Journal of Algebra and Its Applications
(2021) 2150121 (13 pages)

DOI: 10.1142/S0219498821501218

World Scientific
www.worldscientific.com

p-power conjugacy classes in $U(n, q)$ and $T(n, q)$

Silvio Dolfi
Dipartimento di Matematica e Informatica Dini
Università di Firenze, 50134 Firenze, Italy
dolfi@math.unifi.it

Anupam Singh*
IISER Pune, Dr. Homi Bhabha Road
Pashan, Pune 411008 India
anupamk18@gmail.com

Manoj K. Yadav
School of Mathematics, Harish-Chandra Research Institute
HBNI, Chhatnag Road, Jhunsi, Allahabad 211019, India
myadav@hri.res.in

AQ: Pls provide complete affiliation details.

Please check if dates are correct.

Received 15 May 2019
Accepted 18 March 2020
Published

Communicated by

Please provide Communicated by details.

Let q be a p-power where p is a fixed prime. In this paper, we look at the p-power maps on unitriangular group $U(n, q)$ and triangular group $T(n, q)$. In the spirit of Borel dominance theorem for algebraic groups, we show that the image of this map contains large size conjugacy classes. For the triangular group we give a recursive formula to count the image size.

Keywords: Word map; triangular group; unitriangular group.

Mathematics Subject Classification: 20G40

1. Introduction

Let G be a finite group and w be a word. The word w defines a map into G called a word map. It has been a subject of intensive investigation whether these maps are surjective on finite simple and quasi-simple groups; we refer to this paper by Shalev [9] for a survey on this subject. A more general problem is to determine the image $w(G)$ of a word map and, in particular, its size. In this paper, we investigate

*Corresponding author.

power maps, that is, maps corresponding to the word $w = X^p$, for the lower-triangular matrix group $T(n, q)$ and lower unitriangular matrix group $U(n, q)$ over finite fields $\mathbb{F}_q$, where q is a p-power for a fixed prime p. Results concerning the verbal subgroup, that is the group generated by the image of the power map, for triangular and unitriangular group can be found in [1, 11].

Motivated by the Borel's dominance theorem for algebraic groups, Gordeev, Kunyavskiĭ and Plotkin started investigating the image of a non-surjective word map more closely (see [3–6]). In the spirit of questions raised in [6, Sec. 4] for algebraic groups, we address, for the groups $T(n, q)$ and $U(n, q)$, the question: Which semisimple, and unipotent elements lie in the image of the power maps and whether it contains "large" conjugacy classes?

One of the motivations for our interest in the triangular and unitriangular groups lies in the fact that $T(n, q)$ is a Borel subgroup of $\mathrm{GL}(n, q)$ and $U(n, q)$ is a Sylow p-subgroup of $\mathrm{GL}(n, q)$. In the finite groups of Lie type, the regular semisimple elements play an important role as they are dense (see [7]). Considering the image of a word map on maximal tori has turned out to be useful in getting asymptotic results. Thus, we aim at considering the large size conjugacy classes in $U(n, q)$, described in [12], and try to understand if they are in the image under the power map $w = X^p$. (Note that clearly, raising to a power coprime to p gives a bijection of $U(n, q)$). In what follows, we use the notation G^p for the image $w(G)$ of a group G under the word map given by $w = X^p$ (we call it *power map*). So, $G^p = \{g^p \mid g \in G\}$ is the *set* consisting of the p-powers of the elements of G. We remark that the *verbal width* with respect to power maps, that is, the smallest number k such that the product of k-copies of G^p, coincides with the verbal subgroup $\langle G^p \rangle$, has already been determined: see [1, Theorem 5] for $G = U(n, q)$ and [11, Theorem 1] for $G = T(n, q)$.

It is known (see [1, Theorem 3 or Proposition 3.4]) that $U(n, q)^p$ is contained in the subgroup $U_{p-1}(n, q) = \{(a_{ij}) \in U(n, q) \mid a_{ij} = 0, \forall\, i - j \leq p - 1\}$ consisting of the lower triangular matrices with the first $p - 1$ sub-diagonals having zero entries. Moreover, $U(n, q)^p = 1$ if and only if $n \leq p$, and $U(n, q)^p = U_{p-1}(n, q)$ if and only if $n = p + 1$ and $p + 2$. Our first result, for $n \geq p + 3$, is the following estimate on the set of pth powers in $U(n, q)$.

Theorem A. *Let q be a power of a prime p and n an integer such that $n \geq p+3$. Then, the set $U(n, q)^p$ is a proper generating subset of $U_{p-1}(n, q)$ and $|U(n, q)^p| > \frac{1}{3}|U_{p-1}(n, q)|$, when $q \geq n - p - 1$.*

Next, we prove the following result, which reduces the counting of p-powers for $T(n, q)$ to that of unitriangular groups of smaller size.

Theorem B. *Let q be a p-power and suppose $q > 2$. Then for the group $T = T(n, q)$ we have*

$$|T^p| = \sum_{(a_1,\ldots,a_k)\vdash n, k<q} \left(\frac{(q-1)\cdots(q-k)n!}{\prod_{b=1}^{n} m_b!(b!)^{m_b}} \right) \left(\prod_{i=1}^{k} |U(a_i, q)^p| \right) q^{\binom{n}{2} - \sum_{i=1}^{k} \binom{a_i}{2}},$$

where the m_b's are obtained by writing the partition $(a_1,\ldots,a_k)$ in power notation as $1^{m_1}\ldots n^{m_n}$.

Using the estimate in Theorem A, we hence, get the following corollary.

AQ: Pls check the edit.

Corollary C. *Let q be a power of a prime p such that $q > n-p-1 > 2$. Then for the group $T = T(n,q)$ we have*

$$\frac{|T^p|}{|T|} \geq \frac{2^{n-2}}{9(q-1)^{n-2}q^{(p-1)(n-p)}}.$$

We conclude the section with a quick layout. Theorem A is proved in Sec. 3 and Theorem B and Corollary C in Sec. 4. All groups considered in what follows are tacitly assumed to be finite.

2. Conjugacy Classes in $U(n,q)$

The conjugacy classes of the unitriangular group $U(n,q)$, considered as the group of upper unitriangular matrices, have been studied in a series of papers by Arregi and Vera-López; we will use, in particular, the results in [12, 13]. For the convenience of the reader, we reproduce some notations and results from [13] in the setting of lower unitriangular matrices, i.e. swapping the notation by taking transpose.

Let us order the index set $\mathcal{I} = \{(i,j) \mid 1 \leq j \leq i \leq n\}$ in the following manner:

$$(n,n-1) < (n-1,n-2) < (n,n-2) < (n-2,n-3) < \cdots < (n-1,1) < (n,1).$$

To every $A = (a_{ij}) \in U(n,q)$ and $(r,s) \in \mathcal{I}$, one associates a vector $\mu_{(r,s)}(A)$ (the (r,s)-*weight* of A) as follows:

$$\mu_{(r,s)}(A) := (\mu(a_{ij}))_{(i,j)\leq(r,s)},$$

where $\mu(a_{ij}) = 0$ if $a_{ij} = 0$ and $\mu(a_{ij}) = 1$ if $a_{ij} \neq 0$. The vector $\mu_{(n,1)}(A)$ is called the *weight* of A and is simply denoted by $\mu(A)$. So, $\{\mu(A) \mid A \in U(n,q)\} = \{0,1\}^{\frac{n(n-1)}{2}}$ and we totally order this set of weights by lexicographical order (considering $0 < 1$). For a given index $(r,s) \in \mathcal{I}$, we order $\mu_{(r,s)}(A)$ in the same manner. We remark that in [13], the word "type" is used in place of "weight". But we will use "weight" as we use "type" for some other purpose.

For $(r,s) \in \mathcal{I}$, define

$$\mathcal{G}_{(r,s)} := \{A = (a_{ij}) \in U(n,q) \mid a_{ij} = 0 \text{ for all } (i,j) \leq (r,s)\}.$$

It is a routine check to see that $\mathcal{G}_{(r,s)}$ is a normal subgroup of $U(n,q)$ having order $q^{ns-r-\frac{s(s-1)}{2}}$. The tuple $\mu_{(r,s)}(A)$ doesn't depend on the representative A of the coset $\bar{A} := A\mathcal{G}_{(r,s)}$. Thus, it makes sense to define the (r,s)-type of $\bar{A}$ as the (r,s)-type of A. As proved in [13, Theorem 3.2], every conjugacy class in $U(n,q)/\mathcal{G}_{(r,s)}$ contains a unique element of minimum (r,s)-weight. A matrix $A \in U(n,q)$ is said to be *canonical* if $A\mathcal{G}_{(r,s)}$ is the unique element of its conjugacy class in $U(n,q)/\mathcal{G}_{(r,s)}$ having minimal (r,s)-weight for all $(r,s) \in \mathcal{I}$.

For each $(r,s) \in \mathcal{I}$, let us define

$$\mathcal{N}_{(r,s)} := \mathcal{G}_{(r,s)^*}/\mathcal{G}_{(r,s)},$$

where $(r,s)^*$ denotes the preceding pair of (r,s) in the ordering of $\mathcal{I}$ defined above. It follows from [13, Lemma 3.4] that for every $A \in U(n,q)$ and $(r,s) \in \mathcal{I}$ the number of conjugacy classes in $U(n,q)/\mathcal{G}_{(r,s)}$ which intersect with $\bar{A}\mathcal{N}_{(r,s)}$ is either 1 or q, where $\bar{A} = A\mathcal{G}_{(r,s)}$. We say that $(r,s) \in \mathcal{I}$ is an *inert point* of $A \in U(n,q)$ if the number in the preceding statement is 1.

The following two results are restatements of [13, Lemmas 3.7 and 3.8] for lower unitriangular matrices.

Lemma 2.1. *Let $A \in U(n,q)$ be a canonical matrix such that $a_{rs} \neq 0$ and $a_{js} = 0$ for all j such that $s < j < r$. Then the pairs (r,s'), with $s' < s$, are inert points of A.*

Lemma 2.2. *Let $A \in U(n,q)$ be a canonical matrix such that $a_{rs} \neq 0$ and $a_{ri} = 0$ for all i, $s < i < r$. Then the pair (r',s) for any $r' > r$ is an inert point of A if $a_{jr'} = 0$ for all $j > r'$.*

We set the following notation. Given $k \in \{0,1,\ldots,n-1\}$, we say that the array of entries $(a_{k+1,1}, a_{k+2,2}, \ldots, a_{n,n-k})$ is the *kth-sub-diagonal* of the matrix $A = (a_{i,j})$. For l such that $0 \leq l \leq n-1$, define

$$U_l(n,q) := \{A = (a_{ij}) \in U(n,q) \,|\, a_{ij} = 0, \text{ for all } i - j \leq l\},$$

consisting of lower unitriangular matrices whose first l sub-diagonals have all zero entries. We remark that

$$U(n,q) = U_0(n,q) \supset U_1(n,q) \supset \cdots \supset U_l(n,q) \supset \cdots \supset U_{n-1}(n,q) = \{1\},$$

is the lower central series of $U(n,q)$, with $U_l(n,q) = \gamma_{l+1}(U(n,q))$, and that the $U_l(n,q)$ are the only fully invariant subgroups of $U(n,q)$ [1, Theorem 1].

Having fixed a dimension n, in $M(n,q)$ we denote by I the identity matrix and by e_{rs} the elementary matrix with 1 at (r,s)th place and 0 elsewhere. We now turn our attention to some relevant elements of the subgroups $U_l(n,q)$.

For $0 \leq l \leq n-2$, set

$$A(a_1, a_2, \ldots, a_{n-l-1}) = I + \sum_{i=1}^{n-l-1} a_i e_{l+1+i,i} \in U_l(n,q), \tag{2.1}$$

where $a_1, a_2, \ldots, a_{n-l-1} \in \mathbb{F}_q$.

We have the following important property of the elements defined in (2.1).

Lemma 2.3. *For every choice of $0 \leq l \leq n-2$ and $a_1, a_2, \ldots, a_{n-l-1} \in \mathbb{F}_q$, the element $A(a_1, a_2, \ldots, a_{n-l-1})$ is a canonical element of $U(n,q)$.*

Proof. In order to show that $A = A(a_1, a_2, \ldots, a_{n-l-1}) \in U_l(n,q)$ is a canonical element of $U(n,q)$, we need to prove that each nonzero entry on the $l+1$th sub-diagonal of $A\mathcal{G}_{(r,s)}$ will continue to be nonzero in every $U(n,q)/\mathcal{G}_{(r,s)}$-conjugate of

$A\mathcal{G}_{(r,s)}$ for all $(r,s) \in \mathcal{I}$. More generally, we observe that if $A = (a_{i,j}) \in U_l(n,q)$ and $B = (b_{i,j}) \in U(n,q)$, then the $(l+1)$th subdiagonal of A and $B^{-1}AB$ are identical modulo $\mathcal{G}_{(r,s)}$ for all pairs $(r,s) \in \mathcal{I}$. In fact, it is readily checked that the element in the $(l+1+k,k)$th place, for $k = 1, \ldots, n-l-1$, of the $(l+1)$th subdiagonal of both AB and BA, is simply $a_{l+1+k,k} + b_{l+1+k,k}$ modulo $\mathcal{G}_{(r,s)}$. This shows that A is canonical in $U(n,q)$. □

We conclude this section with the following result in which we single out conjugacy classes of $U_l(n,q)$ of considerably large orders, including the largest ones.

Proposition 2.4. *Let $0 \leq l \leq n-2$. For $0 \leq m \leq \lfloor \frac{n-l-1}{2} \rfloor + 1$, set*

$$\mathcal{A}_m = \{A(a_1, a_2, \ldots, a_{n-l-1}) \,|\, a_i = 0 \text{ for } i \leq m, a_i \in F_q^\times \text{ for } i > m\},$$

and for $\lfloor \frac{n-l-1}{2} \rfloor < m \leq n-l$, set

$$\mathcal{B}_m = \{A(a_1, a_2, \ldots, a_{n-l-1}) \,|\, a_i \in F_q^\times \text{ for } i < m, a_i = 0 \text{ for } i \geq m\}.$$

Then, the elements in $\mathcal{A}_m$ are representatives of distinct $U(n,q)$-conjugacy classes of size $q^{\frac{(n-l-1)(n-l-2)}{2} - \frac{m(m-1)}{2}}$ and the elements in $\mathcal{B}_m$ are representatives of distinct $U(n,q)$-conjugacy classes of size $q^{\frac{(n-l-1)(n-l-2)}{2} - \frac{(n-l-m)(n-l-m-1)}{2}}$.

Proof. Since by Lemma 2.3, the elements in $\mathcal{A}_m$ and $\mathcal{B}_m$ are canonical elements of $U(n,q)$, it follows by [13, Corollary 3.3] that these are pair-wise non-conjugate in $U(n,q)$.

Let $A \in \mathcal{A}_m$. Then for each t, $m+1 \leq t \leq n-l-1$, it follows from Lemma 2.1 that there are $t-1$ inert points of A corresponding to a_t. So the number of inert points of A is at least $\frac{(n-l-1)(n-l-2)}{2} - \frac{m(m-1)}{2}$. Thus, by [13, Theorem 3.5], the conjugacy class of A in $U(n,q)$ has size at least $q^{\frac{(n-l-1)(n-l-2)}{2} - \frac{m(m-1)}{2}}$. We claim that it cannot be bigger than this. Let G_m denote the subset of $U_{l+1}(n,q)$ defined as

$$G_m = \{B = (b_{ij}) \in U_{l+1}(n,q) \,|\, b_{ij} = 0 \text{ for all } l+2 < i \leq l+m+1, 1 \leq j < m\}.$$

It is not difficult to see that G_m is a normal subgroup of $U(n,q)$ having order $q^{\frac{(n-l-1)(n-l-2)}{2} - \frac{m(m-1)}{2}}$. Note that $[A, U(n,q)] \subseteq G_m$, where

$$[A, U(n,q)] = \{[A,C] \,|\, C \in U(n,q)\}.$$

This shows that the size of the conjugacy class of A in $U(n,q)$ is at the most $|G_m|$, as claimed. Hence, the assertion for the elements of $\mathcal{A}_m$ holds.

Assertion for the elements in $\mathcal{B}_m$ holds on the same lines using Lemma 2.2, which completes the proof. □

3. Unitriangular Matrix Group

We look at the power map $w = X^p$ on the unitriangular group $U(n, q)$. We begin by stating the following results from [1] to improve readability of this section.

Lemma 3.1. *Let A be a lower unitriangular matrix in $U(n, q)$ such that $A - I = (a_{ij})$. Then the matrix $A^m = I + (b_{ij})$ is given by*

$$b_{ij} = \binom{m}{1} a_{ij} + \binom{m}{2} \left(\sum_{r_1=j+1}^{i-1} a_{i,r_1} a_{r_1,j} \right) + \binom{m}{3} \left(\sum_{r_1=j+1}^{i-1} \sum_{r_2=r_1+1}^{i-1} a_{i,r_2} a_{r_2,r_1} a_{r_1,j} \right)$$
$$+ \cdots + \binom{m}{k} \left(\sum_{r_1=j+1}^{i-1} \sum_{r_2=r_1+1}^{i-1} \cdots \sum_{r_{k-1}=r_{k-2}+1}^{i-1} a_{i,r_{k-1}} a_{r_{k-1},r_{k-2}} \cdots a_{r_1,j} \right)$$
$$+ \cdots + \binom{m}{m} \left(\sum_{r_1=j+1}^{i-1} \sum_{r_2=r_1+1}^{i-1} \cdots \sum_{r_{m-1}=r_{m-2}+1}^{i-1} a_{i,r_{m-1}} a_{r_{m-1},r_{m-2}} \cdots a_{r_1,j} \right).$$

We use Lemma 3.1 to prove the following result for pth powers.

Corollary 3.2. *Let $A \in U(n, q)$ be such that $A - I = (a_{i,j})$ and $A^p = I + (b_{i,j})$. Then, $b_{i,j} = 0$ for all $i - j < p$ and*

$$b_{i,j} = \sum_{r_1=j+1}^{i-1} \sum_{r_2=r_1+1}^{i-1} \cdots \sum_{r_{p-1}=r_{p-2}+1}^{i-1} a_{i,r_{p-1}} a_{r_{p-1},r_{p-2}} \cdots a_{r_1,j},$$

otherwise. In particular, if $n \leq p$, then $A^p = I$, and if $n > p$, then $U(n, q)^p \subseteq U_{p-1}(n, q)$.

Proof. Since the binomial coefficients appearing in the formula of Lemma 3.1 for $m = p$ are all zero modulo p, except possibly the last one, we get

$$b_{i,j} = \sum_{r_1=j+1}^{i-1} \sum_{r_2=r_1+1}^{i-1} \cdots \sum_{r_{p-1}=r_{p-2}+1}^{i-1} a_{i,r_{p-1}} a_{r_{p-1},r_{p-2}} \cdots a_{r_1,j}.$$

If $i - j < p$, this is an empty sum, that is, it's 0. This happens for all pairs (i, j) if $n < p$; giving $A^p = I$. If $i - j \geq p$, which actually implies that $n \geq p$, then $a_{i,j}$'s are given by the expression as stated, and obviously fall in $U_{p-1}(n, q)$. □

As an immediate consequence, we have the following result.

Proposition 3.3. *For $n > p$ and $l = p - 1$, every element of $\mathcal{A}_m$ and $\mathcal{B}_m$ (defined in Proposition 2.4) is a pth power in $U(n, q)$.*

Proof. We first show that the elements $A := A(a_1, a_2, \ldots, a_{n-l-1})$ defined in (2.1) for $a_1, a_2, \ldots, a_{n-l-1} \in \mathbb{F}_q^\times$ are pth powers. Let $b_{2,1} = \cdots = b_{p,p-1} = 1$. Then

iteratively define

$$b_{p+i+1,p+i} := (b_{i+2,i+1} \dots b_{p+i,p+i-1})^{-1} a_{i+1},$$

for $0 \leq i < n-p$. Now, consider the lower unitriangular matrix $C := (c_{i,j})$, where $c_{i,i-1} = b_{i,i-1}$ for $2 \leq i \leq n$ and $c_{i,j} = 0$ for $i - j > 1$. Using Corollary 3.2, it is a routine computation to show that $C^p = A$.

Now, let $A := A(a_1, a_2, \dots, a_{n-l-1}) \in \mathcal{B}_m$. Then, by the definition, $a_i \in F_q^\times$ for $i < m, a_i = 0$ for $i \geq m$. Thus, in the above procedure, $b_{i,i-1} = 0$ for $p + m \leq i \leq n$. Considering $C := (c_{i,j})$, where $c_{i,i-1} = b_{i,i-1}$ for $2 \leq i \leq n$ and $c_{i,j} = 0$ for $i - j > 1$, we see, again using Corollary 3.2, that $C^p = A$.

For $A := A(a_1, a_2, \dots, a_{n-l-1}) \in \mathcal{A}_m$, let $b_{i,i-1} = 0$ for $2 \leq i \leq m+1$, $b_{i,i-1} = 1$ for $m + 2 \leq i \leq m + p$ and then iteratively define

$$b_{p+i+1,p+i} := (b_{i+2,i+1} \dots b_{p+i,p+i-1})^{-1} a_{i+1},$$

for $m \leq i < n-p$. Again, considering $C := (c_{i,j})$, where $c_{i,i-1} = b_{i,i-1}$ for $2 \leq i \leq n$ and $c_{i,j} = 0$ for $i - j > 1$, it follows that $C^p = A$, which completes the proof. □

The following proposition, which follows from the above formulas, is proved in [1, Theorems 2 and 3] (also see [8, III, Satz 16.5]).

Proposition 3.4. *Let q be a p-power. Then,*

(1) *for $n \leq p$, $U(n,q)^p = 1$;*
(2) *for $n = p+1$ and $n = p+2$, $U(n,q)^p = U_{p-1}(n,q)$;*
(3) *for $n \geq p+3$, $U(n,q)^p \subset U_{p-1}(n,q)$ and $\langle U(n,q)^p \rangle = U_{p-1}(n,q)$.*

We now provide a lower bound on $|U(n,q)^p|$.

Proposition 3.5. *Let q be a power of p and n an integer such that $n \geq p+3$. Then, if $n-p$ is even,*

$$|U(n,q)^p| \geq q^{\frac{(n-p)(n-p-1)}{2}}((q-1)^{n-p}) + \sum_{m=1}^{\lfloor \frac{n-p}{2} \rfloor} q^{\frac{(n-p)(n-p-1)}{2} - \frac{m(m-1)}{2}}(2(q-1)^{n-p-m}),$$

and if $n-p$ is odd,

$$|U(n,q)^p| \geq q^{\frac{(n-p)(n-p-1)}{2}}((q-1)^{n-p}) + \sum_{m=1}^{\lfloor \frac{n-p}{2} \rfloor} q^{\frac{(n-p)(n-p-1)}{2} - \frac{m(m-1)}{2}}(2(q-1)^{n-p-m}) + q^{\frac{(n-p)(n-p-1)}{2} - \frac{r(r-1)}{2}}(2(q-1)^{n-p-r}),$$

where $r = \lfloor \frac{n-p}{2} \rfloor + 1$.

Proof. It follows from Proposition 3.3 that every element of $\mathcal{A}_m$ as well as of $\mathcal{B}_m$ is a pth power in $U(n,q)$. The result now follows by considering the sizes of all distinct conjugacy classes of elements of $\mathcal{A}_m$ and $\mathcal{B}_m$ obtained in Proposition 2.4. □

We are now ready to prove Theorem A.

Proof of Theorem A. The first assertion follows from Proposition 3.4. For the second assertion, by Proposition 3.5, we have

$$|U(n,q)^p| > q^{\frac{(n-p)(n-p-1)}{2}}((q-1)^{n-p}+2(q-1)^{n-p-1}).$$

Hence,

$$\frac{|U(n,q)^p|}{|U_{p-1}(n,q)|} > \frac{q^{\frac{(n-p)(n-p-1)}{2}}((q-1)^{n-p}+2(q-1)^{n-p-1})}{q^{\frac{(n-p)(n-p+1)}{2}}},$$

which implies

$$\frac{|U(n,q)^p|}{|U_{p-1}(n,q)|} > \left(1-\frac{1}{q}\right)^{n-p-1}\left(1+\frac{1}{q}\right).$$

Thus, if we take $q \geq n-p-1$, then we get

$$\frac{|U(n,q)^p|}{|U_{p-1}(n,q)|} > \left(1-\frac{1}{q}\right)^{n-p-1}\left(1+\frac{1}{q}\right) \geq \left(1-\frac{1}{q}\right)^{q}\left(1+\frac{1}{q}\right) > \frac{1}{3}.$$

This completes the proof. □

We conclude this section with some computations using Bosma [2], which are as follows.

(n,q)	$\lvert U(n,q)^p\rvert$	$\lvert U_{p-1}(n,q)\rvert$	$\lvert U(n,q)^p\rvert/\lvert U_{p-1}(n,q)\rvert$
(5,2)	52	$2^6 = 64$	$> \frac{1}{3}$
(5,4)	3376	$4^6 = 4096$	$> \frac{1}{3}$
(6,2)	600	$2^{10} = 1024$	$> \frac{1}{3}$
(6,3)	585	$3^6 = 729$	$> \frac{1}{3}$
(7,2)	13344	$2^{15} = 32768$	$> \frac{1}{3}$
(8,2)	573184	$2^{21} = 2097152$	$< \frac{1}{3}$

In view of the values in the last row of this table, we remark that the condition on q in Theorem A cannot be completely dropped.

4. Triangular Matrix Group

In this section, we consider the group of triangular matrices $T(n,q)$, where q is a power of a prime p, aiming at computing the size $|T(n,q)^p|$ of the set of its p-powers. Since the group $T(n,2) = U(n,2)$ we assume $q > 2$, now onwards. We begin with setting up some notation. We denote by $D(n,q)$ the subgroup of $T(n,q)$ consisting of the diagonal matrices. The elements of $D(n,q)$ can be grouped in "types" in such a way that all elements of each type have the isomorphic centralizers in $T(n,q)$. We recall that a *partition* of a positive integer n is a sequence of positive integers $\delta = (a_1,\ldots,a_k)$ such that $a_1 \geq a_2 \geq \cdots \geq a_k > 0$ and $\sum_{j=1}^{k} a_j = n$. One can also

write the partition δ in *power notation* $1^{m_1}2^{m_2}\dots n^{m_n}$ where $m_i = |\{a_j \,|\, a_j = i\}|$ is the number of *parts* a_j's equal to i, for $1 \le i \le n$; so, $m_i \ge 0$ and $\sum_{i=1}^{n} i m_i = n$.

Let $\Pi = \{X_1, X_2, \dots, X_k\}$ be a *set-partition* of $I_n = \{1, 2, \dots, n\}$, i.e. a family of non-empty and pairwise disjoint subsets of I_n, whose union is I_n. Setting $a_i = |X_i|$ and assuming, as we may, that $a_i \ge a_j$ for $i \le j$, the tuple $\delta = (a_1, a_2, \dots, a_k)$ is a partition of the number n; we say that δ is the *type* of Π, and simply denote it as $\delta = \tau(\Pi)$.

A diagonal matrix $d \in D(n,q)$, seen as a map from the set $I_n = \{1, 2, \dots, n\}$ to the set $F_q^\times$ of the nonzero elements of the field F_q, determines in a natural way as set-partition Π_d of I_n, namely the family of the nonempty fibers of the map d. We set $\delta = \tau(\Pi_d)$ as the *type* of d and we write $\delta = \tau(d)$.

We denote the number k of parts in δ by $l(\delta)$, the *length* of δ, and we observe that there exist elements of type δ in D if and only if $l(\delta) < q$. (Thus, not all partitions of n may appear as type of an element in $D(n,q)$, when $q \le n$).

Given a partition δ of n with $l(\delta) < q$, we denote by $D_\delta(n,q) = \{d \in D \,|\, \tau(d) = \delta\}$ the set of all elements in $D(n,q)$ of the given type δ.

Lemma 4.1. *Let n be a positive integer and let $\delta = (a_1, a_2, \dots, a_k)$ be a partition of n. Write δ in power notation as $1^{m_1}\dots n^{m_n}$ and assume that $k = l(\delta) < q$. Then*

$$|D_\delta(n,q)| = \frac{(q-1)!n!}{(q-k-1)!\prod_{i=1}^{n}((i!)^{m_i}\cdot m_i!)}.$$

Proof. Let Δ be the set consisting of the set-partitions of I_n having type δ. As above, we associate to a diagonal element $d \in D_\delta$ a set-partition $\Pi_d \in \Delta$, and observe that all the fibers of the map $\pi : D_\delta \to \Delta$ defined by $\pi(d) = \Pi_d$, have the same size $\frac{(q-1)!}{(q-k-1)!}$ (the number of injective maps from a set of $k = l(\delta)$ elements into a set of $q-1$-elements). On the other hand, the cardinality $|\Delta|$ is easily determined by looking at the natural transitive action of the symmetric group S_n on Δ and observing that the stabilizer in S_n of a partition of type $\delta = 1^{m_1}\dots n^{m_n}$ has size $\prod_{i=1}^{n}((i!)^{m_i}\cdot m_i!)$. □

Lemma 4.2. *For any partition δ of n, with $l(\delta) < q$, and for any element $d \in D_\delta(n,q)$, all centralizers $C_{U(n,q)}(d)$ belong to the same isomorphism class. Moreover, if $\delta = (a_1, a_2, \dots, a_k)$, then $|\, C_{U(n,q)}(d)\,| = q^{\sum_{i=1}^{k}\binom{a_i}{2}}$.*

Proof. Let $\delta = (a_1, a_2, \dots, a_k)$ be a given partition of n, with $k < q$, and let

$$d = (\underbrace{d_1, \dots, d_1}_{a_1}, \dots, \underbrace{d_k, \dots, d_k}_{a_k}),$$

where $d_1, \dots, d_k$ are distinct elements of F_q, be a "standard-form" element in D_δ. Write $G = GL_n(q)$, $U = U(n,q)$. It is well known that $C_G(d) = \prod_{i=1}^{k} \mathrm{GL}_{a_i}(q)$, the subgroup of δ-block matrices.

Let $b = b_\pi \in G$ be a permutation matrix, where $\pi \in S_n$. We will show that $C_U(d^b)$ is isomorphic to $C_U(d)$. In order to do this, it is enough to show that the

two subgroups have the same order, since $C_U(d) = C_G(d) \cap U$ is a Sylow p-subgroup of $C_G(d)$ and $C_U(d^b) = C_G(d)^b \cap U \cong C_G(d) \cap U^{b^{-1}}$ is a p-subgroup. We denote by $M = \prod_{i=1}^{k} M_{a_i}(q)$, the δ-blocks matrix algebra and write $C = C_G(d)$. We observe that $M \cap U = C \cap U$, $M^b \cap U = C^b \cap U$ and that, arguing by induction on the number k of diagonal blocks, in order to prove that $|M \cap U| = |M^b \cap U|$ we can reduce to the case $k = 2$.

Now, $M \cap U = (I_n + V) \cap U = I_n + (V \cap U_0)$, where V is the F_q-space spanned by the set of pairs of elementary matrices $\{e_{i,j}, e_{j,i}\}$, where $1 \leq i < j \leq a_1$ or $a_1 + 1 \leq i < j \leq n$, and the F_q-space U_0 is spanned by the $e_{i,j}$'s with $i < j$. Observing that for every pair i, j we have $e_{i,j}^b = e_{\pi(i),\pi(j)}$ and that the pair $\{e_{i,j}, e_{j,i}\}^b = \{e_{\pi(i),\pi(j)}, e_{\pi(j),\pi(i)}\}$ contains exactly one element in $V^b \cap U$, we conclude that the F_q-spaces $V^b \cap U_0$ and $V \cap U_0$ have the same dimension. Therefore, $|C \cap U| = |M \cap U| = |M^b \cap U| = |C^b \cap U|$.

We finish by note that $|C_{U(n,q)}(d)| = \prod_i q^{\binom{a_i}{2}}$ is independent on the choice of the elements $d_1, \ldots, d_k$ and that every element in D_δ is conjugate by a permutation matrix to a "standard-form" element d as above. □

Before proving Theorem B, we recall some elementary facts.

For any fixed prime number p and an element (of finite order) g of a group G, we can write in a unique way $g = xy$, where x and y commute, x is a p-element and y has order coprime to p. We call x the p-part of g and y the p'-part of g.

Also, if $g, h \in G$ are elements of coprime order and they commute, then $C_G(gh) = C_G(g) \cap C_G(h)$.

Theorem 4.3. *Let $T = T(n,q)$, $U = U(n,q)$ and $D = D(n,q)$. Then,*

$$|T^p| = \sum_{\delta \vdash n} |D_\delta| [U : C_\delta] |C_\delta^p|,$$

where the sum runs over all partitions δ of n with length $\leq q - 1$, $D_\delta = \{d \in D \mid \tau(d) = \delta\}$ and $C_\delta = C_U(d_\delta)$ for some $d_\delta \in D_\delta$.

Proof. We first prove that

$$T^p = \bigcup_{d \in D, v \in C_U(d)^p} (dv)^U, \tag{4.1}$$

where $(dv)^U = \{(dv)^y \mid y \in U\}$ is an orbit under the action by conjugation of U; we call it a U-class.

To prove (4.1), let us consider an element $x = dv$ on the right-hand side where $d \in D$ and $v = u^p$ for some $u \in C_U(d)$. Since $(p, |D|) = 1$ we can write $d = d_0^p$ for some suitable $d_0 \in D$; note that $u \in C_U(d_0) = C_U(d)$. Hence, $x = d_0^p u^p = (d_0 u)^p \in T^p$. Since T^p is U-invariant, this proves that T^p contains the union on the right-hand side of (4.1). Conversely, consider $x = t^p$ with $t \in T$. Now, write $t = d_0 u$ where u and d_0 are the p-part and p'-part of t, respectively. So, in particular, u and d_0 commute. Let $y \in U$ such that $d_0^y \in D$ (such an element certainly exists, as D

is a p-complement of T and the p-complements of T are a single orbit under the action of U). Write $d_1 = d_0^y$ and $v = u^y$. Then $x^y = (t^p)^y = (t^y)^p = ((d_0u)^y)^p = (d_1v)^p = d_1^p v^p$. Now, $d = d_1^p \in D$ and $C_U(d) = C_U(d_1)$. This proves the other inclusion.

Next, we observe that for elements $u, v \in U$ and $c, d \in D$ which satisfy $[u, c] = 1 = [v, d]$ and $(cu)^U = (dv)^U$, it follows that, $c = d$. Let $y \in U$ such that $x = dv = c^y u^y$. Note that v and d are the p-part and p'-part of x, respectively, and that the same is true for u^y and c^y. By uniqueness of p and p'-parts, we hence get $v = u^y$ and $d = c^y$. In particular, $c^{-1}d = c^{-1}c^y = [c, y] \in D \cap U = 1$, so $c = d$.

We also have that if $cu \in (dv)^U$, for $c, d \in D$, $u \in U$ and $v \in C_U(d)^p$, then $cu = du = dv^y$ for some $y \in C_U(d)$. Therefore, the family of U-classes in T^p is in bijection with the set of pairs $(d, v_{d,i})$, where $d \in D$ and $v_{d,1}, \ldots, v_{d,m_d}$ is a set of representatives of the $C_U(d)$-classes in $C_U(d)^p$. For a fixed $d \in D$, write $C = C_U(d)$ and let $v \in C^p$. Observe that $C_U(dv) = C_U(d) \cap C_U(v) = C_C(v)$, because d and v are commuting elements of coprime order, so $|(dv)^U| = |U : C||v^C|$. Hence, we have

$$\left| \bigcup_{v \in C^p} (dv)^U \right| = [U : C] \sum_{i=1}^{m_d} |v_{d,i}^C| = [U : C]|C^p|.$$

By Lemma 4.2, we conclude that

$$|T^p| = \sum_{d \in D} [U : C_U(d)]|C_U(d)^p| = \sum_{\delta \vdash n, l(\delta) < q} |D_\delta|[U : C_\delta]|C_\delta^p|$$

where $C_\delta = C_U(d_\delta)$ for any fixed $d_\delta \in D_\delta$. □

We will now prove Theorem B.

Proof of the Theorem B. Proof of the theorem is obtained by simply substituting the values in the formula obtained Theorem 4.3 above. The value of $|D_\delta|$ is computed in Lemma 4.1. The value of $[U : C_\delta]$ is obtained from Lemma 4.2. Now, to obtain the last term $|C_\delta^p|$ we use the fact that $C_\delta \cong \prod_{i=1}^k U(a_i, q)$. This completes the proof. □

Next, we apply the formula obtained in Theorem B to compute some examples.

Example 4.4. Let $n = 3, q = 5 = p$. Let $T = T(3, 5)$ and we want to compute $|T^5|$. In this case the partitions δ such that $1 \leq l(\delta) \leq \min(n, q-1) = 3$ are (3), $(2, 1)$ and $(1, 1, 1)$. Now, $|\Delta_{(3)}| = 4$, $|\Delta_{(2,1)}| = 3 \cdot (4 \cdot 3) = 2^2 3^2$ and $|\Delta_{(1,1,1)}| = 4 \cdot 3 \cdot 2 = 2^3 3$. Further $|d^T| = [U : C_U(d)]$ is, according to type, as follows: 1 for (3), 5^2 for $(2, 1)$ and 5^3 for $(1, 1, 1)$. Hence,

$$|T^5| = 4 \cdot 1 + 2^2 3^2 \cdot 5^2 + 2^3 3 \cdot 5^3 = 3904.$$

Example 4.5. Let $n = 6$, $q = p = 3$, $T = T(6, 3)$, $D = D(6, 3)$ and $U = U(6, 3)$.

The partitions δ of 6 of length at most two are $(6), (5,1), (4,2), (3,3)$ and for $d_\delta \in D_\delta$ we have the following.

	(6)	$(5,1)$	$(4,2)$	$(3,3)$
$\lvert D_\delta\rvert$	2	12	30	20
$[U : C_U(d_\delta)]$	1	3^5	3^8	3^9
$\lvert C_U(d_\delta)^3\rvert$	585	3^3	3	1

where we have used the fact that $C_U(d_{(6)}) \cong U(6,3)$ and that $|U(6,3)^3| = 585$ (by direct computation).

Hence, we get

$$|T^3| = 2 \cdot 585 + 12 \cdot 3^5 \cdot 3^3 + 30 \cdot 3^8 \cdot 3 + 20 \cdot 3^9 = 1064052.$$

We finish by proving Corollary C.

Proof of Corollary C. We will consider just the partitions (of length 2) $(n-i, i)$ for $1 \leq i \leq \lfloor n/2 \rfloor$. Hence, by Theorems A and B, we have

$$\begin{aligned}
|T^p| &\geq \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{(q-1)(q-2)n!}{2(n-i)!i!} \cdot |U(i,q)^p||U(n-i,q)^p| \cdot q^{\binom{n}{2}-\binom{n-i}{2}-\binom{i}{2}} \\
&\geq \frac{1}{3^2} \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{(q-1)(q-2)}{2} \binom{n}{i} \cdot q^{\binom{n}{2}-\binom{n-i}{2}-\binom{i}{2}+\binom{i-p+1}{2}+\binom{n-i-p+1}{2}} \\
&= \frac{1}{3^2} \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{(q-1)(q-2)}{2} \binom{n}{i} \cdot q^{\binom{n}{2}-(p-1)(n-p)} \\
&\geq \frac{2^{n-2}}{3^2}(q-1)(q-2) \cdot q^{\binom{n}{2}-(p-1)(n-p)}.
\end{aligned}$$

Hence,

$$\frac{|T^p|}{|T|} \geq \frac{2^{n-2}(q-1)(q-2)}{9(q-1)^n q^{(p-1)(n-p)}} \geq \frac{2^{n-2}}{9(q-1)^{n-2} q^{(p-1)(n-p)}}.$$ □

Acknowledgment

We would like to thank the anonymous referee(s) for the report which helped in improving this paper.

The first named author was partially supported by INDAM-GNSAGA during this work and also gratefully acknowledges the hospitality of Harish-Chandra Research Institute (Allahabad) and IISER Pune. The second named author would like to acknowledge support of SERB-MATRICS grant and the hospitality of the Department of Mathematics, University of Florence, Italy during his visit which was supported by ICTP Research in Pairs grant.

References

[1] A. Bier, The width of verbal subgroups in the group of unitriangular matrices over a field, *Int. J. Algebra Comput.* **22**(3) (2012) 1250019, 20 pp.

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235–265.

[3] N. L. Gordeev, B. É. Kunyavskiĭ and E. B. Plotkin, Word maps and word maps with constants of simple algebraic groups, *Dokl. Akad. Nauk* **471**(2) (2016) 136–138; translation in *Dokl. Math.* **94**(3) (2016) 632–634.

[4] N. Gordeev, B. Kunyavskiĭ and E. Plotkin, Word maps, word maps with constants and representation varieties of one-relator groups, *J. Algebra* **500** (2018) 390–424.

[5] N. Gordeev, B. Kunyavskiĭ and E. Plotkin, Word maps on perfect algebraic groups, *Int. J. Algebra Comput.* **28**(8) (2018) 1487–1515.

[6] N. Gordeev, B. Kunyavskiĭ and E. Plotkin, Geometry of word equations in simple algebraic groups over special fields, *Uspekhi Mat. Nauk* **73**(5) (2018) 3–52; translation in *Russian Math. Surveys* **73**(5) (2018) 753–796.

[7] A. Galt, A. Kulshrestha, A. Singh and E. Vdovin, On Shalev's conjecture for type A_n and ${}^2A_n$, *J. Group Theory* **22**(4) (2019) 713–728.

[8] B. Huppert, Endliche Gruppen. I, (German) Die Grundlehren der Mathematischen Wissenschaften, Band, Vol. 134 (Springer-Verlag, Berlin-New York, 1967), xii, 793 pp.

[9] A. Shalev, *Some Results and Problems in the Theory of Word Maps*, Erdös centennial, Bolyai Society Mathematical Studies, Vol. 25 (János Bolyai Mathematical Society, Budapest, 2013).

[10] A. Soffer, Upper bounds on the number of conjugacy classes in unitriangular groups, *J. Group Theory* **19**(6) (2016) 1063–1095.

[11] Y. V. Sosnovskiy, On the width of verbal subgroups of the groups of triangular matrices over a field of arbitrary characteristic, *Int. J. Algebra Comput.* **26**(2) (2016) 217–222.

[12] A. Vera-López and J. M. Arregi, Conjugacy classes in Sylow p-subgroups of $\mathrm{GL}(n,q)$. II, *Proc. Roy. Soc. Edinburgh A* **119**(3–4) (1991) 343–346.

[13] A. Vera-López, A. Antonio and M. Jesus, Conjugacy classes in Sylow p-subgroups of $\mathrm{GL}(n,q)$, *J. Algebra* **152**(1) (1992) 1–19.

AQ: Pls check the edit.

AQ: Pls provide citation in text.