Finding p'-elements in finite groups of Lie type

Frank Lübeck

Abstract. We give estimates for the proportion of elements of order divisible by a given number m in finite groups of Lie type which are defined over finite fields with characteristic prime to m.

1991 Mathematics Subject Classification: primary 20G40; secondary 20D60.

1. Introduction

Let G be a connected reductive algebraic group over an algebraic closure of a finite prime field $\mathbb{F}_p$ with p elements and let F be a Frobenius endomorphism of G. Then some power of F, say F^a, induces on the character group of an F-stable maximal torus of G the map $k \cdot id$, where k is some power of p. We define $q > 0$ by $q^a = k$ and denote $G(q)$ the group of F-fixed points of G. This is a finite group of Lie type. (This definition includes the Suzuki and Ree groups.) We will write W for the Weyl group of G.

Assume that $G(q)$ contains an element of order m. We want to investigate the proportion $c_{G,m}(q) = |M_{G,m}(q)|/|G(q)|$, with

$$M_{G,m}(q) = \{x \in G(q) \mid \ m \text{ divides the order } |x| \text{ of } x\},$$

in the case where m is prime to p.

Our main statement is as follows (we denote by Φ the Euler Φ-function): Let $\gcd(m,p) = 1$. For each constant $0 \leq c < \Phi(m)/m$ and each $l \in \mathbb{N}$ there exists $q_0 \in \mathbb{N}$, such that for all $G(q)$ as above with $q > q_0$ and rank at most l we have $c_{G,m}(q) > c/(2^l \cdot |W|)$. We will also give an explicit q_0 (which becomes bigger for smaller differences $(\Phi(m)/m) - c$).

We mention one consequence of this statement. If we fix the type of G (i.e., its root datum) and consider the case of a prime m which is different from p, then there is a constant $\varepsilon > 0$ such that for all prime powers q the value of $c_{G,m}(q)$ is either zero or at least ε (take some $c < 1/2$ above and for ε the minimum of $c/(2^l \cdot |W|)$ and all nonzero $c_{G,m}(q)$ with $q \leq q_0$). On the other hand it is not difficult to see that $c_{G,p}(q)$ tends to zero when q becomes large. See **[GL99]** for a more precise statement.

This result has an interesting interpretation in computational group theory, where one is often looking for certain elements by a random search. For a fixed probability $\alpha < 1$ there is a number $n \in \mathbb{N}$, depending just on α and the root datum of G, such that for any prime divisor $m \neq p$ of $|G(q)|$ any set of n random elements from $G(q)$ contains, with probability at least α, an element whose order is divisible by m. On the other hand, for growing q it becomes more and more difficult to find a p-singular element by a random search.

Acknowledgement. I would like to thank Bill Kantor for asking me to write this note. He originally wanted to know an estimate for $c_{G,m}(q)$ in the case of exceptional groups G and m a product of two prime powers.

2. A lower bound for finding elements of given order

In this section we will keep the notation from the introduction. Let G, p, F, q, W, m with $\gcd(m,p) = 1$ as above. Recall that the rank of G, denoted $\mathrm{rank}(G)$, is the dimension of a maximal torus of G.

Theorem 2.1. *(a) Let $l \in \mathbb{N}$ and $c < \Phi(m)/m$. There exists $q_0 \in \mathbb{N}$ with the following property: For all $G(q)$ with rank of G at most l and $q > q_0$ which contain an element of order m, the proportion of regular semisimple elements of order divisible by m is at least $c/(2^l \cdot |W|)$ (and so $c_{G,m}(q) > c/(2^l \cdot |W|)$).*

(b) In (a) we can take q_0 such that for all $q > q_0$ we have

$$2 \cdot l^2 \cdot 2^{l-1} \cdot ((q+1)/(q-1))^{l-1}/((\Phi(m)/m) - c) + 1 < q.$$

For example one can choose for q_0 any number greater than

$$2l^2 \cdot 6^{l-1}/((\Phi(m)/m) - c) + 1.$$

To illustrate the statement we give an example of an application.

Corollary 2.2. *Assume that $m \in \mathbb{N}$ has prime factorization of form $r_1^{a_1} r_2^{a_2} r_3^{a_3}$, with different primes r_1, r_2, r_3 not equal to p and given $a_i \geq 0$.*

(a) Let G be of rank l and $q > 2^l \cdot 6^{l-1} \cdot 300/77 + 1$. Further assume that $G(q)$ contains an element of order m. Then the proportion of regular semisimple elements of $G(q)$ which have order divisible by m is at least $1/(100 \cdot 8^l \cdot l!)$.

(b) Let G be of rank at most 8 and $q > 63848$. Assume that $G(q)$ contains an element of order m. Then the proportion of regular semisimple elements of $G(q)$ which have order divisible by m is at least $1/(1.8 \cdot 10^{13})$.

Proof. First we note that $\Phi(m)/m \geq (r_1-1)/r_1 \cdot (r_2-1)/r_2 \cdot (r_3-1)/r_3 \geq 1/2 \cdot 2/3 \cdot 4/5$. For the application of Theorem 2.1 we choose $c = 1/100$ and so we have $(\Phi(m)/m) - c \geq 77/300$.

Putting these numbers into the second formula in 2.1(b) and using the estimate $|W| < 4^l \cdot l!$, we get part (a).

Taking now $l = 8$ a simple calculation shows that all $q > 63848$ fulfill the first inequality in 2.1(b). The largest possible Weyl group of some G with rank at most 8 is the one of type E_8, which has a bit less than $7 \cdot 10^8$ elements. Hence, in this case we see that $c/(2^l \cdot |W|)$ in 2.1(a) is at least $1/(1.8 \cdot 10^{13})$. $\square$

Note that in a statement like 2.2 it is necessary to fix an upper bound for the number of different prime divisors of m since the sequence $a_n = \prod_{i=1}^n (r_i - 1)/r_i$, r_i being the i-th prime, tends to zero with growing n. In 2.3 we show that the proportion of elements with order divisible by m can become arbitrarily small, even for G a torus, when m has many different prime divisors.

Now we collect some propositions needed for the proof of the theorem.

Proposition 2.3. *Let A be a finite Abelian group which contains an element of order m. Then A contains at least $\Phi(m)/m \cdot |A|$ elements whose order is divisible by m.*

Proof. In the case where A is a cyclic group of order r^a, r a prime, it contains $\Phi(r^a) = (r-1)r^{a-1}$ elements of order r^a, and hence of order divisible by r^b for all $b \leq a$.

In the general case let $m = \prod_{i=1}^k r_i^{b_i}$ be the prime decomposition of m. The Abelian group is isomorphic to a direct product of cyclic groups of prime power order. For any $r_i^{b_i}$, $i = 1, \ldots, k$, there must be a direct factor of A which is cyclic of order $r_i^{a_i}$ with $a_i \geq b_i$. The proposition follows from the result for the special case above, applied to these factors, and from $\Phi(m)/m = \prod_{i=1}^k (r_i - 1)/r_i$. $\square$

Proposition 2.4. *Let T be an F-stable torus of G of rank a. Then we can estimate the number of elements of $T(q)$ by*

$$(q-1)^a \leq |T(q)| \leq (q+1)^a.$$

Proof. The order $|T(q)|$ is the specialization at q of the characteristic polynomial of a matrix of finite order (see, e.g., **[Ca85]**, Proposition 3.3.8). Such a polynomial is a product of linear terms $X - \zeta$ with ζ on the unit circle. Since q is real and greater than 1 we have for each such factor $q - 1 \leq |q - \zeta| \leq q + 1$. $\square$

Proposition 2.5. *Let T be a maximal torus of G and $t \in T$.*

(a) *Then the connected component C of the centralizer of t in G is generated by T and the root subgroups U_α with $\alpha \in \Psi(t) = \{\alpha \mid \alpha$ root with respect to T, $\alpha(t) = 1\}$. The subgroup C is again a reductive group and it has root system $\Psi(t)$.*

(b) *Let $Z = Z((G^*)')$ be the center of the commutator subgroup of the dual group of G. If T is F-stable and $t \in T(q)$ then the index of $C(q)$ in the whole centralizer of t in $G(q)$ is at most $|Z|$.*

(c) *Two elements of T which are conjugate in G are conjugate under an element of the Weyl group of G with respect to T.*

Proof. For these results we give references to **[Ca85]**. Part (a) is in Theorem 3.5.3 and 3.5.4. Part (b) follows from **[Ca85]**, Section 4.5, similar to the proof of 4.5.8. And (c) is in 3.7.1. □

Proof (of Theorem 2.1). (1) An element of $G(q)$ of order m with $\gcd(m, p) = 1$ is contained in an F-stable maximal torus T of G. From Proposition 2.3 we know that at least $\Phi(m)/m \cdot |T(q)|$ elements of $T(q)$ have order divisible by m.

(2) The semisimple part of the dual group of G has a center containing at most 2^l elements: For this it is enough to find an upper bound for the order of the center for all simply connected groups of rank at most l. These groups are direct products of simple simply connected groups. And a simple group of rank k has at most $k + 1$ central elements (in case A_k). So the maximal possible order of such a center is that of a direct product of groups of type A_1 which all have centers of order 2.

(3) Let $t \in T(q)$ be non-regular semisimple, i.e., its connected centralizer is not the maximal torus T. It follows from 2.5(a) that there is a root α with respect to T with $\alpha(t) = 1$. Let Ψ be the smallest F-stable root subsystem containing α and consider the subgroup G_Ψ generated by T and the root subgroups U_β with $\beta \in \Psi$. Then t is an element of the center Z of G_Ψ. The connected component of Z is a torus S of rank smaller than $\mathrm{rank}(G)$. As in (2) we see that the index $(Z(q) : S(q))$ is at most 2^{l-1}.

The number of such subgroups G_Ψ is at most the number of positive roots of G. And using the classification of root systems we can estimate this number in all cases by $2 \cdot \mathrm{rank}(G)^2$.

From the upper bound for torus orders in 2.4, applied to the centers of the $G_\Psi(q)$, we find that $T(q)$ contains at most $2 \cdot l^2 \cdot 2^{l-1} \cdot (q+1)^{\mathrm{rank}(G)-1}$ non-regular elements.

(4) We assume now that q fulfills the first inequality in 2.1(b). We subtract 1 and multiply by $(q-1)^{l-1}$ in that inequality. Using the lower bound for $|T(q)|$ in 2.4 and (3) this shows that for such q the proportion of non-regular elements in $T(q)$ is at most $(\Phi(m)/m) - c$. Together with (1) we see that the proportion of regular elements in $|T(q)|$ with order divisible by m is at least c.

(5) We make the same assumption as in (4). We know from 2.5(b) and (2) that each conjugacy class of a regular semisimple element in $T(q)$ has at least $|G(q)|/(2^l \cdot |T(q)|)$ elements. Furthermore (4) and 2.5(c) say that there are at least $c/|W| \cdot |T(q)|$ such conjugacy classes whose elements have order divisible by m. This finishes the proof of the theorem. □

3. A refinement for classical groups

In our quite simple arguments of the last section all the estimates are very rough. In particular we did not take into account that for a given m there can be several non-conjugate maximal tori containing elements of order divisible by m. In this section we will do this for the cases of simple groups G of classical type.

We will use the same notation as in Section 2. Furthermore from now on we assume that G is a simple group and of classical type. Let k be the number of pairwise different prime divisors of m and define $c_k = \frac{1}{2}\prod_{i=1}^{k} \frac{p_i-1}{p_i}$, where p_i is the i-th prime number.

Theorem 3.1. *Let G, m, k as above, G of rank l. Assume that $G(q)$ contains an element of order m and $q > 2l^2 \cdot 6^{l-1}/c_k + 1$. Then the proportion of regular semisimple elements of $G(q)$ of order divisible by m is at least $c(k,l) = c_k/(2(2l)^k(l+1))$. If we assume further that G is simply connected the estimate can be improved to $c(k,l) = c_k/(2(2l)^k)$.*

Proof. **(1)** The smallest possible value of $\Phi(m)/m$ for an m as above is $2c_k$. Taking $c = c_k$ in Theorem 2.1, we get the statement as in the theorem with $c'(k,l) = c_k/(2^l \cdot |W|)$ instead of $c(k,l)$. The restriction on q given in the theorem is taken from the second estimate in 2.1(b).

(2) The term 2^l in $c'(k,l)$ comes from estimating the number of connected components of the center of the dual group of G. Under our current assumption that G is simple, this term can be replaced by $(l+1)$ - the worst case being $G = PGL_{l+1}$. If G is simply connected the dual group has trivial center and hence this term can even be replaced by 1. (See part (2) of the proof of Theorem 2.1.)

(3) The $G(q)$-conjugacy classes of F-stable maximal tori of G are parameterized by the F-conjugacy classes of W. Let $T(q)$ be a maximal torus of $G(q)$ containing an element of order m and let T be parameterized by $w \in W$.

The term $|W|$ in $c'(k,l)$ comes from estimating the number of elements in $T(q)$ which are $G(q)$-conjugate to a fixed regular semisimple element in $T(q)$ (see part (5) of the proof of Theorem 2.1). Using the w parameterizing T we can give the exact number of such elements; it is $|C_{W,F}(w)|$, the order of the F-centralizer of w in W. (See **[Ca85]**, 3.3 and 3.7, for more details.)

(4) Let q be as in the theorem and $w_1, \ldots, w_r \in W$ be representatives of the F-conjugacy classes of W parameterizing classes of tori $T(q)$ containing elements of order m. Adding up the contributions from the single classes of tori as given in (3) we get that the proportion of regular semisimple elements in $G(q)$ whose order is divisible by m is at least $c_k/(l+1) \cdot \sum_{i=1}^{r} 1/|C_{W,F}(w_i)|$.

Hence, to prove the theorem, we have to show that the proportion of elements of W parameterizing maximal tori $T(q)$ which contain an element of order m is at least $1/(2 \cdot (2l)^k)$. We will show this in the next step case by case.

(5) (**Type** A_l). We consider W with respect to a maximally split torus T_0, then F acts trivially on W. Here W is isomorphic to the symmetric group S_n on $n = l+1$ letters. Let $w \in S_n$ be of cycle type $(a_1, \ldots, a_r)$. Then a maximal torus $T(q)$ parameterized by w is isomorphic to a direct product of cyclic groups of order $(q^{a_1}-1)/(q-1)$, $q^{a_2}-1$, $\ldots$, $q^{a_r}-1$. When $T(q)$ contains an element of order m then any prime power dividing m is a divisor of one of the orders of the cyclic factors. Since m is a product of at most k prime powers, we need to answer the following question: Given $b_1, \ldots, b_k \in \mathbb{N}$. What is the proportion of elements of S_n with cycles whose lengths contain multiples of $b_1, \ldots, b_k$? (We must be a bit careful if a prime power dividing m divides $q-1$. But then all maximal tori contain elements with order divisible by this prime power, except the case where n is prime and $T(q)$ corresponds to an n-cycle.)

By replacing $b_1, \ldots, b_k$ by multiples and deleting b_j which divide others, we may assume that $l+1-\sum_{i=1}^{k} b_i < b_j$ for all j. In this case the number of elements in S_n having cycles of length $b_1, \ldots, b_k$ is easily counted by:

$$\frac{n!\,(b_1-1)!}{(n-b_1)!\,b_1!} \cdot \frac{(n-b_1)!\,(b_2-1)!}{(n-b_1-b_2)!\,b_2!} \cdots$$

$$\frac{(n-b_1-\ldots-b_{k-1})!\,(b_k-1)!}{(n-b_1-\ldots-b_k)!\,b_k!} \cdot (n-b_1-\ldots-b_k)! = \frac{n!}{b_1\cdots b_k}$$

Hence the proportion we are looking for can be estimated by $1/(b_1 \cdots b_k) > 1/(l+1)^k$.

(**Type** ${}^2A_l$). Here the argument goes as in type A_l, we only have to replace q by $-q$ and adjust signs.

(**Type** B_l**,** C_l). Here we consider W as a wreath product of a cyclic group with 2 elements with a symmetric group on l letters. The maximal torus parameterized by a $w \in W$ is a direct product of cyclic groups of order q^a-1 for a positive cycle of length a, respectively q^a+1 for a negative cycle of length a.

The argument is now similar to the case of type A_{l-1}, we only need to adjust the sign of each cycle correctly, which gives the additional factor $1/2^k$.

(**Type** D_l). The Weyl group W of this type is a normal subgroup of the Weyl group W' of type B_l of index 2. An element $w \in W'$ is in W, if and only if the number of negative cycles is even. The argument is now similar to case B_l, we only have to assure that we only count elements in the subgroup W of W' in those cases where we count more than one conjugacy class. This gives another factor $1/2$ in the estimate.

(**Type** ${}^2D_l$). Here the F-conjugacy classes of W correspond to the conjugacy classes of W' outside W. The argument is exactly the same as for type D_l. □

References

[Ca85] R.W. Carter. Finite Groups of Lie Type - Conjugacy Classes and Complex Characters. A Wiley-Interscience publication, Chichester, 1985.

[GL99] R. M. Guralnick and F. Lübeck. On p-singular elements in Chevalley groups in characteristic p. In this volume, 1999.

Dr. Frank Lübeck, RWTH Aachen, Lehrstuhl D für Mathematik, Templergraben 64, D-52062 Aachen, Germany
Email: Frank.Luebeck@Math.RWTH-Aachen.De