

CHARACTER VALUES AT REGULAR ELEMENTS

MICHAEL LARSEN

There has been a good deal of work in the last decade or so on computing upper bounds of irreducible character values for finite simple groups [G1, G2, GM, LS2, LP, MS-P, R]. Some of this work concerns permutation groups, some groups of Lie type. Some is aimed at worst-case behavior, some at the character values of typical or at least fairly well-behaved elements. Various applications have been given, to mixing behavior of random walks, to diameters of Cayley graphs, to the conjectures of Ore and Thompson, and to solving word equations in finite simple groups. The novelty of this paper is that it gives a uniform, elementary method that applies to sufficiently good elements in any finite group and which gives respectable results both for alternating groups and groups of Lie type.

Let G be a finite group. We say that $a \in G$ is *regular* if the centralizer $Z(a)$ of a in G is abelian. We give an upper bound for the absolute value of irreducible characters evaluated at regular elements.

Lemma 1. *Let A denote a maximal abelian subgroup of G and $N = N(A)$ its normalizer in G . If $a \in A$ is regular, then $g^{-1}ag \in A$ if and only if $g \in N$.*

Proof. As A is abelian and $a \in A$, $A \subset Z(a)$. As a is regular, $Z(a)$ is abelian. Since A is maximal abelian, $A = Z(a)$. Thus, $g^{-1}Ag = Z(g^{-1}ag)$. If $g^{-1}ag \in A$, then $Z(g^{-1}ag)$ contains A . Since $|Z(g^{-1}ag)| = |A|$,

$$g^{-1}Ag = g^{-1}Z(a)g = Z(g^{-1}ag) = A,$$

so $g \in N$. The converse is trivial. □

Theorem 2. *Let A denote a maximal abelian subgroup of G . Suppose that there exist proper subgroups A_1, \dots, A_n of A such that every element in*

$$A^\circ := A \setminus (A_1 \cup A_2 \cup \dots \cup A_n)$$

is regular. Let $N = N(A)$ denote the normalizer of A . If χ is any irreducible character of G , then

$$|\chi(a)| \leq 4^n [N : A]$$

for all $a \in A^\circ$.

Proof. Let $A^* = \text{Hom}(A, \mathbb{C}^\times)$. We identify $\mathbb{Z}A^*$ with the ring of characters of virtual complex representations on A . Let $\phi \in \mathbb{Z}A^*$ be the character associated to the restriction of χ to A . For each i from 1 to n , let $\phi_i \in A^*$ be

Michael Larsen was partially supported by NSF grant DMS-0354772.

a character which is trivial on A_i and non-trivial on a . For every non-trivial root of unity ω , there exists an integer k such that $|\omega^k - 1| \geq 1$, so replacing ϕ_i by a character of the form ϕ_i^k , we may assume that $|\phi_i(a) - 1| \geq 1$. Let

$$\psi = \phi \prod_{i=1}^n (\phi_i - 1).$$

Let g_1, \dots, g_k denote a set of coset representatives for G/N . By Lemma 1, distinct pairs (g_i, a) , with $a \in A^\circ$, give rise to distinct elements $g_i^{-1}ag_i$. Therefore,

$$\sum_{a \in A^\circ} |\chi(a)|^2 = \frac{1}{k} \sum_{a \in A^\circ} \sum_{i=1}^k |\chi(g_i^{-1}ag_i)|^2 \leq \frac{1}{k} \sum_{g \in G} |\chi(g)|^2 = \frac{|G|}{k} = |N|.$$

As $|\phi_i(a) - 1| \leq 2$ for all i ,

$$\sum_{a \in A} |\psi(a)|^2 = \sum_{a \in A^\circ} |\psi(a)|^2 \leq 4^n \sum_{a \in A^\circ} |\phi(a)|^2 = 4^n \sum_{a \in A^\circ} |\chi(a)|^2 \leq 4^n |N|.$$

Writing ψ as a linear combination $\sum c_i \psi_i$ of $\psi_i \in A^*$, we have

$$\sum_{a \in A} |\psi(a)|^2 = |A| \sum_i c_i^2.$$

Thus,

$$\sum_i c_i^2 \leq 4^n [N : A].$$

As the c_i are integers,

$$|\chi(a)| = |\phi(a)| \leq |\psi(a)| = \left| \sum_i c_i \psi_i(a) \right| \leq \sum_i |c_i| \leq \sum_i c_i^2 \leq 4^n [N : A].$$

□

Corollary 3. *If $a \in G$ is regular with centralizer A , then*

$$|\chi(a)| \leq 4^n [N : A],$$

where n is the number of maximal elements in the partially ordered set

$$\{Z(b) \cap A \mid b \in G \setminus A\}.$$

Proof. If the A_i are taken to be the maximal elements, then $a \notin A_i$ for all i , since a cannot commute with any $b \in G \setminus A$. □

Corollary 4. *Let $a \in G$ be an element of order n which commutes only with its own powers. Then $|\chi(a)| \leq \tau(n)^2 \phi(n)$, where ϕ and τ denote the Euler ϕ -function and the number of divisors respectively, and χ is any irreducible character of G .*

Proof. As $N/A \subset \text{Aut}(A) = (\mathbb{Z}/n\mathbb{Z})^\times$ and the subgroups of A are indexed by divisors of n , the corollary is immediate. □

For example, when G is a subgroup of S_m and a is a product of k cycles of distinct lengths, Corollary 4 applies. In this setting, n is the product of the cycle lengths, and $\phi(n) < n \leq (m/k)^k$, while $\tau(n) = O(n^\epsilon)$ for every $\epsilon > 0$. For $G = S_m$, this bound is not as good as the recently discovered upper bound $2^{k-1}k!$ [LS1]. When k is large, which in this case means on the order of \sqrt{m} , however, the bound of Corollary 4 is only slightly inferior to that of [LS1].

Next we apply Theorem 2 in the case that $G = \mathbf{G}^F$, where \mathbf{G} is the group of $\bar{\mathbb{F}}_p$ -points of a simply connected, almost simple algebraic group and F is a Frobenius map. By Steinberg's theorem [H2, 2.11], the centralizer in a simply connected semisimple algebraic group of any regular semisimple element $a \in G$ is a maximal torus. Thus, a is regular in the sense of this paper.

Proposition 5. *With G as above, if a is any regular semisimple element, and χ any irreducible character of G ,*

$$|\chi(a)| \leq 2^{|\Phi|}|W|,$$

where Φ denote the root system and W the Weyl group of \mathbf{G} .

Proof. Let \mathbf{T} be the centralizer of a in \mathbf{G} . If $g \in N(\mathbf{T}^F)$, then by [H2, 3.1], there exists $n \in N_{\mathbf{G}}(\mathbf{T})$ such that $g^{-1}ag = n^{-1}an$. As a is regular semisimple, $gn^{-1} \in \mathbf{T}$, so $g \in N_{\mathbf{G}}(\mathbf{T})$. Regarding W as the Weyl group of \mathbf{G} with respect to \mathbf{T} , $N(\mathbf{T}^F)/\mathbf{T}^F$ is a subgroup of W . For each pair of characters $\alpha^{\pm 1}$ in the root system of \mathbf{G} with respect to \mathbf{T} , let $A_\alpha = \{t \in \mathbf{T}^F \mid \alpha(t) = 1\}$. The proposition now follows immediately from the main theorem. \square

This result can improved by examining more closely the product $\prod_i (\phi_i - 1)$ appearing in the proof of Theorem 2

Theorem 6. *Let $G = \mathbf{G}^F$, where \mathbf{G} is the group of $\bar{\mathbb{F}}_p$ -points of a simply connected, almost simple algebraic group and F is a Frobenius map. If W is the Weyl group of \mathbf{G} with respect to a maximal torus $\mathbf{T} \subset \mathbf{G}$, χ any irreducible character of G , and $a \in G$ a regular semisimple element,*

$$|\chi(a)| \leq |W|^2.$$

Proof. Without loss of generality we may assume that \mathbf{T} is the centralizer of a in \mathbf{G} . Let X denote the character group of \mathbf{T} , i.e., the group of $\bar{\mathbb{F}}_p$ -homomorphisms $\mathbf{T} \rightarrow \mathbf{G}_m$. Let $\Phi \subset X$ denote the root system of \mathbf{G} with respect to \mathbf{T} . Define Φ^+ with respect to some choice of Weyl chamber, and let δ denote the ‘‘half-sum of positive roots,’’ i.e., the character of \mathbf{T} whose square is the product of the roots in Φ^+ . It is well-known result of Weyl [H1, Lemma 24.3] that there is an identity in $\mathbb{Z}X$

$$\prod_{\alpha \in \Phi^+} (1 - \alpha) = \delta \sum_{w \in W} \text{sgn}(w) \delta^w,$$

where $\text{sgn}: W \rightarrow \{\pm 1\}$ is the determinant function of W acting on X . In particular, fixing an embedding $\iota: \bar{\mathbb{F}}_p^\times \rightarrow \mathbb{C}^\times$ and defining $\phi_\alpha: \mathbf{T}^F \rightarrow \mathbb{C}$ as the composition of the maps $\mathbf{T}^F \hookrightarrow \mathbf{T}$, $\alpha: \mathbf{T} \rightarrow \bar{\mathbb{F}}_p^\times$, and ι , we have

$$\prod_{\alpha \in \Phi^+} (\phi_\alpha(t) - 1) \leq |W|$$

for all $t \in \mathbf{T}$.

As $a \in \mathbf{T}$ is regular semisimple, $\phi_\alpha(a) - 1 \neq 0$ for all α . Thus,

$$\prod_{\alpha \in \Phi^+} (\phi_\alpha(a) - 1)$$

is a non-zero algebraic integer, and it follows that at least one of its conjugates has absolute value ≥ 1 . Replacing ι , therefore, we may assume that this quantity is already ≥ 1 , and now the argument of Proposition 5 goes through as before and yields the desired estimate. \square

We remark that the existence of irreducible principal series representations shows that one cannot, in general, hope for a bound below $|W|$, though for small values of q one might hope for a bound of the form q^{cr} where c is an absolute constant and r is the rank of \mathbf{G} .

As an application, we consider the growth of the invariant

$$\mu(G) := \min_{a \in G} \max_{\chi \in \text{Irr } G} |\chi(a)|$$

with the order of G for finite simple groups G .

Theorem 7. *Let G be a finite simple group. For all $\epsilon > 0$,*

$$\mu(G) = O(\log^{1/2+\epsilon} |G|).$$

Proof. We use classification. We can disregard any finite set of groups, so we do not treat the sporadic groups. For A_n , $n \geq 5$, we choose a to be an $n-2$ -cycle if n is odd and to have two orbits, of lengths 2 and $n-2$ if n is even. We observe that in one case the orbit lengths are even and in the other case they are not pairwise distinct, so in each case the S_n -conjugacy class constitutes a single conjugacy class in A_n . By [LS1, Th. 7.2], $|\chi(a)| \leq 24$ if χ is an irreducible character of S_n . If χ does not extend to a character on S_n , it can still be induced to S_n ; the resulting character of S_n is then irreducible and restricts to $\chi + \chi'$ on A_n , where $\chi(x) = \chi'(x)$ for any x whose A_n -conjugacy class and S_n -conjugacy class are the same. Thus, $\chi(a) = \chi'(a) \leq 12$.

This leaves groups of Lie type. Thus we may assume $G = \mathbf{G}^F/Z$, where \mathbf{G} is the group of $\bar{\mathbb{F}}_p$ -points of a simply connected, almost simple algebraic group, F is a Frobenius map, and Z is the center of \mathbf{G}^F . Every irreducible representation of G is an irreducible representation of \mathbf{G}^F , so it suffices to prove the theorem for \mathbf{G}^F instead of G . By Proposition 5, we need only treat the case that \mathbf{G} has sufficiently high rank, in particular, the case that \mathbf{G}^F is of type A_r , 2A_r , B_r , C_r , D_r , or 2D_r .

Thus there exists a prime power q , a sign $\varepsilon \in \{\pm 1\}$, and a maximal torus $\mathbf{T} \subset \mathbf{G}$ such that $F(t) = t^{\varepsilon q}$ for all $t \in \mathbf{T}$. Let w be an element of the Weyl group W of \mathbf{G} with respect to \mathbf{T} and $n \in N_{\mathbf{G}}(\mathbf{T})$ a coset representative of w . By Lang's theorem, there exists $g \in \mathbf{G}$ such that $F(g)g^{-1} = n$. As n normalizes \mathbf{T} , the torus $g^{-1}\mathbf{T}g$ is F -stable. It depends only on w . Let $A := (g^{-1}\mathbf{T}g)^F$ denote its intersection with \mathbf{G} .

We define a preorder on the root system Φ of G with respect to \mathbf{T} as follows: For $\alpha, \beta \in \Phi$, we write $\alpha \lesssim \beta$ if β lies in the abelian group generated by $\{w^i(\alpha) \mid i \in \mathbb{Z}\}$. If $a \in A$ and $\alpha(gag^{-1}) = 1$, then

$$\begin{aligned} 1 &= F(\alpha(gag^{-1}))^\varepsilon = \alpha(F(g)aF(g)^{-1}) = \alpha(ngag^{-1}n^{-1}) \\ &= w^{-1}(\alpha)(gag^{-1}), \end{aligned}$$

Thus $\alpha \lesssim \beta$ and $\alpha(gag^{-1}) = 1$ imply $\beta(gag^{-1}) = 1$. If $\alpha_1, \dots, \alpha_k$ are representatives of maximal equivalence classes with respect to \lesssim , and $A_i = \{a \in A \mid \alpha_i(gag^{-1}) = 1\}$, then every element in

$$A \setminus \bigcup_i A_i$$

is regular.

We now choose, for each case, a conjugacy class for w . For A_r and 2A_r , we take an $r+1$ -cycle in $S_{r+1} \cong W$. For B_r and C_r , we take an r -cycle in $S_r \subset (\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r \cong W$, and for D_r and 2D_r , we take an r -cycle in $S_r \subset (\mathbb{Z}/2\mathbb{Z})^{r-1} \rtimes S_r \cong W$.

A. For type A , the root system consists of vectors $e_i - e_j$, where $0 \leq i \neq j \leq r$, and w permutes the e_i cyclically; the equivalence class of a root is given by the greatest common divisor $d_{i,j}$ of $i-j$ and $r+1$, and the maximal classes are associated with the values $d_{i,j} = \frac{r+1}{p}$, where p is a prime divisor of $r+1$. The group A has $\frac{q^{r+1}-\varepsilon^{r+1}}{q-\varepsilon} \geq \frac{q^{r+1}-1}{q+1}$ elements, while the subgroup A_i associated to p has $\frac{q^{\frac{r+1}{p}-\varepsilon^{\frac{r+1}{p}}}}{q-\varepsilon} \leq \frac{q^{r/2+1}}{q-1}$ elements.

B. For type B , the roots are $\pm e_i$ and $e_i \pm e_j$, $1 \leq i \neq j \leq r$. The class of $\pm e_i$ is never maximal with respect to the preorder. The class of $e_i - e_j$ is determined by $d_{i,j} := (i-j, r)$ and is maximal if $d_{i,j} = r/p$ for some prime factor p of n . The class of $e_i + e_j$ depends only on $d_{i,j}$ and is maximal if $\frac{r}{d_{i,j}} = 2$. The group A has $q^r - 1$ elements. The subgroup of A associated with a maximal element $e_i - e_j$ with $i-j = r/p$ has $q^{r/p} - 1$ elements, while the subgroup of A associated with $e_i + e_j$ where $i-j = r/2$ (and r is even) has $q^{r/2} + 1$ elements.

C. For type C , the roots are $\pm 2e_i$ and $e_i \pm e_j$, $1 \leq i \neq j \leq r$. The class of $\pm 2e_i$ is maximal with respect to the preorder and the associated subgroup of A is the center of G , of order ≤ 2 . The class of $e_i - e_j$ is determined by $d_{i,j} := (i-j, r)$ and is maximal if $d_{i,j} = r/p$ for some prime factor p of n . The class of $e_i + e_j$ depends only on $d_{i,j}$ and is maximal if $\frac{r}{d_{i,j}} = 2$. The group A has $q^r - 1$ elements. The subgroup of A associated with a maximal

element $e_i - e_j$ with $i - j = r/p$ has $q^{r/p} - 1$ elements, while the subgroup of A associated with $e_i + e_j$ where $i - j = r/2$ (and r is even) has $q^{r/2} + 1$ elements.

D. For type D , the roots are $e_i \pm e_j$, $1 \leq i \neq j \leq r$. The class of $e_i - e_j$ is determined by $d_{i,j} := (i - j, r)$ and is maximal if $d_{i,j} = r/p$ for some prime factor p of n . The class of $e_i + e_j$ depends only on $d_{i,j}$ and is maximal if $\frac{r}{d_{i,j}} = 2$. The group A has $q^r - 1$ elements. The subgroup of A associated with a maximal element $e_i - e_j$ with $i - j = r/p$ has $q^{r/p} - 1$ elements, while the subgroup of A associated with $e_i + e_j$ where $i - j = r/2$ (and r is even) has $q^{r/2} + 1$ elements.

In each case, the number k of maximal equivalence classes is $o(\log r)$. We may assume that r is sufficiently large that A contains a regular semisimple element of \mathbf{G} . By [H2, 3.1], every element of G that normalizes A lies in $N_{\mathbf{G}}(g^{-1}\mathbf{T}g)$. Thus,

$$N_G(A) = \bigcup_{n \in W} (g^{-1}(n\mathbf{T})g \cap G).$$

The union is disjoint, and for each $n \in W$, $g^{-1}(n\mathbf{T})g \cap G$ is either a coset of A or empty. In the former case, we may choose the coset representative $n \in N_{\mathbf{G}}(\mathbf{T})$ such that $g^{-1}ng \in G$ and $F(n) = nt$, $t \in \mathbf{T}$. Thus,

$$g^{-1}ng = F(g^{-1}ng) = F(g)^{-1}ntF(g),$$

or

$$(F(g)g^{-1})n(F(g)g^{-1})^{-1}n^{-1} = ntn^{-1} \in \mathbf{T},$$

i.e., the class of n in W commutes with the class w of $F(g)g^{-1}$. Thus,

$$[N_G(A) : A] = |Z_W(w)|.$$

As $4^k = o(r^\epsilon)$ for all $\epsilon > 0$ and the order of w is $O(\log^{1/2} |G|)$, the theorem follows. □

We remark that the growth of $\mu(G)$ with $|G|$ for finite groups which are not simple need not be polylogarithmic. Indeed, $\mu(G^n) = \mu(G)^n$, so one need only exhibit a group with $\mu(G) > 1$. There appear to be many finite simple groups G with $\mu(G) = 1$, but the character tables [At] provide a number of examples with $\mu(G) > 1$, such as $\mathrm{PSL}_2(\mathbb{F}_{17})$, $\mathrm{PSL}_3(\mathbb{F}_4)$, $\mathrm{PSU}_3(\mathbb{F}_8)$, and $\mathrm{Sz}(32)$.

REFERENCES

- [At] 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. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.
- [G1] Gluck, David: Sharper character value estimates for groups of Lie type. *J. Algebra* **174** (1995), no. 1, 229–266.

- [G2] Gluck, David: Characters and random walks on finite classical groups. *Adv. Math.* **129** (1997), no. 1, 46–72.
- [GM] Gluck, David; Magaard, Kay: Character and fixed point ratios in finite classical groups. *Proc. London Math. Soc. (3)* **71** (1995), no. 3, 547–584.
- [H1] Humphreys, James E.: Introduction to Lie algebras and representation theory. Second printing, revised. Graduate Texts in Mathematics, 9. Springer-Verlag, New York-Berlin, 1978.
- [H2] Humphreys, James E.: Conjugacy classes in semisimple algebraic groups. Mathematical Surveys and Monographs, **43**. American Mathematical Society, Providence, RI, 1995.
- [LS1] Larsen, M.; Shalev, A.: Word maps and Waring type problems, preprint, arXiv: math.GR/0701334.
- [LS2] Larsen, M.; Shalev, A.: Characters of symmetric groups: sharp bounds and applications, preprint, arXiv: math.GR/0701334.
- [LP] Lulov, Nathan; Pak, Igor: Rapidly mixing random walks and bounds on characters of the symmetric group. *J. Algebraic Combin.* **16** (2002), no. 2, 151–163.
- [MS-P] Müller, Thomas W.; Schlage-Puchta, Jan-Christoph: Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks. *Adv. Math.* **213** (2007), no. 2, 919–982.
- [R] Roichman, Yuval: Upper bound on the characters of the symmetric groups. *Invent. Math.* **125** (1996), no. 3, 451–485.

E-mail address: `larsen@math.indiana.edu`

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, IN 47405, U.S.A.