

Some bismash products that are not group algebras

Michael J. Collins

University College, Oxford OX1 4BH, England, UK

Received 10 October 2006

Available online 22 June 2007

Communicated by Ronald Solomon

Abstract

We show that an infinite family of Hopf algebras that arise as a subfamily of the so-called bismash products constructed from factorisations of symmetric groups do not have the structure (as algebras) of group algebras.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Hopf algebras; Bismash products; Symmetric groups; Group algebras; Blocks; Prime to the first power

1. Introduction

Susan Montgomery and others [3,5] have recently studied a family of finite-dimensional complex semisimple Hopf algebras which are constructed as so-called bismash products from the factorisations of symmetric groups. She and Jacques Alev have then asked whether these algebras have the same algebra structure as some group algebra. The purpose of this paper is to show that there is an infinite subfamily of her family for which they do not. The methods that we will use are rather special, but in a way not related to the construction in question; thus our result suggests strongly that, except for some very small cases, the answer will be universally negative.

Following Masuoka [6], she associates to each symmetric group S_n a particular complex Hopf algebra H_n of dimension $n!$ whose definition will be given in the next section. These Hopf algebras are semisimple. Thus, for each n , by Wedderburn's theorem we have

$$H_n \cong \bigoplus_{i=1}^r \mathcal{M}_{n_i}(\mathbb{C}).$$

E-mail address: mjc@herald.ox.ac.uk.

We will establish the following.

Theorem. *Let p be a prime greater than 3. Then, for $n = p + 1$ or $p + 2$, there is no group G for which $H_n \cong \mathbb{C}G$.*

To establish this theorem, we need to show simply that the set of dimensions of the simple H_n -modules, namely n_1, \dots, n_r (which are determined by the actual construction), cannot be the set of degrees of the irreducible representations of any finite group of order $n!$ for the given values of n . Our key tools will be the theory of blocks of characters as developed by Brauer for groups of order divisible by a prime to the first power [1], and a recent result of the author on precise bounds for the orders of finite linear groups, namely that for $n > 12$ a primitive complex linear group of degree n has centre of index at most $(n + 1)!$ [2]. This sharp bound (which corresponds to a symmetric group) will be crucial.

We remark that, by hand, we will show too that the conclusion of the theorem holds for $n = 5$. It does not for $n = 4$.

2. Bismash products and their representations

Let G be a finite group which has a factorisation $G = KL$ where $K \cap L = 1$. Then the elements of L form a set of (right) coset representatives for K so that K has a natural right action on L given by¹

$$k : l \mapsto l^{[k]}$$

where $l^{[k]}$ is uniquely determined by the rule $lk = k'(l^{[k]})$ for some $k' \in K$. Similarly, L has a left action on K denoted by $l : k \mapsto {}^{[l]}k$.

Let \mathbb{C}^L be the $|L|$ -dimensional vector space with basis indexed by, and also denoted by, the elements of L . If we denote the (standard) basis elements of the tensor product $\mathbb{C}^L \otimes \mathbb{C}K$ by $l \# k$ (rather than $l \otimes k$, to indicate that we are constructing a different algebra), the *bismash product* $\mathbb{C}^L \# \mathbb{C}K$ is the associative algebra whose multiplication is given by

$$(l \# k)(\bar{l} \# \bar{k}) = \delta_{l^{[k]}, \bar{l}} l \# (k\bar{k})$$

and $\mathbb{C}^L \# \mathbb{C}K$ can be made into a Hopf algebra H by defining a comultiplication

$$\Delta(l \# k) = \sum_{g \in L} (lg^{-1} \# {}^{[g]}k) \otimes (g \# k),$$

a counit $\varepsilon(l \# k) = \delta_{l,1}$ and an antipode $S(l \# k) = (l^{[k]})^{-1} \# ({}^{[l]}k)^{-1}$.

We have stated these details for completeness; we will not require them. What we do need are the dimensions of the simple H -modules, and these are given as follows.

¹ Our notation differs from that more often used, which is $l \triangleleft k$ and $l \triangleright k$ for the two actions, respectively. We reserve \triangleleft to denote a normal subgroup as standard in group theory.

For each K -orbit in L , fix an element $l \in L$. Let $K_l = \text{Stab}_K(l)$ and, for each simple $\mathbb{C}K_l$ -module V , let

$$\tilde{V} = \text{Ind}_{\mathbb{C}K_l}^{\mathbb{C}K} V.$$

Then \tilde{V} can be given the structure of an H -module² in a way that need not concern us. What is crucial is that we can read off all the dimensions of the simple H -modules from the following.

Proposition 1. (See [4, Corollary 3.5].) *The modules constructed in the above fashion are precisely the simple H -modules.*

Remark. It is easy to show that

$$\sum_V (\dim \tilde{V})^2 = |L| \cdot |K|.$$

Thus the nonisomorphism of the modules (given simplicity) and the semisimplicity of H are equivalent.

3. Symmetric groups and the corresponding bismash products

We carry out the above construction for the symmetric groups. Let $G = S_n$, the symmetric group of degree n . Take $S = \text{Stab}_G(n)$ and let $C = \langle \pi \rangle$ where π is the cycle $\pi = (1, 2, \dots, n)$. Then $G = SC$ and S has exactly two orbits in its action on C with representatives 1 and π and respective stabilisers $\text{Stab}_S(1_C) = S$ and (where we multiply permutations from left to right) $\text{Stab}_S(\pi) = \text{Stab}_G(n-1, n)$. As has also been observed in [3], Proposition 1 now immediately yields the following.

Proposition 2. *Let $G = S_n = SC$ as above and define $H_n = \mathbb{C}^C \# \mathbb{C}S$. Then the dimensions of the simple H_n -modules are given by*

- (i) $(n-1)$ times the degrees of the ordinary irreducible characters of S_{n-2} , and
- (ii) the degrees of the irreducible characters of S_{n-1} ,

counting multiplicities.

We will also dispose of a simple number-theoretic fact here.

Lemma 3. *Let q be a prime with $q < n$ and q^e a divisor of $n!$ Then*

$$e < \begin{cases} n-3 & \text{if } q \text{ is odd,} \\ n & \text{if } q = 2. \end{cases}$$

² The Hopf structure is not relevant here, only the \mathbb{C} -algebra structure.

Proof. We count multiples of q, q^2 and so on that are at most n to obtain the inequalities

$$e \leq \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor + \cdots < \sum_{i=1}^{\infty} \frac{n}{q^i} = \frac{n}{q-1}.$$

The result follows. \square

Remark. This is only a crude bound if q is odd, but it suffices. When $q = 2$, we may have $e = n - 1$, for example when $n = p + 1$ for p a Mersenne prime.

4. The case $n = p + 1$

Let p be a prime greater than 3 and take $n = p + 1$ in Proposition 2. Assume for this section that, as a \mathbb{C} -algebra, $H_{p+1} \cong \mathbb{C}G$ for some group G of order $(p + 1)!$

In this case, all the characters arising from Proposition 2(i) have degrees divisible by p and so lie in blocks of defect zero. Since a Sylow p -subgroup of S_p is self-centralising and of index $p - 1$ in its normaliser, there are precisely p characters having degrees congruent to $\pm 1 \pmod{p}$ in the principal block $B_0(S_p)$ by a theorem of Brauer [1, Theorem 2], with every other character of degree divisible by p . In particular, $B_0(S_p)$ has no exceptional characters. Note that there are precisely two linear characters and two of degree $p - 1$ arising from the character degrees of S_p , but none of degree 2.

Lemma 4. *The irreducible characters of G lie either in the principal p -block $B_0(G)$ or in p -blocks of defect 0. Furthermore, if P is a Sylow p -subgroup of G , then $P = C_G(P)$ and $N_G(P)$ is a Frobenius group of order $(p - 1)p$.*

Proof. By the discussion above, the irreducible characters of G lying outside blocks of defect 0 are in one–one correspondence with the characters of $B_0(S_p)$ and have the same degrees. Applying the same theorem of Brauer as above, it follows that there can be no exceptional characters in $B_0(G)$. This forces $[N_G(P) : C_G(P)]$ to be 1 or $p - 1$. Since there are precisely two linear characters, G cannot be p -nilpotent; thus $[N_G(P) : C_G(P)] = p - 1$ and *all* of these characters lie in $B_0(G)$.

Now there can be no other block of defect 1; thus, by Theorem 1 of [1], $P = C_G(P)$ and $N_G(P)$ is a Frobenius group of order $(p - 1)p$, as claimed. \square

Lemma 5. $[G : G'] = 2$ and G' is simple.

Proof. Since G has just two linear characters, the first statement is immediate; then G' is perfect since G has no character of degree 2. Now let M be a proper subgroup of G' maximal subject to $M \triangleleft G$. If $P \subseteq M$, then the Frattini argument forces $G = M.N_G(P)$ and G/M cyclic, a contradiction. So $P \not\subseteq M$ and $M = O_{p'}(G)$. Since $p^2 \nmid [G : O_{p'}(G)]$, it follows that $G'/O_{p'}(G)$ is a nonabelian simple group.

It remains to show that $O_{p'}(G) = 1$. Suppose otherwise, and put $X = O_{p'}(G).N_G(P)$. Then $O_{p'}(G) \cap N_G(P) \subseteq O_{p'}(G) \cap C_G(P) = O_{p'}(G) \cap P = 1$. For any Sylow q -subgroup Q of $O_{p'}(G)$, the Frattini argument shows that $X = O_{p'}(G).N_X(Q)$; hence we may choose Q with $N_G(P) \subseteq N_X(Q)$.

Now $N_G(P)$ acts on each $N_G(P)$ -chief factor of Q . Since all powers of a generator of P are conjugate, this forces each such chief factor to have order at least q^{p-1} . By Lemma 3, this is an immediate contradiction for q odd. For $q = 2$, we note that the index $[G : O_{p'}(G)]$ is divisible by 8, appealing to the solubility of groups of odd order,³ and Lemma 3 again yields a contradiction.

So $O_{p'}(G) = 1$. \square

We now turn explicitly to the characters of degree $p - 1$. By Lemma 4, $Z(G) = 1$ so that, by Lemma 5, G must act faithfully and, since $|G| > (p - 1)!$, primitively as a linear group of degree $p - 1$. If $p - 1 > 12$, then the author's precise bounds [2, Theorem A]; for primitive groups yields an immediate contradiction since $(p + 1)! > p!$. If $p = 5, 7, 11$ or 13 , the explicit list of groups in Theorem 8 of [2] shows that $G' (= E(G))$ cannot have order $(p + 1)!/2$, contrary to Lemma 5. (Indeed, we could have appealed to just this before, rather than to the full strength of the main result of [2].) This contradiction completes the proof of the Theorem for the case $n = p + 1$. \square

Remark. The conclusion of our Theorem is false for $n = 4$ since Proposition 2 yields dimensions 1, 1, 2, 3 and 3 for the dimensions of the simple H_4 -modules, and these are the degrees of the irreducible characters of S_4 . Thus $H_4 \cong \mathbb{C}S_4$.

5. The case $n = p + 2$

The broad approach in this case is similar to the preceding section, but the detailed application of Proposition 2 is totally different. We start by assuming that H_{p+2} is isomorphic to a group algebra $\mathbb{C}G$. We will still require $p > 3$ (specifically so that $p - 1 > 2$) for our proof.

First, Proposition 2 yields the following.

Lemma 6. *There are precisely $2p$ characters of G that do not lie in blocks of defect 0. Two of them are linear, and all have degrees congruent to $\pm 1 \pmod{p}$. Furthermore, there are (precisely two) characters of degree p .*

Proof. Both S_p and S_{p+1} have self-centralising Sylow p -subgroups of index $p - 1$ in their normalisers. So each has a principal block with exactly p characters of degrees congruent to $\pm 1 \pmod{p}$ and every other character in a block of defect 0. Now Proposition 2 applies, noting that $n - 1 \equiv 1 \pmod{p}$ and that S_{p+1} has two characters of degree p . \square

Lemma 7. *Let P be a Sylow p -subgroup of G . Then $[N_G(P) : C_G(P)] = p - 1$ and $|C_G(P)| = 2p$.*

Proof. We apply Brauer's theorems [1] again. By Lemma 6, $B_0(G)$ contains no exceptional characters and, since G cannot be p -nilpotent as there are only two linear characters, $[N_G(P) : C_G(P)] = p - 1$. Further, $B_0(G)$ contains exactly p characters.

We turn to the nonprincipal blocks. Since $[N_G(P) : C_G(P)] = p - 1$ and all the remaining characters not lying in blocks of defect 0 also have degrees that are congruent to $\pm 1 \pmod{p}$,

³ Since [2] requires the classification of finite simple groups, there is little point in trying to circumvent this use of the Feit–Thompson theorem.

the congruences of Brauer's Theorem 10 force elements of $O_{p'}(C_G(P))$ which are conjugate in $N_G(P)$ to be already conjugate in $O_{p'}(C_G(P))$. Then his Theorem 2 forces all these characters into a single nonprincipal p -block and his Theorem 1 that $O_{p'}(C_G(P))$ has exactly two conjugacy classes. So $|O_{p'}(C_G(P))| = 2$. \square

Lemma 8. $[G : G'] = 2$ and G' is quasisimple with $|Z(G')| \leq 2$.

Proof. As in Lemma 5, there are just two linear characters so that $[G : G'] = 2$. Also, if $M \triangleleft G$ with $M \subset G'$, then $P \not\subseteq M$ as before. Take $M = O_{p'}(G')$; note that, here, we do not necessarily have $O_{p'}(G') = O_{p'}(G)$. However, G'/M is a nonabelian simple group.

If $|C_M(P)| = 1$, then we may argue exactly as in Lemma 5 that $M = 1$. Otherwise, putting $X = M.N_G(P)$ we get that $|M \cap N_G(P)| = 2$. Then, for any prime divisor q of $|M|$ and Sylow q -subgroup Q of M , the Frattini argument yields that $X = M.N_X(Q)$ so that $N_X(Q)$ has a quotient that is a Frobenius group of order $p(p-1)$. Now the arguments of Lemma 5 apply again, this time considering chief factors of $N_X(Q)$ that lie in Q . Any chief factor on which an element of order p acts nontrivially leads to the same contradiction; thus $|M| \leq 2$. Hence G' is either simple or has a centre of order 2. \square

We may now complete the proof of the main theorem. By Lemma 6, G has an irreducible representation of degree p . This is either faithful when necessarily $Z(G') = 1$, or there is a kernel of order 2. In either case, since G' can have no subgroup of index less than p , the representation is primitive. Again, appealing to Theorem A of [2], we have a contradiction if $p \geq 13$ since even $\frac{1}{4}(p+2)! > (p+1)!$ while, for $p = 5, 7$ or 11 , we can appeal to Theorem 8 of [2] again for a contradiction. \square

Remark. The conclusion of our Theorem holds for $n = 5$ since the dimensions of the simple H_5 -modules are 1, 1, 2, 3, 3, 4, 4, and 8 by Proposition 2. The first three degrees must constitute the principal 3-block so that $|O_{3'}(G)| = 20$ and $G/O_{3'}(G) \cong S_3$. But now G has a normal Sylow 5-subgroup S with $|C_G(S)| = 30$ or 60 , and hence a quotient group which is either dihedral of order 10 or a Frobenius group of order 20. This affords a contradiction since neither possibility is consistent with the set of degrees. (Note that the group $Z_2 \times A_5$ shows that the characters of degree 3 do not provide a contradiction alone.)

Acknowledgment

I should like to thank Susan Montgomery for bringing this question to my attention, and for providing me with all the information about, and references on, Hopf algebras.

References

- [1] R. Brauer, On groups whose order contains a prime number to the first power I, *Amer. J. Math.* 64 (1942) 401–420.
- [2] M.J. Collins, Bounds for finite primitive complex linear groups, *J. Algebra* (2007), doi:10.1016/j.jalgebra.2005.11.042, in press.
- [3] A. Jedwab, S. Montgomery, Representations of some Hopf algebras associated to the symmetric group S_n , preprint.
- [4] Y. Kashina, G. Mason, S. Montgomery, Computing the Frobenius–Schur indicator for abelian extensions of Hopf algebras, *J. Algebra* 251 (2002) 888–913.
- [5] R. Landers, S. Montgomery, P. Schauenburg, Hopf powers and orders for some bismash products, *J. Pure Appl. Algebra* 191 (2006) 156–188.
- [6] A. Masuoka, Calculations of some groups of Hopf algebra extensions, *J. Algebra* 191 (1997) 568–588.