GENERATORS FOR THE CENTRE OF THE GROUP ALGEBRA OF A SYMMETRIC GROUP

JOHN MURRAY

ABSTRACT. The ring of symmetric functions is used to obtain an explicit set of generators for the centre of the integral group algebra of a symmetric group, different to those given by H. K. Farahat and G. Higman. This generating set is used to shows that the centre of the 2-modular group algebra is generated by certain sums of 2-classes.

Proper subalgebras of the centre of the 2-modular group algebra are studied in the context of symmetric functions. These include the algebra that is the span of the 2-regular class sums, and the algebra that is generated by the involution class sums. Various related subalgebras of the modular ring of symmetric functions are shown to be polynomial algebras, and furnished with explicit sets of algebraically independent generators.

1. INTRODUCTION

Let S_n be the symmetric group on n symbols. H. K. Farahat and G. Higman [FH] exhibited a set of generators for the centre $Z(\mathbb{Z}S_n)$ of the integral group ring $\mathbb{Z}S_n$, and introduced an infinite dimensional filtered algebra whose structure constants are integer valued rational functions. A. -A. A. Jucys [J] used their methods to show that $Z(\mathbb{Z}S_n)$ coincides with the ring Λ_{n-1} of integer symmetric polynomials in certain elements of $\mathbb{Z}S_n$. A different, and independent, proof of the same result was given by G. E. Murphy in [Mpy]. We will refer to these generating elements (whose definition is recalled in (6.1) below) as the JM-elements of $\mathbb{Z}S_n$. Murphy's proof shows that the $\mathbb{Q}$-algebra generated by the JM-elements coincides with the $\mathbb{Q}$-span of a complete set of primitive idempotents for $\mathbb{Q}S_n$. Theorem 1.9 in [Mpy] also furnishes $Z(\mathbb{Z}S_n)$ with an explicit $\mathbb{Z}$-basis involving monomial symmetric functions in the JM-elements.

The Farahat-Higman generators are the elementary symmetric polynomials in the JM-elements. As Jucys himself mentioned, any other set of generators for the algebra of integral symmetric functions gives a corresponding set of generators for $Z(\mathbb{Z}S_n)$. In this paper we give an explicit generating set that is related to the complete symmetric polynomials.

Let F be a field of characteristic 2. By an n-class we mean a conjugacy class whose elements have n-power order, for $n \geq 1$. Using our generating set, we prove in Theorem 3.8 that the centre $Z(FS_n)$ of the group algebra FS_n is generated by the 2-class sums of S_n. Theorem 4.6 gives a method of finding an explicit set of 2-class sums that generate $Z(FS_n)$. The only involution classes that occur in this set are products of powers of 2 commuting transpositions. The modular representation

Date: Submitted - January 15, 2002,
Revised - January 30, 2003.
1991 *Mathematics Subject Classification.* 05E05, 20C05, 20C30.

theory of S_n shows that no set of p-class sums can generate the centre of the group algebra of S_n over a field of odd characteristic $p > 0$.

It is noteworthy that both the Farahat and Higman paper, and the Murphy paper, include proofs of the so-called Nakayama Conjecture that gives a combinatorial classification of the p-blocks of S_n. Our results have some consequences for the 2-blocks of S_n. Specifically, we show in Section 5 that each 2-block idempotent can be expressed as a polynomial, with coefficients in F, in the involution class sums of S_n.

The latter part of the paper is concerned with various proper subalgebras of $Z(FS_n)$. The author showed in [M] that, for each each $N > 0$, the span of the class sums of elements of S_n whose order is not divisible by 2^N forms a subalgebra of $Z(FS_n)$. When $N = 1$, we obtain an algebra spanned by the sums of those conjugacy classes containing elements of odd order. We give explicit generators for this algebra in Section 7. There is a related subalgebra of the modular ring of symmetric functions, $\Lambda \bigotimes F$, which we call the 2-regular class symbol algebra (an element in a group is said to be 2-regular if it has odd order). We show that this algebra is a polynomial algebra, and furnish it with an explicit set of algebraically independent generators.

There has been some interest in recent times in representing the operation of multiplication by the sum of all transpositions, by means of differential operators acting on symmetric functions. See [LT], for instance. Here we are interested in all involution classes of S_n. In Section 8, we define and study the involution class symbol algebra. This is a subalgebra of $\Lambda \bigotimes F$ that is related to the algebra generated by all involution class sums. In Theorem 8.9 we exhibit an algebraically independent subset of the involution class symbol algebra. We suspect, but cannot yet prove, that this set actually generates the algebra.

The final section of the paper is devoted to showing that the 2-regular class symbol algebra and the involution class symbol algebra together generate a polynomial subalgebra of $\Lambda \bigotimes F$. This algebra is the span of the symmetric functions defined in (9.6). Although this is a theorem about the 2-modular ring of symmetric functions, we suspect that the corresponding conjugacy class sums span a subalgebra of $Z(FS_n)$. Indeed, a central theme of this paper is that there is a closer than expected correspondence between the 2-modular ring of symmetric functions and the centre of the 2-modular group algebra of a symmetric group.

2. The class symbol algebra

Throughout this paper, n denotes an arbitrary positive integer, and F denotes a field of characteristic 2.

Let S_∞ be the group of finitary permutations on $\mathbb{N} = \{1, 2, \dots\}$ i.e. the group of bijections on the set of positive integers that fix all but a finite number of integers. We regard S_n as the set of permutations in S_∞ that fix $\{n+1, n+2, \dots\}$ elementwise. So $S_1 \leq S_2 \leq \dots$, and $S_\infty = \bigcup_{n=1}^{\infty} S_n$.

We employ the notation and methods of I. G. Macdonald [Mac]. A partition is a nonincreasing sequence $\lambda = [\lambda_1 \geq \lambda_2 \geq \dots]$ of nonnegative integers whose sum $|\lambda| = \lambda_1 + \lambda_2 + \dots$ is finite. Call λ a partition of n, and write $\lambda \vdash n$, if $|\lambda| = n$. The nonzero terms of $\lambda_1, \lambda_2, \dots$ are called the *parts* of λ. Let a_i be the number of parts of λ that equal i, for $i \geq 1$. The multi-index notation $\lambda = [i^{\mathrm{a}_i}, j^{\mathrm{a}_j}, \dots]$, where i is omitted if $a_i = 0$, will be employed throughout. We use $l(\lambda)$ to denote the number

of parts of λ. The number of ways of arranging the parts of λ is

$$u_\lambda \;=\; \frac{l(\lambda)!}{\prod_i \mathrm{a}_i!}.$$

Two elements of S_∞ are conjugate if and only if they are conjugate in any subgroup S_n that contains them both. The conjugacy classes of S_n and of S_∞ are labelled by partitions, but in different ways. If λ is a partition of n, we let $K(\lambda)$ be the conjugacy class of S_n whose elements have cycle type λ. The *modified cycle type* of the elements of $K(\lambda)$ is the partition $\mu = [\lambda_1 - 1, \ldots, \lambda_{l(\lambda)} - 1, 0, \ldots]$. If $\sigma \in S_n$, the cycle type of σ depends on n, whereas the modified cycle type of σ does not. We let c_μ denote the set of elements of S_∞ that have modified cycle type μ. Then c_μ is a conjugacy class of S_∞, and each conjugacy class of S_∞ arises in this way. In particular, the identity permutation belongs to $c_{[]}$, where $[]$ is the empty partition. For $m \geq 1$, set $c_\mu(m) := c_\mu \cap S_m$. Then $c_\mu(n) = K(\lambda)$, while $c_\mu(m)$ is the empty set, if $|\mu| + l(\mu) > m$.

We identify $K(\lambda)$ or $c_\mu(n)$ with the sum of the elements of the corresponding class of S_n in $Z(\mathbb{Z}S_n)$. The empty sum is, by fiat, zero. For partitions μ and ν we have

$$c_\mu(n)\, c_\nu(n) \;=\; \sum_\rho \alpha^\rho_{\mu\nu}\, c_\rho(n),$$

where ρ ranges over all partitions and $\alpha^\rho_{\mu\nu}$ are integers that depend on n. Farahat and Higman [FH] have shown that the integer $\alpha^\rho_{\mu\nu}$ is zero if $|\rho| > |\mu| + |\nu|$, is independent of n, if $|\rho| = |\mu| + |\nu|$, and is a rational function of n, if $|\rho| \leq |\mu| + |\nu|$.

A $\mathbb{Z}$-order is a $\mathbb{Z}$-algebra that is free as $\mathbb{Z}$-module. The *Macdonald class symbol algebra* G is the $\mathbb{Z}$-order that is freely generated by the S_∞-class symbols $\{c_\mu\}$, where the multiplication is induced from

$$c_\mu\, c_\nu \;=\; \sum_{\rho \vdash (|\mu|+|\nu|)} \alpha^\rho_{\mu\nu}\, c_\rho. \tag{2.1}$$

A typical element of G has the form $g = \sum a_\mu c_\mu$, where μ ranges over a finite set of partitions, and each a_λ is an integer. We use $g(n)$ to denote the element $\sum a_\mu c_\mu(n)$ of $Z(\mathbb{Z}S_n)$. For $i \leq n$, let $Z(\mathbb{Z}S_n)_i$ be the $\mathbb{Z}$-submodule of $Z(\mathbb{Z}S_n)$ that is spanned by those nonzero $c_\lambda(n)$ with $|\lambda| < i$.

Lemma 2.2. *Suppose that $g_1, g_2, \ldots$ are elements of G that generate G as a $\mathbb{Z}$-order. Then the non-zero $g_1(n), g_2(n), \ldots$ generate $Z(\mathbb{Z}S_n)$ as a $\mathbb{Z}$-algebra.*

Proof. It is enough to show that $c_\lambda(n) \in \mathbb{Z}[g_1(n), g_2(n), \ldots]$ for each partition λ. We prove this using induction on $i = |\lambda|$. If $i = 0$, then λ is the empty partition and $c_\lambda(n) = 1$. Suppose then that $i > 0$ and that $c_\mu(n) \in \mathbb{Z}[g_1(n), g_2(n), \ldots]$, whenever μ is a partition with $|\mu| < i$. By hypothesis there exists $f \in \mathbb{Z}[x_1, x_2, \ldots]$ such that $f(g_1, g_2, \ldots) = c_\lambda$. An inductive argument using (2.1) shows that

$$f(g_1(n), g_2(n), \ldots) \;\equiv\; c_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_i}.$$

The lemma now follows from the inductive hypothesis. □

I. G. Macdonald has shown that G is isomorphic to a polynomial ring in a countable number of variables. Specifically, let Λ be the ring of symmetric functions in the variables $x_1, x_2, \ldots$ over $\mathbb{Z}$. Then there exists a $\mathbb{Z}$-basis $\{g_\lambda\}$ for Λ such that the map $\phi : \Lambda \to G$, defined by $\phi(g_\lambda) = c_\lambda$, is a ring isomorphism. Let $e_n \in \Lambda$ denote the n-th *elementary* symmetric function. Then $e_1, e_2, \ldots$ are algebraically

independent over $\mathbb{Z}$, and $\Lambda = \mathbb{Z}[e_1, e_2, \ldots]$. From now on we will not distinguish between G and Λ, and we identify c_λ with the symmetric function g_λ.

If λ is a partition, let m_λ denote the *monomial* symmetric function of type λ. The n-th *complete* symmetric function h_n is $\sum_{\lambda \vdash n} m_\lambda$. The symmetric functions $h_1, h_2, \ldots$ are algebraically independent and $\Lambda = \mathbb{Z}[h_1, h_2, \ldots]$. Indeed, the map τ that interchanges e_i and h_i, for $i \geq 1$, is an involutary automorphism of λ. For each partition λ, set $h_\lambda := \prod_{i>0} h_{\lambda_i}$. The generating function $H(x) = \sum_{n \geq 0} h_n x^n$ is given (somewhat informally) by the following infinite product of power series:

$$H(x) \;=\; \prod_{n \geq 1} (1 - x_n x)^{-1}.$$

The *power sum* symmetric functions are defined as follows. Set $p_n := m_{[n]}$, and for each partition λ, define $p_\lambda := \prod p_{\lambda_i}$. Then the p_n are algebraically independent, and $\{p_\lambda\}$ forms a basis for $\Lambda \bigotimes \mathbb{Q}$ (but not for Λ). The power series $P(x) = \sum p_n x^{n-1}$ satisfies the equation $P(x) = H'(x)/H(x)$ (see [Mac]). In particular,

$$n\, h_n \;=\; \sum_{i=1}^{n} p_i\, h_{n-i}.$$

Let $<\,,\,>$ denote the nondegenerate symmetric bilinear form on Λ such that

$$< h_\lambda, m_\mu > \;=\; \delta_{\lambda\mu}$$

for all partitions λ and μ. Let f_λ denote the symmetric function that is $<\,,\,>$-dual to e_λ. The f_λ are sometimes called the *forgotten* symmetric functions. Since $\tau(e_\lambda) = h_\lambda$, and it is known that $<\,,\,>$ is τ-invariant, we have $\tau(f_\lambda) = m_\lambda$.

The following theorem [Mac, I.2.24], which we restate here for the convenience of the reader, characterizes the c_λ:

Theorem 2.3. *Let $\{h^*_\lambda\}$ be the $\mathbb{Z}$-basis of Λ that is $<\,,\,>$-dual to $\{c_\lambda\}$. Set $h^*_n := h^*_{[n]}$, for $n \geq 1$. Then the map $h_n \to h^*_n$ induces a $\mathbb{Z}$-algebra involutary autmorphism of Λ. In particular $h^*_\lambda = \prod_i h^*_{\lambda_i}$, for each partition λ. Let $H^*(x) = \sum_{n \geq 0} h^*_n x^n$ be the generating function for the h^*_n. Then $H^*(x)$ is the Lagrange inverse of $H(x)$ i.e. if $y := xH^*(x)$, then $x = yH(y)$.*

If $\{\alpha_\lambda\}$ and $\{\beta_\lambda\}$ are $\mathbb{Z}$-bases of Λ, indexed by partitions, we let $M(\alpha, \beta)$ denote the change of basis matrix from $\{\alpha_\lambda\}$ to $\{\beta_\lambda\}$ i.e.

$$\alpha_\lambda \;=\; \sum_{\mu} M(\alpha, \beta)_{\lambda,\mu}\, \beta_\mu.$$

Note that $M(\beta, \alpha) = M(\alpha, \beta)^{-1}$. Also if $\{\alpha'_\lambda\}$ and $\{\beta'_\lambda\}$ are the $<\,,\,>$-dual bases to $\{\alpha_\lambda\}$ and $\{\beta_\lambda\}$, and ^{t} denotes matrix transposition, then

$$M(\alpha', \beta') \;=\; M(\beta, \alpha)^t, \tag{2.4}$$

If $n \geq 1$, we use $\mathcal{L}(n)$ to denote the number of digits that equal 1 in the binary expansion of n. So n is a sum of $\mathcal{L}(n)$ distinct nonnegative powers of 2. We use $\nu(n)$ to denote the highest power of 2 that divides n. Note that $\mathcal{L}(2n) = \mathcal{L}(n)$ and that $\nu(n!) = n - \mathcal{L}(n)$.

3. Generators for the class symbol algebra

Catalan numbers appear frequently in the combinatorics of symmetric functions. The n-th Catalan number C_n is the integer

$$C_n := \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}.$$

Lemma 3.1. *C_n is odd if and only if $n+1$ is a power of 2.*

Proof. This follows from

$$\begin{aligned}\nu(C_n) &= \nu((2n)!) &&- \nu((n+1)!) &&- \nu(n!)\\ &= (2n - \mathcal{L}(2n)) &&- (n+1-\mathcal{L}(n+1)) &&- (n - \mathcal{L}(n))\\ &= \mathcal{L}(n+1) - 1.\end{aligned}$$

□

For each partition λ, set

$$C_\lambda := \prod_i C_{\lambda_i}.$$

Our interest in the C_λ arises from:

Proposition 3.2.

$$\begin{aligned}e_n &= (-1)^n \sum_{\lambda\vdash n} C_\lambda\, c_\lambda,\\ h_n &= (-1)^n \sum_{\lambda\vdash n} c_\lambda.\end{aligned}$$

Proof. Let λ be a partition of n. Since $e_n = m_{[1^n]}$, we have

$$\begin{aligned}M(e,c)_{[n],\lambda} &= M(m,c)_{[1^n],\lambda}\\ &= M(h^*,h)_{\lambda,[1^n]}, \quad \text{using (2.4)}\\ &= \prod_i M(h^*,h)_{[\lambda_i],[1^{\lambda_i}]}.\end{aligned} \tag{3.3}$$

Macdonald has shown in [Mac, I.2.24] that

$$h_n^* = \sum_{\lambda\vdash n} \frac{(-1)^{l(\lambda)}}{n+1}\binom{n+l(\lambda)}{n} u_\lambda\, h_\lambda.$$

So

$$M(h^*,h)_{[n],[1^n]} = \frac{(-1)^n}{n+1}\binom{n+n}{n} u_{[1^n]} = (-1)^n C_n. \tag{3.4}$$

The identity for e_n follows from (3.3) and (3.4).

Since $\tau(e_n) = h_n$ and $\tau(m_{[1^n]}) = f_{[1^n]}$, we have $h_n = f_{[1^n]}$. So

$$\begin{aligned}M(h,c)_{[n],\lambda} &= M(f,c)_{[1^n],\lambda}\\ &= M(h^*,e)_{\lambda,[1^n]}, \quad \text{using (2.4)}\\ &= \prod_i M(h^*,e)_{[\lambda_i],[1^{\lambda_i}]}.\end{aligned} \tag{3.5}$$

We adopt Macdonald's methods to express h_n^* in terms of the e_λ. Recall from Theorem 2.3 that if $y = xH(x)$, then $x = yH^*(y)$. So

$$dx \;=\; \sum_{n\geq 0} (n+1)\, h_n^*\, y^n\, dy.$$

It follows that $(n+1)h_n^*$ equals the *residue* (coefficient of y^{-1}) of dx/y^{n+1}. Let $E(x) = \sum_{n\geq 0} e_n x^n$ be the generating function for the e_n. Then $H(x) = 1/E(-x)$. So $y = x/E(-x)$, whence $dx/y^{n+1} = dxE(-x)^{n+1}/x^{n+1}$. Thus $(n+1)h_n^*$ equals the coefficient of x^n in $E(-x)^{n+1}$. Since the e_n are algebraically independent, we deduce that

$$h_n^* \;=\; \frac{(-1)^n}{n+1} \sum_{\lambda\vdash n} \left(\begin{array}{c} n+1 \\ l(\lambda) \end{array} \right) u_\lambda\, e_\lambda. \tag{3.6}$$

In particular

$$M(h^*, e)_{[n],[1^n]} \;=\; \frac{(-1)^n}{n+1} \left(\begin{array}{c} n+1 \\ n \end{array} \right) u_{[1^n]} \;=\; (-1)^n. \tag{3.7}$$

The identity for h_n follows from (3.5) and (3.7). □

We use this to prove a result about the 2-modular group algebra of S_n.

Theorem 3.8. *Let F be a field of characteristic 2, and let $\mathcal{L}(n)$ be the number of digits that equal 1 in the binary expansion of n. For $i = 1, \ldots, n - \mathcal{L}(n)$, set*

$$K_i \;:=\; \sum K \;\;\in\;\; Z(FS_n),$$

where K ranges over the 2-classes of S_n whose cycle decomposition contains $n-i$ cycles. Then $K_1, \ldots, K_{n-\mathcal{L}(n)}$ generate the F-algebra $Z(FS_n)$.

Proof. It is enough to prove the result for $F = GF(2)$. We have $\Lambda = \mathbb{Z}[e_1, e_2, \ldots]$. So the nonzero terms in $e_1(n), e_2(n) \ldots$ generate the $\mathbb{Z}$-algebra $Z(\mathbb{Z}S_n)$, by Lemma 2.2. Reduction modulo 2 induces an epimorphism $Z(\mathbb{Z}S_n) \twoheadrightarrow Z(FS_n)$. Using Lemma 3.1 and Proposition 3.2, we see that the image of $e_i(n)$ in $Z(FS_n)$ coincides with K_i, for $i \geq 1$. Suppose that S_n has a 2-class whose cycle type contains $n-i$ parts. Then n is a sum of $n-i$ powers of 2. So $n-i \geq \mathcal{L}(n)$, whence $i \leq n - \mathcal{L}(n)$. It follows that $K_i = 0$, for $i > n - \mathcal{L}(n)$. This completes the proof of the theorem. □

4. Generators for the modular group algebra

In this section we prove a more precise form of Theorem 3.8. Our first result translates Theorem 4.3 of [FH] into the language of symmetric functions.

Proposition 4.1. *Let λ be a partition of n. Then*

$$M(c, h)_{\lambda,[n]} \;=\; (-1)^{l(\lambda)} \left(\begin{array}{c} n-1+l(\lambda) \\ n-1 \end{array} \right) u_\lambda.$$

Proof. We have

$$M(c, h)_{\lambda,[n]} \;=\; M(m, h^*)_{[n],\lambda} \;=\; M(p, h^*)_{[n],\lambda}. \tag{4.2}$$

Recall that $P(x) = H'(x)/H(x)$, and that if $y = xH(x)$, then $x = yH^*(y)$. Thus

$$\frac{dy}{y} \;=\; \frac{H(x) + xH'(x)}{xH(x)}\, dx \;=\; (\frac{1}{x} \;+\; P(x))\, dx.$$

It follows that p_n is the residue of $dy/yx^n = dy/y^{n+1}H^*(y)^n$, which in turn is the coefficient of y^n in $H^*(y)^{-n}$. Write $H^*(y) = 1 + H^*_+(y)$. Then

$$H^*(y)^{-n} = \sum_{l \geq 0} \binom{-n}{l} H^*_+(y)^l.$$

Since the h^*_r are algebraically independent, it follows that

$$p_n = \sum_{\lambda \vdash n} (-1)^{l(\lambda)} \binom{n-1+l(\lambda)}{n-1} u_\lambda h^*_\lambda. \tag{4.3}$$

The proposition follows from (4.2) and (4.3). □

Next we show that each positive integer has a particular representation as a sum of terms of the form $2^i - 1$, for $i \geq 1$. We begin with some technical results.

Let S denote the set of sequences $s = \cdots s_2 s_1 s_0$, where each s_i is one of the symbols $\{1, 0, -1, -2, \ldots\}$, and there are only a finite number of occurrences of 1. For each $i > 0$, let $s_{\geq i}$ denote the subsequence $\cdots s_{i+2} s_{i+1} s_i$ of s. We associate two numerical values to s. These are

$$|s| := |\{i \geq 0 \mid s_i = 1\}|, \quad \text{and}$$

$$\sum s := \sum_{i=0}^{\infty} \operatorname{sgn}(s_i) 2^i (2^{|s_i|} - 1), \quad \text{a formal sum.}$$

Lemma 4.4. *Let $s \in$ S be such that for each $i \geq 0$, either*

(i) $s_i = 1$ *or*
(ii) $s_i = -|s_{\geq i}|$.

Then $\sum s = 2^{|s|} - 1$.

Proof. Since $|s|$ is finite, there is a minimal $N = N(s) \geq 0$, such that $s_n = 0$ when $n \geq N$. We prove the lemma using induction on N. The base case $N = 0$ is trivial.

Suppose that $N > 0$. Then $N(s_{\geq 1}) < N$. The inductive hypothesis gives $\sum s_{\geq 1} = 2^{|s_{\geq 1}|} - 1$, and the definition gives $\sum s = 2 \sum s_{\geq 1} + \operatorname{sgn}(s_0)(2^{|s_0|} - 1)$. If $s_0 = 1$, then $|s_{\geq 1}| = |s| - 1$, and $\sum s = 2(2^{|s|-1} - 1) + (2^1 - 1) = 2^{|s|} - 1$. Otherwise $s_0 = -|s|$ and $|s_{\geq 1}| = |s|$. In this case we have $\sum s = 2(2^{|s|} - 1) - (2^{|s|} - 1) = 2^{|s|} - 1$. This completes the proof. □

Lemma 4.5. *Let $s \in$ S be such that for each $i \geq 0$, either*

(i) $s_i = 1$ *or*
(ii) $s_j \neq 1$, *for some $j < i$, and* $s_i = -|s_{\geq i}|$ *or*
(iii) $s_j = 1$, *for all $j < i$, and* $s_i = -|s_{\geq i}| - 1$.

Then $\sum s = -1$.

Proof. There exists $i \geq 0$ such that $s_j = 1$ for all $j < i$, and $s_{\geq i}$ has initial term $s_i = -|s_{\geq i}| - 1 = i - |s| - 1$. Let x be the word that is obtained from s by replacing s_i by $-|s_{\geq i}|$. Then x satisfies the criteria of Lemma 4.4, and $|x| = |s|$. We compute

$$\begin{aligned} \sum s &= \sum x + 2^i(2^{|s|-i} - 1) - 2^i(2^{|s|+1-i} - 1) \\ &= 2^{|s|} - 1 + 2^{|s|} - 2^{|s|+1}, \quad \text{using Lemma 4.4} \\ &= -1. \end{aligned}$$

□

Theorem 4.6. *There exist nonnegative integers $e_1, e_2, \ldots$ such that $\lambda = [2^{e_1} - 1, 2^{e_2} - 1, \ldots]$ is a partition of n and $M(c,h)_{\lambda,[n]}$ is odd.*

Proof. Since $P(x) = H'(x)/H(x)$ and $H(x) = 1/E(-x)$, we have $-P(-x) = E'(x)/E(x)$. Also $\tau(h_n) = e_n$. It follows that $\tau(p_n) = (-1)^n p_n$. Thus from $p_n = m_{[n]}$, and $\tau(m_{[n]}) = f_{[n]}$, we get $f_{[n]} = (-1)^n p_n$. Now for μ a partition, we have

$$\begin{aligned} M(c,e)_{\mu,[n]} &= M(f,h^*)_{[n],\mu} = (-1)^n M(p,h^*)_{\mu,[n]} \\ &\equiv M(c,h)_{\mu,[n]} \text{ (modulo 2)}, \quad \text{see (4.2)}. \end{aligned}$$

The first statement of Proposition 3.2 then implies that $\sum_\mu M(c,h)_{\mu,[n]}$ is odd, where μ runs over all partitions of n with $\mu_i + 1$ a power of 2, for all i. The theorem follows immediately from this. As an alternative proof, we will explicitly construct a partition of n with the desired properties.

Let b denote the sequence $\ldots b_2 b_1 b_0$ such that $n - 1 = \sum b_i 2^i$ is the binary expansion of $n-1$. As before, $b_{\geq i}$ is the truncated sequence $\ldots b_{i+2} b_{i+1} b_i$. We construct a sequence $s = \ldots s_2 s_1 s_0 \in \mathrm{S}$ as follows. For $i \geq 0$, set

$$s_i := \begin{cases} 1, & \text{if } b_i = 1; \\ -|b_{\geq i}|, & \text{if } b_i = 0, \text{ for some } j < i; \\ -|b_{\geq i}| - 1, & \text{if } b_i = 1, \text{ for all } j < i. \end{cases}$$

Then s satisfies the criteria of Lemma 4.5.

For each $i \geq 0$, set $\mathrm{a}_i := \sum\{2^j \mid j \geq 0 \text{ and } s_j = -i\}$. Lemma 4.5 shows that

$$\sum_{i \geq 0} b_i 2^i - \sum_{i \geq 0} \mathrm{a}_i (2^i - 1) = \sum s = -1.$$

But $\sum b_i 2^i = n - 1$. It follows that

$$\sum_{i \geq 0} \mathrm{a}_i (2^i - 1) = n.$$

Note that $n - 1 + \sum \mathrm{a}_i = 2^r - 1$, where $2^{r-1} \leq n < 2^r$. The construction of a_i shows that

$$r = \mathcal{L}(n - 1 + \sum \mathrm{a}_i) = \mathcal{L}(n-1) + \sum \mathcal{L}(\mathrm{a}_i).$$

Let λ denote the partition of n, whose parts are all of the form $2^i - 1$, for $i \geq 1$, where the multiplicity of $2^i - 1$ is a_i. It follows from Proposition 4.1 that $M(c,h)_{\lambda,[n]}$ is odd. □

Corollary 4.7. *Let F be a field of characteristic 2, and let r be the largest positive integer such that $2^r \leq n < 2^{r+1}$. Then there exist 2-classes $L_1, \ldots, L_{2^r - 1}$ of S_n, whose sums generate the algebra $Z(FS_n)$. These classes can be chosen so that L_i contains $n - i$ cycles, and L_i is an involution class if and only if i is a power of 2.*

Proof. For $i \geq 1$, let λ^i be the partition of i, constructed by the method of Theorem 4.6, such that $M(c,h)_{\lambda^i,[i]}$ is odd. Then clearly $\{c_{\lambda^i} \mid i \geq 1\}$ form a set of algebraically independent generators for Λ. It follows that the images of the nonzero $c_{\lambda^i}(n)$ generate $Z(FS_n)$.

Let t be the largest positive integer such that $2^t \leq i$. The proof of Theorem 4.6 shows that $l(\lambda) = 2^{t+1} - i$. Set $L_i = c_{\lambda^i}(n)$. Then L_i is a conjugacy class of S_n if and only if $i + l(\lambda^i) = 2^{t+1} \leq n$. This occurs if and only if $i < 2^r$. Now L_i is an involution class if and only if all parts of λ^i are 1. The construction of λ^i shows that this occurs if and only if i is a power of 2. □

The table below demonstrates the construction of the 2-classes of S_{16} that is given in the proof of Theorem 4.6.

n	b				s				λ	Class of S_{16}
1	0	0	0	0	0	0	0	–1	$[1]$	$K[2,1^{14}]$
2	0	0	0	1	0	0	–1	1	$[1^2]$	$K[2^2,1^{12}]$
3	0	0	1	0	0	0	1	–2	$[3]$	$K[4,1^{12}]$
4	0	0	1	1	0	–1	1	1	$[1^4]$	$K[2^4,1^8]$
5	0	1	0	0	0	1	–1	–2	$[3,1^2]$	$K[4,2^2,1^8]$
6	0	1	0	1	0	1	–2	1	$[3^2]$	$K[4^2,1^8]$
7	0	1	1	0	0	1	1	–3	$[7]$	$K[8,1^8]$
8	0	1	1	1	–1	1	1	1	$[1^8]$	$K[2^8]$
9	1	0	0	0	1	–1	–1	–2	$[3,1^6]$	$K[4,2^6]$
10	1	0	0	1	1	–1	–2	1	$[3^2,1^4]$	$K[4^2,2^4]$
11	1	0	1	0	1	–1	1	–3	$[7,1^4]$	$K[8,2^4]$
12	1	0	1	1	1	–2	1	1	$[3^4]$	$K[4^4]$
13	1	1	0	0	1	1	–2	–3	$[7,3^2]$	$K[8,4^2]$
14	1	1	0	1	1	1	–3	1	$[7^2]$	$K[8^2]$
15	1	1	1	0	1	1	1	–4	$[15]$	$K[16]$

5. 2-BLOCKS OF SYMMETRIC GROUPS

Each finite dimensional F-algebra $A \neq 0$ has a decomposition

$$A = B_1 \oplus \cdots \oplus B_r$$

into a direct sum of a number r of nonzero indecomposable F-algebras B_i. These are called the *blocks* of A. Let e_i denote the multiplicative identity of the algebra B_i, for $1 \leq i \leq r$. Then e_i is called the block idempotent of B_i. It is known that

$$1_A = e_1 + \cdots + e_r$$

is a decomposition of 1_A into a sum of pairwise orthogonal primitive central idempotents. When A is a group algebra, each block of A has associated to it a family of 2-subgroups of the group, known as its *defect groups*. These groups can be defined using the support of the block idempotent.

Suppose now that A is split over F. Then the centre $Z(A)$ decomposes into

$$Z(A) = N \oplus E,$$

as F-algebras, where N is the nilradical of $Z(A)$, and $E = Fe_1 + \cdots + Fe_r$ is the maximal semisimple subalgebra of $Z(A)$. The projection map $\rho : Z(A) \to E$, with respect to this decomposition, is given by

$$\rho(z) = \sum_{i=1}^{r} \omega_i(z) e_i, \quad \text{for } z \in Z(A),$$

where $\omega_i : Z(A) \to F$ is the unique irreducible F-representation of $Z(A)$ whose kernel does not contain B_i. The map ω_i is called the *central character* of B_i. It is known that $\rho(z)$ is contained in the subalgebra of $Z(A)$ that is generated by z.

In this section we prove two results about the block algebras of FS_n. Our first result is known. It is a consequence of the Nakayama Conjecture, the theorem that classifies the p-blocks of symmetric groups using the p-cores of partitions.

Proposition 5.1. *Let F be a field of characteristic 2 and let D be a 2-subgroup of S_n. Then FS_n has at most one block with defect group D.*

Proof. We use standard block-theoretic notation. See for instance [NT]. Let G be an arbitrary finite group, let p be a prime, and let k be a field of characteristic p. Suppose that B is a block of kG, with central character ω_B and defect group P. The *Brauer correspondent* b of B is a block of $kN_G(P)$, whose central character ω_b satisfies

$$\omega_B(K) = \omega_b \circ \mathrm{Br}_P(K) = \omega_b(K \cap C_G(P)), \quad \text{for all classes } K \text{ of } G,$$

where Br_P denotes the *Brauer homomorphsim* with respect to P. A result of J. Green implies that ω_b vanishes on class sums of elements whose p-parts are not contained in P. Also $\omega_b(L^+) = |L|$, for each conjugacy class L of $N_G(P)$ that is contained in $Z(P)$. It follows that if K is a class of p-elements of G, then

$$\omega_B(K) \;=\; |K \cap Z(P)|\, 1_F. \tag{5.2}$$

This argument is due to G. R. Robinson.

We specialize to $G = S_n$ and $P = D$. The previous section shows that the 2-class sums generate $Z(FS_n)$, and the previous paragraph shows that the values of ω_B on the 2-class sums are determined by D. It follows that ω_B is determined by D. But B is determined by ω_B. We conclude that B is the unique block of FS_n that has defect group D. □

We now present the main result of this section.

Theorem 5.3. *Let F be a field of characteristic 2. Then each idempotent in $Z(FS_n)$ lies in the algebra that is generated by the involution class sums of S_n.*

Proof. Let B be a 2-block of S_n. The Nakayama Conjecture endows B with a positive integer $w \leq n/2$ called its *weight*. Let $w = \sum_i 2^{a_i}$ be the 2-adic decomposition of w. Let W_0 denote the cyclic group of order 2, and define W_i for $i > 0$, inductively by $W_i := W_{i-1} \wr W_0$. Set $D := \prod_i W_{a_i}$. Then D is isomorphic to a Sylow 2-subgroup of S_{2w}, and each defect group of B is isomorphic to D. An inductive argument shows that $Z(W_i)$ is cyclic of order 2, whence $Z(D)$ is elementary abelian. In fact, the centre of a defect group contains exactly one involution that is a product of 2^{a_i} commuting transpositions, for each $a_i \neq 0$, and these involutions form a basis for the centre. It follows from (5.2) that ω_B vanishes on the sum of any 2-class whose elements have order divisible by 4.

Let $Z(FS_n) = N \oplus E$ and $\rho : Z(FS_n) \to E$ be as above. Suppose that $L_1, L_2 \ldots$ are 2-classes of S_n whose sums generate the algebra $Z(FS_n)$. Then clearly $\rho(L_1), \rho(L_2), \ldots$ generate the algebra E. The previous paragraph shows that $\rho(L_i) = 0$ unless L_i is a class of involutions. It follows that E is contained in the algebra generated by the involution class sums in the list $L_1, L_2, \ldots$. □

Corollary 4.7 can be used to strengthen this theorem, in an obvious way.

6. Murphy-Jucys elements

For positive integers $i \neq j$, let (i,j) denote the permutation in S_∞ that transposes i and j. Define the JM-elements of $\mathbb{Z}S_\infty$ as

$$l_u := (1,u) + (2,u) + \ldots + (u-1,u), \quad \text{for } u = 2, \ldots n. \tag{6.1}$$

If f is a polynomial in the variables $x_1, x_2, \ldots$, we use $f(l;n)$ to denote the evaluation of f at $x_1 = l_2, \ldots, x_{n-1} = l_n, x_n = 0, x_{n+1} = 0, \ldots$. So $f(l;n)$ lies in $\mathbb{Z}S_n$. A. -A. A. Jucys [J] has shown the following:

Lemma 6.2. *$Z(\mathbb{Z}S_n)$ coincides with the ring of symmetric polynomials in $l_2, \ldots, l_n$. In particular $Z(\mathbb{Z}S_n) = \mathbb{Z}[e_1(l;n), \ldots, e_{n-1}(l;n)]$. In terms of the class sums,*

$$e_i(l;n) = \sum_{\lambda \vdash i} c_\lambda(n). \quad \text{for } i = 1, \ldots, n-1.$$

The following result gives a connection between the ring of symmetric polynomials in the Jucys elements and Macdonald's class symbol algebra. Recall that τ is an involutary automorphism of Λ that interchanges e_i and h_i, for $i \geq 1$.

Theorem 6.3. *Let $g \in \Lambda$ be a homogeneous symmetric function of degree i. Then*

$$g(l;n) \equiv (-1)^i \tau(g)(n) \pmod{Z(\mathbb{Z}S_n)_i}.$$

Proof. Proposition 3.2 and Lemma 6.2 imply that $e_i(l;n) = (-1)^i h_i(n)$, for each $i \geq 1$. Let λ be a partition. An inductive argument using (2.1) gives

$$e_\lambda(l;n) \equiv (-1)^{|\lambda|} h_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}}.$$

But $h_\lambda = \tau(e_\lambda)$. The proposition follows, as the e_λ form a $\mathbb{Z}$-basis for Λ. □

Corollary 6.4. *Let λ be a partition. Then*

$$m_\lambda(l;n) \equiv (-1)^{|\lambda|} f_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}};$$
$$h_\lambda(l;n) \equiv (-1)^{|\lambda|} e_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}}.$$

In particular, if $i \geq 1$ then

$$h_i(l;n) \equiv \sum_{\lambda \vdash i} C_\lambda \, c_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_i}.$$

Proof. The first statement uses the fact that $\tau(m_\lambda) = f_\lambda$. The other statements use Proposition 3.2. □

7. The 2-regular class symbol algebra

Recall that F is a field of characteristic 2. A conjugacy class of S_n is said to be 2-regular if all its elements have odd order. The author showed in [M, Corollary 5] that the F-span of the class sums of the 2-regular classes forms a subalgebra of $Z(FS_n)$. We call this algebra the 2-*regular algebra* of $Z(FS_n)$. (More generally the centre of the p-modular group algebra of S_n has a p-regular subalgebra, for each prime p.)

We call a partition with all parts even a 2-partition. So a class of S_n is 2-regular if and only if its modified cycle type is a 2-partition. It follows from (2.1) and the previous paragraph that the F-span of $\{ c_\lambda \mid \lambda \text{ is a 2-partition} \}$ forms a subalgebra of $\Lambda \bigotimes F$, which we shall call the 2-*regular class symbol algebra*. The purpose of this section is to show that this is a polynomial subalgebra of $\Lambda \bigotimes F$. This fact will be used to give explicit generators for the 2-regular subalgebra of $Z(FS_n)$.

We extend the notation for Catalan numbers slightly by setting $C_q = 0$, whenever $q \in \mathbb{Q}\backslash\mathbb{Z}$. For each pair λ/n, with λ a partition and n a positive integer, define

$$C_{\lambda/n} := \prod_i C_{\lambda_i/n}.$$

Proposition 7.1. $h_n^2 \equiv \sum_{\lambda\vdash 2n} C_{\lambda/2}\, c_\lambda, \pmod 2$.

Proof. We have $e_n = m_{[1^n]}$. So $e_n^2 \equiv m_{[2^n]} \pmod 2$. Applying the automorphism τ, we get $h_n^2 \equiv f_{[2^n]} \pmod 2$. Now if λ is a partition of $2n$, then

$$\begin{aligned} M(h,c)_{[n^2],\lambda} &\equiv M(f,c)_{[2^n],\lambda}, \pmod 2 \\ &= M(h^*,e)_{\lambda,[2^n]}, \quad \text{by (2.4)} \\ &= \begin{cases} \prod_{i\geq 1} M(h^*,e)_{[\lambda_i],[2^{\lambda_i/2}]}, & \text{if } \lambda_i \text{ is even for all } i \geq 1; \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{7.2}$$

Equation (3.6) gives

$$M(h^*,e)_{[2n],[2^n]} = \frac{(-1)^{2n}}{2n+1}\begin{pmatrix} 2n+1 \\ n \end{pmatrix} u_{[2^n]} = C_n. \tag{7.3}$$

The proposition follows from (7.2) and (7.3). □

Corollary 7.4. *Let F be a field of characteristic 2. Then the 2-regular class symbol algebra coincides with the polynomial algebra $F[h_1^2, h_2^2, \ldots]$.*

Proof. Lemma 3.1 implies that if $j \geq 1$, then $C_{j/2}$ is odd if and only if $j+2$ is a power of 2. It then follows from Proposition 7.1 that

$$h_i^2 \equiv \sum c_\lambda \pmod 2,$$

for each $i \geq 1$, where λ ranges over the partitions of $2i$, with each part λ_j of the form $2^a - 2$, for some $a > 0$. This shows that the subalgebra of $\Lambda \bigotimes F$ generated by the images of $h_1^2, h_2^2, \ldots$ is contained in the 2-regular class symbol algebra.

There is an obvious bijection between the 2-partitions of $2i$ and the partitions of $2i$ whose parts occur with even multiplicities. It then follows from a consideration of $\mathbb{Z}$-ranks, and the previous paragraph, that the images of $\{h_1^2, h_2^2, \ldots\}$ form an algebraically independent generating set for the 2-regular class symbol algebra. □

Theorem 7.5. *Let F be a field of characteristic 2. For $i = 1, \ldots, \lfloor \frac{n}{2} \rfloor$, set*

$$R_i := \sum K \in Z(FS_n),$$

where K ranges over the conjugacy classes of S_n whose cycle decomposition consists of $n-2i$ cycles, each of length $2^e - 1$, for some $e \geq 0$. Then $R_1, \ldots, R_{\lfloor \frac{n}{2} \rfloor}$ generate the 2-regular algebra of $Z(FS_n)$.

Proof. The element R_i coincides with the image of $h_i^2(n)$ in $Z(FS_n)$. Suppose that S_n has a conjugacy class that contains $2i$ cycles. Then $2i \leq n$. So $i \leq \lfloor \frac{n}{2} \rfloor$. Since $\{h_1^2, h_2^2, \ldots\}$ generate the 2-regular class symbol subalgebra in $\Lambda \bigotimes F$, it follows that $\{R_1, \ldots, R_{\lfloor \frac{n}{2} \rfloor}\}$ generate the 2-regular subalgebra of $Z(FS_n)$. □

8. The involution class symbol algebra

Let t_n denote the conjugacy class of S_∞ containing the involutions that are products of n commuting transpositions. So $t_n = c_{[1^n]}$. For convenience we set $t_0 := 1$, and $t_i := 0$ for $i < 0$. If λ is a partition, set

$$t_\lambda := \prod_i t_{\lambda_i}.$$

Also put $t_{[]} := 1$. Recall that F is a field of characteristic 2. The images of $\{t_\lambda \mid \lambda \text{ a partition}\}$ span a subalgebra of $\Lambda \bigotimes F$. We call this algebra the *involution class symbol algebra*. We do not know whether it is a polynomial algebra. In Theorem 8.9 we exhibit a set of algebraically independent involution class symbols. It is possible that these elements actually generate the involution class symbol algebra. In Section 9 we will show that a slightly larger subalgebra of $\Lambda \bigotimes F$ is a polynomial algebra.

Proposition 8.1. $t_n = (-1)^n \sum_{\lambda \vdash n} C_\lambda \, m_\lambda$.

Proof. The map that interchanges h_n and h_n* is an involutary automorphism of Λ. (But note that it does not preserve the bilinear form $<,>$.) It follows that

$$M(c,m) = M(h,h^*)^t = M(h^*,h)^t = M(m,c).$$

Thus

$$M(t,m)_{[n],\lambda} = M(c,m)_{[1^n],\lambda} = M(m,c)_{[1^n],\lambda} = M(e,c)_{[n],\lambda}.$$

The result now follows from Proposition 3.2. □

Set $D_n := \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix}$. Our interest in D_n is partially due to the next lemma.

Lemma 8.2. *Let* $C(x) = \sum_{n=0}^{\infty} (-1)^n C_n \, x^n$. *Then* $C'(x)/C(x) = \sum_{n=1}^{\infty} (-1)^n D_n \, x^{n-1}$.

Proof. The binomial theorem can be used to show that

$$C(x) = \frac{-1 + \sqrt{1+4x}}{2x}.$$

So $xC(x)^2 + C(x) - 1 = 0$. Differentiating, we get

$$\frac{C'(x)}{C(x)} = \frac{-C(x)}{1+2xC(x)} = \frac{1-\sqrt{1+4x}}{2x\sqrt{1+4x}} = \frac{(1+4x)^{-1/2}-1}{2x}.$$

The result follows from another application of the binomial theorem. □

Let $T(x) = \sum_{n \geq 0} t_n x^n$ and set $D(x) := T'(x)/T(x) = \sum_{n \geq 1} d_n x^{n-1}$. So $\{d_n\}$ are symmetric functions that satisfy

$$n \, t_n = \sum_{i=1}^{n} d_i \, t_{n-i}. \tag{8.3}$$

Recall that $p_n = m_n$. Our next result was inspired by Proposition 1.2 of [W].

Proposition 8.4. $d_n = (-1)^n D_n \, p_n$.

Proof. Clearly $T(x) = \prod_{i\geq 1} C(x_i x)$. So

$$\begin{aligned}\frac{T'(x)}{T(x)} &= \frac{d}{dx}\left[\ln T(x)\right] = \sum_{i=1}^{\infty} \frac{d}{dx}\left[\ln C(x_i x)\right] \\ &= \sum_{i=1}^{\infty} \frac{C'(x_i x)}{C(x_i x)}\, x_i = \sum_{i=1}^{\infty} D(x_i x)\, x_i, \quad \text{by Lemma 8.2} \\ &= \sum_{n=1}^{\infty} (-1)^n\, D_n\, p_n\, x^{n-1}.\end{aligned}$$

□

The above Proposition can be used to show that $\{t_n \mid n \geq 1\}$ is a set of algebraically independent generators of $\Lambda \bigotimes \mathbb{Q}$. We omit the details.

Next we determine the parity of D_n.

Lemma 8.5. *Let n be a positive integer. Then D_n is odd if and only if n is a power of 2.*

Proof. This follows from

$$\begin{aligned}\nu(D_n) &= \nu((2n-1)!) - \nu((n-1)!) - \nu(n!) \\ &= \nu((2n)!) - \nu(2n) - \nu(n!) + \nu(n) - \nu(n!) \\ &= (2n - \mathcal{L}(n)) - 2(n - \mathcal{L}(n)) - 1 \\ &= \mathcal{L}(n) - 1.\end{aligned}$$

□

This allows us to prove the following:

Corollary 8.6. *Then the involution class symbol algebra is generated by the images of $\{t_n \mid n \geq 1,\ n \text{ is even or } n = 1\}$ in $\Lambda \bigotimes F$.*

Proof. Suppose that $n \geq 0$. We use induction on n to show that

$$t_{2n+1} \equiv \sum_{i\geq 1} t_1^{2^i-1}\, t_{2n+2-2^i} \pmod 2.$$

If $n = 0$ this equality is trivial. So suppose that $n > 0$. Equation 8.3 and Proposition 8.4 imply that

$$(2n+1)\, t_{2n+1} = \sum_{i=1}^{2n+1} (-1)^i\, D_i\, p_i\, t_{2n+1-i}.$$

It then follows from Lemma 8.5 that

$$t_{2n+1} \equiv \sum_{i\geq 0} p_{2^i}\, t_{2n+1-2^i} \pmod 2.$$

But $p_{2^n} \equiv t_1^{2^n} \pmod 2$. So the inductive hypothesis gives

$$t_{2n+1} \equiv \sum_{i\geq 0} \sum_{j\geq 1} t_1^{2^i+2^j-1} t_{2n+2-2^i-2^j} \pmod 2.$$

Let $i \neq j$ be positive integers. The terms in the above sum arising from (i,j) and (j,i) are the same. So they cancel. We conclude that

$$\begin{aligned} t_{2n+1} &\equiv \sum_{i \geq 0} t_1^{2^i+2^{i-1}} t_{2n+2-2^i-2^i} \pmod 2 \\ &= \sum_{i \geq 1} t_1^{2^i-1} t_{2n+2-2^i}. \end{aligned}$$

□

Next we refine our knowledge of the parity of D_n.

Lemma 8.7. *Let n be a positive integer. Then $(D_n^2 - D_{2n})/2$ is an integer. This integer is odd if and only if n is a power of 2 or a sum of two distinct powers of 2.*

Proof. Since $\mathcal{L}(n) = \mathcal{L}(2n)$, it follows from Lemma 8.5 that D_n and D_{2n} have the same parity. In particular $(D_n^2 - D_{2n})/2$ is an integer.

Suppose that $\mathcal{L}(n) \geq 3$. Then $(D_n^2 - D_{2n})/2$ is even, since both D_n and D_{2n} are divisible by 4.

Suppose that $\mathcal{L}(n) = 2$. Then D_n and D_{2n} are congruent to 2 modulo 4. So D_n^2 is divisible by 4 and $(D_n^2 - D_{2n})/2$ is odd.

Finally, suppose that n is a power of 2. Then D_n is odd. So D_n^2 is congruent to 1 modulo 4. We prove that D_{2n} is congruent to 3 modulo 4 by induction. The base case is $D_2 = 3$. The inductive step follows from

$$\begin{aligned} D_{2n} &= \frac{(4n-1)(4n-3)\dots(4n-(2n-1))}{(2n-1)(2n-3)\dots(2n-(2n-1))} D_n \\ &\equiv \frac{(-1)(-3)\dots(-2n+1)}{(-1)(-3)\dots(-2n+1)} D_n \equiv D_n \pmod 4. \end{aligned}$$

We conclude that $(D_n^2 - D_{2n})/2$ is odd in this case. □

If α and β are partitions, let $\alpha \cup \beta$ denote the partition that is formed by arranging the parts of α and β in nonincreasing order.

If $|\alpha| = |\beta| = n$, write $\alpha \prec \beta$ if $l(\alpha) > l(\beta)$ or $l(\alpha) = l(\beta)$ and α precedes β in the reverse lexocographic order. Then $\prec$ is a total order and

(8.8)
(i) Every partition of n precedes $[n]$;
(ii) $[n^2]$ is the immediate predecessor of $[2n]$.

Moreover, if $\alpha, \beta, \gamma, \delta$ are partitions with $\alpha \prec \gamma$ and $\beta \prec \delta$, then $\alpha \cup \beta \prec \gamma \cup \delta$.

Suppose that n is 1 or an even integer. Define the partition

$$\epsilon(n) := \begin{cases} [n], & \text{if } n \text{ is a power of 2;} \\ [(n/2)^2], & \text{if } n \text{ is not a power of 2.} \end{cases}$$

For λ a partition with each part even or equal to 1, set

$$\epsilon(\lambda) := \bigcup_{i \geq 1} \epsilon(\lambda_i).$$

Then the map $\lambda \to \epsilon(\lambda)$ is injective.

We now prove the main result of this section.

Theorem 8.9. *Let F be a field of characteristic 2. Then*

$$\{t_n \mid \ n \text{ is a power of } 2 \text{ or a sum of two distinct even powers of } 2\}$$

is algebraically independent, when considered as a subset of $\Lambda \bigotimes F$.

Proof. Let $n \geq 1$. Then $M(t,h)_{[n],[n]} = M(c,h)_{[1^n],[n]} = (-1)^n D_n$, using Proposition 4.1. It then follows from Lemma 8.5, and (i) of (8.8), that, modulo 2,

$$(8.10) \quad t_n \equiv \begin{cases} h_n + \sum\{\text{certain } h_\mu \text{ with } \mu \prec [n]\}, & \text{if } n \text{ is a power of 2;} \\ \sum\{\text{certain } h_\mu \text{ with } \mu \prec [n]\}, & \text{otherwise.} \end{cases}$$

Now suppose that n is not a power of 2. We have $m_{[n^2]} = (p_{[n^2]} - p_{[2n]})/2$. So

$$\begin{aligned} M(t,h)_{[2n],[n^2]} &= M(c,h)_{[1^{2n}],[n^2]} = M(m,h^*)_{[n^2],[1^{2n}]} \quad \text{by (2.4)} \\ &= \left(M(p,h^*)_{[n^2],[1^{2n}]} - M(p,h^*)_{[2n],[1^{2n}]}\right)/2 \\ &= (D_n^2 - D_{2n})/2, \quad \text{using (4.3).} \end{aligned}$$

It then follows from Lemma 8.7, (ii) of (8.8), and (8.10), that, modulo 2,

$$(8.11) \quad t_n \equiv \begin{cases} h_{[(n/2)^2]} + \sum\{\text{certain } h_\mu \text{ with } \mu \prec [(n/2)^2]\}, \\ \qquad \text{if } n \text{ is a sum of two distinct even powers of 2;} \\ \sum\{\text{certain } h_\mu \text{ with } \mu \prec [(n/2)^2]\}, \quad \text{otherwise.} \end{cases}$$

Let λ be a partition, such that each part λ_i is a power of 2 or a sum of two even powers of 2. It follows from (8.10) and (8.11) that

$$t_\lambda \equiv h_{\epsilon(\lambda)} + \sum \{\text{certain } h_\mu \text{ with } \mu \prec \lambda\} \pmod 2.$$

The theorem now follows from the injectivity of ϵ. □

9. A polynomial subalgebra of the class symbol algebra

Recall that F is a field of characteristic 2. In this the final section we show that the smallest subalgebra of $\Lambda \bigotimes F$ that contains both the involution class symbol algebra and the 2-regular class symbol algebra is a polynomial algebra. We furnish it with a set of algebraically independent generators in Theorem 9.8. In view of Theorem 8.9, Corollary 9.10 provides evidence that the involution class symbol algebra is itself a polynomial algebra.

For any $\sigma \in S_\infty$, we may write $\sigma = \sigma_2 \sigma_{2'} = \sigma_{2'} \sigma_2$, where σ_2 has order a power of 2 and $\sigma_{2'}$ has odd order. We call σ_2 the *2-part* of σ, and $\sigma_{2'}$ the *2-regular part* of σ. The 2-regular parts of the elements of a class of S_∞ form a single 2-regular conjugacy class. We call the set of classes whose 2-regular parts lie in a given 2-regular class K the *2-regular section* of S_∞ that contains K.

Let λ be a partition and let $N \geq 1$. Extending the notion of a 2-partition, we call a partition λ a *2^N-partition* if

$$\lambda_i \not\equiv -1 \pmod{2^N}, \quad \text{for all } i \geq 1.$$

Then $\{c_\lambda \mid \lambda \text{ is a } 2^N\text{-partition}\}$ are the conjugacy classes of S_∞ whose elements have order not divisible by 2^N. It follows from (2.1), and the remark after Corollary 5 in [M], that these symbols form an F-basis for a subalgebra of $\Lambda \bigotimes F$. We call this algebra the *2^N-regular class symbol algebra.*

Let $\approx$ be the equivalence relation generated on the set of partitions by:

(i) If $n \geq 1$ then $[2n+1] \approx [n^2, 1]$;
(ii) If $\alpha, \beta, \gamma, \delta$ are partitions, with $\alpha \approx \gamma$ and $\beta \approx \delta$, then $\alpha \cup \beta \approx \gamma \cup \delta$.

Both of the following Lemmas are fairly obvious consequences of the definition of $\approx$.

Lemma 9.1. *Each $\approx$ equivalence classes contains a unique partition with all odd parts equal to 1.*

Lemma 9.2. *Let λ, μ be partitions of n. Then $\lambda \approx \mu$ if and only if c_λ and c_μ are contained in the same 2-regular section of S_∞.*

Following Farahat and Higman, we define

$$m(\sigma) := \sum (|N| - 1), \quad \text{for } \sigma \in S_\infty,$$

where N runs over all orbits of σ on $\mathbb{N}$. We call any expression $\sigma = \sigma_1 \dots \sigma_m$, where $\sigma_1, \dots, \sigma_m \in S_\infty$, and $\sum m(\sigma_i) = m(\sigma)$, a *minimal factorization* of σ. Every σ has a minimal factorization into transpositions. If N is an orbit of σ on $\mathbb{N}$, we will use σ^N for the element of S_∞ that agrees with σ on N, and fixes all element of $\mathbb{N} \backslash N$. So $\sigma^N \in S_M$, where $M = \max_{i \in N} i$.

The next two lemmas can be deduced from Lemma 3.5 of [FH].

Lemma 9.3. *Let $\sigma = \sigma_1 \dots \sigma_m$ be a minimal factorization of σ. Then each orbit of σ is a union of orbits of the σ_i.*

Lemma 9.4. *Let $\sigma = \sigma_1 \dots \sigma_m$ be a minimal factorization of σ. Suppose that N is a union of orbits of σ. Then $\sigma^N = \sigma_1^N \dots \sigma_m^N$ is a minimal factorization of σ^N.*

We also need a technical lemma that concerns the multiplication of the class symbols c_μ. Let $\{\mu^i\}$ be a sequence of partitions with $\sum |\mu^i| = n$. We may write

$$\prod c_{\mu^i} = \sum_{\lambda \vdash n} |P(\{c_{\mu^i}\}; c_\lambda)|\, c_\lambda,$$

where, for σ a fixed element of c_λ,

$$P(\{c_{\mu^i}\}; c_\lambda) = \{(\sigma_1, \sigma_2, \dots) \in c_{\mu^1} \times c_{\mu^2} \times \cdots \mid \prod \sigma_i = \sigma\}.$$

Lemma 9.5. *Suppose that $\lambda = \alpha \cup \beta$, where α and β are partitions. Then*

$$|P(\{c_{\mu^i}\}; c_\lambda)| = \sum |P(\{c_{\rho^i}\}; c_\alpha)| \times |P(\{c_{\nu^i}\}; c_\beta)|,$$

where $(\{\rho^i\}; \{\nu^i\})$ range over all pairs of sequences of partitions for which $\rho^i \cup \nu^i = \mu^i$, for all $i \geq 1$, and $\sum |\rho^i| = |\alpha|$ and $\sum |\nu^i| = |\beta|$.

Proof. We demonstrate a bijection

$$P(\{c_{\mu^i}\}; c_\lambda) \longleftrightarrow \bigcup P(\{c_{\rho^i}\}; c_\alpha) \times P(\{c_{\nu^i}\}; c_\beta).$$

Let $\sigma \in c_\lambda$. Then there exists a partition $\mathbb{N} = N \cup M$, with $N^\sigma = N$ and $M^\sigma = M$, such that $\sigma^N \in c_\alpha$ and $\sigma^M \in c_\beta$. Suppose that $(\sigma_i) \in P(\{c_{\mu^i}\}; c_\lambda)$. Then $\sigma_i = \sigma_i^N \sigma_i^M$ for $i \geq 1$, and $\sigma^N = \prod \sigma_i^N$ and $\sigma^M = \prod \sigma_i^M$, using Lemma 9.4. Now $\sigma_i^N \in c_{\rho^i}$ and $\sigma_i^M \in c_{\nu^i}$, for some partitions ρ^i, ν^i. Clearly $\rho^i \cup \nu^i = \mu^i$ and $(\sigma_i^N) \in P(\{c_{\rho^i}\}; c_\alpha)$ and $(\sigma_i^M) \in P(\{c_{\nu^i}\}; c_\beta)$. The map

$$(\sigma_i) \longrightarrow ((\sigma_i^N), (\sigma_i^M))$$

is reversible. This establishes the required bijection, and completes the proof. $\square$

We now concentrate on 4-partitions. Let ν be a 4-partition. Set

$$k_\nu := \sum \{ c_\mu \mid \mu \text{ is a 4-partition of } |\nu| \text{ and } \mu \approx \nu \}. \tag{9.6}$$

The first example where $k_\nu \neq c_\nu$ occurs with $\nu = [5]$. Then $k_{[5]} = c_{[5]} + c_{[2^2,1]}$.

Proposition 9.7. *Let F be a field of characteristic 2. Let λ be a partition and let μ be a 2-partition. Then the product $t_\lambda c_\mu$ lies in the F-span of*

$$\{k_\nu \mid \nu \text{ is a 4-partition of } |\lambda| + |\mu|\}.$$

Proof. Since $[1^n]$ and μ are 4-regular, it follows that $t_\lambda c_\mu$ is contained in the 4-regular class symbol algebra. Also, if α and β are partitions with $\alpha \cup \beta = [1^n]$, then $\alpha = [1^m]$ and $\beta = [1^{n-m}]$, for some m. Similarly, if $\alpha \cup \beta = \mu$, then both α and β are 2-regular. Using Lemma 9.5, and the definition of $\approx$, it is enough to show that

$$|P(t_\lambda, c_\mu; c_{[4n+1]})| \equiv |P(t_\lambda, c_\mu; c_{[(2n)^2,1]})| \pmod 2,$$

whenever $|\lambda| + |\mu| = 4n+1$, for some $n \geq 0$. This follows from Claim 1 and Claim 2 below. □

Claim 1. Let $|\lambda| + |\mu| = 4n+1$. We claim that either $P(t_\lambda, c_\mu; c_{[4n+1]})$ has even cardinality or there is a unique $j \geq 1$ such that λ_j is odd, in which case

$$|P(t_\lambda, c_\mu; c_{[4n+1]})| \equiv |P(t_{\lambda_1}, \ldots, t_{\lambda_j - 1}, \ldots, c_\mu\}; c_{[(2n)^2]})| \pmod 2.$$

Proof. Let $\sigma \in S_\infty$ have modified cycle type $[4n+1]$. We may assume that $\sigma \in S_{4n+2}$. Then σ has a single orbit on $\{1, \ldots, 4n+2\}$. Now $|\mu|$ is even, since all parts of μ are even, while $4n+1$ is odd. It follows that λ_j is odd, for some $j \geq 1$. By a slight abuse of notation, we may assume that λ_1 is odd.

Let $a = \sigma^{2n+1}$. Then $a \in t_{[2n+1]}$ is an involution. Moreover, a generates a Sylow 2-subgroup of the centralizer of σ in S_{4n+2}. There exists $b \in t_{[2n]}$ that inverts σ. Clearly $K =< a, b >$ is elementary abelian of order 4. Assume that $4n+1, 4n+2$ are the unique symbols fixed by b. Then K acts without fixed points on $\{1, \ldots, 4n\}$.

Let $(\{\sigma_i\}, h) \in P(t_\lambda, c_\mu; c_{[4n+1]})$. For $i \geq 1$, set $b_i := \sigma_{i-1}\sigma_{i-2}\ldots\sigma_2\sigma_1 b$. Define

$$\begin{aligned} (\{\sigma_i\}, h)^a &= (\{\sigma_i^a\}, h^a) \\ (\{\sigma_i\}, h)^b &= (\{\sigma_i^{b_i}\}, (h^{-1})^{\sigma^{-1}b}). \end{aligned}$$

A long but routine check establishes that both $(\{\sigma_i\}, h)^a$ and $(\{\sigma_i\}, h)^b$ are elements of $P(t_\lambda, c_\mu; c_{[4n+1]})$, and that this induces an action of the group K on $P(t_\lambda, c_\mu; c_{[4n+1]})$. This generalization of the Brauer homomorphism was discovered by R. Gow. See [G] for further details.

Since K is a 2-group, the cardinality of the set $P(t_\lambda, c_\mu; c_{[4n+1]})$ is equivalent, modulo 2, to the number of ordered tuples $(\{\sigma_i\}, h) \in P(t_\lambda, c_\mu; c_{[4n+1]})$ such that $\sigma_i^a = \sigma_i$, $\sigma_i^{b_i} = \sigma_i$, for all $i \geq 1$, and $h^a = h$ and $h^{b\sigma} = h^{-1}$.

Assume that there is such a tuple $(\{\sigma_i\}, h)$. Then $\sigma_1 \in t_{\lambda_1}$, and $\sigma_1^a = \sigma_1$ and $\sigma_1^b = \sigma_1^{b_1} = \sigma_1$. The 4-group K has n orbits on $\{1, \ldots, 4n\}$, and it acts regularly on each orbit. Let x be one of these orbits. Since $\sigma_1 \in C(K)$, either σ_1 fixes each element of x, or σ_1 fixed no element of x. We deduce that the number of elements of $\{1, \ldots, 4n\}$ that are fixed by σ_1 is divisible by 4. But

$$\lambda_1 = (4n + 2 - \#\{\text{fixed points of } \sigma_1\})/2.$$

Since λ_1 is odd, it follows that σ_1 contains the transposition $(4n+1, 4n+2)$ in its cycle decomposition. Now $\prod \sigma_i h = \sigma$ is a minimal factorization of σ. So

$(4n+1, 4n+2)$ can only occur in the cycle decomposition of σ_1. We deduce that λ_i is even for $i \geq 2$. Also $(4n+1, 4n+2)\sigma$ has modified cycle type $[(2n)^2]$, and $(4n+1, 4n+2)\sigma_1 \in t_{\lambda_1 - 1}$. Claim 1 follows easily from this. $\square$

Claim 2. Let $|\lambda| + |\mu| = 4n+1$. We claim that either $P(t_\lambda, c_\mu; c_{[(2n)^2,1]})$ has even cardinality or there is a unique $j \geq 1$ such that λ_j is odd, and that

$$|P(t_\lambda, c_\mu; c_{[(2n)^2,1]})| \equiv |P(t_{\lambda_1}, \ldots, t_{\lambda_j - 1}, \ldots, c_\mu\}; c_{[(2n)^2]})| \pmod 2.$$

Proof. As in Claim 1, we may assume that λ_1 is odd. Let $\sigma \in S_\infty$ have modified cycle type $[(2n)^2, 1]$. We may assume that $\sigma \in S_{4(n+1)}$ and that $x = \{1, \ldots, 2n+1\}$, $y = \{2n+2, \ldots, 4n+2\}$ and $z = \{4n+3, 4n+4\}$ are the 3 orbits of σ. Let $a \in t_{2n+1}$ be an involution that centralizes σ. So a interchanges the elements of x and y, and fixes both elements of z.

Suppose that $P(t_\lambda, c_\mu; c_{[(2n)^2,1]})$ has odd cardinality. By an argument simpler than that used in Claim 1, there exists $(\{\sigma_i\}, h) \in \prod t_{\lambda_i} \times c_\mu$ with $\prod \sigma_i h = \sigma$, and $\sigma_i^a = \sigma_i$, for all $i \geq 1$, and $h^a = h$. Let $j \in x$. Set $k = a(j)$. Suppose that $\sigma_1(j) \neq j$. Then $\sigma_1(k) = a(\sigma_1(j)) \neq k$. Also $k \in y$. We deduce that the cycle decomposition of σ_1 contains the pair of transpositions $(j, \sigma_1(j))(k, \sigma_1(k))$. As σ_1 has an odd number λ_1 of transpositions in its cycle decomposition, it follows that σ_1 contains the transposition $(4n+3, 4n+4)$. The proof of Claim 2 now proceeds along the same lines as that of Claim 1. $\square$

We now prove the main result of this section.

Theorem 9.8. *Let F be a field of characteristic 2. Then the smallest subalgebra of $\Lambda \bigotimes F$ that contains the involution class algebra and the 2-regular class algebra coincides with the F-span of $\{ k_\nu \mid \nu$ is a 4-partition$\}$. This algebra is a polynomial algebra with algebraically independent generating set*

$$\{t_n \mid n \geq 1 \text{ is a power of } 2\} \cup \{h_n^2 \mid n \geq 1 \text{ is not a power of } 2\}.$$

Proof. It follows from (8.10) that the images of the elements of $\{t_n \mid \mathcal{L}(n) = 1\} \cup \{h_n^2 \mid \mathcal{L}(n) > 1\}$ form an algebraically independent set in $\Lambda \bigotimes F$.

Let A be the subalgebra of $\Lambda \bigotimes F$ generated by the involution class symbol algebra and the 2-regular class symbol algebra. Let Λ_n be the $\mathbb{Z}$-span of $\{ c_\lambda \mid \lambda \vdash n \}$. For λ a partition, and $i \geq 1$, recall that $a_i(\lambda)$ denotes the multiplicity of i as a part of λ. The first paragraph shows that $\dim_F(A \cap \Lambda_n)$ is not smaller than the cardinality of the set

$$\{\lambda \vdash n \mid \mathcal{L}(i) = 1 \text{ or } a_i(\lambda) \text{ is even, for each } i \geq 1\}.$$

There is an obvious bijection between this set and the set

$$\{\nu \vdash n \mid \text{all odd parts of } \nu \text{ equal } 1\}.$$

This bijection sends $\lambda \to \nu$, where

$$a_i(\nu) = \begin{cases} a_i(\lambda), & \text{if } i \text{ is a power of 2;} \\ 0, & \text{if } i > 1 \text{ is odd;} \\ a_{i/2}(\lambda)/2, & \text{otherwise.} \end{cases}$$

It now follows from Proposition 9.7 and Lemma 9.1 that A coincides with the F-span of $\{ k_\nu \mid \nu$ is a 4-partition$\}$. Moreover, A is generated by the elements of $\{t_n \mid \mathcal{L}(n) = 1\} \cup \{h_n^2 \mid \mathcal{L}(n) > 1\}$. This completes the proof of the theorem. $\square$

Note 9.9. *A similar argument shows that*

$$\{t_{2^n} \mid n \geq 0\} \cup \{t_{2^n+2^m} \mid n > m > 0\} \cup \{h_n^2 \mid n \geq 1, \mathcal{L}(n) > 2\}$$

also form a set of algebraically independent generators for the F-algebra spanned by $\{k_\nu \mid \nu$ is a 4-partition$\}$.

Corollary 9.10. *t_{14} lies in the F-algebra generated by $t_1, t_2, t_4, t_6, t_8, t_{10}, t_{12}$.*

Proof. We have $\mathcal{L}(14) = 2$. Note 9.9 implies that t_{14} can be written as an F-polynomial in $\{t_1, t_2, t_4, t_8\} \cup \{t_6, t_{10}, t_{12}\} \cup \{h_{7^2}\}$. However (8.10) and (8.11) show that $M(t,h)_{\lambda,[7^2]} = 0$, for each partition λ of 14. The result follows immediately from this. □

10. Acknowledgement

I thank Arun Ram for alerting me to the existence of Farahat and Higman's results, and for providing me with a copy of Jucys's paper. Thanks are also due to the organizers of the Representations of Finite Groups meeting held at the Mathematisches Forschungsinstitut Oberwolfach, in March 2001.

References

[FH] H. K. Farahat, G. Higman, *The centres of symmetric group rings,* Proc. Royal Soc. London (A) 250 (1959), 212–221.

[G] R. Gow, *Real 2-blocks of characters of finite groups*, Osaka J. Math. 25 (1988), 135–147.

[J] A. -A. A. Jucys, *Symmetric polynomials and the center of the symmetric group ring,* Rep. Math. Phy. 5 (1974), 107–112.

[LT] A. Lascoux, J. Y. Thibon, *Vertex operators and the class algebras of symmetric groups,* Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 283 (2001), Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 6, 156–177, 261.

[Mac] I. G. Macdonald, *Symmetric Functions and Hall Polynomials,* Second Ed., Clarendon Press, Oxford, 1995.

[Mpy] G. E. Murphy, *The idempotents of the symmetric group and Nakayama's conjecture*, J. Algebra 81 (1983), 258–265.

[M] J. Murray, *Squares in the centre of the group algebra of a symmetric group,* Bull. London Math. Soc. 34 (2002), no. 2, 155–164.

[NT] H. Nagao, Y. Tsushima, *Representations of Finite Groups*, Academic Press, Inc., Boston MA, 1989.

[W] G. Walker, *Modular Schur functions,* Trans. Amer. Math. Soc. 346 (1994), 569–604.

Mathematics Department, National University of Ireland, Maynooth, Co. Kildare, Ireland

E-mail address: jmurray@maths.may.ie