On the non-coprime $k(GV)$-problem

Attila Maróti

(Rényi Institute of Mathematics, Budapest, Hungary)

Istanbul, June 7, 2011

Brauer's $k(B)$-problem; part 1

Our story begins with Brauer's $k(B)$-problem.

Let G be a finite group, p a prime, and F an algebraically closed field of characteristic p. Then the group algebra FG can uniquely be written as the sum $FG = B_1 \oplus \cdots \oplus B_\ell$ of minimal two-sided ideals called p-blocks.

Let M be an indecomposable FG-module. Then there is one and only one p-block B of FG which does not annihilate M. In this case we say that M lies inside the block B. In particular every irreducible FG-module lies inside some block of FG.

Brauer's $k(B)$-problem; part 2

It is useful to take a particular algebraically closed field F of characteristic p. Let $\mathbb{C}$ be the field of complex numbers, let R be the ring of all algebraic integers in $\mathbb{C}$, and let I be a maximal ideal of R containing pR. Then $F = R/I$ is an algebraically closed field of characteristic p.

Let $* : R \to F$ be the natural homomorphism (with kernel I).

$U = \{\epsilon \in \mathbb{C} : \epsilon^m = 1 \text{ for some } m \in \mathbb{Z} \text{ with } p \nmid m\}$.

Clearly, $U \subseteq R$ and $*$ maps U isomorphically onto F^*.

Brauer's $k(B)$-problem; part 3

Let M be an FG-module and let $\mathcal{X}$ be an associated F-representation of G. Let $\mathcal{C}$ be the set of p-regular elements of G. We define $\varphi : \mathcal{C} \to \mathbb{C}$ as follows. Let $x \in \mathcal{C}$ and let $\epsilon_1, \ldots, \epsilon_f \in F^*$ be the eigenvalues of $\mathcal{X}(x)$, counting multiplicities. For each i there exists a unique $u_i \in U$ such that $u_i^* = \epsilon_i$. Put $\varphi(x) = \sum_{i=1}^{f} u_i$. This function φ is called the Brauer character of G afforded by $\mathcal{X}$. If $\mathcal{X}$ is an irreducible representation then φ is called an irreducible Brauer character. The set of irreducible Brauer characters is denoted by $\mathrm{IBr}(G)$. Each irreducible Brauer character is associated to a p-block B.

Brauer's $k(B)$-problem; part 4

Let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G. For $\chi \in \mathrm{Irr}(G)$ let $\hat{\chi}$ be the restriction of χ to $\mathcal{C}$. The class function $\hat{\chi}$ can be written as a non-negative integer combination of irreducible Brauer characters belonging to a unique p-block B. In this case we say that χ belongs to the p-block B. Let $k(B)$ be the number of complex irreducible characters of G belonging to the p-block B.

Let $\mathcal{K}$ be a conjugacy class of G. The Sylow p-subgroups of $C_G(x)$ for $x \in \mathcal{K}$ are called the p-defect groups for $\mathcal{K}$. Let B be a p-block of G. Then the p-defect groups of the defect classes of B are called defect groups of B.

Conjecture (Brauer, 1959).

Let B be a p-block of a finite group G and let D be a defect group of B. Then $k(B) \leq |D|$.

Nagao's theorem

In 1962 Nagao showed that for p-solvable groups G Brauer's $k(B)$-problem is equivalent to the so-called $k(GV)$-problem.

To state this conjecture, for a finite group H let $k(H)$ be the number of conjugacy classes of H which is also $|\mathrm{Irr}(H)|$.

$k(GV)$-problem (Nagao, 1962).

Let F be a finite field and G a finite group. Let V be a finite faithful FG-module. Form the semidirect product GV. If $(|G|, |V|) = 1$ then $k(GV) \leq |V|$.

A few lines about the proof of the $k(GV)$-problem

Works of Gow, Knörr, and especially Robinson-Thompson have led to fundamental breakthroughs in attacking the $k(GV)$-problem which have culminated in a complete solution of the conjecture, with the final step completed in 2004 by Gluck, Magaard, Riese, Schmid. The full solution of the problem (not counting the Classification of Finite Simple Groups) is about 500 pages long. A 250 page long book was written about the $k(GV)$-problem in late 2007 by Schmid.

Keller introduced a different approach to the $k(GV)$-problem which gave the result in case the characteristic of the underlying field is sufficiently large.

Summary of the proof of the $k(GV)$-problem; part 1

Nagao showed that for a normal subgroup N of a finite group X we have $k(X) \leq k(N)k(X/N)$. This may suggest that the $k(GV)$-problem has a good inductive nature. But unfortunately this is not the case.

On the other hand, this result of Nagao (and a bit more) enables us to reduce the $k(GV)$-problem to the case where V is an irreducible FG-module.

Summary of the proof of the $k(GV)$-problem; part 2

Theorem (Knörr, 1984).

Let V be a finite faithful coprime FG-module. If there exists a vector v in V with $C_G(v)$ abelian then $k(GV) \leq |V|$.

Let V be a coprime FG-module with F a finite field. We know that V is isomorphic to $\mathrm{Irr}(V) = \mathrm{Hom}(V, \mathbb{C}^*)$ as a G-set. The FG-module $V^* = \mathrm{Hom}_F(V, F)$, with diagonal action $\lambda^x(v) = \lambda(vx^{-1})$ for $\lambda \in V^*$, $x \in G$, $v \in V$, is called the dual module to V. The module V is self-dual provided $V \cong V^*$ (as FG-modules). It can be shown that V is self-dual if and only if its Brauer character is real-valued.

Summary of the proof of the $k(GV)$-problem; part 3

Definition

Let V be a finite faithful coprime FG-module.
(a) A vector $v \in V$ is called real for G if the restriction to $C_G(v)$ of V contains a faithful self-dual submodule (with real-valued Brauer character).
(b) A vector $v \in V$ is called strongly real for G if the restriction to $C_G(v)$ of V is self-dual.

Theorem (Robinson, Thompson, 1996).

Suppose V is a finite faithful coprime FG-module and some $v \in V$ is real for G. Then $k(GV) \leq |V|$ and equality can only hold when v is strongly real for G.

Summary of the proof of the $k(GV)$-problem; part 4

Let V be a finite, faithful coprime FG-module. Assume there is no (strongly) real vector in V for G but that (G, V) is a minimal counterexample in the following sense:
Whenever G_0 is a central extension of a subgroup of G by a p'-subgroup and V_0 is an F_0G_0-module for which $\mathrm{char}(F_0) = p$ and $\dim_{F_0} V_0 < \dim_F V$, then there is a (strongly) real vector in V_0 for G_0.

Theorem

Suppose (G, V) is a minimal counterexample in the above sense (for real or strongly real vectors). Then G has a unique minimal nonabelian normal subgroup, say E, and this is either quasisimple or of extraspecial type. Moreover E is absolutely irreducible on V, and all abelian normal subgroups of G are cyclic and central.

G reduced; (G, V) reduced pair; (G, V) nonreal reduced pair.

Summary of the proof of the $k(GV)$-problem; part 5

Theorem

Up to isomorphism there are just 9 nonreal reduced pairs of extraspecial type. All other reduced pairs (G, V) of extraspecial type admit a strongly real vector $v \in V$ for G such that $C_G(v)$ has a regular orbit on V.

Theorem

Up to isomorphism there are exactly 11 nonreal reduced pairs of quasisimple type. All other reduced pairs (G, V) of quasisimple type admit a real vector $v \in V$ such that $C_G(v)$ has a regular orbit on V.

Summary of the proof of the $k(GV)$-problem; part 6

We call a pair (G, V) nonreal induced provided V is a faithful coprime FG-module which admits no real vector for G and which is induced from some nonreal reduced pair (H, W), that is, $V = \mathrm{Ind}_{G_0}^{G}(W)$ for some subgroup G_0 of G satisfying $H \cong G_0/C_{G_0}(W)$.

Theorem (Riese, Schmid).

Let V be a faithful, irreducible, coprime FG-module admitting no real vector for G. Then (G, V) is nonreal induced (from a nonreal reduced pair (H, W)) and G is not far from being a wreath product $H \wr S$ for some permutation group S.

Summary of the proof of the $k(GV)$-problem; part 7

Theorem (Liebeck, Pyber).

If S is a permutation group of degree n, then $k(S) \leq 2^{n-1}$.

Theorem (Riese, Schmid).

Let (G, V) be properly induced from the nonreal reduced pair (H, W). Then $k(GV) \leq \frac{1}{2}|V|$, except possibly when $p = 5$.

Theorem (Gluck, Magaard, Riese, Schmid).

Let (G, V) be induced from the nonreal reduced pair (H, W) in characteristic $p = 5$. Then we have $k(GV) < |V|$.

Background on the non-coprime $k(GV)$-problem; part 1

The non-coprime $k(GV)$-problem (first form).

What can be said about $k(GV)$ if we drop the assumption that $(|G|, |V|) = 1$ but assume that V is a completely reducible G-module?

The following lemma appeared as a tool in the paper of Guralnick-Tiep and it is a special case of the so-called Clifford-Gallagher formula.

Lemma.

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 the sum is over a set of representatives $\lambda \in \mathrm{Irr}(V)$ of the G-orbits of $\mathrm{Irr}(V)$.

Background on the non-coprime $k(GV)$-problem; part 2

The following example was noticed by Fulman and Guralnick.

Example 1. Let $G = GL(n,p)$ for a prime p and a positive integer n. Then $GV = AGL(n,p)$. By the Lemma above, $k(GV) = k(G) + k(AGL(n-1,p))$. Using induction, we have

$$k(GV) = k(GL(n,p)) + k(GL(n-1,p)) + \ldots + k(GL(2,p)) + k(AGL(1,p)).$$

By a result of Green (1955), we have $p^m - p^{m-1} < k(GL(m,p)) \leq p^m - 1$. Clearly, $k(AGL(1,p)) = p$. This gives $|V| < k(GV) < 2|V|$.

Background on the non-coprime $k(GV)$-problem; part 3

The next example depends on an easy lemma we do not mention.

Example 2. Let $G = GL(2,p) \wr C_m$. This group acts faithfully and irreducibly on $V = F_p^{(2m)}$. We have $k(GV) \geq \frac{1}{m}\left(\frac{p^2+p-1}{p^2}\right)^m |V|$.

The non-coprime $k(GV)$-problem (second form).

In the setup of the previous problem does there exists a universal positive constant c such that $k(GV) \leq c^n |V|$ where n is the dimension of V?

Theorem (Kovács, Robinson).

Let V be a faithful completely reducible G-module where G is a finite p-solvable group. Then $k(GV) \leq c^n |V|$ for some universal constant c.

Later Liebeck and Pyber showed that c can be taken to be 103.
All this was prior to the solution of the (classical) $k(GV)$-problem.
By the $k(GV)$-theorem we can say more. When G is a p-solvable group we have $k(GV) \leq |GV|_p < p^{np/(p-1)^2} |V|$.

Background on the non-coprime $k(GV)$-problem; part 4

Non-coprime $k(GV)$-problem (third form) (Guralnick, Tiep).

In the setup of the previous two problems can one classify all groups G with $k(GV) > |V|$?

Theorem (Guralnick, Tiep).

Let G be almost quasisimple and faithful, irreducible on V. Then $k(GV) \leq \frac{1}{2}|V|$ provided G does not involve A_n for $5 \leq n \leq 16$ or a group of Lie type of (untwisted) rank at most 6 or a classical group with V related to the standard module.

Keller has worked on the imprimitive case of the non-coprime $k(GV)$-problem. He also developed character theoretic arguments along the lines of Knörr.

Theorem (Keller).

Under strong conditions there exists a universal constant c such that $k(GV) \leq c|V| \log |V|$.

The rest of the talk will be based on a work in preparation with Robert M. Guralnick entitled "On the non-coprime $k(GV)$-problem".

The first theorem

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.

The first theorem of the paper is the following.

Theorem (Guralnick, M).

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 $k(GV) \leq \max\{|V|, 5^{88}\}$.

On the proof of the first theorem; part 1

Given an element x in G. Our first task is to give an upper bound for $\dim_F(C_V(x))$.
For this we may assume that F is an algebraically closed field (of characteristic $p > 0$).
More precisely, in many cases, we will give an upper bound for $d(x)$ which is defined to be the maximal dimension of an eigenspace of x on V.
The interesting case is when $Z(G) = Z(R)$ and $x \in G \setminus R$.
Our tool is the Hall-Higman theorem and its variations.

Theorem (Hall, Higman).

Use the above notations and assumptions. 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, $d(x) = \dim(C_V(x)) = b+1 = (r^a+1)/q$.

On the proof of the first theorem; part 2

Let us 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.

On the proof of the first theorem; part 3

Here are the various lemmas we used which are based on the argument of the Hall-Higman theorem.

Lemma

Use the above notations and assumptions. 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 $d(x) \leq (r^a + 1)/m$.

Lemma

Use the above notations and assumptions. 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 $d(x) \leq 1 + (r^a - 1)/m$.

On the proof of the first theorem; part 4

We used slightly more detailed lemmas in small dimensions (r^a) than the two lemmas below (which concern r-elements x).

Lemma.

Let us use the above notations and assumptions. 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 $d(x)/\dim_F(V) \leq ((r+1)/2r)$.

Lemma.

Let us use the above notations and assumptions. 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 $d(x)/\dim_F(V) \leq ((r+1)/2r)$.

On the proof of the first theorem; part 5

Putting the lemmas together and using other results we get the following theorem which is later used in large dimensions (r^a). For small dimensions we need a more detailed analysis.

Theorem.

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 $\dim_F(C_V(x)) \leq ((r+1)/2r) \cdot r^a$.

On the proof of the first theorem; part 6

As said before, for certain small values of r^a we need more detailed information about $\dim_F(C_V(x))$.
Also, we need to know upper bounds for the numbers of elements x in G with large fixed point spaces. These upper bounds are obtained from papers of Wall, Fulman, and Fulman-Guralnick.
Note that G/R can be considered as a subgroup of $Sp(2a, r)$.

Consider the table on the next slide. 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 $c_A < \mathrm{rdim}(x) \leq c_B$.

On the proof of the first theorem; part 7

	11/25	3/7	1/2	5/9	4/7	3/5	2/3	3/4
$Sp(16,2)$			$*$					2^{72}
$Sp(14,2)$			$*$					
$Sp(8,3)$				$*$			$2 \cdot 3^{24}$	
$Sp(12,2)$			$*$					2^{42}
$Sp(10,2)$			$*$					
$Sp(6,3)$				$*$			$2 \cdot 3^{14}$	
$Sp(4,5)$	$*$					1		
$Sp(8,2)$			$*$					2^{20}
$Sp(4,3)$				$*$			1441	
$Sp(6,2)$			$*$					
$Sp(2,7)$		$*$			1			
$Sp(2,5)$	$*$					1		
$Sp(4,2)$			$*$					60
$Sp(2,3)$				$*$			9	
$Sp(2,2)$			$*$					

On the proof of the first theorem; part 8

We recall the following lemma.

Lemma.

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

By Brauer's Permutation Lemma, for any $x \in G$ the number of fixed points $|C_V(x)|$ of x on V is equal to the number of characters $\lambda \in \mathrm{Irr}(V)$ fixed by x. From this, by the Orbit-Counting Lemma, and by our considerations on the previous slides, we may give accurate upper bounds for the number of G-orbits $n(G, V)$ of the set $\mathrm{Irr}(V)$.

At first approach we have

$$n(G, V) = \frac{1}{|G|} \sum_{x \in G} |C_V(x)| \leq \frac{|V|}{|G|} + |V|^{(r+1)/2r},$$

but for small dimensions we may get better upper bounds using the table given before.

On the proof of the first theorem; part 9

Let m be the maximum of $k(\mathrm{Stab}_G(\lambda)) \leq |\mathrm{Stab}_G(\lambda)|$ as λ runs through the non-trivial characters in $\mathrm{Irr}(V)$.

As $(|R|, |V|) = 1$, the R-sets V and $\mathrm{Irr}(V)$ are permutation isomorphic. Hence for any $1 \neq \lambda \in \mathrm{Irr}(V)$ there exists $1 \neq v \in V$ so that $\mathrm{Stab}_R(\lambda) = C_R(v)$. But $C_R(v) \cap Z(R) = 1$ and so $C_R(v)$ can be embedded into $R/Z(R)$ which is abelian. Hence $C_R(v)$ is an abelian subgroup of R and so $|\mathrm{Stab}_R(\lambda)| = |C_R(v)| = r^t$ for some $t \leq a$.

From this we have $m \leq \frac{|G|}{r^{a+1}}$.

On the proof of the first theorem; part 10

Now we can estimate $k(GV)$.

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

$$\leq |G| + (|V|/r^{a+1}) + (|G|/r^{a+1})(|V|^{(r+1)/2r} - 1).$$

It is possible to see that this 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 $r = 7$.
As said before, for these values of a and r we use a better estimate for $n(G, V)$.
The first instance when we need the constant 5^{88} from the statement of the first theorem is when $a = 6$ and $r = 2$. Here we have

$$k(GV) \leq |G| + (|V|/2^7) + 2^{49}|V|^{3/4} + (|G|/2^7)|V|^{1/2} \leq \max\{|V|, 5^{88}\}.$$

The second and third theorems

Our second theorem was obtained using the same lemma. This is the following.

Theorem (Guralnick, M).

Let V be an n-dimensional finite vector space over the field of p elements where p is a prime. A maximal solvable primitive subgroup X of $GL(n, p)$ 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 proofs of the first and second theorems 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 (Guralnick, M).

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

The fourth theorem

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 noting that for every normal subgroup N of most primitive linear groups acting on a module W we have $k(N) < |W|/\sqrt{3}$.

Theorem (Guralnick, M).

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 $k(G) < (2/3)|V|$.

Thank you for your attention!