ON THE NON-COPRIME $k(GV)$ PROBLEM

ROBERT M. GURALNICK AND ATTILA MARÓTI

Abstract. Let V be a finite faithful completely reducible FG-module for a finite field F and a finite group G. In various cases explicit linear bounds in $|V|$ are given for the numbers of conjugacy classes $k(GV)$ and $k(G)$ of the semidirect product GV and of the group G respectively. These results concern the so-called non-coprime $k(GV)$-problem.

1. Introduction

The topic of this paper originates from the long-standing $k(B)$-conjecture of Brauer which states that the number $k(B)$ of complex irreducible characters in any p-block B of any finite group G is at most the order of the defect group of B. Nagao [21] showed that for p-solvable groups G Brauer's $k(B)$-problem is equivalent to the so-called $k(GV)$-problem which is described in the next paragraph.

For a finite group X let $k(X)$ be the number of conjugacy classes of X. Let V be a finite faithful FG-module for some finite field F of characteristic p and finite group G. Form the semidirect product GV. The $k(GV)$-problem states that $k(GV) \leq |V|$ whenever $(|G|, |V|) = 1$. Works of Knörr, Gow, and especially Robinson, Thompson [23] have led to fundamental breakthroughs in attacking the $k(GV)$-problem which have culminated in a complete solution of the problem, with the final step completed by Gluck, Magaard, Riese, Schmid [8]. The full solution of the problem (not counting the Classification of Finite Simple Groups) is written in the book [24].

Let V, G, and F be as in the previous paragraph with not assuming $(|G|, |F|) = 1$ but that V is completely reducible. Is there a universal constant c such that $k(GV) \leq c^n |V|$ where n denotes the F-dimension of V? Can c be taken to be 1 in most cases? This is a weak version of the so-called non-coprime $k(GV)$-problem [11, Problem 1.1] which is also important in a character theoretic point of view. Indeed, as pointed out by Robinson, the inequality $k(GV) \leq |V|$ combined with [22, Lemma 5] would imply the $k(B)$-conjecture for a wider class of p-constrained groups.

Date: December 18, 2012.

2000 *Mathematics Subject Classification.* 20C99.

Key words and phrases. linear representation, number of conjugacy classes.

The first author was partially supported by NSF grant DMS-1001962. The research of the second author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by OTKA K84233.

There has been progress made on the non-coprime $k(GV)$-problem. Kovács and Robinson [17, Theorem 4.1] gave an affirmative answer to our first question above in case G is a p-solvable group. In fact, for p-solvable groups, Liebeck and Pyber [18] showed that c can be taken to be 103. Guralnick and Tiep [11] have proved $k(GV) < |V|/2$ for many almost quasi-simple groups G, Keller [15] has obtained results in case V is an imprimitive irreducible module, and there are some interesting character theoretic arguments developed by Keller [16].

Our first result concerns the extraspecial case of the non-coprime $k(GV)$-problem.

Theorem 1.1. *Let r be a prime and let R be an r-group of symplectic type with $|R/Z(R)| = r^{2a}$ for some positive integer a. Let V be a faithful, absolutely irreducible KR-module of dimension r^a for some finite field K. View V as an F-vector space where F is the prime field of K. Let G be a subgroup of $GL(V)$ which contains R as a normal subgroup. Then $k(GV) \leq |V|$ unless one of the following cases holds.*

(1) *$r^a = 2^6$ and $|K| = 3$. In this case $k(GV) \leq 2^{120}$.*
(2) *$r^a = 2^5$ and $|K| = 3$, 5, 7, 9, or 11. In this case $k(GV) \leq 2^{119}$.*
(3) *$r^a = 3^3$ and $|K| = 4$ or 7. In this case $k(GV) \leq 2^{82}$.*
(4) *$r^a = 2^4$ and $|K| = 3$, 5, 7, 9, 17, 25, or 27. In this case $k(GV) \leq 2^{82}$.*
(5) *$r^a = 2^3$ and $|K| = 3$, 5, 7, 9, 25, 27, 49, 81, or 125. We have $k(GV) \leq 2^{58}$.*
(6) *$r^a = 3^2$ and $|K| = 4$, 16, or 25. In this case $k(GV) \leq 2^{44}$.*
(7) *$r^a = 2^2$ and $|K| = 3$, 5, 9, 25, 27, 81, 125, or 243. We have $k(GV) \leq 2^{32}$.*

The next result deals with the case where G is a meta-cyclic group. Here the bound $|V|$ is best possible in infinitely many cases. (Just consider a Singer cycle G acting on V.)

Theorem 1.2. *Let V be an n-dimensional finite vector space over the field of p elements where p is a prime. The group $X = GL(1, p^n).n$ acts naturally on V. Then for any subgroup G of X we have $k(GV) \leq |V|$ unless $GV \cong D_8$ or S_4.*

The ideas in the proof of Theorem 1.1 together with Theorem 1.2 yield a general result on $k(GV)$ in case the group G has nilpotent generalized Fitting subgroup and when V is a faithful primitive irreducible module.

Theorem 1.3. *Let V be a finite faithful primitive irreducible FG-module for some group G with $\mathrm{Fit}^*(G) = \mathrm{Fit}(G)$. Then $k(GV) \leq \max\{|V|, 2^{1344}\}$.*

What can be said about $k(G)$ in the setting of the non-coprime $k(GV)$-problem? Clearly, $k(G) \leq k(GV)$. Interestingly, in case $(|G|, |V|) = 1$, the fact that $k(G) \leq |V|$ was only derived from the full solution of the $k(GV)$-problem. Is it true that $k(G) \leq |V|$ whenever V is a completely reducible module? We make a first step in answering this question.

Theorem 1.4. *Let V be a finite faithful irreducible FG-module for some finite field F and finite group G. Suppose that V can be induced from a primitive irreducible FL-module W for some finite group L with $k(N) < |W|/\sqrt{3}$ for every normal subgroup N of $L/C_L(W)$. Then $k(G) < (2/3)|V|$.*

Note that the bound $k(N) < |W|/\sqrt{3}$ in Theorem 1.4 is satisfied for all normal subgroups N of 'many' L. For example, if L is the G and W in the V considered in Section 5, then $|L| < |W|/\sqrt{3}$ for sufficiently large characteristics.

Finally, it may be possible that the 2-power estimates for $k(GV)$ in Theorem 1.1 and in Theorem 1.3 can all be taken to be 11 as $k(AGL(2,3)) = 11$.

2. Bounding the dimensions of eigenspaces

Throughout this section we will use the following notations and assumptions. Let r be a prime. An r-group R is said to be of symplectic type if either r is odd and R is extraspecial of exponent r, or $r = 2$, $R/Z(R)$ is elementary abelian, R' has order 2, R has exponent 4 and $Z(R)$ has order 2 (in which case R is extraspecial) or has order 4. Let V denote a faithful irreducible FG-module where F is an algebraically closed field of characteristic $p > 0$ and G is a finite group. Suppose that the group G has a normal subgroup R of symplectic type with $|R/Z(R)| = r^{2a}$ for some prime r and positive integer a. This r-group R acts absolutely irreducibly on V, $\dim_F(V) = r^a$, and $O_p(G) = 1$. Suppose that R is such that $Z(G) = Z(R)$. The non-identity elements of G/R act faithfully on $R/Z(R)$ and trivially on $Z(R)$.

Let x be an element of G. For a field element $\lambda \in F$ we denote the eigenspace of λ of a matrix representation of x on V by $\mathrm{Eigen}(\lambda, x)$. In this section we wish to bound $d(x) = \max_{\lambda\in F} \dim(\mathrm{Eigen}(\lambda, x))$ (but in the end we will be interested in $\dim_F(C_V(x))$).

Let the element x be in R. If x is central then $d(x) = r^a$. Otherwise if x is non-central in R then the value of the character (of V) at x is 0 and so $d(x) = r^{a-1}$.

From now on, assume that $x \in G \setminus R$.

The following important theorem considers the case when $\langle x\rangle$ is irreducible on the vector space $R/Z(R)$ and has order a power of p.

Theorem 2.1 (Hall-Higman, [12]). *Use the notations and assumptions of this section. Let x be an element of $G \setminus R$ of prime power order q divisible by p, the characteristic of the field F. Assume that $\langle x\rangle$ acts irreducibly on $R/Z(R)$ (where $|R/Z(R)| = r^{2a}$). Then there exists a non-negative integer b so that* $\dim(V) = r^a = (q-1)+bq$*, and the Jordan canonical form of x on V consists of $b+1$ Jordan blocks, b of size q and 1 of size $q-1$. In particular,* $d(x) = \dim(C_V(x)) = b+1 = (r^a+1)/q$.

It is necessary to say a few words about the proof of the Hall-Higman theorem. Put x (viewed as a linear transformation of V) in Jordan canonical form. Suppose that x has m Jordan blocks of sizes: $a_1, \ldots, a_m$. We seek to find the a_i's explicitly. We certainly have one restriction, namely, $\dim(V) = r^a = \sum_{i=1}^m a_i$. For another one, let E be the enveloping algebra of the group of linear transformations R of V. Then $E = \mathrm{End}(V)$ (and so $\dim_F(E) = r^{2a}$). Hall and Higman proceed to calculate $\dim_F(C_E(x))$ in two different ways. On one hand, this is $\sum_{i=1}^m (2i-1)a_i$, while on the other, it is $1 + (r^{2a} - 1)/q$, the number of $\langle x\rangle$-orbits of the set $R/Z(R)$. This gives our second restriction on the a_i's. It turns out that these two restrictions are sufficient to determine the m non-negative integers.

Now let x be an element of $G \setminus R$ of prime power order q such that p does *not* divide q. As before, suppose that $\langle x \rangle$ is irreducible on the vector space $R/Z(R)$. By this we are also assuming that q is not a power of r. (The following argument is taken from the series of exercises in [9, Pages 371-372].) In this case the Jordan canonical form of x on V is a diagonal matrix (since F is algebraically closed). Let the number of distinct eigenvalues of x be m, and let a_i be the multiplicity of the i-th eigenvalue. Then $r^a = \sum_{i=1}^{m} a_i$. Again, let E be the enveloping algebra of R. Clearly, $\dim_F(C_E(x)) = \sum_{i=1}^{m} {a_i}^2$. On the other hand, it is easy to see that $\dim_F(C_E(x))$ is again the number of $\langle x \rangle$-orbits of the set $R/Z(R)$. This gives us two equations involving the a_i's which are sufficient to determine the m non-negative integers we are looking for. In particular, we find that the multiplicity of any eigenvalue is at most $(r^a + 1)/q$. Hence $d(x) \leq (r^a + 1)/q$ (as in the case when q *was* a power of p).

Using the same argument as before, one can show even more.

Lemma 2.2. *Use the notations and assumptions of this section. Let x be an element of $G \setminus R$ so that $\langle x \rangle$ is irreducible on $R/Z(R)$. Let the order of x be m. (The positive integer m divides $r^{2a} - 1$.) Then $d(x) \leq (r^a + 1)/m$.*

The Jordan canonical form of a matrix is a block matrix consisting of Jordan blocks in the main diagonal and zero matrices everywhere else where a Jordan block is a block matrix with the same companion matrix in the diagonal, identity matrices just above the diagonal and zero matrices everywhere else.

At this point let us mention another result.

Lemma 2.3. *Use the notations and assumptions of this section. Let x be an element of $G \setminus R$, and let R_1, R_2 be two maximal abelian subgroups of R whose intersection is $Z(R)$. Suppose that the Jordan canonical form of x on $R/Z(R)$ consists of two a-by-a Jordan blocks that are the same where one leaves $R_1/Z(R)$ invariant and the other leaves $R_2/Z(R)$ invariant. Suppose that $\langle x \rangle$ is irreducible on both $R_1/Z(R)$ and on $R_2/Z(R)$, and x has order m. Then $d(x) \leq 1+(r^a-1)/m$.*

Proof. The group R, which is a product of the maximal abelian subgroups R_1 and R_2, acts absolutely irreducibly on the vector space V. We can diagonalize R_1 (and R_2) on V and all eigenspaces are one dimensional.

Apart from a single eigenspace, the element x permutes all other eigenspaces in regular orbits. This means that V is a direct sum of a single module of dimension 1 and some free $\langle x \rangle$-modules. Hence, $d(x) \leq 1 + (r^a - 1)/m$. □

Let us modify the proof of the Hall-Higman theorem to include the case when x is an element of order a power of r. In this case we cannot assume irreducibility. Instead, suppose that the Jordan canonical form of our element $x \in G \setminus R$ viewed as a linear transformation of $R/Z(R)$ consists of a unique Jordan block of size $2a$ or of two Jordan blocks each of size a. In the latter case suppose that x leaves two maximal totally singular subspaces of $R/Z(R)$ invariant, both of order r^a.

Notice that a Jordan block of an r-element is a matrix with 1's in the main diagonal, 1's in the diagonal just above the main diagonal, and 0's elsewhere. Hence the order of x is r^k and r^ℓ, respectively, where k and ℓ are the smallest non-negative integers such that $r^k \geq 2a$ and $r^\ell \geq a$, respectively.

Observe (as in the previous two cases) that the Jordan canonical form of x viewed as a linear transformation on V is a diagonal matrix. Hence if $a_1, \ldots, a_m$ denotes the list of the multiplicities of the distinct eigenvalues of x, then $r^a = \sum_{i=1}^{m} a_i$. Again let E be the enveloping algebra of R. Since x can be diagonalized on V, we certainly have $\dim(C_E(x)) = \sum_{i=1}^{m} a_i^2$. However, $\dim(C_E(x))$ is *not* necessarily equal to the number d of $\langle x \rangle$-orbits of the set $R/Z(R)$.

Let us number the $\langle x \rangle$-orbits of the set of all r^{2a} vectors of $R/Z(R)$ from 1 to d, and for all $1 \leq i \leq d$ let v_i be a representative of a coset in the i-th orbit. If ℓ_i denotes the length of the i-th orbit, then the elements $v_i^{x^j}$ form a set of coset representatives for the cosets of $R/Z(R)$ where i and j run through the set of numbers $1, \ldots, d$ and $1, \ldots, \ell_i$, respectively.

We claim that $\dim(C_E(x))$ is equal to the number of i's for which $v_i = {v_i}^{x^{\ell_i}}$.

For each i let E_i be the $\langle x \rangle$-invariant subspace of E generated by the vector v_i. It is easy to see that $C_E(x) = \sum_{i=1}^{d} C_{E_i}(x)$. This implies that, in order to prove the claim, it is sufficient to show that $\dim(C_{E_i}(x)) = 1$ for all $1 \leq i \leq d$ for which $v_i = {v_i}^{x^{\ell_i}}$ and that $\dim(C_{E_i}(x)) = 0$ otherwise. This is clear for those i's for which $\ell_i = 1$. It is also clear that if i is so that $v_i = {v_i}^{x^{\ell_i}}$, then $\dim(C_{E_i}(x)) \geq 1$. So let i be such that $\ell_i > 1$ and that $\dim(C_{E_i}(x)) > 0$. Let $v \in C_{E_i}(x)$ be an arbitrary non-zero element. Write v in the form $\sum_{j=1}^{\ell_i} c_j v_i^{x^j}$ for some field elements c_j of F. Since v is $\langle x \rangle$-invariant and since the $v_i^{x^j}$'s are linearly independent, it follows that all the c_j's are equal. Hence $C_{E_i}(x)$ is indeed 1-dimensional. This proves our claim.

It remains to find an expression for d. Recall that there are two cases we are interested in: if the Jordan canonical form of x considered as a linear transformation on the vector space $R/Z(R)$ consists of a unique $2a$-by-$2a$ Jordan block or if it consists of two a-by-a Jordan blocks. In the first case let us denote d by d_1 while in the second case denote d by d_2.

First suppose that the Jordan canonical form of x consists of a unique Jordan block. Then, as noted before, the order of x is r^k where k is the smallest positive integer such that $r^k \geq 2a$. Every $\langle x \rangle$-orbit has prime power length. It is easy to see that the number of orbits of length 1 is $r = r^{\min\{r^0, 2a\}}$, and for each $1 \leq i \leq k$ the number of orbits of length r^i is $(1/r^i) \cdot (r^{\min\{r^i, 2a\}} - r^{\min\{r^{i-1}, 2a\}})$. This gives

$$d_1 = r + \sum_{i=1}^{k} (1/r^i) \cdot (r^{\min\{r^i, 2a\}} - r^{\min\{r^{i-1}, 2a\}}). \tag{1}$$

By a similar argument, if the Jordan canonical form of x consists of two a-by-a Jordan blocks, then

$$d_2 = r^2 + \sum_{i=1}^{\ell} (1/r^i) \cdot (r^{2\min\{r^i, a\}} - r^{2\min\{r^{i-1}, a\}}) \tag{2}$$

where ℓ is the smallest positive integer such that $r^\ell \geq a$.

In the first case it is easy to see that $d_1 \leq (1/4) \cdot r^{2a}$ unless $a = 1$ and x has order 2, 3, 5, or 7. Let $a = 1$. If x has order 2, then $d(x) = \max_i\{a_i\} = 1$. If x has order 3 or 5, then $d(x) \leq 2$. If x has order 7, then $d(x) \leq 3$. In all cases we have $d(x) \leq ((r+1)/2r) \cdot r^a$. In fact, we have $d(x) \leq (1/2) \cdot r^a$ unless $a = 1$, $r = 3$ and x has order 3 in which case $d(x) \leq (2/3) \cdot r^a$ holds. Let us summarize this result in the following lemma.

Lemma 2.4. *Let us use the notations and assumptions of the first paragraph of this section. Let x be an element of $G \setminus R$. Suppose that the Jordan canonical form of x on $R/Z(R)$ consists of a unique $2a$-by-$2a$ Jordan block, and that x has order a power of r. Then $d(x)/\dim_F(V) \leq ((r+1)/2r)$. Moreover we have $d(x) \leq (1/2) \cdot r^a$ unless $a = 1$, $r = 3$ and x has order 3 in which case $d(x) \leq (2/3) \cdot r^a$ holds.*

In the second case, $d_2 \leq (1/4) \cdot r^{2a}$ unless x has order 4 and $a = 3$ or $a = 4$, or x has order 2 and $a = 2$, or x has order 3 and $a = 2$ or $a = 3$. In all cases we will have $d(x) \leq ((r+1)/2r) \cdot r^a$.

Lemma 2.5. *Let us use the notations and assumptions of the first paragraph of this section. Let x be an r-element in $G \setminus R$, and let R_1, R_2 be two maximal abelian subgroups of R whose intersection is $Z(R)$. Suppose that the Jordan canonical form of x on $R/Z(R)$ consists of two a-by-a Jordan blocks that are the same where one leaves $R_1/Z(R)$ invariant and the other leaves $R_2/Z(R)$ invariant. Then $d(x)/\dim_F(V) \leq ((r+1)/2r)$. Moreover we have $d(x) \leq (1/2) \cdot r^a$ unless $a = 2$, $r = 2$ and x has order 2 in which case $d(x) \leq (3/4) \cdot r^a$, or $a = 2$, $r = 3$ and x has order 3 in which case $d(x) \leq (5/9) \cdot r^a$.*

Proof. Let the order of the non-identity element x be q. Since q is a power of r, the element x can be diagonalized over V. Suppose there are m distinct eigenvalues. Let a_i be the multiplicity of the i-th eigenvalue. Then $d(x) = \max_{1 \leq i \leq m}\{a_i\}$. By the above, we have $r^a = \sum_i a_i$ and $d_2 \geq \sum_i a_i^2$ where d_2 is as in (2).

If $q = r$, then we can say even more. Indeed, in this case it is easy to see that $r^{2a-1} + r^2 - r = d_2 = \dim_F(C_E(x)) = \sum_i a_i^2$.

By the remark made just before the statement of the lemma, it is sufficient to consider the following five cases.

Let $q = 2$ and $a = 2$. Then we have the equations $\sum_{i=1}^m a_i = 4$ and $\sum_{i=1}^m a_i^2 = 10$. Hence $d(x) = 3$.

Let $q = 3$ and $a = 2$. Then we have the equations $\sum_{i=1}^m a_i = 9$ and $\sum_{i=1}^m a_i^2 = 33$. We see that $d(x) \leq 5$.

Let $q = 3$ and $a = 3$. Then x acts on the set of distinct eigenspaces of R_1 on V having 8 cycles of length 3 and 3 fixed points. Hence $d(x) \leq 11$.

Let $q = 4$ and $a = 3$. Then x acts on the set of distinct eigenspaces of R_1 on V having 1 cycle of length 4, 1 cycle of length 2, and 2 fixed points. Hence $d(x) \leq 4$.

Let $q = 4$ and $a = 4$. Then x acts on the set of distinct eigenspaces of R_1 on V having 3 cycles of length 4, 1 cycle of length 2, and 2 fixed points. Hence $d(x) \leq 6$. □

Now let x be *any* element of $G \setminus R$ of prime order. We will use the previous lemmas of this section to show that $d(x) \leq ((r+1)/2r) \cdot r^a$. For this purpose and for the rest of this section we will use yet another lemma.

Lemma 2.6 (Guralnick, Malle, [10])**.** *Let V_1 and V_2 be an $F\langle x_1\rangle$- and an $F\langle x_2\rangle$-module respectively for any field F and for group elements x_1 and x_2. Then $V_1 \otimes V_2$ can naturally be viewed as an $F\langle (x_1, x_2)\rangle$-module. Moreover, if $d(x_1) \leq c \cdot \dim_F(V_1)$ for some constant c, then $d((x_1, x_2)) \leq c \cdot \dim_F(V_1 \otimes V_2)$.*

Put c to be $(r+1)/2r$. By Lemmas 2.4 and 2.2, it is easy to see that if x acts indecomposably on $R/Z(R)$, then $d(x) \leq c \cdot r^a$. So we may (and do) assume that x does not act indecomposably but decomposably on $R/Z(R)$. We claim that $d(x) \leq c \cdot r^a$. We will argue by induction on the number of indecomposable summands appearing in a direct sum decomposition of the $\langle x\rangle$-module $R/Z(R)$.

First assume that the order of x is coprime to r. Let R_1 be a minimal $\langle x\rangle$-invariant subspace in R. If R_1 is non-degenerate, then, by 19.2 of [1], so is ${R_1}^{\perp}$ and $R = R_1 \circ {R_1}^{\perp}$. By the induction hypothesis, we conclude that $d(x) \leq c \cdot r^a$. So we may (and do) suppose that R_1 is degenerate. By the minimality of R_1, we have $R_1 \subseteq R_1^{\perp}$ (since $R_1 \cap R_1^{\perp}$ is a submodule of R_1). Since R is completely reducible, there exists an $\langle x\rangle$-submodule R_2 of R so that $R = R_1^{\perp} R_2$. If R_2 is non-degenerate, then we can cook up the decomposition $R = R_2 \circ R_2^{\perp}$ and use the induction hypothesis as before. So we may (and do) assume that both R_1 and R_2 are degenerate. Now $R_2 \cap R_2^{\perp}$ is an $\langle x\rangle$-submodule in the completely reducible module R_2 so $R_2 \subseteq R_2^{\perp}$ or there exists a non-degenerate submodule R_3 such that $R_2 = (R_2 \cap R_2^{\perp})R_3$. In the latter case we may write $R = R_3 \circ R_3^{\perp}$ and apply the induction hypothesis to get the desired conclusion. From now on we assume that both R_1 and R_2 are degenerate and $R_1 \subseteq R_1^{\perp}$, $R_2 \subseteq R_2^{\perp}$. Put $\widetilde{R} = R_1 R_2$. We claim that $\widetilde{R}$ is non-degenerate. We must show that $\mathrm{Rad}(\widetilde{R}) \subseteq Z(R)$. Clearly, $\mathrm{Rad}(\widetilde{R}) \subseteq R_1^{\perp}$. Since $R = R_1^{\perp} R_2$, we have $R_2 \cap R_1^{\perp} \subseteq Z(R)$. The previous two statements imply $R_2 \cap \mathrm{Rad}(\widetilde{R}) \subseteq Z(R)$. From this it is not difficult to conclude that $\mathrm{Rad}(\widetilde{R}) \subseteq R_1 \circ Z(R)$. This means that whenever $x \in \mathrm{Rad}(\widetilde{R})$, then $[x, y] = 1$ for all $y \in R_1^{\perp} \cup R_2$. Since $R = R_1^{\perp} R_2$, we conclude that $Z(R) \subseteq \mathrm{Rad}(\widetilde{R}) \subseteq \mathrm{Rad}(R) \subseteq Z(R)$ which is exactly what we wanted; $\widetilde{R}$ is indeed non-degenerate. If $\widetilde{R} \neq R$, then $R = \widetilde{R} \circ \widetilde{R}^{\perp}$ where both $\widetilde{R}$ and $\widetilde{R}^{\perp}$ are non-degenerate and we may use the induction hypothesis to get what we want. So we may assume that $\widetilde{R} = R$.

Now assume that the order of x is r.

For r odd Hesselink [13] showed that in the Jordan normal form of x on $R/Z(R)$ each 'indecomposable part' consists of a Jordan block of even size or of two Jordan blocks (of the same) odd size. (Note that [13, Remark, Page 172] points out that the field of order r need not be quadratically closed.) In the first case, the Jordan block of even size acts on a non-degenerate space, while in the second case, the two Jordan blocks act on totally singular subspaces. By our induction hypothesis and [1, 19.2], we may assume that every 'indecomposable part' consists of two Jordan blocks of odd size.

If $r = 2$ and x is an involution then it is still true that in the Jordan normal form of x on $R/Z(R)$ each 'indecomposable part' consists of a single Jordan block (acting on a non-degenerate space) or of two Jordan blocks (acting on totally singular subspaces). This is because any 2-dimensional subspace of $R/Z(R)$ is either totally singular or non-degenerate with respect to an alternating form. Again by our induction hypothesis and [1, 19.2], we may assume that every 'indecomposable part' of x consists of two Jordan blocks.

Write $R = (R_1R_2) \circ \ldots \circ (R_\ell R_{\ell+1})$ for some odd integer ℓ, where, for all odd $1 \leq i \leq \ell$, the cyclic group $\langle x \rangle$ acts indecomposably on each of the two totally singular $\langle x \rangle$-modules R_i and R_{i+1} with R_iR_{i+1} acting absolutely irreducibly on a vector space V_i where $V = V_1 \otimes V_3 \otimes \ldots \otimes V_\ell$. By Lemma 2.6, it is sufficient to show that for each odd i the invariant $d(x)$ is at most $c \cdot r^{a_i}$ where $r^{a_i} = \dim(V_i)$. But this follows from Lemmas 2.3 and 2.5.

Let us summarize the results obtained so far in this section (with bounds on $\dim_F(C_V(x))$ rather than on $d(x)$).

Theorem 2.7. *Let V be a faithful irreducible FG-module where F is an algebraically closed field of characteristic $p > 0$ and G is a finite group. Suppose that G has a normal subgroup R of symplectic type with $|R/Z(R)| = r^{2a}$ for some prime r and that R acts absolutely irreducibly on V, $\dim_F(V) = r^a$ and $O_p(G) = 1$. Suppose that R is the unique normal subgroup of G that is minimal with respect to being non-central. Let x be an arbitrary non-identity element in G. Then $\dim_F(C_V(x)) \leq ((r+1)/2r) \cdot r^a$.*

Proof. If $1 \neq x \in R$, then $\dim_F(C_V(x)) \leq (1/2) \cdot r^a$. If $x \in G \setminus R$ and x has prime order, then $\dim_F(C_V(x)) \leq ((r+1)/2r) \cdot r^a$. (These were shown earlier.)

Finally, if $1 \neq x \in G$ is arbitrary and q is a prime proper divisor of the order m of x, then $\dim_F(C_V(x)) \leq \dim_F(C_V(x^{m/q})) \leq ((r+1)/2r) \cdot r^a$. □

However we will also need a more detailed result than Theorem 2.7. We start with a lemma.

Lemma 2.8. *Let E be a group of symplectic type with $|E/Z(E)| = 2^{2a}$. Let V be an absolutely irreducible E-module of dimension 2^a. If $1 \neq x$ is a 2-element in the normalizer of E in $GL(V)$ outside E then one of the following holds.*

(1) $\dim C_V(x) \leq (1/2) \dim V$.

(2) *x is an involution and in its action on $E/Z(E)$ each of the $2m$ Jordan blocks of size 2 act on totally singular subspaces. (All other Jordan blocks have size 1.) In this case* $\dim C_V(x) = (1/2)(1 + 2^{-m}) \dim V$.

Proof. Since any element of $E \setminus Z(E)$ has trace 0 on V, the fixed point space of any non-trivial element of E has dimension at most $(1/2) \dim V$. It suffices to assume that x has order 2 or 4. We may also assume that $\langle x \rangle \cap E = 1$.

First suppose that x is an involution. If x leaves a non-degenerate 2-space invariant in its action on $E/Z(E)$, then x normalizes a non-abelian subgroup of order 8, say F. Then V restricted to $J := \langle F, x \rangle$ is a direct sum of 2-dimensional submodules (because $J/Z(J)$ is elementary abelian of order 8 and the derived subgroup of J contains a non-trivial central element of E). Since x is an involution and does not act trivially (since the normal closure of x in J contains the derived subgroup of J), x has trace 0, whence the result.

Thus we may assume that all Jordan blocks of x (in its action on $E/Z(E)$) act on totally singular subspaces. Let the number of Jordan blocks of size 2 be $2m$. These form m pairs acting on the symplectic type 2-groups $E_1, \ldots, E_m$ whose central product with another symplectic type 2-group E_0 is E. (The element x acts trivially on E_0.) Then the $\langle x \rangle$-module V has the form $V_1 \otimes \cdots \otimes V_m \otimes V_0$ where V_i is an irreducible E_i-module for every i with $0 \leq i \leq m$. Now x has trace 2 on each V_i with $1 \leq i \leq m$ and trace $\dim V_0$ on V_0. Hence the trace of x on V is $2^m \dim V_0$ while $\mathrm{tr}(1) = \dim V = 4^m \dim V_0$. But then

$$\dim C_V(x) = (1/2)(\mathrm{tr}(x) + \mathrm{tr}(1)) = (1/2)(1 + 2^{-m}) \dim V.$$

So now assume that x has order 4. Let $F/Z(E)$ be a 3-dimensional subspace of $E/Z(E)$ so that x acts as a single Jordan block on $F/Z(E)$. Suppose that $F/Z(E)$ is totally singular (i.e. F is abelian). Then F has exactly 8 distinct eigenvalues on V and x permutes them in orbits of sizes 1, 1, 2, 4, whence $\dim C_V(x) \leq (1/2) \dim V$.

So we may assume that $F/Z(E)$ is not totally singular. Note that since $[F, F] \cap Z(E) \neq 1$, it follows that every irreducible F-submodule has dimension at least 2. Since $F/Z(F)$ is elementary abelian of order 8, it follows that every absolutely irreducible F-submodule (in any characteristic) has dimension at most 2 (it suffices to see this in characteristic 0, but then we know that every irreducible representation has dimension at most $[F : Z(F)]^{1/2} < 3$). Thus, every irreducible F-submodule (after extending scalars if necessary) of V has dimension 2.

Put $J := \langle F, x \rangle$. Let W be an irreducible J-submodule of V. So W is a direct sum of irreducible F-submodules. If they are not isomorphic, then x is permuting the homogeneous components and so $\dim C_W(x) \leq (1/2) \dim W$. Suppose that W is homogeneous as an F-submodule. Let U be an F-irreducible submodule of W. Thus, W embeds in $X := U_F^J$. If W is 2-dimensional, then as the normal closure of x contains $[F, F]$, x is not trivial. Note that $\dim C_W(x) \leq \dim C_X(x) = 2$. Thus, the result holds for $\dim W > 2$. This completes the proof. □

Let x be the identity or an arbitrary element of $G \setminus R$. View x as a linear transformation on the vector space $R/Z(R)$ and also as an element of $Sp(2a, r)$. We say that x is of type $B(2a, k)$ if the $GL(2a, r)$ Jordan canonical form of x consists of two Jordan blocks each with minimal polynomial f^k for some irreducible polynomial f such that the $GL(2a, r)$ Jordan canonical form of x^q (where q is some power of r) consists of $2k$ Jordan blocks that can be paired off in such a way that each pair of blocks is of the kind treated in Lemma 2.3. Similarly, we say that x is of type $C(2a)$ (or $D(2a)$) if the $GL(2a, r)$ Jordan canonical form of x is the kind treated in Lemma 2.4 (or Lemma 2.5), respectively. We say that x has a part of type $B(2b, k)$, $C(2b)$, or $D(2b)$ if there exists an $\langle x \rangle$-invariant non-degenerate subspace R_1 of R such that the restriction of x to $R_1/Z(R_1)$ is of type $B(2b, k)$, $C(2b)$, or $D(2b)$. Furthermore we say that x has a part of type I_{2b} if there exists an $\langle x \rangle$-invariant non-degenerate subspace R_1 of R such that the restriction of x to the vector space $R_1/Z(R_1)$ of order r^{2b} is the identity.

In the next two sections the following kinds of elements $x \in Sp(2a, r)$ will play a fundamental role. In each case, using Lemma 2.8, Lemmas 2.2, 2.3, 2.4, 2.5, Lemma 2.6, and the argument above, we will give an estimate for $\mathrm{rdim}(x) = \dim_F(C_V(x))/\dim_F(V)$.

(i) Let $r = 2$, i be a positive integer at most 4, and $2i \leq a \leq 8$. The element x has i parts of type $D(4)$ and a part of type $I_{2(a-2i)}$. $\mathrm{rdim}(x) = (1/2)(1 + 2^{-i})$.

If $r = 2$, $a \leq 8$, and $x \neq 1$ is not of case (i) then $\mathrm{rdim}(x) \leq 1/2$.

(ii) Let $r = 3$ and $a \leq 4$. Let i and j be non-negative integers with $1 \leq i + j \leq 4$ and $j \leq 1$. The element x has i parts of order 2 of type $B(2, 1)$, j parts of type $C(2)$, and a part of type $I_{2(a-i-j)}$. $\mathrm{rdim}(x) \leq 2/3$.

If $r = 3$, $a \leq 4$, and $x \neq 1$ is not of case (ii) then $\mathrm{rdim}(x) \leq 5/9$.

(iii) Let $r = 5$ and $a \leq 2$. Let i be 1 or 2 with $i \leq a$. The element x has i parts of order 2 of type $B(2, 1)$ and a part of type $I_{2(a-i)}$. $\mathrm{rdim}(x) \leq 3/5$.

If $r = 5$, $a \leq 2$, and $x \neq 1$ is not of case (iii) then $\mathrm{rdim}(x) \leq 11/25$.

(iv) Let $r = 7$ and $a = 1$. The element x has a part of order 2 of type $B(2, 1)$. $\mathrm{rdim}(x) \leq 4/7$.

If $r = 7$, $a = 1$, and $x \neq 1$ is not of case (iv) then $\mathrm{rdim}(x) \leq 3/7$.

3. Counting certain elements

In this section we are going to keep all the notations and assumptions introduced in Section 2. In particular, let R, F, V, and G be as before.

For our future purposes we need to obtain an upper bound for the number of non-identity elements $x \in G$ where $\dim_F(C_V(x))$ is (relatively) large. We are only interested in certain small cases, when $a \leq 8$ and $r = 2$, $a \leq 4$ and $r = 3$, $a \leq 2$ and $r = 5$, and when $a = 1$ and $r = 7$.

The factor group G/R is isomorphic to a subgroup of the symplectic group $Sp(2a, r)$ or to a subgroup of one of the orthogonal groups $O^{\epsilon}(2a, 2)$.

In this section let L be one of the groups $Sp(2a, r)$ or $O^{\epsilon}(2a, r)$ where ϵ is either $+$ or $-$. By [25], [4] and [2], one can determine the number of elements of L with a given Jordan canonical form.

Much of the following is due to Wall [25], but we also follow Fulman [3].

Let K be the field with r elements, and let $\phi(t) = \alpha_0 + \alpha_1 t + \ldots + t^{deg(\phi)}$ be an irreducible monic polynomial in $K[t]$ such that $\phi(0) = \alpha_0 \neq 0$. Define $\bar{\phi}(t)$ to be the monic polynomial $({\alpha_0}^{-1})t^{deg(\phi)}\phi(t^{-1}) = {\alpha_0}^{-1} + \ldots + ({\alpha_0}^{-1}\alpha_1)t^{deg(\phi)-1} + t^{deg(\phi)}$.

Let x be an element of L. Consider its Jordan canonical form. To each power ϕ^i of an irreducible monic polynomial ϕ one can associate a non-negative integer $m(\phi^i)$, the multiplicity of a Jordan block with characteristic polynomial ϕ^i. Similarly, to every irreducible monic polynomial $\phi \neq t$ one can associate a partition λ_ϕ of the non-negative integer $|\lambda_\phi|$ such that for each i the number of parts equal to i in λ_ϕ is $m(\phi^i)$. For convenience, put $m_i = m(\phi^i)$. In this way we can associate an (ordered) sequence Λ_x of $\ell(a,r)$ partitions to every element $x \in L$ where $\ell(a,r)$ is the number of (monic) irreducible polynomials in $K[t]$ different from t whose degrees are no greater than $2a$. (Note that $\emptyset$ is also considered to be a partition.) Fix such a sequence of partitions Λ. In what follows we will count $\mathcal{N}(\Lambda)$, the number of elements of L whose associated sequence of partitions is Λ.

Our first observation (probably due to Wall) is that $\mathcal{N}(\Lambda) = 0$ unless Λ is such that for all irreducible polynomials ϕ different from t we have $\lambda_\phi = \lambda_{\bar{\phi}}$ and $\sum_{\phi \neq t} |\lambda_\phi| deg(\phi) = 2a$.

The Jordan canonical form of $x \in L$ alone does not determine the conjugacy class of x in L.

In this paragraph let $r \neq 2$. Wall [25] showed that a conjugacy class of $Sp(2a,r)$ corresponds to the following data. To each monic, non-constant, irreducible polynomial $\phi \neq t \pm 1$ associate a partition λ_ϕ (as before), and to $\phi = t \pm 1$ associate a symplectic signed partition $\lambda^{\pm}_\phi$, by which is meant a partition of some natural number $|\lambda^{\pm}_\phi|$ such that the odd parts have even multiplicity, together with a choice of sign for the set of parts of size i for each even $i > 0$. These data represent a conjugacy class of $Sp(2a,r)$ if and only if (1) $|\lambda_t| = 0$, (2) $\lambda_\phi = \lambda_{\bar{\phi}}$ and (3) $\sum_{\phi \neq t} |\lambda_\phi| deg(\phi) = 2a$.

Again, let $r \neq 2$. The orthogonal groups are the subgroups of $GL(m,r)$ preserving a non-degenerate symmetric bilinear form. For $m = 2l+1$ odd, there are two such forms up to isomorphism, with inner product matrices A and δA, where δ is a non-square element of K and A is equal to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0_l & I_l \\ 0 & I_l & 0_l \end{pmatrix}.$$

Denote the two corresponding orthogonal groups by $O^+(m,r)$ and $O^-(m,r)$. This distinction will be useful, even though these groups are isomorphic. For $m = 2l$ even, there are again two non-degenerate symmetric bilinear forms up to isomorphism with inner product matrices

$$\begin{pmatrix} 0_l & I_l \\ I_l & 0_l \end{pmatrix}$$

and

$$\begin{pmatrix} 0_{l-1} & I_{l-1} & 0 & 0 \\ I_{l-1} & 0_{l-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\delta \end{pmatrix}$$

where δ is a non-square element in K. Denote the corresponding orthogonal groups by $O^+(2l,r)$ and $O^-(2l,r)$. These groups are not isomorphic.

Consider the following combinatorial data. To each monic, non-constant, irreducible polynomial $\phi \neq t \pm 1$ associate a partition λ_ϕ of some non-negative integer $|\lambda_\phi|$ (as above), and to $\phi = t \pm 1$ associate an orthogonal signed partition $\lambda^{\pm}_\phi$, by which is meant a partition of some natural number $|\lambda^{\pm}_\phi|$ such that all even parts have even multiplicity, and all odd $i > 0$ have a choice of sign. Wall [25] proved that these data represent a conjugacy class of some orthogonal group if $r \neq 2$ or if $r = 2$ and $\lambda_{t+1} = \emptyset$.

From now on let Λ be the associated sequence of partitions of an element x of L. For an irreducible polynomial ϕ such that $\lambda_\phi \neq \emptyset$, $\phi \neq t$ and $\phi \neq t+1$ when $r = 2$, define

$$B(\phi) = r^{deg(\phi)\left(\sum_{i<j} i m_i m_j + \frac{1}{2}\sum_i (i-1) m_i^2\right)} \prod_i A(\phi^i),$$

where

$$A(\phi^i) = \begin{cases} |Sp(m_i, r)| & \text{if } i \equiv 1 (\text{mod} 2), r \neq 2, \phi = t \pm 1 \text{ and } L = Sp(2a, r); \\ r^{\frac{1}{2}m_i}|O(m_i, r)| & \text{if } i \equiv 0 (\text{mod} 2), r \neq 2, \phi = t \pm 1 \text{ and } L = Sp(2a, r); \\ |O(m_i, r)| & \text{if } i \equiv 1 (\text{mod} 2), r \neq 2, \phi = t \pm 1 \text{ and } L = O^\epsilon(2a, r); \\ r^{-\frac{1}{2}m_i}|Sp(m_i, r)| & \text{if } i \equiv 0 (\text{mod} 2), r \neq 2, \phi = t \pm 1 \text{ and } L = O^\epsilon(2a, r); \\ |U(m_i, r^{deg(\phi)})| & \text{if } t \pm 1 \neq \phi = \bar{\phi}; \\ |GL(m_i, r^{deg(\phi)})|^{1/2} & \text{if } t \pm 1 \neq \phi \neq \bar{\phi}. \end{cases}$$

where, in the second and third cases above, $|O(m_i, r)|$ is $|O^+(m_i, r)|$ if the sign chosen for the parts equal to i is $+$, and is $|O^-(m_i, r)|$ if the sign chosen for the parts equal to i is $-$.

We are now in the position to state the first theorem of this section.

Theorem 3.1 (Wall, [25]). *Use the notations of this section. If Λ is such that $\mathcal{N}(\Lambda) \neq 0$ and $\lambda_{t+1} = \emptyset$ when $r = 2$, then the number of elements in L with associated sequence of partitions Λ is $|L| / \prod_\phi B(\phi)$.*

We will demonstrate Theorem 3.1 with two-three examples, but only after the statement of Theorem 3.2.

We also need some information on proportions of unipotent elements in the group L when $r = 2$. The $GL(2a, r)$ Jordan canonical form of a unipotent element in L can be labelled by a partition μ of $2a$.

Let μ be a partition of a non-negative integer. Let μ_i be the i-th largest part of μ, and let $o(\mu)$ be the number of odd parts of μ. The symbol m_i will denote the number of parts of μ of size i, and μ' is the partition dual to μ in the sense that the i-th largest part μ'_i of μ' is $m_i + m_{i+1} + \dots$. Let $n(\mu) = \sum_i \binom{\mu'_i}{2}$. Then we have

Theorem 3.2 (Fulman, Guralnick, [4]). *The number of elements of $Sp(2a, r)$ which are unipotent and have $GL(2a, r)$ rational canonical form of type μ is 0 unless all odd parts of μ occur with even multiplicity. If all odd parts of μ occur with even multiplicity, it is*

$$\frac{r^{a^2}\prod_{i=1}^{a}(r^{2i}-1)}{r^{n(\mu)+a+o(\mu)/2}\prod_i (1-1/r^2)\dots(1-1/r^{2[m_i(\mu)/2]})}.$$

Note that this theorem holds even when r is a prime power, however, we are only interested in the case when r is a prime and mostly when $r = 2$.

Next we will give a few examples on how Theorems 3.1 and 3.2 can be used to estimate the numbers of certain kinds of elements. For the reader's convenience we recall the formulas for the orders of the classical groups we will be working with.

$$|Sp(2m,r)| = r^{m^2}\prod_{i=1}^{m}(r^{2i}-1);$$

$$|O^{\epsilon}(2m,r)| = 2r^{m(m-1)}(r^m-\epsilon)\prod_{i=1}^{m-1}(r^{2i}-1);$$

$$|O^{\epsilon}(2m+1,r)| = 2r^{m}\prod_{i=0}^{m-1}(r^{2m}-r^{2i}).$$

Example (i). Using Theorem 3.2 we count elements x of $Sp(2a,2)$ of type (i) of Section 2. (The group $Sp(2a,2)$ has two 2-transitive permutation representations, one with point-stabilizer $O^{+}(2a,2)$ and one with point-stabilizer $O^{-}(2a,2)$. So the groups $O^{\epsilon}(2a,2)$ can be considered as subgroups of $Sp(2a,2)$.) Here $\mu = (2^{2i},1^{2a-4i})$, $o(\mu) = 2a-4i$, $m_2 = 2i$, $m_1 = 2a-4i$, $\mu'_1 = 2a-2i$, $\mu'_2 = 2i$, and $n(\mu) = (a-i)(2a-2i-1)+i(2i-1)$. Thus the number of elements x we are looking for is (at most)

$$\frac{2^{i(i+1)}\prod_{j=1}^{a}(2^{2j}-1)}{\Big(\prod_{j=1}^{a-2i}(2^{2j}-1)\Big)\cdot\Big(\prod_{j=1}^{i}(2^{2j}-1)\Big)}.$$

Example (ii). Using Theorem 3.1 we count elements x of $Sp(2a,3)$ of type (ii) of Section 2. If $\phi = t+1$ then $m_1 = 2i$ and $B(\phi) = |Sp(2i,3)|$ where $|Sp(0,3)| = 1$. If $\phi = t-1$ then $m_1 = 2(a-i-j)$, $m_2 = j$ and

$$B(\phi) = 3^{2(a-i-j)j+(1/2)j(j+1)}|Sp(2(a-i-j),3)|\cdot|O^{\epsilon}(j,3)|$$

where $|O^{\epsilon}(0,3)| = 1$ and ϵ is the sign chosen for the parts of size 2. Hence the number of elements x we are looking for is (at most)

$$\left(\frac{|Sp(2a,3)|}{3^{2(a-i-j)j+(1/2)j(j+1)}\cdot|Sp(2i,3)|\cdot|Sp(2(a-i-j),3)|}\right)\left(\frac{1}{|O^{+}(j,3)|}+\frac{1}{|O^{-}(j,3)|}\right).$$

Example (iii). Using Theorem 3.1 we count elements x of $Sp(2a,r)$ of types (iii) and (iv) of Section 2. (We have $r=5$ in the first case and $r=7$ in the second.) Suppose first that $(r,a,i)\neq(5,2,1)$. Then $\phi = t+1$, $m_1 = 2a$, and $B(\phi) = |Sp(2a,r)|$. Hence the number of such elements x is 1. Now let $(r,a,i) = (5,2,1)$. Then the number of such elements x is $5^2(5^2+1)$.

Consider the table below. The star in a row corresponding to the group $Sp(2a,r)$ stands for the positive integer $|Sp(2a,r)|$. Let A and B be two consecutive entries in the row corresponding to $Sp(2a,r)$. Suppose that A (respectively B) lies in the column corresponding to the fraction c_A (respectively c_B). (Clearly $c_A < c_B$.) Now $|R|B$ is an upper bound for the number of elements x in G with $c_A < \mathrm{rdim}(x) \leq c_B$.

	3/7	11/25	1/2	17/32	5/9	9/16	4/7	3/5	2/3	5/8	3/4
$Sp(16,2)$			*	2^{72}		2^{67}				2^{53}	2^{31}
$Sp(14,2)$			*			2^{55}				2^{45}	2^{27}
$Sp(8,3)$					*				3^{29}		
$Sp(12,2)$			*			2^{43}				2^{37}	2^{23}
$Sp(10,2)$			*							2^{29}	2^{19}
$Sp(6,3)$					*				3^{13}		
$Sp(4,5)$		*						651			
$Sp(8,2)$			*							2^{21}	2^{15}
$Sp(4,3)$					*				982		
$Sp(6,2)$			*								2^{11}
$Sp(2,7)$	*						1				
$Sp(2,5)$		*						1			
$Sp(4,2)$			*								2^7
$Sp(2,3)$					*				10		
$Sp(2,2)$			*								

4. The proof of Theorem 1.1

Let $k(X)$ denote the number of conjugacy classes of a finite group X. This is also the number of complex irreducible characters of X. We will use the following important result.

Lemma 4.1. *Let G be a group of linear transformations of the finite vector space V, and let GV be the semidirect product of V and G. Then*

$$k(GV) = \sum k(\mathrm{Stab}_G(\lambda))$$

where λ is a complex irreducible character of V and the sum is over a set of representatives ($\lambda \in \mathrm{Irr}(V)$) of the G-orbits of $\mathrm{Irr}(V)$.

Notice that, in the previous two sections, our vector space was finite dimensional over an algebraically closed field. If F is a finite subfield of an algebraically closed field K and V is an $F\langle x\rangle$-module for some cyclic subgroup $\langle x\rangle$, then, in a natural way, V also has the structure of an $K\langle x\rangle$-module where $\dim_K(V) = \dim_F(V)$. Notice that we also have $\dim_K(C_V(x)) = \dim_F(C_V(x))$.

In this section G will denote a slightly different subgroup as in the previous two sections. Let r be a prime and let R be an r-group of symplectic type with $|R/Z(R)| = r^{2a}$ for some positive integer a. Let V be a faithful, absolutely irreducible KR-module of dimension r^a for some finite field K. View V as an F-vector space where F is the prime field of K. Let G be a subgroup of $GL(V)$ which contains R as a normal subgroup. Let $A = C_G(K^*)$.

The group A is such that $A/R \leq Sp(2a, r)$ or $A/R \leq O^{\epsilon}(2a, 2)$ (latter only if $r = 2$ and $|Z(R)| = 2$) and $|G/A| \leq k$ where $|K| = p^k$ and p is prime. We have $\dim(C_V(x))/\dim V \leq 1/2$ for every $x \in G \setminus A$. (Indeed, there exists $z \in K^*$ with $1 \neq [x,z] \in K^*$ and thus $C_V([x,z]) = 1$. Hence $C_V(x^{-1}) \cap C_V(x^z) = 1$. This implies $|V| \geq |C_V(x^{-1})C_V(x^z)| = |C_V(x^{-1})||C_V(x^z)| = |C_V(x)|^2$.) By this fact, by Theorem 2.7, and by the Orbit-Counting Lemma, the number of G-orbits on V is at most $(|V|/|G|)+|V|^c$ where $c=(r+1)/2r$. By Brauer's Permutation Lemma, the number of G-orbits on $\mathrm{Irr}(V)$ is also at most $(|V|/|G|)+|V|^c$.

Let m be the maximum of the $k(\mathrm{Stab}_G(\lambda))$'s as λ runs through the set of all non-trivial linear characters of V. Then Lemma 4.1 gives

$$k(GV) \leq k(G) + m((|V|/|G|) + |V|^c - 1). \tag{3}$$

Let λ be a non-trivial character in $\mathrm{Irr}(V)$. Then $R \cap \mathrm{Stab}_G(\lambda)$ is an Abelian subgroup of R of order r^t for some non-negative integer t at most a. Hence $|G : \mathrm{Stab}_G(\lambda)| \geq r^{2a+1-t}$. This gives $m \leq |G|/r^{a+1}$. Applying these estimates to (3) we get

$$k(GV) \leq |G| + (|V|/r^{a+1}) + (|G|/r^{a+1})(|V|^c - 1). \tag{4}$$

It is possible to see that the right-hand-side of (4) is less than $|V|$ unless $a \leq 8$ and $r=2$, $a \leq 4$ and $r=3$, $a \leq 2$ and $r=5$, or $a=1$ and $r=7$. (Here we used the fact that $r \mid (|K|-1)$ and that $|K| \geq 5$ in case $|Z(R)|=4$.)

Now let (a,r) be such an exceptional pair.

For $r=3, 5, 7$ let $c_1 = 2/3, 3/5, 4/7$ and $c_2 = 5/9, 1/2, 1/2$ respectively. By use of the table of the previous section, we may give an upper bound d_1 for the number of elements x in G with $c_2 < \dim(C_V(x))/\dim V \leq c_1$. Using this, Lemma 4.1 and our bound for m, we get

$$\begin{aligned} k(GV) &\leq k(G) + m((|V|/|G|) + (d_1/|G|)|V|^{c_1} + |V|^{c_2}) \\ &\leq |G| + (|V|/r^{a+1}) + (d_1/r^{a+1})|V|^{c_1} + (|G|/r^{a+1})|V|^{c_2}. \end{aligned} \tag{5}$$

For $r=2$ we use a slightly more detailed bound for $k(GV)$. For each integer i with $1 \leq i \leq 4$ let d_i be the upper bound (coming from the table of the previous section) for the number of elements x in G with

$$\dim(C_V(x))/\dim V = (1/2)(1+2^{-i}).$$

Note that $d_i = 0$ whenever $a < 2i$. Then, as before,

(6)

$$\begin{aligned} k(GV) &\leq k(G) + m((|V|/|G|) + \sum_{i=1}^{4}((d_i/|G|)|V|^{(1/2)(1+2^{-i})}) + |V|^{1/2}) \\ &\leq |G| + (|V|/2^{a+1}) + \sum_{i=1}^{4}((d_i/2^{a+1})|V|^{(1/2)(1+2^{-i})}) + (|G|/2^{a+1})|V|^{1/2}. \end{aligned}$$

Now let $a=8$ and $r=2$. By the last paragraph of Section 2 and the table of Section 3, there are at most 2^{49} elements x in G with $\mathrm{rdim}(x) = \dim(C_V(x))/\dim V = 3/4$, at most 2^{71} elements x with $\mathrm{rdim}(x) = 5/8$, at most 2^{85} elements x with $\mathrm{rdim}(x) = 9/16$, and at most 2^{90} elements x with $\mathrm{rdim}(x) = 17/32$. This together with (6) shows that $k(GV)$ is at most

$$|G| + (|V|/2^9) + 2^{40}|V|^{3/4} + 2^{62}|V|^{5/8} + 2^{76}|V|^{9/16} + 2^{81}|V|^{17/32} + (|G|/2^9)|V|^{1/2} \leq |V|.$$

Now let $a=7$ and $r=2$. By the last paragraph of Section 2, the table of Section 3, and (6) we have

$$k(GV) \leq |G| + (|V|/2^8) + 2^{35}|V|^{3/4} + 2^{53}|V|^{5/8} + 2^{63}|V|^{9/16} + (|G|/2^8)|V|^{1/2} \leq |V|.$$

Now let $a = 4$ and $r = 3$. By the table of the previous section, Theorem 2.7, and (5) we have

$$k(GV) \leq |G| + (|V|/3^5) + (3^{33})|V|^{2/3} + (|G|/3^5)|V|^{5/9} \leq |V|.$$

Now let $a = 5$ and $r = 2$. By the last paragraph of Section 2, the table of Section 3, and (6) we have

$$k(GV) \leq |G| + (|V|/2^6) + 2^{25}|V|^{3/4} + 2^{35}|V|^{5/8} + (|G|/2^6)|V|^{1/2}.$$

This is at most $|V|$ for $|V| \geq 17^{32}$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, 7, 11, 17, 31, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 3$, 5, 7, 9, or 11. In all these exceptional cases we have $k(GV) \leq 2^{119}$.

Now let $a = 3$ and $r = 3$. By the table of the previous section, Theorem 2.7, and (5) we have

$$k(GV) \leq |G| + (|V|/3^4) + 3^{16}|V|^{2/3} + (|G|/3^4)|V|^{5/9}.$$

This is at most $|V|$ for $|V| \geq 13^{27}$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, 7, 13, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 4$ or 7. In all these exceptional cases we have $k(GV) \leq 2^{82}$.

Now let $a = 2$ and $r = 5$. By the table of the previous section, Theorem 2.7, and (5) we have

$$k(GV) \leq |G| + (|V|/5^3) + 651 \cdot 5^2|V|^{3/5} + (|G|/5^3)|V|^{1/2} \leq |V|.$$

Now let $a = 4$ and $r = 2$. By the last paragraph of Section 2, the table of Section 3, and (6) we have

$$k(GV) \leq |G| + (|V|/2^5) + 2^{20}|V|^{3/4} + 2^{26}|V|^{5/8} + (|G|/2^5)|V|^{1/2}.$$

This is at most $|V|$ for $|V| \geq 41^{16}$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, 7, 17, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 3$, 5, 7, 9, 17, 25, or 27. In all these exceptional cases we have $k(GV) \leq 2^{82}$.

Now let $a = 2$ and $r = 3$. By the table of the previous section, Theorem 2.7, and (5) we have

$$k(GV) \leq |G| + (|V|/3^3) + 8838|V|^{2/3} + (|G|/3^3)|V|^{5/9}.$$

This is at most $|V|$ for $|V| \geq 31^9$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 4$, 16, or 25. In all these exceptional cases we have $k(GV) \leq 2^{44}$.

Now let $a = 3$ and $r = 2$. By the last paragraph of Section 2, the table of Section 3, and (6) we have

$$k(GV) \leq |G| + (|V|/2^4) + 2^{15}|V|^{3/4} + (|G|/2^4)|V|^{1/2}.$$

This is at most $|V|$ for $|V| \geq 191^8$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, 7, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 3$, 5, 7, 9, 25, 27, 49, 81, or 125. In all these exceptional cases we have $k(GV) \leq 2^{58}$.

Now we turn to the treatment of the case $a = 6$ and $r = 2$. We need a couple of lemmas.

Lemma 4.2 (Nagao, [21])**.** *Let N be a normal subgroup in a finite group X. Then $k(X) \leq k(N) \cdot k(X/N)$.*

Lemma 4.3. *Let H be a subgroup of a finite group X. Then $k(H) \leq \sqrt{|X| \cdot k(X)}$.*

Lemma 4.3 is an easy consequence of a result of Gallagher [6] saying that $k(H) \leq (X : H)k(X)$.

Recall what m and k were above.

Lemma 4.4. *Let $a = 6$ and $r = 2$. Then $m \leq 2^{50}k$.*

Proof. Let λ be a non-trivial linear character of V with $k(\mathrm{Stab}_G(\lambda)) = m$. Put $T = \mathrm{Stab}_G(\lambda)$. Since $R \cap T$ is normal in T, we have $k(T) \leq k(R \cap T) \cdot k(T/(R \cap T))$ by Lemma 4.2, which is at most $r^a \cdot k(TR/R)$. By Lemma 4.2 again, we see that $k(TR/R) \leq k \cdot k((TR \cap A)/R)$. Now $H := (TR \cap A)/R$ can be viewed as a subgroup of $X := Sp(12, 2)$, and thus, by Lemma 4.3, we have $k(H) \leq \sqrt{|X| \cdot k(X)} < 2^{44}$. (Here the estimate for $k(X)$ came from [5, Theorem 3.13].) Summing up, we have $k(T) \leq 2^{50}k$. □

By the last paragraph of Section 2, the table of Section 3, and (6) we have that

$$k(GV) \leq |G| + (|V|/2^7) + 2^{34}|V|^{3/4} + 2^{52}|V|^{5/8} + 2^{62}|V|^{9/16} + m|V|^{1/2}.$$

By using the bound of Lemma 4.4 for m, we see that this is at most $|V|$ provided that $|V| \geq 5^{64}$, and is less than 2^{120} if $|V| = 3^{64}$.

Finally we turn to the treatment of the cases $a = 1$ and $(a, r) = (2, 2)$. The following lemma can be verified by GAP [7].

Lemma 4.5. *Let $a = 1$. If $r = 7$, 5, 3, 2, then m is at most $98k$, $50k$, $9k$, $6k$ in the respective cases. If $(a, r) = (2, 2)$ then $m \leq 44k$.*

Now let $a = 1$ and $r = 7$. By the table of the previous section, Theorem 2.7, (5), and Lemma 4.5 we have

$$k(GV) \leq |G| + (|V|/7^2) + 7|V|^{4/7} + m|V|^{1/2} \leq |V|.$$

Now let $a = 1$ and $r = 5$. By the table of the previous section, Theorem 2.7, (5), and Lemma 4.5 we have

$$k(GV) \leq |G| + (|V|/5^2) + 5|V|^{3/5} + m|V|^{1/2} \leq |V|.$$

Now let $a = 1$ and $r = 3$. By the table of the previous section, Theorem 2.7, (5), and Lemma 4.5 we have

$$k(GV) \leq k(G) + (|V|/3^2) + m|V|^{2/3},$$

which is at most $|V|$ whenever $|V| \geq 13^3$. If $|V| = 7^3$ then $|G|$ is coprime to $|V|$ and hence we have $k(GV) \leq |V|$ by the (classical) $k(GV)$ theorem. If $|V| = 4^3$ then the inequality $k(GV) \leq |V|$ can be checked by GAP [7].

Now let $a = 1$ and $r = 2$. By the last paragraph of Section 2, the table of Section 3, (6), and Lemma 4.5 we have

$$k(GV) \leq k(G) + (|V|/2^2) + m|V|^{1/2},$$

which is at most $|V|$ provided that $|V| \geq 13^2$. By the (classical) $k(GV)$ theorem, we may assume that the action of G on V is non-coprime, that is, the cases remaining are $|V| = 3^2$ and $|V| = 9^2$. In both these cases we have $k(GV) \leq \max\{|V|, 11\}$ by use of GAP [7].

Finally let $a = 2$ and $r = 2$. By the last paragraph of Section 2, the table of Section 3, (6), and Lemma 4.5 we have

$$k(GV) \leq |G| + (|V|/2^3) + 44k|V|^{3/4}.$$

This is at most $|V|$ for $|V| > 243^4$. Notice that the possible prime divisors of $|G|$ are 2, 3, 5, and the prime divisors of k. Thus by the (classical) $k(GV)$ theorem we have $k(GV) \leq |V|$ unless $|K| = 3$, 5, 9, 25, 27, 81, 125, or 243. In all these exceptional cases we have $k(GV) \leq 2^{32}$.

This completes the proof of Theorem 1.1.

5. Another estimate for $k(GV)$

Let $t \geq 2$ be a positive integer. For all integers i such that $1 \leq i \leq t$ define r_i, R_i, a_i, V_i, G_i in the following way. Let r_i be a prime and let R_i be an r_i-group of symplectic type with $|R_i/Z(R_i)| = r_i^{2a_i}$ for some positive integer a_i. Suppose also that $r_i \neq r_j$ whenever $i \neq j$. Let V_i be a faithful, absolutely irreducible KR_i-module of dimension $r_i^{a_i}$ for some finite field K. View V_i as an F-vector space where F is the prime field of K. Let G_i be a subgroup of $GL(V_i)$ which contains R_i as a normal subgroup. Let G be the central product of the G_i's with Z for some group of scalars Z. (Put $A = C_G(K^*)$.) Then the vector space $V = V_1 \otimes_F \cdots \otimes_F V_t$ can be considered as an FG-module.

In this section we will bound $k(GV)$ using Lemma 4.1.

Let R be the central product of all the R_i's and Z. Moreover put $n = \prod_{i=1}^t r_i^{a_i}$ which is the K-dimension of the vector space V.

Lemma 5.1. *Use the notations of this section. If λ is a non-trivial linear character of V then $|\mathrm{Stab}_G(\lambda)| \leq |G/R| \cdot n$.*

Proof. The inertia group $\mathrm{Stab}_R(\lambda)$ of a non-trivial linear character λ of V in R is abelian since it embeds injectively into the abelian group $R/Z(R)$. For all i the subgroup $\mathrm{Stab}_R(\lambda) \cap R_i$ is abelian of order at most $r_i^{a_i}$. Hence $|\mathrm{Stab}_G(\lambda)| \leq |G/R||\mathrm{Stab}_R(\lambda)| \leq |G/R| \cdot n$. □

By [19, Pages 82-83] we have $\dim(C_V(x))/\dim V \leq 3/4$ for all non-identity elements x in G. This and Lemma 4.1 imply (as in the previous section) that

$$k(GV) \leq |G| + m((|V|/|G|) + |V|^{3/4})$$

where m is the maximum of the $k(\mathrm{Stab}_G(\lambda))$'s as λ runs through the set of non-trivial linear characters of V. By Lemma 5.1 this number is at most $|G/R| \cdot n$, hence we get

$$k(GV) \leq |G| + ((|V| \cdot n)/|R|) + ((|G| \cdot n)/|R|)|V|^{3/4}. \tag{7}$$

Now $n^2 \leq |R| \leq n^3|K|$ and

$$|G/R| \leq k \cdot \prod_{i=1}^{t} |Sp(2a_i, r_i)| \leq k \cdot n^{3\log_2 n}$$

where $|K| = p^k$ and $|F| = p$. Hence (7) gives

$$k(GV) \leq p^k \cdot k \cdot n^{3+3\log_2 n} + (|V|/n) + p^k \cdot k \cdot n^{1+3\log_2 n}|V|^{3/4}$$

which is, by inspection, at most $\max\{|V|, 2^{1344}\}$.

Summarizing the content of this section with Theorem 1.1 we get the following.

Theorem 5.2. *Use the notations of this section with allowing $t = 1$. Then $k(GV) \leq \max\{|V|, 2^{1344}\}$.*

6. The meta-cyclic case

In this section we prove Theorem 1.2.

Let p be a prime. Let X be $GL(1, p^n).n$ for some positive integer n. Then X has a maximal abelian normal subgroup S which is cyclic of order $p^n - 1$ and $|X| = n(p^n - 1)$. Furthermore, X is meta-cyclic and any element x of X can be written in the form $x = a^k b^l$ for some integers k and l with $0 \leq k < p^n - 1$ and $0 \leq l < n$ where $\langle a \rangle = S$, $\langle bS \rangle = X/S$, and $a^p b = ba$.

Let G be a subgroup of X. Then $G/(S \cap G)$ is cyclic of order d for some d dividing n and $1 \leq d \leq n$. Suppose that $S \cap G = \langle a^m \rangle$ where m is an integer with $0 < m \leq p^n - 1$ and is as small as possible. By our choice of m the integer $p^n - 1$ is divisible by m. Let $c \in G$ so that $c(S \cap G)$ generates $G/(S \cap G)$. Then there exists an integer k with $0 \leq k < p^n - 1$ so that c is of the form $a^k b^{n/d}$.

The group G acts in a natural way on the n-dimensional vector space V over $GF(p)$. Let the semidirect product of G with the abelian (additive) group V be GV. Let us view V as a field of order p^n and let a_0 be a generator of the multiplicative group of V so that the equations $b^{-1}a_0^t b = a_0^{tp}$ and $a^{-1}a_0^t a = a_0^{t+1}$ hold for every integer t with $0 \leq t < p^n - 1$.

In order to prove Theorem 1.2 we wish to bound the number $k(GV)$ of complex irreducible characters of the group GV. By [7], Theorem 1.2 can be verified for all prime powers p^n at most 1024. Hence from now on in our considerations we will assume that $p^n > 1024$.

We will use several lemmas to show Theorem 1.2.

Lemma 6.1 (Gallagher, [6])**.** *Let H be a finite group, N be a normal subgroup in H, χ be an irreducible character of N, and $I(\chi)$ be its inertia subgroup. Then the number of irreducible characters of H which lie over (H-conjugates of) χ is at most $k(I(\chi)/N)$.*

Clearly, to apply the above lemmas, we are interested in the G-orbits of the set $\mathrm{Irr}(V)$. In case $|G|$ is not divisible by p, then $\mathrm{Irr}(V)$ and V are permutation isomorphic G-sets, however this is not always so in case p divides $|G|$. In any case, the following two consequences of Brauer's Permutation Lemma ([14, Theorem 6.32]) will be used.

Lemma 6.2. *The number of G-orbits on $\mathrm{Irr}(V)$ is equal to the number of G-orbits on V.*

Lemma 6.3. *Let H be a finite group, N be an abelian normal subgroup in H, and suppose that H/N is cyclic. Then there is a size preserving bijection between the set of H/N-orbits of $\mathrm{Irr}(N)$ and the set of H/N-orbits of N.*

We may assume that $d > 1$. Indeed, if $d = 1$, then $G = S \cap G$, and so G acts semiregularly on the set of non-zero vectors of V. Since p does not divide $|G|$, the G-sets V and $\mathrm{Irr}(V)$ are permutation isomorphic. Hence, by Lemma 4.1, $k(GV) = k(G) + m = ((p^n - 1)/m) + m \leq p^n$ which is exactly what we wanted.

From now on assume that $d > 1$ and let q be the smallest prime divisor of d.

Lemma 6.4. *With the above notations and assumptions we have*

$$k(G) \leq \frac{q^2-1}{q^2} d(p^{n/d}-1) + \frac{d(p^n-1)}{q^2 m}.$$

Proof. We see that

$$[a^m, c^{-1}] = [a^m, b^{-n/d}] = a^{-m} b^{n/d} a^m b^{-n/d} = a^{m(p^{n/d}-1)} \in G'.$$

Hence $|G'| \geq \frac{p^n-1}{m(p^{n/d}-1)}$ and so $|G/G'| \leq d(p^{n/d}-1)$. This means that the number of linear complex irreducible characters of G is at most $d(p^{n/d}-1)$. By the fact that $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|$ and by Ito's Theorem ([14, Corollary 6.15]) we have

$$|\mathrm{Irr}(G)| \leq d(p^{n/d}-1) + \frac{|G| - d(p^{n/d}-1)}{q^2} = \frac{q^2-1}{q^2} d(p^{n/d}-1) + \frac{d(p^n-1)}{q^2 m}.$$

□

Lemma 6.5. *Use the above notations and assumptions. Let g be a non-identity element of G. Then $|C_V(g)| \leq |V|^{1/q}$.*

Proof. Let $g = a^l b^{r(n/d)}$ be a non-identity element of G for some integers l and r with $0 \leq l < p^n - 1$ and $0 \leq r < d$. We may assume that $0 < r$.

Let t be an integer with $0 \leq t < p^n - 1$ so that ${a_0}^t$ is centralized by g. Then

$$a_0^t = g^{-1} a_0^t g = b^{-r(n/d)} a^{-l} {a_0}^t a^l b^{r(n/d)} = b^{-r(n/d)} {a_0}^{t+l} b^{r(n/d)} = {a_0}^{(t+l)p^{r(n/d)}}.$$

This implies that $t \equiv (t+l)p^{r(n/d)} \pmod{p^n - 1}$, that is,

$$(p^{r(n/d)} - 1)t \equiv -lp^{r(n/d)} \pmod{p^n-1}.$$

Let s_0 be the smallest positive integer s so that $p^n - 1 \mid s(p^{r(n/d)} - 1)$. Then $s_0 \mid p^n - 1$.

It is easy to see that for any integer x there is either no solution t to the congruence

$$(p^{r(n/d)}-1)t \equiv x \pmod{p^n-1}$$

or there are exactly $(p^n-1)/s_0$ solutions t in the range $0 \leq t < p^n-1$. For $x=0$ there is a solution hence there must be $(p^n-1)/s_0$. So in order to maximize $|C_V(g)|$ we may assume that $s_0 = 1$ and thus $-lp^{r(n/d)} \equiv 0 \pmod{p^n-1}$, that is, $l=0$ and thus $g = b^{r(n/d)}$. But in this case $C_V(g)$ can be considered as a subfield of V of order at most $p^{n/q}$ (where q is the smallest prime divisor of d). □

Lemma 6.6. *The number of G-orbits on* $\mathrm{Irr}(V)$ *is at most* $(|V|/|G|)+|V|^{1/q}$.

Proof. This follows from Lemmas 6.2 and 6.5. □

We may assume that $m < p^n-1$. For otherwise $|G| = d$ and $G = \langle c\rangle$. By Lemmas 6.3, 6.5, and 6.6, there are at most $|V|^{1/q}$ G-invariant irreducible characters of V and all other complex irreducible characters of V lie in G-orbits of lengths at least q. By Lemmas 6.1 and 6.6 we find that

$$k(GV) \leq \frac{d}{q}\frac{|V|}{d} + d|V|^{1/q} = \frac{|V|}{q} + d|V|^{1/q} \leq |V|$$

unless $p^n \leq 64$ (but we assumed that $p^n > 1024$).

Lemma 6.7. *Let χ be an irreducible character of V. Then $I(\chi)/V$ is a cyclic group of order at most d.*

Proof. This follows from the fact that $(I(\chi)/V)\cap(S\cap G)$ is trivial since $S\cap G$ acts semiregularly on $V\setminus\{1\}$ and hence acts semiregularly on $\mathrm{Irr}(V)\setminus\{1\}$ (since V and $\mathrm{Irr}(V)$ are permutation isomorphic $S\cap G$ sets). □

Lemma 6.8. *Use the above notations and assumptions. We have*

$$k(GV) \leq \frac{q^2-1}{q^2}d(p^{n/d}-1) + \frac{(p^n-1)d}{q^2m} + \frac{p^n}{p^n-1}m + dp^{n/q}.$$

Proof. By Lemmas 6.1, 6.6, and 6.7 we have $k(GV) \leq k(G) + d((|V|/|G|)+|V|^{1/q})$. Finally, the claim follows from Lemma 6.4. □

Using Lemma 6.8 and our assumptions including the hypothesis that $p^n > 1024$, we may assume that $m < d$. Indeed, if $m = (p^n-1)/2$, then $k(GV) \leq |V|$. (Cases $d=2$, $d=3$, and $d \geq 4$ should be treated separately.) Also, if $m = (p^n-1)/3$, then $k(GV) \leq |V|$. Finally, if $d \leq m \leq (p^n-1)/4$, then $k(GV) \leq |V|$. (Cases $d=2$ and $d \geq 3$ should be treated separately.)

Let $n=2$. Then $d=2=n$. Since $m<d$, we have $m=1$, and so $G=X$. There are $p-1$ fixed points of $\langle b\rangle$ on S and $(p^2-p)/2$ orbits of length 2. Hence, by Lemmas 6.3 and 6.1, we have $k(G) \leq 2(p-1)+(p^2-p)/2$. This and the proof of Lemma 6.8 gives

$$k(GV) \leq 2(p-1) + \frac{p^2-p}{2} + \frac{p^2}{p^2-1} + 2p$$

which is at most p^2 (provided that $p^2 > 1024$).

By the previous paragraph we may assume that $n > 2$.

By Zsigmondy's Theorem, there is a primitive prime divisor p_n of $p^n - 1$. By a primitive prime divisor we mean a prime which divides $p^n - 1$ but divides none of the integers $p^r - 1$ where $1 \leq r < n$. Such a primitive prime divisor is congruent to 1 modulo n, in particular, $p_n \geq n + 1$. Since $m < d \leq n < p_n$, the prime p_n does not divide m.

For every integer t with $1 \leq t \leq (p^n - 1)/m$ and for every integer r with $1 \leq r \leq d$ we have

$$c^r a^{mt} c^{-r} = a^{p^{nr/d} mt}.$$

If $p_n \nmid t$, then $p_n \nmid mt(p^{nr/d} - 1)$ for $r < d$, and so $p^n - 1 \nmid mt(p^{nr/d} - 1)$ for $r < d$. This means that a^{mt} is not fixed by any element c^r for $r < d$. We conclude that if $p_n \nmid t$, then a^{mt} lies in a $\langle c \rangle$-orbit of $S \cap G$ of length d. There are at most $(p^n - 1)/mp_n$ elements of $S \cap G$ which lie in $\langle c \rangle$-orbits of lengths less than d. Hence there are at most

$$\frac{p^n - 1}{mp_n} + \frac{p^n - 1}{md} - \frac{p^n - 1}{mdp_n}$$

$\langle c \rangle$-orbits of $S \cap G$.

Lemma 6.9. *By the above notations and assumptions including $m < d$, we have*

$$k(GV) \leq \frac{d(p^n - 1)}{mp_n} + \frac{p^n - 1}{md} - \frac{p^n - 1}{mdp_n} + \frac{p^n}{p^n - 1} m + dp^{n/q}.$$

Proof. This follows from Lemmas 6.3, 6.1, and 6.6. □

By Lemma 6.9, we may assume that $m = 1$. This follows by treating the three cases $m \geq 3$, $m = 2$ and $d = 2$, and $m = 2$ and $d \geq 3$ separately. Since $m = 1$, we may assume that $c = b^{n/d}$.

Lemma 6.10. *If $m = 1$, then*

$$k(GV) < \sum_{r|d} \left(\frac{d}{r^2} p^{nr/d} \right) + 2 + dp^{n/q}.$$

Proof. By Lemma 6.9 and its proof it is sufficient to show that

$$k(G) < \sum_{r|d} \left(\frac{d}{r^2} p^{nr/d} \right).$$

For any positive integer r dividing d and any integer t the element a^t of S is fixed by c^{-r} if and only if $p^n - 1 \mid t(p^{nr/d} - 1)$. Hence there are less than $p^{nr/d}/r$ orbits of length r of $\langle c \rangle$ on S. Now apply Lemma 6.3 and Lemma 6.1 to obtain the desired conclusion. □

Using Lemma 6.10 and the assumption that $p^n > 1024$, we find that $k(GV) \leq |V|$ for d a prime and for $d = 4$, 6, 8, and 9. Hence we may assume that $d \geq 10$.

Finally, again by Lemma 6.10, if $d \geq 10$ and $p^n > 1024$, we have

$$k(GV) < \frac{p^n}{d} + \frac{4p^{n/2}}{d} + \frac{9 \cdot p^{n/3}}{d} + n^2 p^{n/4} + 2 + n \cdot p^{n/2} \leq p^n.$$

This finishes the proof of Theorem 1.2.

7. Primitive linear groups

Let V be a finite faithful irreducible primitive FG-module. Suppose that the generalized Fitting subgroup of G is nilpotent. In this section we will prove the estimates $k(GV) \leq \max\{|V|, 2^{1344}\}$. This will verify Theorem 1.3.

Put $q = |F|$ and let n be the F-dimension of V. We may consider G as a primitive (irreducible) subgroup of $GL(n, q)$. We may also assume that G is absolutely irreducible. (For suppose that $F \neq K := \mathrm{End}_{FG}(V)$. Then V can be viewed as a K-vector space of dimension $n/|K : F|$. In fact V is an absolutely irreducible, primitive and faithful KG-module. So if we prove the bound for $k(GV)$ where V is a KG-module, then the same bound will hold when V is an FG-module.)

Let us recall a consequence of Clifford's theorem. A normal subgroup of a primitive (irreducible) linear group acts homogeneously on the underlying vector space. This means that any two simple submodules of the normal subgroup are isomorphic. One importance of this observation is that if $N \leq GL(n, q)$ is a normal subgroup of a primitive group, then N is irreducible or N can be considered to be an irreducible subgroup of $GL(d, q)$ where $d < n$ and $d \mid n$.

First suppose that whenever N is a normal subgroup of G, then every irreducible FN-submodule of V is absolutely irreducible.

As we have noted before, every normal subgroup of G acts homogeneously on V. In particular, any abelian normal subgroup acts homogeneously, and so is cyclic by Schur's lemma. Furthermore, by our hypothesis on the normal subgroups of G, an abelian normal subgroup of G must be central (in G).

If all normal subgroups of G are central, then G is abelian, $n = 1$ and $|G| \leq q^n - 1$. In this case $k(GV) \leq |V|$.

From now on suppose that G has at least one non-central normal subgroup.

Let R be a normal subgroup of G that is minimal with respect to being non-central. We see that R is non-abelian. Since $Z(R)$ is abelian and normal in G, we have $Z(R) \leq Z(G)$. By the minimality of R, the factor group $R/Z(R)$ is characteristically simple. So either R is a central product of say ℓ quasi-simple groups Q_i (with $Q_i/Z(Q_i)$ all isomorphic), or $R/Z(R)$ is an elementary abelian r-group for some prime r. The previous case does not occur since we assumed that G has no non-abelian component. In the latter case it follows that R is of symplectic type with $|R/Z(R)| = r^{2a}$ for some prime r and some positive integer a.

Let $J_1, \ldots, J_t$ denote the distinct normal subgroups of G that are minimal with respect to being non-central in G. Put $J = J_1 \cdots J_t$. Then $C_G(J) = Z(G)$. (The containment $C_G(J) \supseteq Z(G)$ is clear. Suppose that $C_G(J)$ properly contains $Z(G)$. Since $C_G(J)$ is a normal subgroup of G which is not central, $C_G(J)$ contains a normal subgroup of G which is minimal with respect to being non-central. Without loss of generality, let such a subgroup be J_1. Then J_1 must be abelian and so central (by the fifth paragraph of this section).) Thus, $G/Z(G)J$ embeds into the direct product of the outer automorphism groups of the minimal normal non-central subgroups. If R is of symplectic type with $|R/Z(R)| = r^{2a}$, then this outer automorphism group is isomorphic to $Sp(2a, r)$ or to $O^{\epsilon}(2a, 2)$ in case $r = 2$ and $|Z(R)| = 2$.

Since G is primitive on V, the normal subgroup J acts homogeneously on V. Let W be an irreducible constituent for J. It follows that $W \cong U_1 \otimes \cdots \otimes U_t$ where U_i is an irreducible FJ_i-module. Furthermore, W is an irreducible faithful FG-module as the one treated in Section 5; hence Theorem 5.2 applies.

Lemma 7.1. *Use the notations and assumptions of this section. Suppose that G is an absolutely irreducible subgroup of $GL(n,q)$ and that whenever N is a normal subgroup of G, then every irreducible FN-submodule of V is absolutely irreducible. Then $k(GV) \leq \max\{|V|, 2^{1344}\}$.*

There are two cases remaining: G either preserves a field extension structure on V or it does not. (We say that G preserves a field extension structure on V if there is an F-subalgebra $K \subseteq \mathrm{End}_F(V)$ (properly containing F) so that G preserves K (and there is a homomorphism from G into $\mathrm{Gal}(K|F)$).)

Suppose that G preserves no field extension structure. Let N be a normal subgroup of G. Then N must act homogeneously on V (since G acts primitively on V) and moreover, the irreducible constituents for N must be absolutely irreducible (otherwise the center of $\mathrm{End}_N(V)$ is K for some field extension of F, and would be normalized by G, whence G preserves a field extension structure on V). Hence, in this case, Lemma 7.1 gives the desired conclusion.

Now suppose that G preserves a field extension structure on V over a field K with K as large as possible. Let $|K| = q^e$ with $e > 1$. Let $A = G \cap GL(n/e, q^e)$. Let U denote V considered as a vector space over K (and as a KA-module). Then G embeds in $GL(n/e, q^e).e$. Let $W = V \otimes_F K$. Now $W \cong \oplus_{\sigma \in \mathrm{Gal}(K|F)} U^\sigma$ as an FA-module. Then G permutes the U^σ. Moreover, A acts irreducibly on U (or G acts reducibly on W, a contradiction to the fact that V is absolutely irreducible as an FG-module). Also A acts faithfully on U (x trivial on U implies that x is trivial on U^σ for all σ, whence x is trivial on W). By the maximality of K it follows that A preserves no field extension structure on U. We may assume that A is absolutely irreducible on U. The group A has no non-abelian component for such a subgroup would also be a component of G. Hence the generalized Fitting subgroup of A is nilpotent.

Suppose that A is not abelian. Then A and G are as in Sections 4 and 5. Hence Theorem 5.2 gives $k(GV) \leq \{|V|, 2^{1344}\}$.

Finally, if A is abelian, then G is meta-cyclic. Hence, by Theorem 1.2, we have $k(GV) \leq \max\{|V|, 5\}$.

8. The imprimitive case

In this section we prove Theorem 1.4.

Let F be a finite field, V an n-dimensional vector space over F and also an irreducible FG-module for a finite group G. Suppose that V admits a direct sum decomposition $V = V_1 \oplus \ldots \oplus V_t$ as an FG-module. Let H be the kernel of this linear G-action on the t direct summands. In particular, H is a normal subgroup in G and G/H can be considered as a permutation group of degree t. Suppose that V_1 is an irreducible FL-module where L is the stabilizer of V_1 in G. Then H is a subdirect product of irreducible subgroups $H_1, \ldots, H_t$ on the vector spaces

$V_1, \ldots, V_t$, respectively. This means that H is such a subgroup of $H_1 \times \ldots \times H_t$ that projects onto every direct factor. Suppose that for every normal subgroup N of any H_i we have $k(N) < |V_i|/\sqrt{3}$. We will prove by induction on t that $k(H) < (|V_1|/\sqrt{3})^t$. The case $t = 1$ is trivial. Suppose that $t > 1$ and the statement is true for $t - 1$. Let H^* be the projection of H onto all but the last direct factor of $H_1 \times \ldots \times H_t$. Let the kernel of this map be K. Then $H/K \cong H^*$ which in turn is a subdirect product of $H_1, \ldots, H_{t-1}$. By the induction hypothesis we have $k(H^*) < (|V_1|/\sqrt{3})^{t-1}$. Now $K \lhd H_t$ hence $k(K) < (|V_t|/\sqrt{3})$. By Lemma 4.2, we have $k(H) < (|V_1|/\sqrt{3})^t$. By [20] this gives

$$k(G) \leq k(H)k(G/H) < (|V|/(\sqrt{3})^t)(\sqrt{3})^{t-1} = |V|/\sqrt{3}$$

for $t > 2$ and $k(G) < (2/3)|V|$ for $t = 2$.

This proves Theorem 1.4.

References

[1] Aschbacher, M. Finite group theory. Second edition. Cambridge Studies in Advanced Mathematics, **10**. Cambridge University Press, Cambridge, 2000.

[2] Conway, J. H; Curtis, R. T; Norton, S. P; Parker, R. A; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).

[3] Fulman, J. Cycle indices in the finite classical groups. *J. Group Theory* **2** (1999) 251–289.

[4] Fulman, J.; Guralnick, R. M. Conjugacy class properties of the extension of $\mathrm{GL}(n, q)$ generated by the inverse transpose involution. *J. Algebra* **275** (2004), no. 1, 356–396.

[5] Fulman, J.; Guralnick, R. M. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023-3070.

[6] Gallagher, P. X. The number of conjugacy classes in a finite group. *Math. Z.* **118** (1970), 175–179.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2005, (`http://www.gap-system.org`).

[8] Gluck, D.; Magaard, K.; Riese, U.; Schmid, P. The solution of the $k(GV)$-problem. *J. Algebra* **279** (2004), no. 2, 694–719.

[9] Gorenstein, D. Finite groups. Second edition. Chelsea Publishing Co., New York, 1980.

[10] Guralnick, R. M.; Malle, G. Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.* **25** (2012), 77–121.

[11] Guralnick, R. M.; Tiep, P. H. The non-coprime $k(GV)$ problem. *J. Algebra* **293** (2005), no. 1, 185–242.

[12] Hall, P.; Higman, G. On the p-length of p-soluble groups and reduction theorems for Burnside's problem. *Proc. London Math. Soc.* (3) **6** (1956), 1–42.

[13] Hesselink, W. H. Nilpotency in classical groups over a field of characteristic 2. *Math. Z.* **166** (1979), no. 2, 165-181.

[14] Isaacs, I. M. Character theory of finite groups. Academic Press, New York, 1976.

[15] Keller, T. M. Fixed conjugacy classes of normal subgroups and the $k(GV)$-problem. *J. Algebra* **305** (2006), no. 1, 457–486.

[16] Keller, T. M. Counting characters in linear group actions. *Israel J. Math.* **171** (2009), 367–384.

[17] Kovács, L. G.; Robinson, G. R. On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), no. 2, 441-460.

[18] Liebeck, M. W.; Pyber, L. Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), no. 2, 538-562.

[19] Manz, O.; Wolf, T. R. Representations of solvable groups. London Mathematical Society Lecture Note Series, 185. Cambridge University Press, Cambridge, 1993.

[20] Maróti, A. Bounding the number of conjugacy classes in a permutation group. *J. Group Theory* **8** (3) (2005) 273–289.

[21] Nagao, H. On a conjecture of Brauer for p-solvable groups. *J. Math. Osaka City Univ.* **13** (1962) 35–38.

[22] Robinson, G. R. On Brauer's $k(B)$-problem for blocks of p-solvable groups with non-Abelian defect groups. *J. Algebra* **280** (2004), no. 2, 738–742.

[23] Robinson, G. R.; Thompson, J. G. On Brauer's $k(B)$-problem. *J. Algebra* **184** (1996), no. 3, 1143–1160.

[24] Schmid, P. The solution of the $k(GV)$ problem. ICP Advanced Texts in Mathematics, 4. Imperial College Press, London, 2007.

[25] Wall, G. E. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Austral. Math. Soc.* **3** (1963), 1–62.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA

E-mail address: guralnic@usc.edu

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: maroti.attila@renyi.mta.hu