J. Group Theory, Ahead of Print
DOI 10.1515/JGT.2010.081

Journal of Group Theory

The number of conjugacy classes in pattern groups is not a polynomial function

Zoltán Halasi and Péter P. Pálfy

(Communicated by Nigel Boston)

Abstract. A famous open problem due to Graham Higman asks if the number of conjugacy classes in the group of $n \times n$ unipotent upper triangular matrices over the q-element field can be expressed as a polynomial function of q for every fixed n. We consider the generalization of the problem for pattern groups and prove that for some pattern groups of nilpotency class two the number of conjugacy classes is not a polynomial function of q.

1 Introduction

In 1960 Graham Higman [3, p. 29] asked if the number of conjugacy classes in the group $U_n(q)$ of $n \times n$ upper unitriangular matrices over the q-element field $\mathbb{F}_q$ is a polynomial function of q for every fixed n. This has been verified for $n \leqslant 13$ with polynomials of degree $[n(n+6)/12]$ (see Vera-Lopez and Arregi [10]) However, in full generality the problem is wide open, despite various attempts to solve it (see, for example, Thompson [9]).

We follow here the advice of George Pólya [7, p. 9]: "If you cannot solve the proposed problem try to solve first some related problem." We will consider a generalization of the problem and in this paper we give a negative answer for a particular case of the generalized problem. Although the case we solve is quite diametrical to the one that corresponds to the original question, nevertheless, we hope our result will shed some light on the problem.

We will deal with pattern groups as defined in Isaacs [5]. (See Section 4 below.) We note that pattern groups already appeared in the 1955 paper of Weir [11] under the name "partition subgroups".

We will prove (Corollary 4.5) that there exists a pattern P such that the number of conjugacy classes in the corresponding pattern group $G_P(q)$ over $\mathbb{F}_q$ is not a polynomial function of q. This result might raise some doubt about the validity of the

Research supported by Hungarian National Research Fund (OTKA) under grant number NK72523.

conjecture on the number of conjugacy classes in $U_n(q)$. We will only consider pattern groups of nilpotency class two. In Section 3 we derive a general formula for the class number of algebra groups of nilpotency class two.

The main technique of our study is to count those matrices in which the rank of several submatrices is prescribed. We introduce the concept of a system of rank constraints in Section 2. In Section 2.1 we present two examples where the number of matrices over $\mathbb{F}_q$ satisfying the given system of rank constraints is not a polynomial function of q. In Section 2.2 we show that for every finite set of polynomial equations and inequalities it is possible to construct an appropriate system of rank constraints such that the number of matrices satisfying these constraints is equal to the number of solutions of the given system of polynomial equations and inequalities, multiplied by a suitable power of $q-1$. (The results of this section are not used later in the paper.) In Section 2.3 we show that for a special type of a system of rank constraints, namely, when each submatrix with prescribed rank is at the top right corner, the number of solutions is a polynomial function of q. This result is used in Section 5 to show that the number of conjugacy classes in normal pattern subgroups of $U_n(q)$ is a polynomial function of q.

Our notation is mainly standard. We denote by $k(G)$ the number of conjugacy classes in the finite group G, and by $rk(X)$ the rank of the matrix X.

2 Matrices with rank constraints

First we will consider an auxiliary problem. Let $k, m \geqslant 1$ be integers, and let us denote by $\mathscr{M}_{k\times m}(\mathbb{F}_q)$ the set of all $k \times m$ matrices over the q-element field. We will put restrictions on the rank of some submatrices and we will be interested in the number of matrices satisfying these constraints. We formalize our setting in the following way.

Definition 2.1.

(i) By a *system of rank constraints for $k \times m$ matrices* we mean a set

$$\mathscr{R} = \{(K_v, M_v, r_v) \mid v \in \{1, \dots, N\}\},$$

where for each $v \in \{1, \dots, N\}$ we have subsets $K_v \subseteq \{1, \dots, k\}$, $M_v \subseteq \{1, \dots, m\}$ and an integer $0 \leqslant r_v \leqslant \min(|K_v|, |M_v|)$. For any prime power q we denote by $\mathscr{R}(\mathbb{F}_q)$ the set of those matrices from $\mathscr{M}_{k\times m}(\mathbb{F}_q)$ such that for each $v \in \{1, \dots, N\}$ the rank of the submatrix corresponding to the rows with indices in K_v and columns with indices in M_v is the prescribed number r_v.

(ii) If all pairs of subsets of $\{1, \dots, k\}$ and $\{1, \dots, m\}$ appear among the constraints then we say that $\mathscr{R}$ is a *complete system of rank constraints.*

(iii) If the index sets in each constraint have the form $K_v = \{1, 2, \dots, k_v\}$ and $M_v = \{m_v, m_v + 1, \dots, m\}$ with some

$$1 \leqslant k_v \leqslant k \quad \text{and} \quad 1 \leqslant m_v \leqslant m \quad (v \in \{1, \dots, N\}),$$

then we call $\mathscr{R}$ a *system of corner rank constraints.*

(iv) If all pairs of initial segments of $\{1,\dots,k\}$ and terminal segments of $\{1,\dots,m\}$ appear in a system of corner rank constraints then we say that $\mathscr{R}$ is a *complete system of corner rank constraints*.

Note that the set of constraints $\mathscr{R}$ is independent of the field $\mathbb{F}_q$. For the applications in mind we have to allow trivial constraints $(\varnothing, M_v, 0)$, $(K_v, \varnothing, 0)$ as well (but not in systems of corner rank constraints). Then the number of rank constraints in a complete system is 2^{k+m}, while in a complete system of corner rank constraints it is km.

2.1 Examples. In our first simple example the number of matrices satisfying the rank constraints is given by one polynomial for q even and by another polynomial for q odd. In the second example there is not even a finite set of polynomials $f_1,\dots,f_N \in \mathbb{Q}[x]$ such that $|\mathscr{R}(q)| \in \{f_1(q),\dots,f_n(q)\}$ for every prime power q.

Proposition 2.2. *Let $\mathscr{R}$ be the following system of rank constraints for 3×4 matrices*:

$$(\{1\},\{1\},1),\ (\{1\},\{2\},1),\ (\{1\},\{3\},1),(\{1\},\{4\},1),\ (\{2\},\{1\},1),\ (\{3\},\{1\},1),$$
$$(\{1,2\},\{1,4\},1),\ (\{1,2\},\{2,3\},1),\ (\{2,3\},\{1,2\},1),$$
$$(\{1,3\},\{1,3\},1),\ (\{1,3\},\{2,4\},1),\ (\{2,3\},\{3,4\},1).$$

Then $|\mathscr{R}(\mathbb{F}_q)| = (q-1)^6$ for q even, whereas $|\mathscr{R}(\mathbb{F}_q)| = 2(q-1)^6$ for q odd.

Proof. The first six constraints mean that all entries in the first row and in the first column are non-zero. Multiplying a row or a column by a non-zero number does not affect the rank of any submatrix. Considering two matrices equivalent if they are obtained from one another by multiplying rows and columns by non-zero numbers, we see that each equivalence class contains now a unique matrix with all 1's in the first row and first column, and each equivalence class contains exactly $(q-1)^6$ matrices. So we will count only matrices with 1's in the first row and column, and in the end we have to multiply by $(q-1)^6$ the number of such matrices satisfying all constraints.

Let us denote the $(2,2)$ entry of the matrix by x. Now constraints of the form $(\{1,i\},\{j,j'\},1)$ mean that the (i,j) entry of the matrix is the same as the (i,j') entry (since the first row is filled with 1's). Similarly, a constraint of the form $(\{i,i'\},\{1,j\},1)$ means that the (i,j) entry and the (i',j) entry of the matrix are equal. Hence any matrix with 1's in the first row and first column satisfying the next five constraints has the form

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & x & x & 1 \\ 1 & x & 1 & x \end{bmatrix}.$$

Finally, the last constraint is satisfied iff $x^2-1=0$, so for $x=1$ if q is even and for $x=\pm 1$ if q is odd. $\square$

Our second example is based on one of the most well known elliptic curves $y^2 = x^3 - x$. Below we give the number of pairs $(x, y) \in \mathbb{F}_p^2$ satisfying $y^2 = x^3 - x$, see, e.g., the standard texts by Ireland and Rosen [4, p. 307] and by Silverman [8, p. 142]. (For another use of this elliptic curve for counting problems in group theory, see du Sautoy [2].)

Let p be an odd prime. If $p \equiv 1 \pmod 4$ then the number of solutions is given by $p - 2a$, where $p = a^2 + b^2$, a is odd and $a - 1 \equiv b \pmod 4$. (Note that in contrast to [4] we do not count the point at infinity.) By the Sato–Tate conjecture the term $2a$ is distributed in the interval $(-2\sqrt{p}, 2\sqrt{p})$ obeying the semicircle law, see [6]. If $p \equiv 3 \pmod 4$ then the number of pairs $(x, y) \in \mathbb{F}_p^2$ on the curve is p. In this case let $a = 0$.

Let us now consider the curve over the field of $q = p^n$ elements, where p is an odd prime and $n \geqslant 1$. Let α and β be the complex conjugate solutions of the equation $z^2 - 2az + p = 0$, with a as above. Then the number of points on the curve over the field of $q = p^n$ elements is

$$p^n - \alpha^n - \beta^n.$$

Finally, if q is a power of 2, then the number of points on the curve is obviously q. Hence the number of solutions of $y^2 = x^3 - x$ in $\mathbb{F}_q$ is not a polynomial function of q, and we cannot even partition the set of prime powers into finitely many subsets so that for each subset there is a polynomial giving the number of solutions.

Now we will model this elliptic curve using rank constraints.

Proposition 2.3. *There exists a system of rank constraints for 6×6 matrices such that the number of matrices in $\mathscr{M}_{6\times 6}(\mathbb{F}_q)$ satisfying these constraints is*

$$(q-1)^{11}|\{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 - x\}|,$$

hence it is not a polynomial function of q.

Proof. As in the previous construction we will require that all 1×1 submatrices in the first row and in the first column should have rank 1. Then we count only those matrices satisfying the constraints that have all 1's in the first row and first column, and in the end we multiply the number of these matrices by $(q-1)^{11}$. We will also use the "copying" technique without specific mention. (Actually, in our construction below we will need it 18 times.) In addition, we will require that some 1×1 submatrices ought to have rank 0, that is, the corresponding entry of the matrix must be 0.

Apart from these, we take four further constraints:

$$(\{2,3\}, \{2,4\}, 1),\ (\{2,3\}, \{2,6\}, 1),\ (\{4,6\}, \{2,3\}, 1),\ (\{4,5,6\}, \{4,5,6\}, 2).$$

Denoting the $(2,2)$ entry by x and the $(4,2)$ entry by y, the reader can find the necessary "copying" constraints (using 2×2 submatrices of rank 1) guaranteeing that the matrices satisfying all but the last constraints have the form

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x & x^2 & x^2 & x^3 \\ 1 & 1 & x & x & x^2 & x^2 \\ 1 & y & 1 & 1 & 0 & 1 \\ 1 & y & y & 0 & 1 & 1 \\ 1 & y^2 & y & x & y^2 & x^3 \end{bmatrix}$$

Moreover, the last constraint is satisfied iff $y^2 = x^3 - x$. □

2.2 General theory. Clearly any system $\mathscr{R}$ of rank constraints can be extended to a complete system, and the number of matrices over $\mathbb{F}_q$ satisfying the given system of rank constraints $\mathscr{R}$ can be obtained as the sum of $|\mathscr{R}^*(\mathbb{F}_q)|$ taken over all complete extensions $\mathscr{R}^* \supseteq \mathscr{R}$. A complete system of rank constraints is obviously equivalent to specifying which square submatrices have non-zero determinant. If we denote the entries of the matrix by distinct indeterminates, this means that for a complete system $\mathscr{R}^*$ of rank constraints, $|\mathscr{R}^*(\mathbb{F}_q)|$ is the same as the number of solutions of a certain system of polynomial equations and inequalities over $\mathbb{F}_q$.

In Section 2.1 we constructed examples where $|\mathscr{R}(\mathbb{F}_q)|$ depended on the number of solutions of a polynomial (e.g., $x^2 - 1$ or $y^2 - x^3 + x$). Now we are going to show this behaviour in a general form. All the machinery of the proof has already been used in the proof of Propositions 2.2 and 2.3.

Theorem 2.4. *Let $f_0, f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials in n indeterminates. Then there exist an integer N and a system of rank constraints $\mathscr{R}$ for $4 \times N$ matrices such that the number of solutions $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ of*

$$f_0(x_1, \ldots, x_n) \neq 0, f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0$$

is equal to

$$|\mathscr{R}(\mathbb{F}_q)|/(q-1)^{N+3}.$$

Proof. We will be considering $4 \times N$ matrices where the number of columns $N \geqslant n+1$ will vary. First we take the constraints $(\{1\}, \{j\}, 1)$ $(j \in \{1, \ldots, N\})$ and $(\{i\}, \{1\}, 1)$ $(i \in \{2, 3, 4\})$ and count only matrices with all 1's in the first row and first column. Then $|\mathscr{R}(\mathbb{F}_q)|$ will be obtained by multiplying by $(q-1)^{N+3}$ the number of such matrices satisfying all constraints. We denote by x_j the $(2, j+1)$ entry of the matrix, and add the constraint $(\{3, 4\}, \{2, \ldots, n+1\}, 0)$ in order to fix the first $n+1$ columns of the matrix to be

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & \cdots \\ 1 & x_1 & \cdots & x_n & \cdots \\ 1 & 0 & \cdots & 0 & \cdots \\ 1 & 0 & \cdots & 0 & \cdots \end{bmatrix}.$$

We will extend the matrix step by step, adding three new columns every time. At every stage the entries of the matrix will be polynomials from $\mathbb{Z}[x_1, \ldots, x_n]$.

Let a and b be two entries in the second row, say, in positions $(2, j_a)$ and $(2, j_b)$. First we show how to obtain $a - b$. We add the following constraints to the previous ones:

$$(\{1\}, \{N+1\}, 1),\ (\{1\}, \{N+2\}, 1),\ (\{1\}, \{N+3\}, 1),$$
$$(\{1,2\}, \{j_a, N+1\}, 1),\ (\{1,2\}, \{j_b, N+2\}, 1),$$
$$(\{1,3\}, \{1, N+1, N+2\}, 1),\ (\{3\}, \{N+3\}, 0),$$
$$(\{1,4\}, \{1, N+1, N+3\}, 1),\ (\{4\}, \{N+2\}, 0),$$
$$(\{2,3,4\}, \{N+1, N+2, N+3\}, 2),$$

then we obtain that the extended matrix has the form

$$\begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & 1 & 1 \\ 1 & \cdots & a & \cdots & b & \cdots & a & b & a-b \\ 1 & \cdots & * & \cdots & * & \cdots & 1 & 1 & 0 \\ 1 & \cdots & * & \cdots & * & \cdots & 1 & 0 & 1 \end{bmatrix},$$

so we have given an extension of the system of rank constraints in such a way that the matrices satisfying the extended system will contain the polynomial $a - b$ in the second row.

We can obtain ab in a similar fashion, by adding the constraints

$$(\{1\}, \{N+1\}, 1),\ (\{1\}, \{N+2\}, 1),\ (\{1\}, \{N+3\}, 1),$$
$$(\{1,2\}, \{j_a, N+1\}, 1),\ (\{1,2\}, \{j_b, N+2\}, 1),$$
$$(\{2,3\}, \{1, N+1\}, 1),\ (\{1,3\}, \{1, N+2\}, 1),\ (\{1,3\}, \{N+1, N+3\}, 1),$$
$$(\{4\}, \{N+1, N+2, N+3\}, 0),\ (\{2,3\}, \{N+2, N+3\}, 1),$$

which yield a matrix of the form

$$\begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & 1 & 1 \\ 1 & \cdots & a & \cdots & b & \cdots & a & b & ab \\ 1 & \cdots & * & \cdots & * & \cdots & a & 1 & a \\ 1 & \cdots & * & \cdots & * & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Thus the set of polynomials that can occur in the second row of some $4 \times N$ matrix (N varies) specified by an appropriate system of rank constraints is closed under subtraction and multiplication and it contains all indeterminates $x_1, \ldots, x_n$, as well as the constant 1; hence every polynomial can be obtained this way. In particular, we can construct a system of rank constraints such that the matrices satisfying this system (and having all 1's in the first row and first column) have each f_t

$(t = 0, \dots, s)$ at some position $(2, j_t)$. Then adding the constraints $(\{2\}, \{j_0\}, 1)$, and $(\{2\}, \{j_1\}, 0), \dots, (\{2\}, \{j_s\}, 0)$ we obtain our claim. □

2.3 Corner rank constraints. In contrast to the general problem, the number of solutions of a system of corner rank constraints is always a polynomial function of q. We will use this result in Section 5 for computing the number of conjugacy classes in normal pattern subgroups of nilpotency class two.

Proposition 2.5. *Let*

$$\mathscr{R} = \{(\{1, \dots, k_v\}, \{m_v, \dots, m\}, r_v) \mid v \in \{1, \dots, N\}\}$$

with $1 \leqslant k_v \leqslant k$, $1 \leqslant m_v \leqslant m$ *be a system of corner rank constraints for* $k \times m$ *matrices. Then* $|\mathscr{R}(\mathbb{F}_q)|$ *is a polynomial function of* q; *in fact, it is a polynomial in* $q - 1$ *with non-negative integer coefficients.*

Proof. Clearly, it is enough to show the statement for complete systems of corner rank constraints. We use induction on k. First consider the constraints of the form $(\{1\}, \{j, \dots, m\}, r_j)$ with $j \in \{1, \dots, m\}$, where each $0 \leqslant r_j \leqslant 1$. If there exist $j < j'$ with $r_j = 0$, $r_{j'} = 1$, then there are no matrices satisfying all constraints simultaneously, hence $|\mathscr{R}(\mathbb{F}_q)| = 0$. If $r_1 = \cdots = r_m = 0$, then the first row of any matrix satisfying the constraints should consist of 0's, and we can obviously reduce our system of rank constraints $\mathscr{R}$ to another system of corner rank constraints $\mathscr{R}'$ for $(k-1) \times m$ matrices, provided $k > 1$. Namely, if $k_v > 1$ then we remove the first row and decrease the indices of the other rows by 1. Formally, we replace $(\{1, \dots, k_v\}, \{m_v, \dots, m\}, r_v)$ by $(\{1, \dots, k_v - 1\}, \{m_v, \dots, m\}, r_v)$, and we omit the constraints with $k_v = 1$ (in which cases $r_v = 0$ by our assumption). If $k = 1$, then $|\mathscr{R}(\mathbb{F}_q)| = 1$ in this case.

Otherwise, $r_1 = \cdots = r_j = 1$ and $r_{j+1} = \cdots = r_m = 0$ for some $1 \leqslant j \leqslant m$. Then the $(1, j)$ entry of any matrix in $\mathscr{R}(\mathbb{F}_q)$ is non-zero, while the entries $(1, j')$ for $j' > j$ are zeros. Let us consider the following elementary transformations of matrices:

- multiplying the first row by a non-zero number;
- adding a multiple of the first row to the i-th row for $1 < i \leqslant k$;
- adding a multiple of the j-th column to the j'-th column for $1 \leqslant j' < j$.

None of these transformations changes the rank of any submatrix in the top-right corner. Consider two matrices equivalent if they can be obtained from each other by a finite sequence of the above elementary transformations. Clearly, every equivalence class of matrices in $\mathscr{R}(\mathbb{F}_q)$ consists of $(q-1)q^{k-1+j-1}$ matrices and each equivalence class contains a unique matrix of the form

$$\begin{bmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ * & \cdots & * & 0 & * & \cdots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ * & \cdots & * & 0 & * & \cdots & * \end{bmatrix}$$

(with the 1 at the $(1, j)$ position). If we want to count these matrices, we can reduce the original system of corner rank constraints $\mathscr{R}$ for $k \times m$ matrices to another system of corner rank constraints $\mathscr{R}'$ for $(k-1) \times (m-1)$ matrices in the following way. Take a constraint $(\{1, \dots, k_v\}, \{m_v, \dots, m\}, r_v) \in \mathscr{R}$ and

- omit it if $k_v = 1$;
- replace it by $(\{1, \dots, k_v - 1\}, \{m_v - 1, \dots, m-1\}, r_v)$ if $k_v > 1$, $m_v > j$;
- replace it by $(\{1, \dots, k_v - 1\}, \{m_v, \dots, m-1\}, r_v - 1)$ if $k_v > 1$, $m_v \leqslant j$.

It is straightforward to see that $|\mathscr{R}(\mathbb{F}_q)| = (q-1)q^{k-1+j-1}|\mathscr{R}'(\mathbb{F}_q)|$, so the result follows by induction. □

3 The number of conjugacy classes in algebra groups of nilpotency class two

Let A be a nilpotent algebra over $\mathbb{F}_q$. The *algebra group* $1 + A$ has the obvious multiplication: $(1+x)(1+y) = 1 + (x + y + xy)$, and inverse

$$(1+x)^{-1} = 1 + (-x + x^2 - x^3 + \cdots)$$

(where the sum is finite since A is nilpotent). We will consider algebras satisfying $A^3 = 0$. Let B be a subspace containing A^2 and satisfying $AB = BA = 0$. (Clearly, $B = A^2$ would do, but we need this slightly more general formulation.) It is easy to see that $(1+A)' \leqslant 1 + B \leqslant \mathbf{Z}(1+A)$, so in our case the algebra group $1 + A$ has nilpotency class at most 2. Two group elements $1 + x$ and $1 + y$ commute if and only if x and y commute in the algebra A, that is, the algebra commutator $[x, y] = xy - yx$ equals zero.

It is well known that the number of conjugacy classes in a finite group is equal to the number of commuting pairs of elements divided by the order of the group. We will use this fact to obtain a formula for the number of conjugacy classes of the algebra group $1 + A$.

Let B^* denote the dual space of B, and for any $f \in B^*$ let $\tilde{f}$ be the symplectic form on A defined by $\tilde{f}(x, y) = f([x, y])$. (Since B annihilates the whole of A, we may consider $\tilde{f}$ as a symplectic form on A/B as well.) For $0 \leqslant r \leqslant \dim(A/B)$ let $N_r = N_r(A, B)$ denote the number of linear functions $f \in B^*$ for which $\tilde{f}$ has rank r. (Of course, the rank of a symplectic form is always even, so for r odd we have $N_r = 0$.) Furthermore, let $d = \dim(A/B)$.

Lemma 3.1. *Let $1 + A$ be an algebra group, where A is an $\mathbb{F}_q$-algebra with $A^3 = 0$. Using the above notation, the number of conjugacy classes of $1 + A$ is*

$$k(1+A) = \sum_{r=0}^{d} N_r q^{d-r}.$$

Proof. Let us count in two different ways those triples $(f, x, y) \in B^* \times A \times A$ for which $\tilde{f}(x, y) = f([x, y]) \neq 0$. If $\tilde{f}$ has rank r then the number of pairs $(x, y) \in A^2$

with $\tilde{f}(x,y) \neq 0$ is $|A|(1-q^{-r})|A|(1-q^{-1})$. If x and y do not commute then the number of linear functions $f \in B^*$ not annihilating $[x,y]$ is $|B|(1-q^{-1})$. Hence we obtain

$$(|A|^2 - |A|k(1+A))|B|(1-q^{-1}) = \sum_{r=0}^{d} N_r |A|(1-q^{-r})|A|(1-q^{-1}).$$

Taking into account that $\sum N_r = |B|$ we obtain the result. □

4 Pattern groups of nilpotency class two

First we recall the definition of a pattern group (see [5, 1]). Let $n > 1$ and let $P \subseteq \{(i,j) \mid 1 \leqslant i < j \leqslant n\}$ be a transitive relation, i.e., if $(i,j),(j,k) \in P$ then $(i,k) \in P$. Then the corresponding *pattern algebra* over $\mathbb{F}_q$ is the subalgebra of the matrix algebra $\mathscr{M}_{n\times n}(\mathbb{F}_q)$ spanned by the matrix units E_{ij} with $(i,j) \in P$. The *pattern group* $G_P(q)$ determined by P over $\mathbb{F}_q$ is just the corresponding algebra group obtained by adding the identity matrix to each element of the pattern algebra.

We will deal with very particular pattern groups.

Definition 4.1. Let $k \geqslant 1$, $m \geqslant 1$, $\ell \geqslant 0$, $n = k + \ell + m$, and let us be given sequences of subsets $K_v \subseteq \{1,\dots,k\}$, $M_v \subseteq \{1,\dots,m\}$ for $v \in \{1,\dots,\ell\}$. The *pattern of type* (k,m) corresponding to (K_v, M_v) $(v \in \{1,\dots,\ell\})$ consists of the following pairs:

$$\begin{aligned} &(i, k+v) \quad \text{for } i \in K_v,\ v \in \{1,\dots,\ell\},\\ &(k+v, k+\ell+j) \quad \text{for } j \in M_v,\ v \in \{1,\dots,\ell\}, \quad \text{and}\\ &(i, k+\ell+j) \quad \text{for all } i \in \{1,\dots,k\},\ j \in \{1,\dots,m\}. \end{aligned}$$

We also say that the corresponding *pattern algebra* and *pattern group have type* (k,m).

Note that for patterns of type (k,m) both ℓ and, consequently, n can be arbitrarily large.

Let A be a pattern algebra over $\mathbb{F}_q$ of type (k,m) as defined above, and let us denote the subalgebra spanned by the matrix units $E_{i,k+\ell+j}$ $(i \in \{1,\dots,k\},\ j \in \{1,\dots,m\})$ by B. Then, clearly, $B \supseteq A^2$, $AB = BA = 0$, so we can apply Lemma 3.1 to determine the number of conjugacy classes of pattern groups of type (k,m).

In order to use that formula we have to calculate the rank of the symplectic form $\tilde{f}$ for each $f \in B^*$. Let $f_{ij} \in B^*$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant m)$ denote the linear functions forming the dual basis to $E_{i,k+\ell+j}$, and take an arbitrary linear combination $f = \sum_{i=1}^{k}\sum_{j=1}^{m} \lambda_{ij} f_{ij}$. Denote the $k \times m$ matrix formed by the coefficients λ_{ij} by L, and for any $v \in \{1,\dots,\ell\}$ let L_v be the submatrix of L corresponding to the rows belonging to K_v and columns belonging to M_v.

Lemma 4.2. *With the above notation we have*

$$rk(\tilde{f}) = 2\sum_{v=1}^{\ell} rk(L_v).$$

Proof. Note that

$$[E_{i,k+v}, E_{k+\mu,k+\ell+j}] = -[E_{k+\mu,k+\ell+j}, E_{i,k+v}] = \delta_{v,\mu} E_{i,k+\ell+j}$$

and all other commutators of pairs of basis elements of A are 0.

Let us list the basis elements of A/B in the following order: $E_{i,k+v}$ precedes $E_{i',k+v'}$ if either $v < v'$ or $v = v'$ and $i < i'$, all these basis elements precede those of the form $E_{k+v,k+\ell+j}$, and among the basis elements of the latter type $E_{k+v,k+\ell+j}$ precedes $E_{k+v',k+\ell+j'}$ if either $v < v'$ or $v = v'$ and $j < j'$. With respect to the basis ordered this way the matrix of $\tilde{f}$ has the following block matrix form

$$\begin{bmatrix} 0 & \cdots & 0 & L_1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & L_\ell \\ -L_1^\top & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & -L_\ell^\top & 0 & \cdots & 0 \end{bmatrix}$$

and the result follows. □

Corollary 4.3. *If for every rank constraint problem for $k \times m$ matrices the number of solutions is a polynomial function of the order q of the base field, then the number of conjugacy classes of every pattern group of type (k,m) is also a polynomial in q.*

Proof. Let us fix a pattern P of type (k,m), that is, choose subsets $K_v \subseteq \{1,\dots,k\}$, $M_v \subseteq \{1,\dots,m\}$ for $v \in \{1,\dots,\ell\}$, and let us take an arbitrary finite field $\mathbb{F}_q$. For arbitrary $r_1,\dots,r_\ell$ let $\mathscr{R}_{r_1,\dots,r_\ell}$ denote the set of rank constraints

$$\{(K_v, M_v, r_v) \mid v \in \{1,\dots,\ell\}\}.$$

Combining Lemma 3.1 and Lemma 4.2 we obtain an expression of the number of conjugacy classes of the pattern group $G_P(q)$ as the sum of finitely many polynomial functions of q:

$$k(G_P(q)) = \sum_{r_1} \dots \sum_{r_\ell} |\mathscr{R}_{r_1,\dots,r_\ell}(\mathbb{F}_q)| q^{d-2\sum r_v},$$

which proves the statement. □

Our main result is the following converse of the previous corollary. For some applications it is convenient to formulate the statement using any infinite set Q of prime powers instead of all prime powers.

Theorem 4.4. *Let Q be an infinite set of prime powers, and $k, m \geqslant 1$. If for each pattern P of type (k,m) there is a polynomial $c_P(x) \in \mathbb{Q}[x]$ such that $k(G_P(q)) = c_P(q)$ for all $q \in Q$, then for every system of rank constraints $\mathscr{R}$ for $k \times m$ matrices there is a polynomial $c^*_{\mathscr{R}}(x) \in \mathbb{Q}[x]$ such that $|\mathscr{R}(\mathbb{F}_q)| = c^*_{\mathscr{R}}(q)$ for all $q \in Q$.*

Proof. Let us take a system of rank constraints for $k \times m$ matrices

$$\mathscr{R} = \{(K_v, M_v, r_v) \mid v \in \{1, \dots, \ell\}\},$$

where $K_v \subseteq \{1, \dots, k\}$, $M_v \subseteq \{1, \dots, m\}$, and $0 \leqslant r_v \leqslant \min(|K_v|, |M_v|)$. Choose a number $b > \min(k,m)$ and define a pattern P of type (k,m) by repeating K_v and M_v b^{v-1} times, that is, P is determined by the sets K'_μ, M'_μ where $K'_\mu = K_v$, $M'_\mu = M_v$ for $(b^{v-1}-1)/(b-1) < \mu \leqslant (b^v - 1)/(b-1)$, $v \in \{1, \dots, \ell\}$. Let A be the pattern algebra over $\mathbb{F}_q$ corresponding to P and let us use the same notation as before. Then for $f \in B^*$ Lemma 4.2 gives

$$rk(\tilde{f}) = 2 \sum_{\mu=1}^{(b^\ell-1)/(b-1)} rk(L'_\mu) = 2 \sum_{v=1}^{\ell} b^{v-1} rk(L_v).$$

Let $r' = 2(r_1 + br_2 + \cdots + b^{\ell-1} r_\ell)$. Since each $rk(L_v) \leqslant \min(k,m) < b$, it follows that $rk(\tilde{f}) = r'$ if and only if $rk(L_v) = r_v$ for each $v \in \{1, \dots, \ell\}$. Thus

$$|\mathscr{R}(\mathbb{F}_q)| = N_{r'}(A, B) = N_{r'}(q),$$

the number of linear functions $f \in B^*$ such that $\tilde{f}$ has rank r'.

For $t \geqslant 1$ we define the pattern tP of type (k,m) by repeating t times each K'_μ and M'_μ, that is, we take $K''_\kappa = K'_\mu$, $M''_\kappa = M'_\mu$ for

$$t(\mu - 1) < \kappa \leqslant t\mu, \quad \mu \in \{1, \dots, (b^\ell - 1)/(b-1)\}.$$

For any prime power $q \in Q$ we consider the pattern algebra $A^{(t)}$ over $\mathbb{F}_q$ corresponding to the pattern tP. Note that (up to renumbering) the subalgebra B is the same for all $A^{(t)}$, while $\dim(A^{(t)}/B) = t \dim(A/B) = td$, where $d = \dim(A/B)$. For $f \in B^*$ let $\tilde{f}$ be the corresponding symplectic form on A/B and $\tilde{f}^{(t)}$ the corresponding symplectic form on $A^{(t)}/B$. By Lemma 4.2 we obtain that

$$rk(\tilde{f}^{(t)}) = 2 \sum_{\kappa=1}^{t(b^\ell-1)/(b-1)} rk(L''_\kappa) = 2t \sum_{\mu=1}^{(b^\ell-1)/(b-1)} rk(L'_v) = t \cdot rk(\tilde{f}),$$

and hence Lemma 3.1 yields

$$k(G_{tP}(q)) = \sum_{r=0}^{d} N_r(q) q^{t(d-r)}.$$

In addition, notice that $\sum_{r=0}^{d} N_r(q) = |B| = q^{km}$, which can be considered as the number of conjugacy classes in the abelian pattern group $G_{0P}(q) = 1 + B$. We can express these equations in a matrix form as follows.

$$\begin{bmatrix} k(G_{0P}(q)) \\ k(G_{1P}(q)) \\ \vdots \\ k(G_{dP}(q)) \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & q & \cdots & q^d \\ \vdots & \vdots & \ddots & \vdots \\ 1 & q^d & \cdots & q^{d^2} \end{bmatrix} \begin{bmatrix} N_d(q) \\ N_{d-1}(q) \\ \vdots \\ N_0(q) \end{bmatrix}$$

We make use of the assumption that $k(G_{tP}(q)) = c_{tP}(q)$ for all $q \in Q$ with suitable polynomials $c_{tP}(x) \in \mathbb{Q}[x]$. By inverting the coefficient matrix of Vandermonde type, we obtain that each $N_r(q)$ can be expressed as a rational function for $q \in Q$. However, the values of N_r are integers, and Q is an infinite set, hence these rational functions must be polynomials. So $|\mathscr{R}(\mathbb{F}_q)| = N_{r'}(q)$ is a polynomial function of $q \in Q$, as we wanted to prove. □

From Theorem 4.4 and Proposition 2.2 we derive the result in the title of the paper.

Corollary 4.5. *There exists a pattern P such that the number of conjugacy classes in the pattern group $G_P(q)$ is not a polynomial function of q.*

If we use Proposition 2.3 instead of Proposition 2.2 we can even conclude that there exists a pattern P such that there is no finite set of polynomials $f_1, \ldots, f_N \in \mathbb{Q}[x]$ with the property that $k(G_P(q)) \in \{f_1(q), \ldots, f_N(q)\}$ for all prime powers q.

Unfortunately, our proof provides only a very large bound for n with the property that there exists a pattern subgroup in $\mathrm{GL}_n(q)$ for which the number of conjugacy classes is not a polynomial in q. Even if we decrease the number of repetitions (by taking into consideration that $rk(L_v) \leqslant \min(|K_v|, |M_v|)$) our method yields only that $n < 2.2 \cdot 10^9$ will do.

In Proposition 2.2 two polynomials depending on the parity of q give the number of solutions of the system of rank constraints. However, if we use the system of rank constraints from Proposition 2.3, encoding the elliptic curve $y^2 = x^3 - x$, we see that there exists a pattern of type $(6, 6)$ such that the number of conjugacy classes in the corresponding pattern groups cannot be given by finitely many polynomials. The bound for the size of matrices in this case is even larger; our proof yields $n < 10^{29}$.

5 Normal pattern subgroups of nilpotency class two

In this section we will consider pattern groups of nilpotency class two that are normal in the group $U_n(q)$ of all $n \times n$ unipotent upper triangular matrices over $\mathbb{F}_q$. By Weir [11, Theorem 2] the pattern group $G_P(q)$ is normal in $U_n(q)$ iff "the boundary of P should move monotonically downward and to the right", that is, if $(i,j) \in P$ and $i' \leqslant i, j \leqslant j'$ then $(i',j') \in P$ as well. Let us fix a pattern P such that $G_P(q)$ is normal in $U_n(q)$ and the nilpotency class of $G_P(q)$ is two. Both properties are determined only by P and do not depend on q. Let $k+1$ be the smallest number such that $(1,k+1) \in P$, and let $n-m$ be the largest number with $(n-m,n) \in P$. Then for any $(i,j) \in P$ we have $i \leqslant n-m$ and $j \geqslant k+1$. If $k+m \geqslant n$, then $G_P(q)$ is abelian, so we have $\ell := n-k-m > 0$. We cannot have any $(i,j) \in P$ with $k+1 \leqslant i < j \leqslant n-m$, since otherwise as $(1,i) \in P$, $(j,n) \in P$ we could get a non-trivial commutator $[1+E_{1i}, 1+E_{ij}, 1+E_{jn}] = 1+E_{1n}$, contrary to our assumption on the nilpotency class of $G_P(q)$. Let $P_0 = \{(i,j) \mid i \leqslant k, j \geqslant n-m+1\}$; then $G_{P_0}(q)$ is an abelian group centralizing $G_P(q)$. Hence

$$k(G_{P \cup P_0}(q)) = k(G_P(q) \cdot G_{P_0}(q)) = q^{|P_0 \setminus P|} k(G_P(q)),$$

so it will suffice to consider patterns containing P_0, that is, patterns of type (k,m) as it was defined in Section 4. In the present case $G_P(q) \lhd U_n(q)$ implies that the sets $K_v \subseteq \{1,\dots,k\}$ and $M_v \subseteq \{1,\dots,m\}$ ($v \in \{1,\dots,\ell\}$) have the form $K_v = \{1,\dots,k_v\}$ and $M_v = \{m_v,\dots,m\}$ with appropriate $1 \leqslant k_v \leqslant k$, $1 \leqslant m_v \leqslant m$ for $v \in \{1,\dots,\ell\}$. (We also have $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_\ell$ and $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_\ell$ but we shall not make use of it.) Hence Lemmas 3.1, 4.2 and Proposition 2.5 readily imply the following.

Proposition 5.1. *Let P be a pattern such that the pattern group $G_P(q)$ is normal in $U_n(q)$ and has nilpotency class two. Then $k(G_P(q))$ is a polynomial function of q; in fact, it is a polynomial in $q-1$ with non-negative integer coefficients.*

Acknowledgement. We thank the referee for the very careful reading of our manuscript and for his/her helpful comments.

References

[1] P. Diaconis and N. Thiem. Supercharacter formulas for pattern groups. *Trans. Amer. Math. Soc.* **361** (2009), 3501–3533.

[2] M. du Sautoy. A nilpotent group and its elliptic curve: Non-uniformity of local zeta functions of groups. *Israel J. Math.* **126** (2001), 269–288.

[3] G. Higman. Enumerating p-groups. I: Inequalities. *Proc. London Math. Soc.* **3** (1960), 24–30.

[4] K. Ireland and M. Rosen. *A classical introduction to modern number theory* (Springer–Verlag, 1990).

[5] I. M. Isaacs. Counting characters of upper triangular groups. *J. Algebra* **315** (2007), 698–719.

[6] B. Mazur. Finding meaning in error terms. *Bull. Amer. Math. Soc. (N.S.)* **45** (2008), 185–228.

[7] G. Pólya. *How to solve it* (Princeton University Press, 1945).
[8] J. H. Silverman. *The arithmetic of elliptic curves* (Springer–Verlag, 2008).
[9] J. G. Thompson. $k(U_n(\mathbb{F}_q))$. Preprint (2004). http://www.math.ufl.edu/fac/thompson/kUnFq.pdf.
[10] A. Vera-Lopez, J. M. Arregi. Conjugacy classes in unitriangular matrices. *Linear Algebra Appl.* **370** (2003), 85–124.
[11] A. J. Weir. Sylow p-subgroups of the general linear groups over finite fields of characteristic p. *Proc. Amer. Math. Soc.* **6** (1955), 454–464.

Received 18 August, 2010; revised 22 November, 2010

Zoltán Halasi, Alfréd Rényi Institute of Mathematics, Budapest, Hungary
E-mail: zhalasi@renyi.hu

Péter P. Pálfy, Alfréd Rényi Institute of Mathematics, Budapest, Hungary
E-mail: ppp@renyi.hu