

FSZ-groups and Frobenius–Schur indicators of quantum doubles

M. IOVANOV, G. MASON AND S. MONTGOMERY

We study the higher Frobenius–Schur indicators of the representations of the Drinfel’d double of a finite group G , in particular the question as to when all the indicators are integers. This turns out to be an interesting group-theoretic question. We show that many groups have this property, such as alternating and symmetric groups, $PSL_2(q)$, M_{11} , M_{12} and regular nilpotent groups. However, we show there is an irregular nilpotent group of order 5^6 with non-integer indicators.

1. Introduction

In the representation theory of finite groups, Frobenius–Schur indicators and their higher analogs are an important set of invariants. For Hopf algebras, the second indicator was generalized in [LM], and higher indicators in [KSZ]. They were then extended to quasi-Hopf algebras [MN05] and tensor categories [NS07, NS11]. An important property is that they are gauge invariants, that is, invariants of the tensor category of representations. They proved to have many interesting applications; for example, in [KSZ] it is proved that for H a semi-simple Hopf algebra over \mathbb{C} , the exponent of H and the dimension of H have the same prime factors, answering a question of [EG]. They can also be used to distinguish between the tensor categories having the same Grothendieck ring, such as the 8 types of non-isomorphic semi-simple quasi-Hopf algebras (tensor categories) of dimension 8 over \mathbb{C} . Thus knowing the possible values of the indicators is an interesting problem. In this paper, we study the case of $H = D(G)$, the Drinfel’d double of a finite group G .

Throughout we work over the complex numbers \mathbb{C} . We refer to [M] for basic facts about Hopf algebras. Let H be a semi-simple Hopf algebra over \mathbb{C}

1991 *Mathematics Subject Classification*. MSC Primary 20D99, 20C99; Secondary 16T05.

and let V be an irreducible representation of H with character χ . As defined in [KSZ], the n th Frobenius–Schur indicator of V is given by

$$\nu_n(V) := \chi(\Lambda^{[n]}),$$

where n is a positive integer, Λ is a normalized integral of H and for any $h \in H$, $h^{[m]}$ is the n th Hopf power of h . That is, $h^{[m]} = (\mu^{n-1} \circ \Delta_{n-1})(h) = \sum_h h_1 h_2 \dots h_m$, where Δ_{n-1} is the $(n-1)$ st iteration of the comultiplication Δ of H and μ is multiplication.

In the classical case of a group algebra, $H = \mathbb{C}G$ for a finite group G , $\nu_n(V) := \chi(|G|^{-1} \sum_{g \in G} g^n)$, and it is known (see (2.6) below) that all higher indicators are integers.

For arbitrary Hopf algebras this is not the case. Let $e = e(H)$ denote the exponent of H : this is the smallest number m such that $h^{[m]} = \varepsilon(h)1$ for all $h \in H$, and always exists if H is semi-simple. Kashina *et al.* [KSZ, Section 3.2] show that $\nu_n(V)$ is an algebraic integer in $\mathbb{Q}(\zeta_e)$, the e th cyclotomic field, and moreover $\nu_n(V) \in \mathbb{Q}(\zeta_{e/\gcd(n,e)}) \cap \mathbb{Q}(\zeta_n)$. They construct an example in which the value is not a rational integer.

In this paper, we are concerned with the Hopf algebra $D(G)$, the Drinfeld double of G . It was an open question whether or not all indicator values for $D(G)$ are integers.

Definition 1.1. For a positive integer n , we say that G is an FSZ_n -group if every n th indicator $\nu_n(V)$ for $D(G)$ is an integer. We say that G is an FSZ -group if it is FSZ_n for all n .

Thus the question amounts to this: is every finite group FSZ_n for all n ? We will show that a variety of finite groups indeed have this property. These include symmetric and alternating groups, 2-dimensional linear groups $PSL_2(q)$, the sporadic simple groups M_{11} and M_{12} , regular CN -groups (the centralizer of each non-identity element is a direct product of regular p -groups in the sense of P. Hall [H]), and groups whose exponent is “not too composite”. In a slightly different direction, we show that *every* G is FSZ_n for $n = 2, 3, 4$ or 6 (in fact Linchenko and Montgomery [LM] show $\nu_2(V) \in \{0, \pm 1\}$), and that if G is not FSZ_n then there is an element $g \in G$ of order 5 or greater than 7 such that $C_G(g)$ is not FSZ_n . These results suggest that the class of FSZ -groups is extensive. Indeed, we have made no attempt to be as general as possible, and there are certainly other classes of finite groups which can be shown to be FSZ using the methods that we develop in the present paper. The most tantalizing open question is whether every finite simple group is FSZ .

Despite the proliferation of *FSZ*-groups, it turns out that there are indeed non-*FSZ*-groups, indeed there are infinitely many of them. Because of the results mentioned in the previous paragraph, a natural first place to look for a non-*FSZ* group would be an irregular 5-group of order 5^6 and exponent 5^2 , and we shall see that indeed there are non-*FSZ*-groups of this type.

The paper is arranged as follows. In Section 2 we give the basic definitions and some results about the indicators of $D(G)$ of a combinatorial and character-theoretic nature. In Section 3, we use these results to give (Theorem 3.1) various characterizations of *FSZ*-groups. We also introduce *FSZ*⁺-groups; these are finite groups satisfying a natural group-theoretic condition that is qualitatively stronger than the *FSZ* condition. *FSZ*⁺-groups have a very convenient inductive property (Theorem 3.8) that we use extensively in Sections 4 and 5 to show that various classes of groups are *FSZ*⁺. Indeed, we know of no group that is *FSZ* but *not* *FSZ*⁺. In Section 6 we show that all symmetric and alternating groups are *FSZ*. Section 7 is devoted to counterexamples, i.e., the existence of non-*FSZ*-groups, including dedicated computer programs that can run on GAP to test the *FSZ* property.

Etingof’s result, that wreathed products $S_n \wr A$ (A abelian) are *FSZ*, is discussed in Section 6. It has now appeared [E].

2. The sets $G_n(u, g)$

From now on, G will always denote a finite group. Let $I(G)$ denote the *irreducible characters* of G , $R(G)$ the ring of *virtual characters* of G (\mathbb{Z} -linear combinations of irreducible characters), $cf(G)$ the \mathbb{C} -algebra of *class functions* of G , and $\langle \ , \ \rangle_G$ the usual inner product defined on $cf(G)$. We also let \mathbb{C}^G denote the Hopf algebra of functions on G .

Fix a conjugacy class \mathcal{C} of G and an element $u \in \mathcal{C}$. Let $C(u)$ be the centralizer of u in G , and let W be an irreducible representation of $C(u)$. Then with a suitable action of \mathbb{C}^G , $V = \mathbb{C}G \otimes_{\mathbb{C}C(u)} W$ is an irreducible representation of $D(G)$; moreover all irreducible representations of $D(G)$ are obtained in this way [KMM].

Let η denote the character of $C(u)$ furnished by W , and $\chi = \chi_\eta$ denote the corresponding $D(G)$ -character of V . Given this data, we use the notation $V = V_{C(u), \eta}$ and $W = W_\eta$.

For $g \in G$, define (as in [KSZ, 7.2])

$$G_n(u, g) = \{a \in G \mid (au^{-1})^n = a^n = g\}$$

with

$$G_n(u) = \bigcup_{g \in G} G_n(u, g) = \{a \in G \mid (au^{-1})^n = a^n\}.$$

For a subgroup $H \subseteq G$ we also set

$$G_n^H(u, g) = \{a \in H \mid (au^{-1})^n = a^n = g\}.$$

It is easy to see that if $a \in G_n(u)$, then $a^n \in C(u)$. Thus $G_n(u, g) = \emptyset$ unless $g \in C(u)$, $G_n(u, g) = G_n^{C(u)}(u, g)$, and

$$G_n(u) = \bigcup_{g \in C(u)} G_n(u, g).$$

Combining the formula for $\nu_n(V)$ given in [KSZ, 7.4] with our remarks about $G_n(u)$, we see

$$(2.1) \quad \nu_n(\chi_\eta) = |C(u)|^{-1} \sum_{g \in C(u)} |G_n(u, g)|\eta(g)$$

$$(2.2) \quad = |C(u)|^{-1} \sum_{a \in G_n(u)} \eta(a^n).$$

The following character-theoretic characterization of the n th indicator will be useful. First we introduce

$$\zeta_n^{C(u)} = \zeta_n : C(u) \rightarrow \mathbb{Z}, \quad g \mapsto |G_n(u, g)|.$$

Note that $\zeta_n \in cf(C(u))$.

Proposition 2.3. *The following hold:*

$$(2.4) \quad \zeta_n = \sum_{\eta \in I(C(u))} \nu_n(\chi_\eta)\eta,$$

$$(2.5) \quad \nu_n(\chi_\eta) = \langle \zeta_n, \eta \rangle_{C(u)}.$$

Proof. Because ζ_n is a class function, there is a decomposition $\zeta_n = \sum_{\eta \in I(C(u))} \alpha_n(\eta)\eta$, for scalars $\alpha_n(\eta)$. Since $\alpha_n(\eta) = \langle \zeta_n, \eta \rangle_{C(u)} = |C(u)|^{-1} \sum_{g \in C(u)} |G_n(u, g)|\eta(g)$, we must have $\alpha_n(\eta) = \nu_n(\chi_\eta)$ by (2.1), whence (2.4) and (2.5) follow. □

It will be worthwhile to make explicit the special case when $u = 1$, corresponding to the original n th indicators $\nu^G(\eta)$ of the irreducible characters

η of G . (Here, η is also an irreducible character for $D(G)$ and coincides with χ_η). In this case we write φ_n^G in place of ζ_n . Then

$$(2.6) \quad \varphi_n^G = \sum_{\eta \in I(G)} \nu_n^G(\eta)\eta,$$

and it is well known that $\varphi_n^G \in R(G)$. Indeed by (2.2), $\nu_n^G(\eta) = \langle 1, \lambda^n(\eta) \rangle_G$, where 1 is the trivial 1-dimensional character and $\lambda^n(\eta)$ is the virtual character given by the n th Adams operator applied to η (see [CR, Section 12.B] for Adams operators).

Lemma 2.7. *There is a bijection of sets*

$$G_n(u, g) \rightarrow G_n(u, g^{-1}), \quad a \mapsto ua^{-1}.$$

Proof. This is straightforward to check. The inverse map is $b \mapsto b^{-1}u$. □

Remark 2.8. The indicators of all representations of $D(G)$ are real.

Indeed, apply complex conjugation to (2.1). Since $\overline{\eta(y)} = \eta(y^{-1})$, we see $\overline{\nu_n(\chi_\eta)} = \nu_n(\chi_\eta) \in \mathbb{R}$. (S-H. Ng has shown that the indicators of the double $D(H)$ for any H are real [N]; our special case is much easier to prove.)

We also give a simpler proof for $D(G)$ of the result of [KSZ, Section 2.3] that $\nu_n(V)$ is an algebraic integer in $\mathbb{Q}(\zeta_{e/\gcd(n,e)})$. It will follow that to determine whether G is an *FSZ*-group, it suffices to consider $\nu_d(V)$ for $d \mid e$.

Lemma 2.9. *Let e be the exponent of G , n a positive integer and $d = \gcd(n, e)$. For any irreducible representation V of $D(G)$, $\nu_d(V)$ and $\nu_n(V)$ are integers in $\mathbb{Q}(\zeta_{e/d})$ and there is $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{e/d})/\mathbb{Q})$ depending only on n such that $\nu_n(V) = \sigma(\nu_d(V))$.*

In particular, to show all indicators of V are rational integers it is enough to show that $\nu_d(V) \in \mathbb{Z}$ for all $d \mid e$.

Proof. We use the formula in equation (2.2) for the indicators of a general irreducible representation of $D(G)$. Let $d = \alpha n + \beta e$; we note that $h^n = (hu^{-1})^n$ implies $h^d = h^{n\alpha + e\beta} = (h^n)^\alpha = (hu^{-1})^{n\alpha} = (hu^{-1})^{n\alpha + e\beta} = (hu^{-1})^d$. Hence $G_n(u) = G_d(u)$. So $\sum_{h \in G_n(u)} \eta(h^n) = \sum_{h \in G_d(u)} \eta((h^d)^a)$, where $n = dq$; moreover, $h^d = (h^n)^\alpha \in C(u)$. Since $(h^d)^{e/d} = 1$, we see that $\eta(h^d)$ is an algebraic integer in $\mathbb{Q}(\zeta_{e/d})$, since it is the trace of a matrix of order e/d . Since $\gcd(e/d, q) = 1$, $\sigma = \{t \mapsto t^q\} \in \text{Gal}(\mathbb{Q}(\zeta_{e/d})/\mathbb{Q})$, and we obviously have $\sigma(\eta(h^d)) = \eta(h^n)$. Therefore, $\sigma(\nu_d(V)) = \nu_n(V)$. □

This lemma was used in [C] and is used in some of our computations in Section 7.

3. Characterizations of FSZ -groups

In this section, we give various characterizations of FSZ -groups. We also introduce the idea of FSZ^+ -groups; these are special kinds of FSZ -groups that are very natural and are better behaved from a group-theoretic perspective (Theorem 3.8). It will turn out that for most of the examples considered in the following sections, it is the stronger FSZ^+ property that we will establish. Indeed, we do not know of a group that is FSZ but *not* FSZ^+ .

We begin with some character-theoretic characterizations. We fix some notation which is standard. Let H be a subgroup of $C(u)$. If η is a character of $C(u)$, then $\text{Res}_H^{C(u)}(\eta)$ is the restriction of η to H ; conversely for λ a character of H , $\text{Ind}_H^{C(u)}(\lambda)$ denotes the induced character from H to $C(u)$. We use ζ_n as in Proposition 2.3. The *rational conjugacy class* of $g \in C(u)$ consists of all $C(u)$ -conjugates of g^m for all integers m coprime to $|C(u)|$.

Theorem 3.1. *Let n be a positive integer. The following are equivalent:*

- (1) $\nu_n(\chi_\eta) \in \mathbb{Z}$ for each $\eta \in I(C(u))$;
- (2) $\zeta_n \in R(C(u))$;
- (3) $\langle \text{Res}_H^{C(u)}\zeta_n, \lambda \rangle \in \mathbb{Q}$ for each cyclic $H \subseteq C(u)$ and $\lambda \in I(H)$; and
- (4) ζ_n is constant on rational conjugacy classes of $C(u)$.

Proof. The equivalence of (1) and (2) is an immediate consequence of (2.4). Moreover, if $\zeta_n \in R(C(u))$ then $\text{Res}_H^{C(u)}\zeta_n \in R(H)$ for any subgroup $H \subseteq C(u)$, and therefore $\langle \text{Res}_H^{C(u)}\zeta_n, \lambda \rangle \in \mathbb{Z}$ for $\lambda \in I(H)$. In particular, (2) \Rightarrow (3).

Let $\eta \in I(C(u))$. By Artin’s theorem, there are cyclic subgroups $H_{i,\eta} \subseteq C(u)$, $\lambda_{i,\eta} \in I(H_{i,\eta})$ and $c_{i,\eta} \in \mathbb{Q}$ such that $\eta = \sum_i c_{i,\eta} \text{Ind}_{H_{i,\eta}}^{C(u)}(\lambda_{i,\eta})$. Using (2.2), we have

$$\begin{aligned} \nu_n(\chi_\eta) &= \langle \zeta_n, \eta \rangle_{C(u)} = \sum_i c_{i,\eta} \langle \zeta_n, \text{Ind}_{H_{i,\eta}}^{C(u)}(\lambda_{i,\eta}) \rangle_{C(u)} \\ &= \sum_i c_{i,\eta} \langle \text{Res}_{H_{i,\eta}}^{C(u)}(\zeta_n), \lambda_{i,\eta} \rangle_{H_{i,\eta}}, \end{aligned}$$

where the third equality uses Frobenius Reciprocity [S, 7.2]. Since $\nu_n(\chi_\eta)$ is an algebraic integer, it follows that a sufficient condition for $\nu_n(\chi_\eta) \in \mathbb{Z}$ is that for each i we have $\langle \text{Res}_{H_{i,\eta}}^{C(u)}(\zeta_n), \lambda_{i,\eta} \rangle_{H_{i,\eta}} \in \mathbb{Q}$. Hence, (3) \Rightarrow (1).

We have seen that ζ_n is a rational-valued class function on $C(u)$. Then it is well-known ([S], Proposition 34 and Theorem 29) that (4) holds if, and only if, ζ_n is a \mathbb{Q} -linear combination of (rational) characters of $C(u)$. This in turn is equivalent to the statement $\nu_n(\chi_\eta) \in \mathbb{Q}$ for $\eta \in I(C(u))$ thanks to (2.4), and because each $\nu_n(\chi_\eta)$ is an algebraic integer, this is equivalent to (1). The theorem is proved. \square

We restate Theorem 3.1(4) more explicitly, as it is fundamental for later results.

Corollary 3.2. *Let n be a positive integer. Then G is an FSZ_n -group if, and only if, for all commuting pairs of elements u, g and all integers m with $\gcd(m, |G|) = 1$, we have*

$$(3.3) \qquad |G_n(u, g)| = |G_n(u, g^m)|.$$

We give two immediate applications of Theorem 3.1.

Lemma 3.4. *Let n be a positive integer, and suppose that $G_n(u)$ is closed with respect to all power maps $a \mapsto a^m$, for $\gcd(m, |G|) = 1$. Then (1)–(4) of Theorem 3.1 hold.*

Proof. Using (2.2), the hypotheses of the Lemma imply that $\nu_n(\eta)$ is invariant under all Galois automorphisms of the cyclotomic field of order $|G|$ for each $\eta \in I(C(u))$. It is therefore rational, and hence integral, as required. Alternatively, the assumptions of the Theorem state that $a^n = (au^{-1})^n$ implies $a^{mn} = (a^m u^{-1})^n$ whenever $(m, |G|) = 1$. Then (3.3) holds because the map $x \mapsto x^m$ is bijective on G whenever $\gcd(m, |G|) = 1$. \square

Lemma 3.5. *Let n be a positive integer, and suppose that the centralizer of every element of G of order not 1, 2, 3, 4 or 6 is FSZ_n . Then G is FSZ_n .*

Proof. We show that (3.3) holds for every pair of commuting elements $u, g \in G$. Suppose first that g has order 1, 2, 3, 4 or 6. Then $g^m = g^{\pm 1}$, and (3.3) follows from Lemma 2.7. Now suppose that the order of g is 5 or at least 7. If $\gcd(m, |G|) = 1$ then $u \in C(g)$ and $G_n(u, g), G_n(u, g^m) \subseteq C(g)$. Therefore, $|G_n(u, g)| = |G_n(u, g^m)|$ by Corollary 3.2 because $C(g)$ is an FSZ_n -group by hypothesis. This proves the lemma. \square

To facilitate further applications of Corollary 3.2, we introduce the idea of FSZ^+ -groups. To this end, notice that the subgroup $C_G(u, g) \subseteq G$ that

commutes with both u and g acts by conjugation on $G_n(u, g^m)$. We can thus consider two properties that qualitatively strengthen (3.3):

(3.6) $G_n(u, g)$ and $G_n(u, g^m)$ are *isomorphic* $C_G(u, g)$ -sets.

(3.7) $G_n(u, g)$ and $G_n(u, g^m)$ afford *isomorphic permutation modules* for $C_G(u, g)$.

Remark. It is well known that (3.7) is a weaker condition than (3.6). That is, for a group H , isomorphic H -sets afford isomorphic permutation modules for H ; but the converse is generally false.

Definition 3.7. G is called an FSZ_n^+ -group if (3.7) holds for all commuting pairs of elements $u, g \in G$ and all integers m with $\gcd(m, |G|) = 1$, and G is called an FSZ^+ -group if it is FSZ_n^+ for all n .

Thus an FSZ_n^+ -group is necessarily an FSZ_n -group, and an FSZ^+ -group is necessarily an FSZ -group.

Theorem 3.8. *Let n be a positive integer. The following are equivalent:*

- (a) G is an FSZ_n^+ -group;
- (b) *The centralizer of every non-identity element in G is an FSZ_n -group.*

Proof. Condition (3.7) means that each $h \in C(u, g)$ leaves invariant (i.e., commutes with) the *same number* of elements in both $G_n(u, g)$ and $G_n(u, g^m)$. Thus, we have

$$\begin{aligned}
 G \text{ is } FSZ_n^+ &\Leftrightarrow |G_n(u, g) \cap C(h)| = |G_n(u, g^m) \cap C(h)| \\
 &\quad (h \in C(u, g), ug = gu) \\
 &\Leftrightarrow |G_n^{C(h)}(u, g)| = |G_n^{C(h)}(u, g^m)| \quad (\langle h, u, g \rangle \text{ abelian}) \\
 &\Leftrightarrow |G_n^{C(h)}(u, g)| = |G_n^{C(h)}(u, g^m)| \quad (u, g \in C(h), ug = gu) \\
 &\Leftrightarrow C(h) \text{ is } FSZ_n \quad (h \in G) \\
 &\Leftrightarrow C(h) \text{ is } FSZ_n \quad (1 \neq h \in G).
 \end{aligned}$$

Here, we applied Corollary 3.2 (with G replaced by $C(h)$) to get the penultimate equivalence, and Lemma 3.5 to get the last equivalence. \square

4. Some classes of *FSZ*-groups

We start by applying Theorem 3.8 to show that various families of groups G are FSZ^+ .

Example 4.1 ($PSL_2(q)$). Abelian groups are obviously *FSZ*, and dihedral groups are too [K]. Because $PSL_2(q)$ ($q \geq 2$ a prime power) has the property that every non-identity element has an abelian or dihedral centralizer, we can conclude that $PSL_2(q)$ is an FSZ^+ -group. ($PSL_2(q)$ simple if $q \geq 4$.)

Example 4.2 (CA -groups). G is a *CA*-group if the centralizer of every non-identity element is *abelian*. By Theorem 3.8, every *CA*-group is FSZ^+ . With more effort, we can give explicit formulas for, and interpretations of, the indicators in this case.

First we remark that if $g \neq 1$, then $G_n(u, g) = \{a \in C(u) \mid a^n = g\}$, and if $G_n(u, g) \neq \phi$, then $u^n = 1$. This holds since if $a \in G_n(u, g)$, then au^{-1} and a commute with g , hence with each other. Thus $a \in C(u)$, $(au^{-1})^n = a^n u^{-n} = a^n$, and $u^n = 1$.

Case 1. $u^n \neq 1$. In this case, the remark shows that $G_n(u, g) = \phi$ if $g \neq 1$. Thus, $\zeta_n(g) = 0$ for $g \neq 1$, and of course we also have $\zeta_n(1) = |G_n(u, 1)|$. Next, $C(u)$ acts by conjugation on $G_n(u, 1)$, and by definition the *permutation character* π of $C(u)$ furnished by $G_n(u, 1)$ satisfies $\pi(g) = |\{x \in G_n(u, 1) \mid gxg^{-1} = x\}|$ for $g \in C(u)$.

We assert that $\zeta_n = \pi$. Certainly $\pi(1) = |G_n(u, 1)|$. Furthermore, if $1 \neq g \in C(u)$ and $x \in G_n(u, 1)$, then x and u both commute with g , hence with each other. But then $(xu^{-1})^n = x^n$ implies that $u^n = 1$, contradiction. So there is no such x , whence $\pi(g) = 0$ for $g \neq 1$. Having shown that $\zeta_n(g) = \pi(g)$ for all $g \in C(u)$, our assertion is proved.

By a standard (and straightforward) result, a character μ of $C(u)$ that vanishes away from the identity element is necessarily a multiple of the *regular representation* $\rho_{C(u)}$ of $C(u)$, and the multiplicity is $\mu(1)/|C(u)|$. Since this applies with $\mu = \zeta_n$, we have $\zeta_n = (\zeta(1)/|C(u)|)\rho_{C(u)}$. But the decomposition of the regular representation into irreducibles is standard, namely $\rho_{C(u)} = \sum_{\eta \in I(C(u))} \eta(1)\eta$. Putting all of this together, we find that

$$\zeta_n = \frac{|G_n(u, 1)|}{|C(u)|} \sum_{\eta \in I(C(u))} \eta(1)\eta.$$

Then comparison with (2.4) shows that

$$\nu_n(\chi_\eta) = \frac{|G_n(u, 1)|\eta(1)}{|C(u)|}.$$

So either the indicators $\nu_n(\chi_\eta)$ are all *positive*, or else $G_n(u, 1) = \phi$ and they are all 0.

Case 2. $u^n = 1$. In this case, $C(u) \subseteq G_n(u)$, but once this is taken into account the arguments of Case 1 carry over. Thus by the previous remark, $\zeta_n(g) = |\{a \in C(u) \mid a^n = g\}|$ when $g \neq 1$. Comparing this with (2.6), we see that ζ_n and $\varphi_n^{C(u)}$ agree away from the identity, so that $\zeta_n - \varphi_n^{C(u)}$ is a multiple of $\rho_{C(u)}$. The multiple in question is

$$(\zeta_n(1) - \varphi_n^{C(u)}(1))/|C(u)| = (|G_n(u, 1)| - |\{a \in C(u) \mid a^n = 1\}|)/|C(u)|,$$

the number of orbits of the conjugation action of $C(u)$ on $G_n(u, 1) \setminus \{a \in C(u) \mid a^n = 1\}$. As before, this leads to

$$\zeta_n - \varphi_n^{C(u)} = \frac{|G_n(u, 1)| - |\{a \in C(u) \mid a^n = 1\}|}{|C(u)|} \sum_{\eta \in I(C(u))} \eta(1)\eta,$$

and

$$\nu_n(\chi_\eta) = \nu_n^C(\eta) + \frac{\eta(1)(|G_n(u, 1)| - |\{a \in C(u) \mid a^n = 1\}|)}{|C(u)|}.$$

Example 4.3 (Regular p -groups). Fix a prime p . For an introduction to *regular* p -groups, see [H, Chapter 12.4]. All we need to know is that in a regular p -group, the equation $a^k = b^k$ holds if, and only if, $(ab^{-1})^k = 1$ for $k \in \mathbb{Z}$ [H, Theorem 12.4.4]. We show that a regular p -group G is FSZ^+ .

If $a \in G$ then $(au^{-1})^n = a^n \Leftrightarrow (au^{-1}a^{-1})^n = 1 \Leftrightarrow u^n = 1$. This shows that either $u^n \neq 1$ and $G_n(u) = \phi$; or $u^n = 1$ and $G_n(u) = G$. Now Lemma 3.4 applies, and shows that G is FSZ . But every subgroup of a regular p -group is also regular (loc. cit.), so Theorem 3.8 now tells us that G is FSZ^+ . We can again make the indicators more explicit. If $G_n(u) = \phi$ then ζ_n vanishes identically and the corresponding indicators $\nu_n(\chi_\eta) = 0$. On

the other hand, if $u^n = 1$ then $G_n(u, g) = \{a \in G \mid a^n = g\}$. Since $\zeta_n(g) = |G_n(u, g)|$, this means that for $g \in C(u)$ the values of ζ_n coincide with those of the generalized character $\varphi_n^G = \sum_{\eta} \nu_n^G(\eta)\eta$ (2.6), i.e.,

$$\zeta_n = \text{Res}_{C(u)}^G \varphi_n^G.$$

We note that all p -groups of order less than p^{p+1} , nilpotence class less than p , or exponent p , are regular [H], and therefore *FSZ*. We will see later that there are groups of order 5^6 and exponent 5^2 which are not *FSZ*.

Example 4.4 (Wreathed products $Z_p \wr Z_p$). This p -group (the regular wreathed product of Z_p with itself), is an irregular p -group of order p^{p+1} . We will show that it is *FSZ*⁺, so that the class of *FSZ* p -groups is strictly larger than the class of regular p -groups.

G has a normal elementary abelian p -subgroup V of order p^p (which we consider as a $GF(p)$ -vector space of dimension p) and a cyclic subgroup $J = \langle j \rangle$ of order p such that j cyclically permutes a basis of V . We identify j with the $p \times p$ Jordan block

$$j = \begin{pmatrix} 0 & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}.$$

Then $G = J \ltimes V$, and multiplication in G is $(j^r, x)(j^s, y) = (j^{r+s}, j^s x + y)$. The subgroup of G generated by p th powers coincides with the center $Z := Z(G)$. $Z \subseteq V$ is 1-dimensional and spanned by the all 1's vector $\mathbf{1}$. The operator $k := 1 + j + \dots + j^{p-1}$ plays a rôle below; k is the all 1s matrix and $kV = Z$.

Because G has exponent p^2 , in proving that G is *FSZ* it suffices to consider only the cases $n = p, p^2$, and of these only $n = p$ is in doubt. Fix some $u^{-1} := (j^d, t) \in G$. By what we have said, $G_p(u, g) = \phi$ unless $g \in Z$. We show that (3.3) holds with $n = p$ and $1 \neq g \in Z$.

An element $a = (j^i, v)$ satisfies $a^p = (1, kv)$ if $j^i \neq 1$, and otherwise $a^p = 1$. Moreover, $au^{-1} = (j^{i+d}, j^d v + t)$. Therefore, $(au^{-1})^p = a^p = g$ if, and only if, the four conditions $i \not\equiv 0 \pmod p$, $i + d \not\equiv 0 \pmod p$, $kv = g$, $k(j^d v + t) = g$ all hold. But $k(j^d v + t) = kv + kt$ (because k is the all 1s matrix and j^d

a permutation matrix). So if the four conditions hold then we must have $kt = 0$. Turned around, if $u^{-1} = (j^d, t)$ and $kt \neq 0$ then $G_p(u, g) = \phi$ for any non-zero $g \in Z$. If, on the other hand, $kt = 0$, then $G_p(u, g) = \{(j^i, v) \mid i \not\equiv 0, -d \pmod{p}, kv = g\}$ has cardinality $(p-1)p^{p-1}$ or $(p-2)p^{p-1}$ depending on whether or not $d \equiv 0 \pmod{p}$. So in all cases, the desired property of $G_p(u, g)$ is established. Note that the hypotheses of Lemma 3.4 do *not* hold in this case, so they are sufficient but not necessary.

Example 4.5 (Direct products). It follows easily from the definition that, in an obvious sense, $|G_n(u, g)|$ is *multiplicative* over direct products of groups. Thus the class of *FSZ* groups is closed under direct products; for example, a nilpotent group, all of whose Sylow subgroups are regular, is *FSZ*. On the other hand, the direct product of two groups, one of which is *FSZ* and one which is not, is itself *not FSZ*. So once we have found a non-*FSZ* group F , say, there are large numbers of non-*FSZ* groups having F as a direct factor.

Example 4.6 (Regular CN-groups). G is a *CN*-group if the centralizer of every non-identity element is nilpotent (i.e., a direct product of p -groups). We call G a *regular CN*-group if the centralizer of every non-identity element is a direct product of regular p -groups. By Theorem 3.8 together with Examples 4.3 and 4.5 above, every regular *CN*-group is *FSZ*.

Example 4.7 (Mathieu group M_{11}). We show that M_{11} is *FSZ* by applying Lemma 3.5. Indeed, it is readily checked [AT] that centralizers of elements of order 5 or greater than 6 are *FSZ*, and the result follows.

5. A sufficiency condition and groups of special orders

We start by showing that (3.6) holds automatically for *some* values of m .

Lemma 5.1. *Suppose that $m \in \mathbb{Z}$ satisfies $\gcd(m, |G|) = 1$ and $m \equiv \pm 1 \pmod{n}$. Then for all pairs of commuting elements $u, g \in G$, there is an isomorphism of $C(u, g)$ -sets*

$$G_n(u, g) \rightarrow G_n(u, g^m), \quad a \mapsto a^m.$$

Proof. Let $a \in G_n(u, g)$, so that $(au^{-1})^n = a^n = g$, and suppose first that $m \equiv 1 \pmod{n}$. Then

$$\begin{aligned} (a^m u^{-1})^n &= (a^{m-1} a u^{-1})^n \\ &= a^{(m-1)n} (a u^{-1})^n \quad (\text{because } a^{m-1} \in \langle a^n \rangle \subseteq C(u)) \\ &= a^{mn}. \end{aligned}$$

This argument shows that the m th power map $\varphi_m : a \mapsto a^m$ induces an injection $G_n(u, g) \rightarrow G_n(u, g^m)$. If m' is the inverse of $m \pmod{n}$, then $\varphi_{m'}$ is the inverse of φ_m , so that φ_m is a bijection. Moreover, because conjugation commutes with power maps, φ_m is also a morphism of $C(u, g)$ -sets.

This completes the proof of the lemma when $m \equiv 1 \pmod{n}$. If $m \equiv -1 \pmod{n}$, the result follows from the case $m \equiv 1 \pmod{n}$ together with Lemma 2.7, because the bijection of Lemma 2.7 is $C(u, g)$ -equivariant. \square

For some groups, Lemma 5.1 tells us all we need to know in order to deduce the FSZ_n^+ property. This is the essential content of

Theorem 5.2. *Suppose that for each element $a \in G$ we have*

$$o(a^n)/o(a^{n^2}) \in \{1, 2, 3, 4, 6\}.$$

Then G is an FSZ_n^+ -group.

Proof. It suffices to show that (3.6) holds for all commuting pairs of elements u, g and integers m coprime to $|G|$. For in this case, the Remark that follows (3.7) shows that G is FSZ_n^+ .

Suppose that $o(g) = t$. If $G_n(u, g^m) = \phi$ for all m there is nothing to prove, so assume that $a \in G_n(u, g^m)$ for some m . Thus $a^n = g^m$ has order t , and $a^{n^2} = g^{mn}$ has order $t/\gcd(t, n)$. Thus $o(a^n)/o(a^{n^2}) = \gcd(t, n)$. As a result, the hypothesis of the Theorem tells us that

$$(5.2) \quad \gcd(t, n) \in \{1, 2, 3, 4, 6\}.$$

Set $d = \gcd(t, n)$. Because m is coprime to t (Cauchy’s theorem) it is also coprime to d . Because of (5.2), it follows that

$$m \equiv \pm 1 \pmod{d}.$$

There are integers a, b such that $at + bn = d$. Then for some integer k we have $m = \pm 1 + kd = \pm 1 + kat + kbn$ and therefore $g^m = g^{\pm 1 + kbn}$. Now by

Lemma 5.1 we see that there is an isomorphism of $C(u, g)$ -sets $G_n(u, g) \rightarrow G_n(u, g^m)$, as required. This completes the proof of the theorem. \square

The theorem has some interesting consequences.

Corollary 5.3. *Suppose that the order of each element of G divides $2^\alpha 3^\beta q$, where q is a squarefree integer coprime to 6 and either $\alpha, \beta \leq 3$ or $\beta \leq 1$ and $\alpha \leq 5$. Then G is FSZ^+ .*

Proof. The hypothesis of the previous theorem hold for all n . \square

Corollary 5.4. *Suppose that $n \in \{1, 2, 3, 4, 6\}$. Then every group G is FSZ_n^+ .*

Proof. We always have $o(a^n)/o(a^{n^2})|n$ for $a \in G$ (see the proof of Theorem 5.2). \square

Corollary 5.5. *All groups of order less than 100 are FSZ^+ .*

Apropos of our introductory comments that some of our stated results are not best-possible, this is certainly true of the preceding Corollary. Because all groups of order $512 = 2^9$ are FSZ (Section 7), one could check all groups up to order $728 = 3^6 - 1$ rather easily. It is very likely that the non-FSZ-groups of *least order* are irregular p -groups of order 2^k ($10 \leq k \leq 13$), 3^k ($6 \leq k \leq 8$), or 5^6 .

Corollary 5.6. *The Mathieu groups M_{11} , M_{12} are FSZ^+ .*

Proof. We have seen before that the Mathieu Group M_{11} is FSZ. Alternatively, the exponent of both M_{11} and M_{12} is $2^3 \cdot 3 \cdot 5 \cdot 11$. Thus we may apply Corollary 5.3 to see that, in fact, both M_{11} and M_{12} are FSZ^+ . \square

6. Symmetric groups

The next theorem was proved independently by the present authors and Pavel Etingof; here we give our proof.

Theorem 6.1. *The symmetric group S_N is an FSZ-group.*

Proof. We have to show that (3.3) holds for all commuting pairs $u, g \in S_N$ and all m coprime to $N!$. There is nothing to prove if $g = 1$, so assume that $1 \neq g$ is a product of e_i cycles of length i . Thus $\sum_i i e_i = N$, and $C(g)$ is

contained in a subgroup of S_N isomorphic to $S_{e_1} \times S_{2e_2} \times \cdots \times S_{Ne_N}$. Using induction on N and the multiplicativity of $G_n(u, g)$ over direct products (Section 4, Example 5), we may, and shall, assume that g is a product of e cycles of length r , with $N = er$. Then $C(g) = S_e \wr Z_r = S \ltimes V$ where $S = S_e$ and $V = Z_r^e$. We use additive notation for V , and write $g = (1, g_0, \dots, g_0)$ with $(g_0, \dots, g_0) \in Z_r^e$ for some *generator* g_0 of Z_r . In effect, V is a right $Z_r S$ -module with S -action denoted exponentially by v^s (which is right conjugation $s^{-1}vs$ in $C(g)$), and multiplication in $C(g)$ is

$$(s, v)(t, w) = (st, v^t + w).$$

Then

$$(s, v)^n = (s^n, v + v^s + \cdots + v^{s^{n-1}}).$$

Let $(s, v) = sv \in C(g)$ ($s \in S, v \in V$), and let $s = s_1 \dots s_q$ be a representation of s as a product of disjoint cycles in S_e . There is a corresponding decomposition of $v = v_1 + \cdots + v_q$ such that for each index i , s_i has length f_i , $v_i \in W_i \cong Z_r^{f_i}$, and $sv = (s_1 v_1) \dots (s_q v_q) \in (S_{f_1} \wr Z_r) \times \cdots \times (S_{f_q} \wr Z_r)$.

Now suppose that $(s, v)^n = g^m = (1, mg) = (1, mg_0, \dots, mg_0)$. Then for each index i we have $(s_i, v_i)^n = (1, mg_0, \dots, mg_0) \in S_{f_i} \wr Z_r$. Then $s_i^n = 1$, whence $f_i | n$; moreover $(mg_0, \dots, mg_0) = v_i + v_i^{s_i} + \cdots + v_i^{s_i^{n-1}} = (n/f_i)(v_i + v_i^{s_i} + \cdots + v_i^{s_i^{f_i-1}})$. We can write this more compactly as

$$(6.1) \quad m(g_0, \dots, g_0) = (n/f_i)N_{s_i}(v_i) \in Z_r^{f_i},$$

where N_{s_i} denotes *norm* with respect to $\langle s_i \rangle$. Note that because the left-hand side of (6.1) has order exactly r (as an element of V), then $\gcd(n/f_i, r) = 1$. Setting $l = \gcd(n, r)$, it follows that the condition $l | f_i$ (for all indices i) is *necessary* in order that there be *any* solutions of the equation $(s, v)^n = g^m$.

It is also sufficient: if $\gcd(n/f_i, r) = 1$, we can always find $v'_i \in W_i := Z_r^{f_i}$ whose norm is $(n/f_i)^{-1}m(g_0, \dots, g_0)$. The element $v''_i = (g_0, 0, \dots, 0, g_0, 0, \dots, 0, \dots, g_0, \dots, 0)$, of length f_i and with g_0 's occurring after $l - 1$ zeros, has norm $(f_i/l)(g_0, \dots, g_0)$, and we take $v'_i = m(n/l)^{-1}(v''_i)^s$. Here inverses are taken modulo r .

The set of *all* $v_i \in W_i$ satisfying (6.1) is

$$v'_i + \ker N_{s_i} = v'_i + [W_i, s_i],$$

where $[W_i, s_i] \subseteq W_i$ is spanned by $w - w^{s_i}, w \in W_i$. Because s_j acts trivially on W_i for $i \neq j$, we have $[W_i, s_i] = [W_i, s]$. It follows that, for fixed $s \in S$ as

above, the set of all $v \in V$ satisfying $(s, v)^n = g^m$ is

$$v'_1 + \dots + v'_q + [V, s].$$

Fix a second element $(t, w) \in C(g)$, so that $(s, v)(t, w) = (st, v^t + w)$. By the foregoing, the set of $x \in V$ such that $(st, x)^n = g^m$ is the coset

$$x'_1 + \dots + x'_p + [V, st],$$

where st is a product of p disjoint cycles of lengths k_1, \dots, k_p and $x'_i = m(n/l)^{-1}(x''_i)^{st}$ with $x''_i = (g_0, 0, \dots, 0, g_0, 0, \dots, 0, g_0, \dots, 0)$ similarly to the previous case. Hence, for fixed $s \in S$ and fixed $(t, w) \in C(g)$, the cardinality of the set of elements $v \in V$ such that $(s, v)^n = ((s, v)(t, w))^n = g^m$ is

$$\begin{aligned} & \left| (x'_1 + \dots + x'_p + [V, st]) \cap (w + (v'_1 + \dots + v'_q + [V, s])^t) \right| \\ &= \left| m(n/l)^{-1} \left\{ \left(\sum_{i=1}^p (x''_i)^{st} + [V, st] \right) \right. \right. \\ & \quad \left. \left. \cap \left(m^{-1}(n/l)w^{t^{-1}} + \sum_{i=1}^q (v''_i)^s + [V, s] \right)^t \right\} \right|. \end{aligned}$$

Now we have gone out of our way to arrange that $\sum_i x''_i = \sum_i v''_i$. Because s and st leave invariant $[V, s]$ and $[V, st]$, respectively, it follows that the cardinality of the last set is

$$\begin{aligned} & \left| \left(\sum_{i=1}^p x''_i + [V, st] \right)^{st} \cap \left(m^{-1}(n/l)w^{(st)^{-1}} + \sum_{i=1}^q v''_i + [V, s] \right)^{st} \right| \\ &= \left| ([V, st]) \cap \left(m^{-1}(n/l)w^{(st)^{-1}} + [V, s] \right) \right| \end{aligned}$$

This equals 0 if $m^{-1}(n/l)w^{(st)^{-1}} \notin [V, st] + [V, s]$, and equals $|[V, st] \cap [V, s]|$ if $m^{-1}(n/l)w^{(st)^{-1}} \in [V, st] + [V, s]$, and in both cases the condition is independent of m coprime to r . This completes the proof of the theorem. \square

The proof of the theorem also yields

Corollary 6.2. *The alternating group A_N is an FSZ-group.*

Proof. Keep the same notation as before, now with $g \in A_N$. Then $C_{A_N}(g) = C_{S_N}(g) \cong S_e \wr Z_r$ if r is even, and $C_{A_N}(g) \cong A_e \wr Z_r$ if r is odd. In either case,

the proof of the theorem carries over *verbatim*, because once s, t, w are fixed the rest of the calculation takes place in $V \subseteq A_N$. \square

Somewhat later Etingof proved [E] a natural extension of Theorem 6.1, namely

Theorem 6.3 (Etingof). *$S_N \wr A$ is an FSZ-group for any finite abelian group A .*

The proof, which we omit, runs along similar lines to that of Theorem 6.1, but is more elaborate. As an application, recall that every centralizer in S_N is a direct product of wreathed products of the type occurring in Theorem 6.3. Then by Theorem 3.8 we deduce

Corollary 6.4. *S_N is an FSZ^+ -group.*

7. Counterexamples

In this section, we consider groups of order $5^6 = 15,625$. We present two GAP programs, one optimized for testing these 5-groups, and the second which is optimized to be used to test the FSZ property any arbitrary group G .

Using Corollary 3.2, the first [GAP] program can be used to test integrality of indicators for doubles of p -groups of exponent p^2 . On a dual core 3.33 Mz computer with 8 Gb of Ram, after approximately 6 h of running for the 555 groups of exponent 25 among the 684 groups of order $15,625 = 5^6$, it found 32 groups whose indicators for the Drinfel’d double are not all integers (only indicator ν_5 can be non-integer, and all the other groups of order 5^6 can easily be seen to be FSZ). These are the groups `SmallGroup(12625,k)` (in the small library) for k being the ID numbers 632–635, 637, 638, 640–650, 653–655, and 657–668. We note that groups 662, 665 and 668 have few conjugacy classes, many of which give rise to representations of the Drinfeld double with non-integer indicators, and also several groups G among these have a large number of conjugacy classes and still produce representations of the double with non-integer indicators.

One particular such group is `SmallGroup(15625,668)`. The GAP program takes parameters G, p, m and is designed to test the integrality of the m -indicators of representations of $D(G)$ induced from cyclic subgroups of prime order p (only). This is enough to test the FSZ property for a p -group

of exponent p^2 . The command

$$\text{FSInd}(\text{SmallGroup}(15625, 668), 5, 5)$$

tests the integrality of indicators ν_5 for representations induced from cyclic groups of order 5 and determines those conjugacy classes (that is, their GAP ID) for which there are associated representations of the double which have non-integral indicators. It runs in a few seconds on the computer hardware configuration mentioned above for group $\text{SmallGroup}(15625, 668)$.

By Lemma 2.9 all indicators are in $\mathbb{Q}(\zeta_5)$, and since they are also real by Remark 2.8, the non-integer indicators are algebraic integers in $\mathbb{Q}(\sqrt{5}) \setminus \mathbb{Q}$. We confirmed this using a GAP program of Rebecca Courter [C], which computes values for the FS-indicators of irreducible representations of the double of $\text{SmallGroup}(15625, 668)$.

```

FSInd:=function(G,m,p)
local GG,list,Gm,slist,gucoef,u,Cl,T,H,nu;

GG:=EnumeratorSorted(G);
elG:=Size(G);
Gm:=[];
list:=[]; slist:=[]; gucoef:=[];
for i in [1..elG] do Gm[i]:=Position(GG,GG[i]^m); od;

for i in [1..elG] do list[i]:=[]; slist[i]:=0; od;
for i in [1..elG] do Add(list[Gm[i]],i); od;

for Cl in ConjugacyClasses(G) do
  u:=Representative(Cl);
  Print("u=",Position(GG,u)," ");
  for i in [1..elG] do gucoef[i]:=0; od;
  for i in [1..elG] do
    for j in list[i] do if Position(GG,GG[j]*u) in list[i]
      then gucoef[i]:=gucoef[i]+1; fi; od;
  od;

H:=1;
Print("INDICATORS:\n");
for i in [1..elG] do T:=1; if Order(GG[i])=p then
  nu:=0;
  for j in [0..Order(GG[i])-1] do
    nu:=nu+ (E(p)^j)*gucoef[Position(GG,GG[i]^j)]; od;

```

```

Print(nu, ", ");
for j in [2..Order(GG[i])-1] do if
gucoef[i]=gucoef[Position(GG,GG[i]^j)] then;
    else T:=0;; H:=0;; fi; od; fi;
#This checks it for rep's induced
from prime order subgroups;

od;
if H=1 then Print("\n OK - Integer");
    else Print("\n !!! N O N - I N T E G E R !!!"); fi;
Print("\n");

od;

return;
end;

```

Our second program provides a general computational test for whether the indicators ν_m of *all* the representations of the double of a group G are integers; it takes the integer m and the group G as parameters. It uses the test provided by Corollary 3.2, and it is optimized to attempt the least possible number of computations of products in G (but uses more memory). This is necessary since products of elements (usually represented as compositions of permutations) tend to take the most time under GAP.

The algorithm runs as follows. The program first creates a list [Gm] with all the m th powers of elements of G (GAP works with list position), and then another variable [list] such that which for each element $x \in G$, list[x] retains all h for which $h^m = x$ (this saves doing computations of the type $\underbrace{h * h * h \cdots * h}$ each time we compute an indicator). Then, we create the list variable [glist], which will retain the sets $\{g^k \mid \gcd(\text{ord}(g), k) = 1\}$ — elements generating the same cyclic subgroup, on which we have to test the condition of Corollary 3.2. Next, for each conjugacy class Cl of G , we pick an element of Cl and we create a list [gucoef] which for each element g of G will count the number of solutions of the equation $h^m = (hu)^m = g$ (obviously, for the purpose of testing integrality of all indicators, we can just work with u instead of u^{-1}). This uses the previously created variable [list] for the m th roots of g (so that we don't need to perform supplementary multiplications). Once this is done, using Corollary 3.2, one only needs to check that the number of these solutions is constant on the sets contained in the variable [list]. The printout also shows the GAP ID of some representative u of each

conjugacy class and whether $Cl(u^{-1})$ produces some representation of $D(G)$ with non-integer indicator ν_m . The program could be slightly optimized to jump out of the loop whenever a non-integer indicator is found, and it can be easily modified to find the indicators for all the representations.

```

FSIndG:=function(G,m)
local GG,list,Gm,gucoef,u,Cl,H,expo,
      glist,aux,listaux,Gaux,g,h,og,gaux;

GG:=EnumeratorSorted(G); expo:=Exponent(G);
elG:=Size(G);
Gm:=[];
list:=[]; gucoef:=[];
for i in [1..elG] do Gm[i]:=Position(GG,GG[i]^m); od;
      #create the list of m-powers of elements
for i in [1..elG] do list[i]:=[]; od;
for i in [1..elG] do Add(list[Gm[i]],i); od;
      #create for each element x the list of its m-"radicals" h
glist:=[]; og:=Size(G); Gaux:=G;
while og>0 do g:=Representative(Gaux); aux:=[];
      if Order(g) * m < expo+1 then
        for j in PrimeResidues(Order(g)) do
          h:=g^j; Add(aux,Position(GG,h)); og:=og-1;
          Gaux:=Difference(Gaux,[h]); od;
          Add(glist,aux);
        else og:=og-1; Gaux:=Difference(Gaux,[g]); fi;
        od;
      #this creates the list "glist" whose members are sets
      #of elements of G generating the same subgroup
for Cl in ConjugacyClasses(G) do
  u:=Representative(Cl);
  Print("u=",Position(GG,u),"; ");
  for i in [1..elG] do gucoef[i]:=0; od;
  for i in [1..elG] do
    for j in list[i] do if Position(GG,GG[j]*u) in list[i]
      then gucoef[i]:=gucoef[i]+1; fi; od;
  od;
  #gucoef[g] counts the number of solutions of h^m=(hu)^m=g

H:=1;
for i in glist do
  #nu:=0;
  for j in i do if gucoef[i[1]]=gucoef[j] then;

```

```

        else H:=0;; fi; od;

        #This uses our results to check integrality by testing
        #that the number of solutions in  $H_m(g)$  of  $h^m=g^k$  and
        # $h^m=g^l$  is the same for  $\gcd(k, \text{ord}(g))=\gcd(l, \text{ord}(g))$ 
        #H retains whether the integer condition is verified

        od;
        if H=1 then Print(" OK - Integers");
            else Print(" !!! N O N - I N T E G E R !!!"); fi;
        Print("\n");
    od;

return;
end;

```

Using this last program, we observed that all the 2-groups up to order 512 are *FSZ*. Since 2-groups can in general behave differently than other p -groups, it is natural to ask whether perhaps all 2-groups are *FSZ*.

It is also known that all the indicators of the representations of the group S_n are *non-negative* integers [Scf]. Thus one might ask whether this is true for $D(S_n)$ as well. This has been shown in [C] for $n \leq 10$. It is also known that for any dihedral group, all indicators of its double are non-negative [K].

Acknowledgments

The first author was supported by an AMS-Simons travel grant and by CNCS grant TE45, no. 88/02.02.2010. The second author was supported by NSF grant DMS-1139676 and the third author by NSF grant DMS-1001547. We thank Siu-Hung Ng and Pavel Etingof for communicating some of their unpublished results to us.

References

- [AT] J.H. Conway et al., *Atlas of finite groups*, Oxford University Press, 1985.
- [C] R. Courter, *Computing higher indicators for the double of a symmetric group*, Ph.D. thesis, USC, 2012, [arXiv:1206.6908](https://arxiv.org/abs/1206.6908).
- [CR] C. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*, 1, Wiley, New York, 1981.

- [E] P. Etingof, *On some properties of quantum doubles of finite groups*, J. Algebra **394** (2013), 1–6.
- [EG] P. Etingof and S. Gelaki. *On the exponent of finite-dimensional Hopf algebras*. Math. Res. Lett. **6** (1999), 131–140.
- [H] M. Hall Jr., *The theory of groups*, Macmillan, New York, 1959.
- [GAP] The GAP Group, *GAP — groups, algorithms, and programming*, Version 4.5.5, 2012, available at: <http://www.gap-system.org>.
- [KMM] Y. Kashina, G. Mason and S. Montgomery, *Computing the Frobenius–Schur indicator for abelian extensions of Hopf algebras*, J. Algebra **251** (2002), 11–24.
- [KSZ] Y. Kashina, Y. Sommerhäuser and Y. Zhu, *On higher Frobenius–Schur indicators*, Mem. Amer. Math. Soc. 181 (2006), no. 855, viii + 65pp.
- [K] M. Keilberg, *Higher indicators for some groups and their doubles*, J Algebra Appl. **11**(2) (2012), 38pp.
- [LM] V. Linchenko and S. Montgomery, *A Frobenius–Schur theorem for Hopf algebras*, Algebr. Represent. Theory **3** (2000), 347–355.
- [MN05] G. Mason and S-H. Ng, *Central invariants and Frobenius–Schur indicators for semisimple quasi-Hopf algebras*, Adv. Math. **190** (2005), 161–195.
- [M] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Conf. Ser. Math., **82**, Amer. Math. Soc., Providence, 1993.
- [N] S-H. Ng, private communication, March 2011.
- [NS07] S-H. Ng and P. Schauenburg, *Frobenius–Schur indicators and exponents of spherical categories*, Adv. Math. **211**(1) (2007), 34–71.
- [NS11] S-H. Ng and P. Schauenburg, *Congruence subgroups and generalized Frobenius–Schur indicators*, Comm. Math. Phys. **300**(1) (2010), 1–46.
- [Scf] T. Scharf, *Die Wurzelanzahlfunktion in symmetrischen Gruppen*, J. Algebra **139** (1991), 446–457.
- [S] J.P. Serre, *Linear representations of finite groups*, GTM 42, Springer-Verlag, New York–Berlin–Heidelberg, 1977.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF IOWA AND UNIVERSITY OF BUCHAREST
IOWA CITY, IA AND BUCHAREST
ROMANIA
E-mail address: miodrag-iovanov@uiowa.edu, yovanov@gmail.com

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA AT SANTA CRUZ
SANTA CRUZ, CA
USA
E-mail address: gem@ucsc.edu

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CA
USA
E-mail address: smontgom@usc.edu

RECEIVED AUGUST 17, 2012

