 1$. In the strict case, e^{-t} converges, and the series converges in norm, because $||\delta_k|| = 1$ and $|t^k/k!| \to 0$, and the moments match, by Dobinski's formula, see [24] for its history. □

For instance, at $p = 2$ and $t = 2$ we have a bounded measure, of norm 1, but the Dobinski series diverges, because e^{-2} does not converge in $\mathbf{Q}_2$. The program `padic.py` checks the formula $b_n = t^n/n!$, and the boundedness, for $p = 2, 3, 5$. Regarding now the Gaussian laws, the situation is different. Their unboundedness was investigated by Khrennikov and Endo [34], with variance $b \in \mathbf{Q}_p^*$, by using the same transform, and their main result covers the case where p is odd, and the case $p = 2$ with $v_2(b/2)$ even. The following short proof, based on a differential equation, covers all variances σ^2 with $\sigma \in \mathbf{C}_p^*$, including the case $p = 2$:

Theorem 7.4. *For any $\sigma \in \mathbf{C}_p^*$, the Gaussian law of variance σ^2 is not a bounded measure on $\mathbf{Z}_p$. The same holds for its translates by elements $a \in \mathbf{Z}_p$, and in particular for the law with moments the involution numbers, $m_n = |P_{12}(n)|$.*

Proof. The Amice transform is $A(z) = \exp(\sigma^2 L(z)^2/2)$, as a formal power series, and it satisfies $A' = \sigma^2 L(z)A/(1+z)$. Assume that the coefficients are bounded by M. Then A converges

on the open unit disc of $\mathbf{C}_p$, and the differential equation holds there. If $A(z_0) = 0$, with a zero of order $m \geq 1$, then A'/A would have a pole at z_0, while $\sigma^2 L/(1+z)$ is analytic, so A has no zeros in the open disc. By the theory of the Newton polygon, $|A(z)| = |A(0)| = 1$ for $|z| < 1$. Also, for $|z| \leq \rho < 1$ we have $|A'(z)| \leq \max_n |nb_n|\rho^{n-1} \leq M/\rho$. Thus $|\sigma^2 L(z)| \leq M/\rho$ on the disc of radius ρ, for any $\rho < 1$. But L is unbounded on the open unit disc, because $\max_{|z|=\rho} |L(z)| = \max_n \rho^n/|n| \geq \rho^{p^j} p^j$, which equals p^{j-1} for $\rho = p^{-p^{-j}}$. This is a contradiction. For the translates by $a \in \mathbf{Z}_p$, the result follows from the fact that $x \to x+a$ is a homeomorphism of $\mathbf{Z}_p$. Finally, the involution numbers are the moments of the Gaussian law translated by 1. □

The unboundedness here can be very slow. For instance at $p = 5$, with $\sigma = 25$, the program `padic.py` finds that the binomial moments b_n with $n < 160$ satisfy $|b_n| \leq 5$, the bound being attained for the first time at $n = 150$. Observe also that, for p odd, the involution numbers satisfy $m_{n+p} \equiv m_n$ modulo p, because modulo p we have $m_n \equiv \sum_{2j<p} \binom{n}{2j}(2j-1)!!$, which is a polynomial in n with p-integral coefficients. At $p = 2$ this fails, because $m_0 = 1$ and $m_2 = 2$. The program `padic.py` finds that they are also periodic modulo p^2, with period p^2, for $p = 3, 5, 7$. Let us discuss now the free laws:

Proposition 7.5. *The free Poisson law π_1, which is the law of χ for S_N^+ with $N \geq 4$, and the semicircle law γ_1, which is the law of χ for O_N^+ with $N \geq 2$, are not bounded measures on $\mathbf{Z}_p$, for any prime p.*

Proof. The moments are the Catalan numbers $C_k = \binom{2k}{k}/(k+1)$, and we use Proposition 7.2, along with Kummer's theorem, stating that $v_p\binom{2k}{k}$ is the number of carries when adding $k+k$ in base p. Assume that π_1 is bounded, with $||\pi_1|| \leq p^c$. For p odd, take $m \geq 3$, large enough so that $r = m-1$ satisfies $r > c$, and $k = (p^m-1)/2$, whose digits are all $(p-1)/2$, so that C_k is a unit. The number $k' = k+(p-1)p^{r-1}$ has digits $(p-3)/2$ at position $r-1$ and $(p+1)/2$ at position r, so adding $k'+k'$ produces a carry, while $k'+1$ is a unit, so $p|C_{k'}$. Thus $v_p(C_{k'} - C_k) = 0$, which contradicts Proposition 7.2. For $p = 2$ we take m with $r = m > c$, $k = 2^m - 1$ and $k' = k + 2^{m-1}$, and we have $v_2(C_k) = 0$ and $v_2(C_{k'}) = 1$, because $v_2(C_k) = s_2(k+1) - 1$. For γ_1, observe that the image of a bounded measure on $\mathbf{Z}_p$ by the continuous map $x \to x^2$ is a bounded measure on $\mathbf{Z}_p$, and that the image of γ_1 has moments $m_{2k}(\gamma_1) = C_k$, so it is π_1, which is not bounded. The program `padic.py` checks these valuations. □

By contrast, the laws μ_N for S_N, with $N \geq 1$, are finitely atomic, supported on $\{0, \ldots, N\} \subset \mathbf{Z}_p$, and so are bounded measures on $\mathbf{Z}_p$. However, their norms satisfy $||\mu_N|| \geq |c_N| = |1/N!|$, and go to infinity with N, for any fixed prime p, in agreement with the fact that their moments converge to the Bell numbers, which are the moments of p_1, and p_1 is not bounded, by Proposition 7.3. Thus the analytic behavior over $\mathbf{Q}_p$ is quite different from the one over $\mathbb{R}$, where all these laws are probability measures, the free ones, π_1 and γ_1, as well as the laws μ_N, being compactly supported, while the Poisson and the Gaussian laws have unbounded support.

The Bell numbers nevertheless have remarkable congruences, found by Touchard [47], $B_{n+p} \equiv B_n + B_{n+1}$ modulo p, and extended by Barsky [11] to higher powers, $B_{n+\lambda_p p^{r-1}} \equiv B_n$ modulo p^r, with $\lambda_p = (p^p - 1)/(p-1)$, for p odd. For $p = 2$, the period is 3 modulo 2, and $3 \cdot 2^r$ modulo 2^r, for $r \geq 2$. At $r = 1$, the number $\lambda_p = 1 + p + \ldots + p^{p-1}$ can be understood as follows. Touchard's congruence states that, modulo p, the Bell numbers form a linear recurrent sequence, with characteristic polynomial $x^p - x - 1$, which is irreducible over $\mathbb{F}_p$, by Artin-Schreier theory. Its roots in $\mathbb{F}_{p^p}$ are the elements $\theta + j$ with $j \in \mathbb{F}_p$, and the product of these roots being 1, we have $\theta^{\lambda_p} = \theta^{1+p+\ldots+p^{p-1}} = 1$. Thus the period of B_n modulo p divides λ_p, and this holds for $p = 2$ as well. The program `padic.py` checks these congruences, along with the

classical valuations $v_2((2k-1)!!)=0$, $v_p((2k-1)!!)=(k+s_p(k)-s_p(2k))/(p-1)$ for p odd, and $v_2(C_k)=s_2(k+1)-1$. Regarding the Haar functional itself, we have:

Proposition 7.6. *The Haar functional of an easy quantum group satisfies, on products of k coordinates, when $\det G_{kN}\neq 0$,*

$$h(u_{i_1j_1}\ldots u_{i_kj_k})\in\mathbb{Z}\left[\frac{1}{\det G_{kN}}\right]$$

and so is p-integral when $p\nmid\det G_{kN}$. For S_N^+ with $N\geq 3$ and $k\leq 4$, this sufficient condition reads $p\nmid N(N-1)(N-2)(N^2-3N+1)$.

Proof. This follows from the Weingarten formula, and from Propositions 2.4 and 2.5. In the singular case, $\det G_{kN}=0$, the denominators divide instead $\det(X^tX)$, with X as in the proof of Theorem 2.3. The program `gram.py` checks for instance that at $k=4$ and $N=5,9$ the Weingarten matrix of S_N^+ has entries with $v_{11}=-1$, coming from the factor N^2-3N+1, which is 11 and 55, while for S_N this does not happen. □

Summarizing, we have the following result, which shows that the p-adic analysis separates the classical laws in a way which is quite different from the real case:

Theorem 7.7. *Over $\mathbf{C}_p$, the following hold:*

1. *The Poisson law p_t is a bounded measure on $\mathbf{Z}_p$ if and only if $v_p(t)\geq 1/(p-1)$.*
2. *The Gaussian laws of nonzero variance, and their translates by $a\in\mathbf{Z}_p$, are never bounded measures on $\mathbf{Z}_p$.*
3. *The laws of the main characters of S_N^+ with $N\geq 4$, and of O_N^+ with $N\geq 2$, are not bounded measures on $\mathbf{Z}_p$.*
4. *The laws of the main characters of S_N are bounded measures, with norms going to ∞ with N, for each fixed p.*

Proof. This follows from Propositions 7.3, 7.5, Theorem 7.4, and the above discussion. □

8. Questions and perspectives

We have seen that the easy quantum groups are absolute objects, defined over $\mathbb{Q}$, and that the dependence on the field comes from the forms, and from the analysis. There are many questions left. The first one concerns the representation theory over $\mathbb{Q}$:

Question 8.1. Is the algebra $End(u^{\otimes k})=span_{\mathbb{Q}}(T_\pi|\pi\in D(k,k))$ split semisimple over $\mathbb{Q}$, for any category of partitions D, so that all irreducible corepresentations of the easy quantum groups are defined over $\mathbb{Q}$? Is there a direct algebraic proof of Theorem 2.3 (2), via a Tannakian duality over $\mathbb{Q}$?

For S_N and O_N, and for O_N^+, where the Jones-Wenzl projections have rational coefficients, the answer is positive. In characteristic p, the maps T_π still make sense, but the Gram determinants can vanish, and the representation theory becomes modular:

Question 8.2. What are the easy quantum groups over $\mathbb{F}_p$, or over $\mathbb{Z}$? Are the intertwiner spaces still spanned by the maps T_π, and how does the representation theory relate to the factorizations of the Gram determinants, in the spirit of the modular theory of the Temperley-Lieb algebras?

Regarding the F-forms, the non-split ones are given by abstract Galois descent, and it would be interesting to have presentations for them:

Question 8.3. Given a central simple algebra Z with orthogonal involution, is there a natural presentation of the corresponding form of O_N^+, for instance as a universal coaction on Z? Over $\mathbb{R}$, what is the free analogue of $SO^*(N)$ obtained in this way, as a Hopf $*$-algebra?

Similarly, for the quantum permutation groups, we do not know all the forms, because we do not know the automorphisms of $\mathcal{O}(S_N^+)$, which might be bigger than S_N, the space $Hom(u^{\otimes 2}, u)$ being 5-dimensional for $N \geq 3$:

Question 8.4. What is $Aut(\mathcal{O}(S_N^+)_{\bar{F}})$? Are all F-forms of S_N^+ of type A_K? What happens at $N = 6$, for the twin sextic algebras? Which F-forms of S_N^+ admit involutions as in Proposition 1.6, making them noncompact quantum groups?

Regarding the free quadrics, we have only discussed the case of 2 variables, and the case of 3 variables, that of the free quadric surfaces, is open over $\mathbb{R}$ too, see [31]. In higher degree, the quantum symmetry groups of the free hypersurfaces are related to the quantum groups of the preregular multilinear forms of Bichon and Dubois-Violette [19]. Over $\mathbb{Q}$ and $\mathbf{Q}_p$ the classification of the binary forms up to similarity is well understood, but the points of the free conics, in the sense of the matricial representations, are not:

Question 8.5. What are the matricial points of the free conics over $\mathbf{Q}_p$, and over the number fields? Is there a local-global principle for the existence of such points, of a given size?

On the analytic side, Theorem 7.4 shows that the Gaussian laws are never bounded on $\mathbf{Z}_p$, for every nonzero variance, and Proposition 7.5 shows that the same holds for γ_1 and π_1. We would like to know if this persists after dilation, for the free laws, the growth of the binomial moments computed by `padic.py` being quite slow:

Question 8.6. Is any dilation of γ_1 or π_1 a bounded measure on $\mathbf{Z}_p$? More generally, is there a p-adic free probability theory, with a notion of free independence for bounded p-adic measures, in the spirit of the work of Van Peski on p-adic random matrices [49]?

The Bell numbers are not the moments of a bounded measure on $\mathbf{Z}_p$, but their period modulo p divides the order of a root of $x^p - x - 1$ in $\mathbb{F}_{p^p}$. This suggests the following question, where the integers of an unramified extension are compact, and support measures with moment congruences of period dividing $(p^p - 1)p^{r-1}$:

Question 8.7. Is the Poisson law p_1 a bounded measure on the ring of integers of the unramified extension of degree p of $\mathbf{Q}_p$? What are the analogues of the Barsky congruences for the Catalan and Fuss-Catalan numbers, and for the moments of the other easy quantum groups?

Finally, let us mention that the Galois action, and more specifically the motivic and cosmic Galois groups of Connes and Marcolli [22], are an important ingredient of the modern approach to quantum field theory, and it is natural to ask whether the Galois forms found here, and notably the rational form of the color quantum group G_3, have a role to play in connection with the Standard Model program from [8].

References

[1] M. Aigner, Catalan-like numbers and determinants, *J. Combin. Theory Ser. A* **87** (1999), 33–51.
[2] Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964), 117–180.
[3] N. Andruskiewitsch, About finite dimensional Hopf algebras, *Contemp. Math.* **294** (2002), 1–57.
[4] N. Andruskiewitsch and J. Bichon, Examples of inner linear Hopf algebras, *Rev. Un. Mat. Argentina* **51** (2010), 7–18.
[5] N. Andruskiewitsch and H.J. Schneider, On the classification of finite-dimensional pointed Hopf algebras, *Ann. of Math.* **171** (2010), 375–417.
[6] O. Arizmendi and D. Perales, Cumulants for finite free convolution, *J. Combin. Theory Ser. A* **155** (2018), 244–266.
[7] T. Banica, Basic quantum algebra (2025), arXiv:2507.11459.
[8] T. Banica and C. Opus, Quantum permutations and the Standard Model algebra (2026), hexagon:2611.00722.

[9] T. Banica and S. Curran, Decomposition results for Gram matrix determinants, *J. Math. Phys.* **51** (2010), 113503.
[10] T. Banica and R. Speicher, Liberation of orthogonal Lie groups, *Adv. Math.* **222** (2009), 1461–1501.
[11] D. Barsky, Analyse p-adique et suites classiques de nombres, *Sém. Lothar. Combin.* **5** (1981), B05b.
[12] S.T. Belinschi and A. Nica, η-series and a Boolean Bercovici-Pata bijection for bounded k-tuples, *Adv. Math.* **217** (2008), 1–41.
[13] S.T. Belinschi and A. Nica, On a remarkable semigroup of homomorphisms with respect to free multiplicative convolution, *Indiana Univ. Math. J.* **57** (2008), 1679–1713.
[14] J. Bichon, The representation category of the quantum group of a non-degenerate bilinear form, *Comm. Algebra* **31** (2003), 4831–4851.
[15] J. Bichon, Corepresentation theory of universal cosovereign Hopf algebras, *J. Lond. Math. Soc.* **75** (2007), 83–98.
[16] J. Bichon, Algebraic quantum permutation groups, *Asian-Eur. J. Math.* **1** (2008), 1–13.
[17] J. Bichon, Hopf-Galois objects and cogroupoids, *Rev. Un. Mat. Argentina* **55** (2014), 11–69.
[18] J. Bichon, A. De Rijdt and S. Vaes, Ergodic coactions with large multiplicity and monoidal equivalence of quantum groups, *Comm. Math. Phys.* **262** (2006), 703–728.
[19] J. Bichon and M. Dubois-Violette, The quantum group of a preregular multilinear form, *Lett. Math. Phys.* **103** (2013), 455–468.
[20] J. Bichon and S. Natale, Hopf algebra deformations of binary polyhedral groups, *Transform. Groups* **16** (2011), 339–374.
[21] B. Collins and S. Matsumoto, On some properties of orthogonal Weingarten functions, *J. Math. Phys.* **50** (2009), 113516.
[22] A. Connes and M. Marcolli, Noncommutative geometry, quantum fields and motives, AMS (2008).
[23] R.E. Curto and L.A. Fialkow, Solution of the truncated complex moment problem for flat data, *Mem. Amer. Math. Soc.* **119** (1996).
[24] A. Dayan, J.L. Fernández and M.J. González, Hausdorff measures, dyadic approximations, and the Dobinski set, *Illinois J. Math.* **65** (2021), 515–531.
[25] P. Deligne, La catégorie des représentations du groupe symétrique S_t, lorsque t n'est pas un entier naturel, in "Algebraic groups and homogeneous spaces", Tata Inst. (2007), 209–273.
[26] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.
[27] M.S. Dijkhuizen and T.H. Koornwinder, CQG algebras: a direct algebraic approach to compact quantum groups, *Lett. Math. Phys.* **32** (1994), 315–330.
[28] M. Dubois-Violette and G. Launer, The quantum group of a non-degenerate bilinear form, *Phys. Lett. B* **245** (1990), 175–177.
[29] K. Dykema, Multilinear function series and transforms in free probability theory, *Adv. Math.* **208** (2007), 351–407.
[30] K. Ebrahimi-Fard and F. Patras, Cumulants, free cumulants and half-shuffles, *Proc. R. Soc. A* **471** (2015), 20140843.
[31] C. Fable and T. Banica, Noncommutative curves and surfaces in small degree (2026), hexagon:2611.00818.
[32] R. Friedrich and J. McKay, Formal groups, Witt vectors and free probability, arXiv:1204.6522.
[33] C. Galindo and S. Natale, Normal Hopf subalgebras in cocycle deformations of finite groups, *Manuscripta Math.* **125** (2008), 501–504.
[34] A.Yu. Khrennikov and M. Endo, Unboundedness of a p-adic Gaussian distribution, *Russian Acad. Sci. Izv. Math.* **41** (1993), 367–375.
[35] M.A. Knus, A. Merkurjev, M. Rost and J.P. Tignol, The book of involutions, AMS (1998).
[36] G. Kreweras, Sur les partitions non croisées d'un cycle, *Discrete Math.* **1** (1972), 333–350.
[37] B. Lindström, Determinants on semilattices, *Proc. Amer. Math. Soc.* **20** (1969), 207–208.
[38] K. Mahler, An interpolation series for continuous functions of a p-adic variable, *J. Reine Angew. Math.* **199** (1958), 23–34.
[39] A.W. Marcus, D.A. Spielman and N. Srivastava, Finite free convolutions of polynomials, *Probab. Theory Related Fields* **182** (2022), 807–848.
[40] M. Mastnak and A. Nica, Hopf algebras and the logarithm of the S-transform in free probability, *Trans. Amer. Math. Soc.* **362** (2010), 3705–3743.
[41] S. Natale, Semisolvability of semisimple Hopf algebras of low dimension, *Mem. Amer. Math. Soc.* **186** (2007), no. 874.
[42] A. Nica and R. Speicher, Lectures on the combinatorics of free probability, Cambridge Univ. Press (2006).
[43] A.M. Robert, A course in p-adic analysis, Springer (2000).

[44] J.P. Serre, Galois cohomology, Springer (1997).
[45] J.P. Serre, A course in arithmetic, Springer (1973).
[46] M.E. Sweedler, Hopf algebras, Benjamin (1969).
[47] J. Touchard, Propriétés arithmétiques de certains nombres récurrents, *Ann. Soc. Sci. Bruxelles A* **53** (1933), 21–31.
[48] A. Van Daele and S. Wang, Universal quantum groups, *Internat. J. Math.* **7** (1996), 255–263.
[49] R. Van Peski, Limits and fluctuations of p-adic random matrix products, *Selecta Math.* **27** (2021), 98.
[50] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).
[51] S. Wang, Quantum symmetry groups of finite spaces, *Comm. Math. Phys.* **195** (1998), 195–211.
[52] W.C. Waterhouse, Introduction to affine group schemes, Springer (1979).
[53] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.
[54] S.L. Woronowicz, Tannaka-Krein duality for compact matrix pseudogroups. Twisted SU(N) groups, *Invent. Math.* **93** (1988), 35–76.