Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 37 (1996), No. 1, 103-118.

Blocks for Symmetric Groups and their Covering Groups and Quadratic Forms

Karin Erdmann and **Gerhard O. Michler**

Mathematical Institute, Oxford University
24-29 St. Giles, Oxford OX1 3LB, England

Institut für Experimentelle Mathematik, University of Essen
Ellernstr. 29, D-45326 Essen, Germany

Introduction.

Let p be a prime number, K a field of characteristic p and let $\mathcal{S}_n$ be the group of permutations of degree n. We are interested in the p-blocks of the group algebra $K\mathcal{S}_n$. It is conjectured that for $p \geq 5$ and all n the group algebra $K\mathcal{S}_n$ has p-blocks of all possible defects; that is of any defect d where p^d divides $n!$. This is equivalent to the conjecture that for all n the group algebra $K\mathcal{S}_n$ has a p-block of defect zero, see [5], [6]. It appears to be folklore that the existence of blocks of defect zero should be true for large n, and this is supported by work of [4], [1], [2] by means of modular forms. We consider an elementary approach which is motivated by representation theory.

It is well-known that the irreducible characters of $\mathcal{S}_n$ are parametrized by partitions of n; and moreover the "Nakayama conjecture" holds: Irreducible characters χ^λ and χ^μ belong to the same p-block if and only if λ and μ have the same p-core, see [3; 6.1.42]. In particular χ^λ belongs to a block of defect zero if and only if λ is a p-core. One of the (combinatorial) tools to study p-modular representations of symmetric groups is to represent partitions on an abacus with p runners, see Ch. 1 or [3; 2.7]. In fact one of the possible proofs of the Nakayama conjecture uses the abacus representation. More recently it was proved in [9] that the number of Morita equivalence classes of p-blocks of symmetric groups with a fixed defect group is finite; for this work the abacus representation was crucial. (This was one of our motivations.)

Here we study p-blocks of defect zero, by exploiting the abacus method. Our work is aimed at giving an elementary approach to the existence conjecture, and to show how this is related to problems of representing integers as sums of squares. Suppose a partition is represented on an abacus with p runners. Then it belongs to a p-block of defect zero if and only if it is not possible to move a bead upwards on its runner. Hence the abaci representing a p-core are completely characterized by the set of p-tuples of integers ≥ 0 giving the number of beads per column. (For a list without repetitions one may take p-tuples where the first number is zero, which corresponds to the abacus with first column being empty, that is, the beads represent the first column-hook lengths.)

The problem is that for such a partition it is not obvious which integer N it represents. Our first result is to determine closed formulae for the number N, each formula is a sum of a quadratic form and a linear form. The variables are the number of beads per column. (As a Corollary we also get the form representing N of [2].)

Then we discuss change of variables and we use an orthogonal system of variables to prove that the conjecture holds for p = 5 and p = 7.

We also consider spin blocks, by a similar approach. The same question arises, namely for which n does a covering group $\hat{\mathcal{S}}_n$ of $\mathcal{S}_n$ have a spin block over characteristic p of defect zero. It was proved in [7] that the spin blocks of a covering group $\hat{\mathcal{S}}_n$ can be parametrized by "p-bar cores" which are certain partitions of n. Moreover, p-bar partitions λ may also be represented on an abacus in a way such that Λ is a p-bar core if and only if it is not possible to slide a bead upwards on a runner and in addition either column i or column p_i is empty. However, the rule for representing a partition is different here; for details see [7].

For a p-bar partition λ with a given abacus representation we determine a closed form for the integer n with $\lambda \vdash n$. This is also the sum of a quadratic form and a linear form. We are able to get a complete answer for spin cores when $p = 5$ and $p = 7$. For $p = 5$ there are exceptions, and we have a complete characterization of integers n such that $\hat{\mathcal{S}}_n$ has a 5-spin block of defect zero, see 2.1. If $p = 7$ then for every n, the covering group $\hat{\mathcal{S}}_n$ has 7-spin blocks of defect zero (and hence spin blocks of all possible defects).

Our results for spin blocks are new. Moreover it seems that methods using modular forms cannot be used here in the same way as for symmetric groups.

In Chapter 1 we describe the abacus representations of partitions and determine the quadratic and linear forms. In the second chapter we deal with spin cores. In Chapter 3 we describe the diagonalization and in Chapter 4 we study p-cores of symmetric groups for $p = 5$ and $p = 7$. The last section contains the number theoretic results.

1. Preliminaries

1.1 Let λ be a partition of n, so $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, where the λ_i are non-negative decreasing integers whose sum is n. Take an integer $s \geq k$ and set $\lambda_m = 0$ for $k+1 \leq m \leq s$ then the s-element set of β-numbers for λ is by definition the set $\{\beta_1, \beta_2, \ldots, \beta_s\}$ where

$$\beta_i = (\lambda_i - i) + s.$$

$(1 \leq i \leq s)$, see [3; 2.7]. Thus $\beta_1 > \beta_2 \ldots > \beta_s \geq 0$ and the the partition λ may be reconstructed from the set of β-numbers, for any such s.

Fix a positive integer p (which at the moment need not be a prime). We wish to represent λ on an abacus with p runners. The runners, which go vertical (and which we also call columns) are labelled $0, 1, \ldots, p-1$. The rows of the abacus are numbered $1, 2, \ldots$ A bead placed at position (j, i) where $0 \leq i \leq p-1,\ 1 \leq j$ represents the number $(j-1)p + i$.

An abacus display for λ with s beads, where $s \geq k$, is an abacus which represents the s-element set of β-numbers for λ. Observe that given an abacus display, one can reconstruct λ. Namely, λ_i is equal to the total number of gaps before the i-th bead. In particular, the last part of λ is non-zero if and only if there is no bead at position zero.

A partition is a p-core if and only it is not possible to slide a bead up on its runner, in some abacus display; if so then this holds in all possible abacus displays. Hence an abacus display of a p-core may be identified with a p-tuple

$$\Gamma = (y_0, y_1, \ldots, y_{p-1})$$

where y_i is the number of beads on the i-th runner.

For example, let $p = 5$ and $\lambda = (4, 1^2)$. The abacus display on an abacus with three beads is identified with $\Gamma = (0, 2, 1, 0, 0)$. If we take four beads then we get $\Gamma = (1, 0, 2, 1, 0)$.

In general, we identify the core with any such Γ. In particular taking all such abacus displays where the runner 0 is empty gives a bijection between all p-cores and the set of all p-tuples $\vec{y} = (0, y_1, \ldots, y_{p-1})$ with $y_i \geq 0$.

1.2 Now assume that p is a prime number. We consider p-blocks of the group algebra $\mathcal{S}_n$. As usual, we say that a partition λ belongs to a p-block if the irreducible character χ^λ parametrized by λ belongs to this block. It is well-known that the partitions λ, μ belong to the same p-block if and only if they have the same p-core; this is the Nakayama conjecture. In particular, a partition represents a block of defect zero if and only if it is a p-core. Hence there is a bijection between blocks of defect zero and p-cores.

1.3 We fix a prime p. Suppose $n \in \mathbf{N}$, then we say that n is an abacus number if there is an abacus which is a p-core representing n.

1.4 We describe now some abacus operations. Suppose $\Gamma = (y_0, y_1, \ldots, y_{p-1})$ is a core abacus representing n. Then n is also represented by the core abacus

$$(y_{p-1} + 1, y_0, \ldots, y_{p-2}).$$

We have the following general result which we will use later.

1.5 Lemma *Suppose the integer n has an abacus representation $\Gamma = (0, y_1, \ldots, y_{p-1})$. Then $n + y_{p-1} + 1$ also is an abacus number, represented by the abacus*

$$(y_{p-1} + 1, 0, y_1, \ldots, y_{p-2}).$$

In particular if such Γ exists with $y_{p-1} = 0$ then $n + 1$ is an abacus number.

Proof. The abacus given represents the same integer as the abacus $\Gamma' = (y_{p-1} + 1, 0, y_1, \ldots, y_{p-2})$. Moving all beads of the first column to the right gives a core abacus representing $n + y_{p-1} + 1$.

1.6 Proposition *Let N be the integer which is represented by the abacus $\Gamma = (y_0, y_1, y_2, \ldots, y_{p-1})$. Then*

$$(*) \qquad N = \frac{p}{2}\sum_{i=0}^{p-1} y_i^2 + \sum_{i=0}^{p-1} iy_i - \frac{s(s+p-1)}{2}\ .$$

Alternatively, $N = q(\vec{y}) + \ell(\vec{y})$ where
(i) $q(\vec{y}) = \frac{p-1}{2}(\sum_{i=0}^{p-1} y_i^2) - \frac{1}{2}\sum_{i\neq j} y_i y_j$ *and*
(ii) $\ell(\vec{y}) = \sum_{i=0}^{p-1}(i - \frac{p-1}{2})y_i$.

Proof. Recall that the l-th bead in Γ which is in the k-th row and the i-th column represents the β-number

$$\beta_l = (\lambda_l - l) + s$$

so that $(\lambda_l - l) + s = (k-1)p + i$, for $1 \leq l \leq s$ (see 1.1).
Consider a fixed column Γ_i of Γ. We have

$$\sum_{\beta_l \in \Gamma_i} (\lambda_l - l) = \sum_{k=1}^{y_i}((k-1)p + i - s) = (y_i - 1)y_i p/2 + iy_i - sy_i.$$

It follows that

$$\sum_{l=1}^{s} \lambda_l = \sum_{l=1}^{s}(\lambda_l - l) + \sum_{l=1}^{s} l = (\sum_{i=0}^{p-1}\sum_{\beta_l \in \Gamma_i}(\lambda_l - l)) + s(s+1)/2$$

and by the above this is equal to

$$(\sum_{i=0}^{p-1}((y_i - 1)y_i p/2 + iy_i - sy_i)) + s(s+1)/2$$

$$= ((p/2)\sum_{i=0}^{p-1} y_i^2) + (\sum_{i=0}^{p-1} y_i i) - (\sum y_i)((p/2) + s) + s(s+1)/2$$

and since $\sum y_i = s$ the last two terms give $-s(s+p-1)/2$.
To obtain the alternative formula, one substitutes $s = \sum_{i=0}^{p-1} y_i$.

1.6.1 *Remark* In [2], a different quadratic form for the abacus numbers was obtained. This formula follows easily from 1.6.

Take an abacus Γ as in 1.6 where s is chosen such that $y_i > 0$ for all i and also that $s = \bar{s}p$ for some $\bar{s} \in \mathbf{N}$. Now define $n_i := y_i - \bar{s}$; then clearly $\sum_{i=0}^{p-1} n_i = 0$. Substituting these n_i into 1.6 $(*)$ gives that

$$N = (p/2)\sum_{i=0}^{p-1} n_i^2 + \sum_{i=0}^{p-1} in_i.$$

1.7 We complete squares in the formula $(*)$ of 1.6. We get

$$\frac{p}{2}(y_i^2 + \frac{2iy_i}{p}) = \frac{(py_i+i)^2}{2p} - \frac{i^2}{2p}\,.$$

Using the standard formula for sums of squares gives

$$N = \frac{1}{2p}\sum_{i=0}^{p-1} z_i^2 - \frac{(p-1)(2p-1)}{12} - \frac{s(s+p-1)}{2} \qquad (1.7\,*)$$

where $z_i = py_i + i$.

1.8 Now we will determine a quadratic form for p-bar cores of spin blocks, for covering groups of symmetric groups. It was proved in [7], that spin blocks also may be parametrized by p-cores, but of a slightly different kind. Here one represents the parts of a partition on the abacus with p runners (instead of β-numbers). The p-cores are then exactly those partitions which are represented as follows:

(i) The position 0 of the abacus is empty;
(ii) It is not possible to slide a bead up its runner;
(iii) For $1 \le j \le p-1$, at least one of column j or column $p-j$ is empty.

We say that n is a bar abacus number if there is such an abacus which is a p-core representing n.
We identify such a core with a p-tuple

$$\Gamma = (0, l_1, \ldots, l_{p-1})$$

with $l_j l_{p-j} = 0, 1 \le j \le p-1$. Noting that here a bead of the abacus represents some part of λ we get that λ is a partition of N where

$$N = \sum_{i=1}^{p-1}((l_i-1)l_ip/2 + l_ii) = (p/2)\sum_{i=1}^{p-1} l_i^2 + \sum_{i=1}^{p-1} l_i(i-(p/2)).$$

1.8.1 We complete squares. First we have

$$(p/2)l_i^2 + l_i(i-p/2) = \frac{1}{8p}(2pl_i + (2i-p))^2 - \frac{1}{8p}(2i-p)^2.$$

This gives the formula

$$N = 1/8p\sum_{i=1}^{p-1}(2pl_i + (2i-p))^2 - (p-1)(p-2)/24.$$

But then since $l_i l_{p-i} = 0$ half of the terms are always zero. Therefore we prefer the following alternative: Set

$$X_i = \begin{cases} 2pl_i + (2i - p) & l_i \neq 0 \\ 2pl_{p-i} + (p - 2i) & l_i = 0 \end{cases}$$

and then

$$N = \frac{1}{8p} \sum_{i=1}^{(p-1)/2} X_i^2 - \frac{(p-1)(p-2)}{48}\,.$$

2. Abacus numbers for spin blocks when p = 5 and p = 7.

Assume first that $p = 5$ where $\operatorname{char} K = 5$. Then the group algebra $K\hat{\mathcal{S}}_n$ may or may not have spin blocks of defect zero. Our result gives a complete answer when this is the case.

2.1 Theorem *Let $G = \hat{\mathcal{S}}_n$. Then the following are equivalent.*
(a) *G has a 5-spin block of defect zero.*
(b) *There are integers X, Y such that $10(4n + 1) = X^2 + Y^2$.*
(c) *Each prime factor r of $10(4n + 1)$ with $r \equiv 3$ (mod 4) occurs to an even power as a factor of $10(4n + 1)$.*

Proof. It is well-known that (b) and (c) are equivalent, see for example [8; 9.2]. We will establish the equivalence of (a) and (b).

Recall that the 5-bar cores are in 1–1 correspondence with 5-tuples of integers $\Gamma = (0, l_1, l_2, l_3, l_4)$ such that $l_i \geq 0$ and $l_1 l_4 = 0 = l_2 l_3$. Given such Γ, it corresponds to a spin block of defect zero of $\hat{\mathcal{S}}_n$ where

$$n = 1/40(X_1^2 + X_2^2) - 1/4, \quad X_i = \begin{cases} 10l_i + (2i - 5), & l_i \neq 0 \\ 10l_{5-i} + (5 - 2i), & l_i = 0 \end{cases}$$

Hence (a) is true if and only if there is a solution of

$$10(4n + 1) = X^2 + Y^2$$

where $X \equiv \pm 3$ (mod 10) and $Y \equiv \pm 1$ (mod 10). The proof is therefore complete if we show that

2.2 *Suppose n is an integer such that the equation $10(4n+1) = X^2 + Y^2$ has a solution in integers. Then there is also a solution where $X \equiv \pm 3$ (mod 10) and $Y \equiv \pm 1$ (mod 10).*

Proof. By 5.2 (with $m = 5(4n + 1)$) there are integers X, Y which are $\not\equiv 0$ (mod 5) satisfying

$$10(4n + 1) = X^2 + Y^2.$$

Then X, Y must be odd. Since the numbers are $\not\equiv 5 \pmod{10}$ they can only be $\equiv \pm 1$ or $\pm 3 \pmod 5$. Suppose X, Y are both $\equiv \pm 1 \pmod{10}$, say, then $X^2 + Y^2 \equiv 2 \pmod{10}$, a contradiction. Hence, without loss of generality $X \equiv \pm 3 \pmod{10}$ and $Y \equiv \pm 1 \pmod{10}$, as required.

Now we consider the case when $p = 7$. Here we have the following result.

2.3 Theorem *Let $G = \hat{\mathcal{S}}_n$ for $n \geq 1$. Then G has always at least one 7-spin block of defect zero.*

Proof. Let $n \geq 1$. We must show that there is a 7-bar core λ with $\lambda \vdash n$. That is, we require some $\Gamma = (0, l_1, \ldots, l_6)$ with $l_i \geq 0$ and $l_i l_{7-i} = 0$ and

$$n = N(\Gamma) = \frac{1}{56}\sum_{i=1}^{3} X_i^2 - \frac{30}{48}, \quad X_i = \begin{cases} 14l_i + (2i-7) & l_i \neq 0 \\ 14l_{7-i} + (7-2i) & \text{otherwise} \end{cases}$$

Such Γ exists if and only if the equation

$$(*) \qquad 56n + 35 = \sum_{i=1}^{3} X_i^2$$

has integer solutions X_i such that $X_1 \equiv \pm 5 \pmod{14}$, $X_2 \equiv \pm 3 \pmod{14}$ and $X_3 \equiv \pm 1 \pmod{14}$.

Since $56n+35$ is not of the form $4^a(8b+7)$ we know that $(*)$ has integer solutions. By 5.3 there is also a solution where the X_i^2 are $\equiv 1, 2, 4 \pmod 7$. So we may set $X_1 = 7x+5$, $X_2 = 7y + 3$ and $X_3 = 7z + 1$. Since $56n + 35 \equiv 3 \pmod 8$, the X_i are odd and hence x, y, z are even. This completes the proof.

3. Diagonalization

Let k be a positive integer, and let $z_1, z_2, \ldots, z_k$ be indeterminates. Consider the quadratic form

$$q(\vec{z}) = m(\sum_{i=1}^{k} z_i^2) - (1/2)(\sum_{i\neq j} z_i z_j)$$

where m is a non-zero integer. Let A be the corresponding symmetric matrix. Then A has eigenvalues

$$\lambda_1 = m - (k-1)/2, \quad \lambda_2 = \lambda_3 = \ldots \lambda_k = m + (1/2).$$

(An eigenvector for eigenvalue λ_1 is given by $(1, 1, \ldots, 1)^t$, and eigenvectors for the other eigenvalues are for example $(1, 0, \ldots, -1, 0, \ldots)$.) We assume that the λ_i are non-zero; and we are interested in the case when k is a 2-power, say $k = 2^d$.

3.1 Under these hypotheses, it is easy to diagonalize the quadratic form over $\mathbf{Q}$. Namely there is a symmetric integral matrix P whose columns are orthogonal eigenvectors of A, and where all entries of P are ± 1. (For example, one may take the character table of an elementary abelian 2-group.) As a convention, we take $(1, 1, \dots, 1)$ as the first row of P. It follows that $P^2 = P^t P = 2^d I$. We change variables; let $\vec{w} = \vec{z}P$; so that $\vec{z} = 2^{-d}(\vec{w}P)$; then it is clear that

$$q(\vec{w}) = 2^{-d}(\sum_{i=1}^{k} \lambda_i w_i^2).$$

3.2 We consider now a linear form $\ell(\vec{z}) = a_1 z_1 + a_2 z_2 + \dots a_k z_k$ with $a_i \in \mathbf{Z}$. We wish to express $\ell(\vec{z})$ in terms of the variables w_i in 3.1. Suppose $\vec{p_i}$ is the i-th row vector of P for $1 \leq i \leq k$ and let $\vec{a} = (a_1, \dots, a_k)$. Then it follows easily that

$$\ell(\vec{w}) = 2^{-d}(\sum_{i=1}^{k} \mu_i w_i)$$

where $\mu_i = \langle \vec{a}, \vec{p_i} \rangle$. Here $\langle -, - \rangle$ is the usual inner product on $\mathbf{R}^k$.

Consider the number $C := \sum_{i=2}^{k} \mu_i^2$ (we will need it later.) We claim that $C = [2^d(\sum_{i=1}^{k} a_i^2)] - (\sum_{i=1}^{k} a_i)^2$. This holds because

$$\sum_{i=1}^{k} \mu_i^2 = \langle (\mu_i), (\mu_i) \rangle = \langle \vec{a}P, \vec{a}P \rangle = \langle \vec{a}P^2, \vec{a} \rangle = 2^d \langle \vec{a}, \vec{a} \rangle,$$

and $\mu_1 = \sum_{i=1}^{k} a_i$; recall that $\vec{p_1} = (1, 1, \dots, 1)$.

3.3 Consider now the function $N : \mathbf{Z}^k \to \mathbf{Z}$ given by $N(\vec{z}) = q(\vec{z}) + \ell(\vec{z})$. We change variables as described above and obtain

$$N(\vec{w}) = q(\vec{w}) + \ell(\vec{w}) = 2^{-d}(\sum_{i=1}^{k} \lambda_i w_i^2 + \sum_{i=1}^{k} \mu_i w_i).$$

Recall that the eigenvalues $\lambda_2, ..., \lambda_k$ are all equal, set $\lambda = \lambda_2$. Now define

$$(*) \qquad N_1 = 2^{-d}(\lambda_1 w_1^2 + \mu_1 w_1)$$

and let $\rho := N - N_1$. We complete squares and obtain for ρ the formula

$$(**) \qquad \rho = 2^{-d-2} \lambda^{-1} (\sum_{i=2}^{k} (2\lambda w_i + \mu_i)^2 - C).$$

where $C = \sum_{i=2}^{k} \mu_i^2$, see 3.2.1.

3.4 From now we assume that $k = 4$ and that $m = (p-1)/2$ where p is a prime ≥ 5. Then $\lambda = p/2$ and $\lambda_1 = (p-4)/2$. The formulae in 3.3 become now

$$N_1 = [(p-4)/8] w_1^2 + (\mu_1/4) w_1$$

and

$$\rho = (1/8p)(\sum_{i=2}^{4}(pw_i + \mu_i)^2 - C).$$

3.5 Consider now $\vec{w} = \vec{z}P$; then $\vec{z} = (1/4)\vec{w}P$. We say that the values w_i are *admissible* if the corresponding z_i are non-negative integers. We investigate now in detail conditions for the w_i to be admissible.
For $k = 4$ we may take the variables w_i as follows.

$$w_1 = z_1 + z_2 + z_3 + z_4, \quad w_2 = z_1 + z_2 - z_3 - z_4,$$
$$w_3 = z_1 - z_2 - z_3 + z_4, \quad w_4 = z_1 - z_2 + z_3 - z_4.$$

Then we have that

$$z_1 = (1/4)(w_1 + w_2 + w_3 + w_4), \quad z_2 = (1/4)(w_1 + w_2 - w_3 - w_4),$$
$$z_3 = (1/4)(w_1 - w_2 - w_3 + w_4), \quad z_4 = (1/4)(w_1 - w_2 + w_3 - w_4).$$

We obtain now the following criterion.

3.5.1 Lemma *The numbers w_i are admissible if and only if they satisfy the following conditions:*
(i) $w_1 \equiv w_i$ *(mod 2) and* $\sum w_i \equiv 0$ *(mod 4);*
(ii) $w_1 + w_i \geq |w_j + w_k|$ *for* $\{i, j, k\} = \{1, 2, 3\}$.

4. Abacus numbers for symmetric groups when p = 5 and p = 7.

4.1 Assume first that $p = 5$. We consider cores for the symmetric group. We take as an abacus for a general core $\Gamma = (0, y_1, ..., y_4)$. This represents the integer $N(\Gamma) = q(\vec{y}) + \ell(\vec{y})$; where

$$q(\vec{y}) = 2(\sum_{i=1}^{4} y_i^2) - (1/2)(\sum_{i \neq j} y_i y_j)$$

and

$$\ell(\vec{y}) = -y_1 + y_3 + 2y_4.$$

This was proved in 1.6. For the change of variables described in Chapter 3 (with $y_i = z_i$) we must set

$$a_1 = -1, \ a_2 = 0, \ a_3 = 1, \ a_4 = 2$$

(with the notation of 3.2). Therefore using 3.5 and 3.2 we obtain that

$$\mu_1 = 2, \qquad \mu_2 = a_1 + a_2 - a_3 - a_4 = -4,$$
$$\mu_3 = a_1 - a_2 - a_3 + a_4 = 0, \qquad \mu_4 = a_1 - a_2 + a_3 - a_4 = -2.$$

Hence $C = 20$. Consequently we have

$$N_1 = (1/8)w_1^2 + (1/2)w_1$$

and

$$\rho = N - N_1 = 1/40((5w_2 - 4)^2 + (5w_3)^2 + (5w_4 - 2)^2 - 20).$$

Note that the variable w_1 is the total number of beads of the abacus.

4.2 Theorem *Assume $p = 5$. Then every integer $n \geq 1$ is an abacus number. That is, the group algebra $K\mathcal{S}_n$ has at least one 5-block of defect zero, for any $n \geq 1$.*

Actually we prove something slightly stronger. Namely there is a block of defect zero whose core has number of parts $\equiv -1 \pmod 4$ if $n \geq 105$.

Proof. Given any integer $n \geq 1$; then there are unique integers k and n_0 with $k, n_0 \geq 0$ such that
(1) $n = (2k^2 + k) + n_0$ with $0 \leq n_0 < 4k + 3$.
This is clear, noting that $2(k + 1)^2 + (k + 1) - (2k^2 + k) = 4k + 3$.
We will now show that n can be represented on a core abacus with $4k - 1$ beads, if $k > 6$.

Let $w_1 = 4k - 1$; then $N_1 = 2k^2 + k - (3/8)$. Define now $m = m(n)$ to be the integer
(2) $m = 40(N - N_1) + 20 = 40n_0 + 35$
Our aim is to show that there are integers w_2, w_3, w_4 such that $m = (5w_2 - 4)^2 + (5w_3)^2 + (5w_4 - 2)^2$ and moreover such that the w_i are admissible, in the sense of 3.5.1.

Since $m \equiv 3 \pmod 8$ and $m \equiv 0 \pmod 5$, we know by 6.1 that there is a solution in integers of

$$(*) \qquad m = X^2 + Y^2 + Z^2$$

with $X \equiv 1 \pmod{10}$, $Y \equiv 5 \pmod{10}$ and $Z \equiv 3 \pmod{10}$. Now set

$$\begin{array}{ll} X = 5w_2 - 4 & \text{where } w_2 = 2r_2 + 1 \\ Y = 5w_3 & \text{where } w_3 = 2r_3 + 1 \\ Z = 5w_4 - 2 & \text{where } w_4 = 2r_4 + 1. \end{array}$$

Then the w_i are odd, hence $\equiv w_1 \pmod 2$. By 3.5.1 we also require that $\sum w_i \equiv 0 \pmod 4$, that is, $\sum_{i=2}^4 r_i \equiv 1 \pmod 2$. Suppose that instead we have $\sum r_i \equiv 0 \pmod 2$. Observe that $Y = 10r_3 + 5 = -(10(-r_3 - 1) + 5)$. Replace r_i by r'_i where

$$r'_3 = -r_3 - 1, \quad r'_j = r_j \quad \text{otherwise}.$$

Then $\sum r'_i \equiv 1 \pmod 2$, as required.

It remains to investigate the condition $w_1 + w_i \geq |w_j + w_k|$. Without loss of generality, assume that $w_1 + w_2 < |w_3 + w_4|$. We assume in (1) that $0 \leq n_0 < 4k + 3$, hence

$$35 \leq m = 40n_0 + 35 < 40(4k + 3) + 35 = 160k + 155.$$

We use now Lemma 4.3. This gives that $|r_i| < \frac{6}{10}k$ since $k > 6$. Then we get

$$w_1 + w_2 = (4k-1) + (2r_2+1) < |2(r_3+r_4)+2|$$

which implies that

$$4k < 2 + \frac{18}{5}k$$

and $k \leq 5$, contrary to the hypothesis.

This proves that any integer n with $n \geq 2 \cdot 7^2 + 7 = 105$ is an abacus number. For integers $n \leq 104$ one may directly find a core abacus representing n (see also 4.3.1).

4.3 Lemma *Suppose $X = 10r_2 + 1$, $Y = 10r_3 + 5$ and $Z = 10r_4 + 3$ with integers r_i, and assume that k is an integer such that*

$$X^2 + Y^2 + Z^2 < 160k + 155.$$

Then $|r_i| < \frac{6}{10}k$ unless $k \leq 6$.

Proof. The worst case to consider is the possibility that $(-r_3) \geq \frac{6}{10}k$. If so then

$$(6k-5)^2 \leq (10r_3+5)^2 < 160k + 155.$$

Hence $(6k)^2 - 220k < 130$ and therefore

$$(6k - \frac{55}{3})^2 < 130 + (\frac{55}{3})^2 < \frac{(65)^2}{9}$$

and $k < \frac{40}{6}$ and consequently $k \leq 6$.

4.3.1 *Remark* With the notation of 4.2, suppose $n = 2k^2 + k + n_0$ and $0 \leq n_0 \leq 2k+1$. Then we have that $0 \leq 40n_0 + 35 \leq 80k + 105$. Now one can prove that, with X, Y, Z as in 4.3, if $X^2 + Y^2 + Z^2 \leq 80k + 105$ then $|r_i| \leq \frac{6}{10}k$ unless $k \leq 4$. Hence for $k = 5, 6$ one deduces that n is an abacus number if

$$2k^2 + k \leq n \leq 2k^2 + 3k + 1.$$

This leaves for each of these values for k only $2k+2$ integers to be considered; and also the integers $n \leq 55$.

4.4 Now assume that $p = 7$. We will consider cores for the symmetric group with abacus representations of the form $\Gamma = (0, y_1, y_2, y_3, 0, y_5, 0)$. This is a partition of n where $n = N(\Gamma) = q(\vec{y}) + \ell(\vec{y})$ where

$$q(\vec{y}) = 3\sum_i y_i^2 - \frac{1}{2}\sum_{i \neq j} y_i y_j$$

and

$$\ell(\vec{y}) = -2y_1 - y_2 + 2y_5.$$

We change variables as in Ch. 3. Set

$$z_i = \begin{cases} y_i & i = 1,2,3 \\ y_5 & i = 4 \end{cases}$$

and $\vec{w} = \vec{z}P$, and with the notation of 3.2 we have $(a_1, a_2, a_3, a_4) = (-2, -1, 0, 2)$. It follows then with P and μ_i as in 3.5 that

$$\mu_1 = -1, \quad \mu_2 = -5, \quad \mu_3 = 1, \quad \mu_4 = -3.$$

Hence we get the constant $C = 35$. (This was chosen because $C \equiv 0 \pmod 7$.)

Consequently $N_1 = 3/8w_1^2 + (-1/4)w_1$ and

$$N - N_1 = \frac{1}{56}((7w_2 - 5)^2 + (7w_3 + 1)^2 + (7w_4 - 3)^2 - 35).$$

4.5 Theorem *Assume $p = 7$, then every integer $n \geq 1$ is an abacus number. That is, the group algebra $K\mathcal{S}_n$ has at least one 7-block of defect zero, for any $n \geq 1$.*

Proof. We use the abacus representation as in 4.4. By 1.5 it suffices to consider odd integers n.

Given an odd integer $n \geq 1$, there are integers k and $n_0 \geq 0$ such that
(1) $n = 6k^2 - 4k + n_0$ with $0 < n_0 < 12k + 2$.
This is clear noting that $[6(k+1)^2 - 4(k+1)] - (6k^2 - 4k)] = 12k + 2$. We will now show that n can be represented on a core abacus with $4k - 1$ beads if $k > 12$.

Let $w_1 = 4k - 1$ then we have $N_1 = 6k^2 - 4k + (5/8)$ and hence $N - N_1 = n_0 - (5/8)$. Define now $m = m(N)$ to be the integer
(2) $m = 56(N - N_1) + 35 = 56n_0$.
Our aim is to show that there are integers w_2, w_3, w_4 such that

$$m = (7w_2 - 5)^2 + (7w_3 + 1)^2 + (7w_4 - 3)^2$$

and moreover such that the w_i are admissible, in the sense of 3.5.1.

Since n_0 is odd, m is not of the form $4^a(8b + 7)$. So there is a solution in integers of the equation

$$m = X^2 + Y^2 + Z^2. \tag{$*$}$$

By 5.3, there is also a solution with $X, Y, Z \not\equiv 0 \pmod 7$. Since $m \equiv 0 \pmod 7$, the equation $(*)$ has modulo 7 essentially one non-trivial solution, namely $X \equiv \pm 5 \pmod 7$, $Y \equiv \pm 1 \pmod 7$ and $Z \equiv \pm 3 \pmod 7$.

Define integers w_i by setting $X = 7w_2 - 5$, $Y = 7w_3 + 1$ and $Z = 7w_4 - 3$. Since $m \equiv 0 \pmod 8$, we must have that X, Y, Z are even and hence the w_i are odd. Set $w_i = 2r_i + 1$, we will show that these w_i are admissible.

Clearly $w_i \equiv w_1 \pmod 2$. Recall that $w_1 = 4k - 1$, hence $\sum w_i \equiv 2(r_2 + r_3 + r_3 + 1) \pmod 4$. Let $u = 7r_2 + 1$, $v = 7r_3 + 4$ and $w = 7r_4 + 2$. Then we have that

$$u^2 + v^2 + w^2 \equiv 0 \pmod 2$$

(since $4(u^2 + v^2 + w^2) = m \equiv 0 \pmod 8$). Now calculating mod 2 we have $u^2 \equiv (r_2^2 + 1)^2 \equiv r_2 + 1$, $v^2 \equiv r_3^2 \equiv r_3$ and $w \equiv r_4^2 \equiv r_4$ and hence $r_2 + 1 + r_3 + r_4 \equiv 0 \pmod 2$, as required.

It remains to investigate the condition $w_1 + w_i \geq |w_j + w_k|$. Assume that, say, $w_1 + w_2 < |w_3 + w_4|$. We assume in (1) that $0 \leq n_0 < 12k + 2$, hence

$$0 \leq m = 56n_0 < 56(12k + 2) = 21 \cdot 32k + 7 \cdot 16.$$

From Lemma 4.6 below we get $|r_i| < \frac{8}{14}k$ for $k > 12$. This implies now that $4k < \frac{24}{7}k + 2$ and $k \leq 3$, contrary to the hypothesis.

This proves that every integer n with $n \leq 13^2 \cdot 6 - 13 \cdot 4$ is an abacus number. For the remaining integers one may directly find a core abacus representing n (see also 4.6.1).

4.6 Lemma *Suppose $X = 14r_2 + 2$, $Y = 14r_3 + 8$ and $Z = 14r_4 + 4$, with $r_i \in \mathbf{Z}$, such that*

$$X^2 + Y^2 + Z^2 < 21 \cdot 32k + 7 \cdot 16.$$

Then $|r_i| < \frac{8}{14}k$ unless $k \leq 12$.

Proof. The worst possibility arises when $(-r_3) \geq \frac{8}{14}k$. Then

$$(8k - 8)^2 < 21 \cdot 32k + 7 \cdot 16.$$

We complete squares and deduce

$$(8k - 50)^2 < 16 \cdot 11 + 4 \cdot (25)^2 = 4 \cdot 669.$$

Hence $8k - 50 < 2 \cdot 26$ and $k < \frac{102}{8}$ and hence $k \leq 12$.

4.6.1 (1) With the notation of 4.5, suppose $n = 6k^2 - 4k + n_0$ where $0 < n_0 \leq 6k + 1$. Then $0 < 56n_0 \leq 21 \cdot 16k + 56$. One may prove that if X, Y, Z are as in 4.6 and

$$X^2 + Y^2 + Z^2 < 21 \cdot 16k + 56$$

then $|r_i| \leq \frac{8}{14}k$ unless $k \leq 7$. So for $8 \leq k \leq 12$ one obtains by this method also (using 1.6) that n is an abacus number when

$$6k^2 - 4k \leq n \leq 6k^2 + 2k + 2.$$

(2) A further improvement is obtained by taking the number of beads w_1 to be of the form $w_1 = 4k + 1$. Then $N_1 = 6k^2 + 2k + \frac{1}{8}$. We express now an integer n in the form $n = 6k^2 + 2k + n_0$ with $0 \leq n_0 < 12k + 8$. Then we have $N - N_1 = n_0 - \frac{1}{8}$. Therefore if we set

$$m = 56(N - N_1) + 35 = 56n_0 + 28$$

then we obtain similarly as in 4.5 that for at least two successive values of n_0 the equation

$$m = X^2 + Y^2 + Z^2$$

has an admissible solution for k not too small. If we restrict ourselves to $0 \leq n_0 < 6k + 4$ then $56n_0 + 28 < 21 \cdot 16k + 72$. One may prove that if X, Y, Z are as in 4.6 and $X^2 + Y^2 + Z^2 < 21 \cdot 16k + 9 \cdot 28$ then $|r_i| \leq \frac{8}{14}k$ unless $k \leq 7$. So for $8 \leq k \leq 12$ one obtains that n is an abacus number if

$$6k^2 + 2k \leq n \leq 6k^2 + 8k + 4.$$

Combining (1) and (2) gives all integers n with $n > 280$.

5. Representing integers as a sum of three squares

First we will prove the results required for $p = 5$.

5.1 Lemma *Suppose $m \equiv 3$ (mod 8) and $\equiv 0$ (mod 5). Then the equation*

$$m = X^2 + Y^2 + Z^2$$

has a solution in integers such that $X \equiv 1$ (mod 10), $Y \equiv 5$ (mod 10) and $Z \equiv 3$ (mod 10).

Proof. The conditions on m ensure that there are integers $u, v, w \in \mathbf{Z}$ such that $m = u^2 + v^2 + w^2$.

(1) We claim that there is such a representation in which not all of u, v, w are $\equiv 0$ (mod 5). This is clear if $m \not\equiv 0$ (mod 25). Now suppose $m = 25m_1$, then $m_1 \equiv 3$ (mod 8) and hence there are integers u, v and w with $m_1 = u^2 + v^2 + w^2$ where $u \not\equiv 0$ (mod 5), by the induction hypothesis. Now consider the representations

$$\begin{aligned} 25m_1 &= (3u + 4v)^2 + (4u - 3v)^2 + 25w^2 \\ 25m_1 &= (3v + 4u)^2 + (4v - 3u)^2 + 25w^2. \end{aligned}$$

We claim that one of $3u + 4v$, $3v + 4u$ must be $\not\equiv 0$ (mod 5). Otherwise we would have $3u + 4v \equiv 0$ (mod 5) and $u \equiv 2v$ (mod 5) and in addition $3v + 4u \equiv 0$ (mod 5) and $v \equiv 2u$ (mod 5); and consequently $u \equiv 4u$ (mod 5) and $u \equiv 0$ (mod 5), contrary to the hypothesis. Hence m has the required representation, and (1) is proved.

Take now a representation where not all of u, v, w are $\equiv 0 \pmod 5$. The squares modulo 5 are $\{0, 1, 4\}$; therefore to obtain $u^2 + v^2 + w^2 \equiv 0 \pmod 5$ we must have that $\{u^2, v^2, w^2\} = \{0, 1, 4\}$. Hence without loss of generality,
(2) $v^2 \equiv 0, w^2 \equiv 4$ and $u^2 \equiv 1 \pmod 5$.
(3) Let u, v, w be as before, then u, v and w are odd:
Squares are $\equiv 0, 4$ or $1 \pmod 8$; and we are given that $u^2 + v^2 + w^2 \equiv 3 \pmod 8$. Suppose that u, say, is even. Then $u^2 + v^2 + w^2$ is either $\equiv 4 + v^2 + w^2$ or $\equiv v^2 + w^2 \pmod 8$ and $v^2 + w^2 \equiv 7$ or $3 \pmod 8$, which is not possible.

Now we have that v is odd and $\equiv 0 \pmod 5$, so $v \equiv 0 \pmod{10}$. Moreover $w \equiv \pm 2 \pmod 5$ and w is odd, so $w \equiv \pm 3 \pmod{10}$. Similarly $u \equiv \pm 1 \pmod 5$ and u is odd, so $u \equiv \pm 1 \pmod{10}$. This completes the proof.

5.2 Lemma *Suppose m is an odd integer such that the equation*

$$2m = X^2 + Y^2$$

has a solution in integers. Then there is a solution in which $X, Y \not\equiv 0 \pmod 5$.

Proof. This is clear if $m \not\equiv 0 \pmod{25}$. Now suppose $m = 25m_1$, and assume X, Y are some solution. Suppose $X = 5X_1$, then also $Y = 5Y_1$ and $50m_1 = 25(X_1^2 + Y_1)^2$, and hence $2m_1 = X_1^2 + Y_1^2$.

By the induction hypothesis, there are u, v such that $2m_1 = u^2 + v^2$ with $u, v \not\equiv 0 \pmod 5$. Then

$$(3u + 4v)^2 + (4u - 3v)^2 = 2m, \text{ and}$$
$$(3v + 4u)^2 + (4v - 3u)^2 = 2m.$$

It follows that at least one of $3u + 4v$, $3v + 4u$ must be $\not\equiv 0 \pmod 5$, as in 5.1. Say $X = 3u + 4v \not\equiv 0 \pmod 5$, then $Y = (4u - 3v) \not\equiv 0 \pmod 5$ as well since $m \equiv 0 \pmod 5$, and this gives a required solution.

Now we study the equations occuring when $p = 7$.

5.3 Lemma *Suppose $m \in \mathbf{Z}$ and $m \equiv 0 \pmod 7$. Assume that the equation*

$$m = u^2 + v^2 + w^2$$

has a solution in $\mathbf{Z}$. Then there is also a solution where u^2, v^2 and w^2 are $\equiv 1, 2$ and $4 \pmod 7$.

Proof. By inspection, there is only one non-trivial solution for $m \equiv u^2 + v^2 + w^2 \pmod 7$. Therefore it suffices to show that there is a solution where at least one of u, v, w is $\not\equiv 0 \pmod 7$. We proceed by induction on m. The statement is clear if $m \not\equiv 0 \pmod{49}$. Now suppose $m = 49m_1$. We assume that m is a sum of three squares, therefore m is not of the form $4^a(8b + 7)$; and then m_1 is not of this form too. Therefore by induction there are integers u, v, w with $m_1^2 = u^2 + v^2 + w^2$ and $u \not\equiv 0 \pmod 7$. Now consider the two expressions

$$\begin{aligned}49m_1 =&(6u + 3v - 2w)^2 + (3u - 2v + 6w)^2 + (2u - 6v - 3w)^2\\ 49m_1 =&(6u + 3w - 2v)^2 + (3u - 2w + 6v)^2 + (2u - 6w - 3v)^2.\end{aligned}$$

Suppose both $6u + 3v - 2w$ and $6u + 3w - 2v$ are $\equiv 0 \pmod 7$. Then it follows that also the difference $5v - 5w \equiv 0 \pmod 7$; that is, $v \equiv w \pmod 7$. Consequently $6u + v \equiv 0 \pmod 7$ and $6u - v \equiv 0 \pmod 7$ and it follows that $u \equiv 0 \pmod 7$, a contradiction.

Acknowledgement. This work was supported by the SERC (via a Visiting Fellowship of the second author and also via the Warwick Algebra Symposium 1991), and by the Graduierten-Kolleg Essen. The authors are grateful to the hospitality of the Mathematics Departments at Oxford, Warwick and of the Institut für Experimentelle Mathematik at Essen. The authors are grateful to H. G. Rück for valuable help.

References

[1] Andrews, G. E.: *private communication*

[2] Garwan, F.; Kim, D.; Stanton, D.: *Cranks and t-cores.* Invent. Math. **101**, 1–17 (1990).

[3] James, G. D.; Kerber, A.: *The Representation Theory of the Symmetric Group.* Encyclopedia of Mathematics and its Applications **16**, Addison and Wesley 1981.

[4] Klyachko, A. A.: *Modular forms and representations of symmetric groups.* J. Sov. Math. **26**, 1879–1887 (1984) (Translation).

[5] Michler, G. O.; Olsson, J. B.: *Character correspondences in finite General Linear, Unitary and Symmetric groups.* Math. Z. **184**, 203–233 (1983).

[6] Olsson, J. B.: *Lower defect groups in symmetric groups.* J. Algebra **104**, 37–56 (1986).

[7] Olsson, J. B.: *Frobenius symbols for partitions and degrees of spin characters.* Math. Scand. **61**, 223–247 (1987).

[8] Rose, H. E.: *A course in number theory.* Clarendon Press, Oxford 1988.

[9] Scopes, J.: *Cartan matrices and Morita Equivalence for Blocks of the Symmetric Groups.* J. Algebra **142**, 441–455 (1991).

Received April 10, 1995

MSC 1991: 20C30, 11E25; 20C20