On a Remarkable Sequence of Polynomials

A. A. KIRILLOV* A. MELNIKOV†

Abstract

A remarkable sequence of polynomials is considered. These polynomials in q describe in particular the number of solution to the equation $X^2 = 0$ in triangular $n \times n$ matrices over a field $\mathbb{F}_q$ with q elements. They have at least three other important interpretations and a conjectural explicit expression in terms of the entries of the Catalan triangle.

Résumé

Nous considérons une suite remarquable de polynômes. Ces polynômes en q décrivent en particulier le nombre de solutions de l'équation $X^2 = 0$ dans les matrices $n \times n$ sur un corps $\mathbb{F}_q$ ayant q elements. Ils ont au moins trois autres interprétations importantes et une forme explicite conjecturale en termes des entrées du triangle de Catalan.

Recently the first author has discovered a remarkable sequence of polynomials in one variable. We give below several different definitions which apparently lead to the same sequence of polynomials.

1. We start with the set $A_n(\mathbb{F}_q)$ of solutions to the equation

$$X^2 = 0 \tag{1}$$

in $n \times n$ upper-triangular matrices with elements from $\mathbb{F}_q$. The cardinality of this set is, as we show below, a polynomial in q which will be denoted by $A_n(q)$.

Unfortunately, we do not know any direct recurrence relation between these polynomials. So, we will split the set $A_n(\mathbb{F}_q)$ into subsets consisting of matrices of a given rank r. The corresponding quantity is denoted by $A_n^r(q)$ so that we have

AMS 1980 *Mathematics Subject Classification* (1985 *Revision*): 15A57, 22E25, 05A15

*University of Pensylvania, Math. Dept., Philadelphia, PA 19104-6395, USA, and Institute for Problems of Information Transmission of RAS, B. Karetnyi, 19, Moscow 101 477, GSP-4, Russia

†Weizmann Institute, Dept. of Pure Math., Rehovot, Israel

We are grateful to Jacques Alev for the invitation to the Rencontre Franco-Belge which was very interesting and useful for all the participants.

During this work we use the package "Mathematica" intensively. In this matter the first author has profited from the contacts with Herb Wilf and the second one – with Michael Shapiro both of whom we would like to thank.

$A_n(q) = \sum_{r\geq 0} A_n^r(q)$. The new quantities satisfy the simple recurrence relations (see [1])

$$A_{n+1}^{r+1}(q) = q^{r+1} \cdot A_n^{r+1}(q) + (q^{n-r} - q^r) \cdot A_n^r(q); \quad A_{n+1}^0(q) = 1 \tag{2}$$

which imply in particular that they are polynomials in q . One can express $A_n^r(q)$ in terms of q-Hermite polynomials. Namely, in [1] the following equality is proved

$$(2z)^n = \sum_r A_n^r(q) \cdot q^{r(r-n)} \cdot H_{n-2r}(z;\ q^{-1}), \tag{3}$$

where $H_n(x;\ q)$ is the q-Hermite polynomial defined by

$$H_n(x;\ q) := \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q e^{i(n-2k)\theta}, \quad x = \cos\theta,$$

and $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the Gauss q-binomial coefficient:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)\cdots(1-q^k)\cdot(1-q)\cdots(1-q^{n-k})}.$$

Using the orthogonality of Hermite polynomials with respect to a suitable inner product or by direct computations using (3) we can find $A_n^r(q)$ for small n and see that they are polynomials of general type. However in the $A_n(q)$ the dramatical cancelation takes place so that only a few monomials survive. Here are the first dozen of the polynomials $A_n(q)$:

$$\begin{aligned}
A_0 &= 1,\\
A_1 &= 1,\\
A_2 &= q,\\
A_3 &= 2q^2 - q,\\
A_4 &= 2q^4 - q^2,\\
A_5 &= 5q^6 - 4q^5,\\
A_6 &= 5q^9 - 5q^7 + q^5,\\
A_7 &= 14q^{12} - 14q^{11} + q^7,\\
A_8 &= 14q^{16} - 20q^{14} + 7q^{12},\\
A_9 &= 42q^{20} - 48q^{19} + 8q^{15} - q^{12},\\
A_{10} &= 42q^{25} - 75q^{23} + 35q^{21} - q^{15},\\
A_{11} &= 132q^{30} - 165q^{29} + 44q^{25} - 10q^{22}.
\end{aligned}$$

There are many remarkable features of these polynomials which hit the eye when one looks at the table. Let us mention here only the following three:

(i) A_n has only $[\frac{n+3}{3}]$ non-zero monomials.

(ii) Their coefficients have alternating signs.

(iii) The highest coefficients are the well known Catalan numbers.

We postpone the further discussion on coefficients and degrees of monomials till section 3.

2. The second source of polynomials is the so called *generalized Euler-Bernoulli triangle*. It was introduced in [2] in connection with the study of coadjoint orbits of the triangular matrix group over $\mathbb{F}_q$. The elements of this triangle are polynomials $e_{k,l}$ in two variables t and q. Here we are interested in the special case when $t = q$. It is also more convenient to deal with the "restricted" triangle. Namely, we throw away the side entries, divide all the rest by $q-1$ and reenumerate remaining entries starting with the term $b_{0,0}$. The new triangle thus obtained has elements $\{b_{k,l}(q)\}$, $k \geq 0, l \geq 0$ where $b_{k,l} = \frac{e_{k+1,l+1}(q,q)}{q-1}$. One can easily show that $b_{k,l}$ satisfy

$$
\begin{aligned}
&b_{k,l} = q^{-1}b_{k-1,\ l+1} + (q^{l+1} - q^l)b_{l,\ k-1} \text{ for } k > 0;\\
&b_{0,l} = q^l b_{l-1,0} \text{ for } l > 0; \quad b_{0,0} = 1.
\end{aligned}
\tag{4}
$$

In fact, we can take (4) as the definition of the restricted Euler-Bernoulli triangle. Now put $B_n(q) := b_{n-1,0}(q),\ n > 0, \quad B_0(q) = 1$. This is our second sequence of polynomials. The computation shows that polynomials $B_n(q)$ coincide with $A_n(q)$ for $0 \leq n \leq 26$ leaving no doubt that they are equal for all n.

3. Define the Catalan triangle $\{c_{k,l}\},\ k \geq 1,\ |l| \leq k,\ k - l \equiv 0 \pmod 2$, by

$$
c_{k,l} = \operatorname{sign} l \quad \text{for} \quad k = 1; \quad c_{k,l} = c_{k-1,l-1} + c_{k-1,l+1} \quad \text{for} \quad k \geq 2. \tag{5}
$$

This is the same rule as for the Pascal triangle, but with different initial condition. One can easily see that

$$
c_{k,k-2s} = \binom{k-1}{s} - \binom{k-1}{s-1}. \tag{6}
$$

It is convenient to put $c_{k,l} = 0$ for $|l| > k$ in agreement with (6).

Remark that the numbers $c_n := c_{2n+1,1},\ n \geq 0$, are the ordinary Catalan numbers[1]: 1, 1, 2, 5, 14, 42, 132, ... It is pertinent to remark that for a positive l the entry $c_{k,l}$ of the Catalan triangle is the dimension of the irreducible representation of

[1]Which are usually defined by the recurrence $c_{n+1} = \sum_{k=0}^{n} c_k \cdot c_{n-k}$ and the initial conditions $c_0 = c_1 = 1$.

the symmetric group $\mathbf{S}_{k-1}$ corresponding to the partition $(2^{\frac{k-l}{2}}, 1^{l-1})$. In particular, the ordinary Catalan number c_n corresponds to the rectangular diagram (2^n).

Here are the first few lines of the Catalan triangle:

$$\begin{array}{ccccccccccccccccccc}
&&&&&&&&-1&&1&&&&&&&& \\
&&&&&&&-1&&0&&1&&&&&&& \\
&&&&&&-1&&-1&&1&&1&&&&&& \\
&&&&&-1&&-2&&0&&2&&1&&&&& \\
&&&&-1&&-3&&-2&&2&&3&&1&&&& \\
&&&-1&&-4&&-5&&0&&5&&4&&1&&& \\
&&-1&&-5&&-9&&-5&&5&&9&&5&&1&& \\
&-1&&-6&&-14&&-14&&0&&14&&14&&6&&1& \\
-1&&-7&&-20&&-28&&-14&&14&&28&&20&&7&&1
\end{array}$$

One can see immediately that the entries of the Catalan triangle are related to the coefficients of the polynomials $A_n(q)$ or $B_n(q)$. More detailed observation is as follows. Put

$$C_n(q) = \sum_s c_{n+1,s} \cdot q^{\frac{n^2}{4} + \frac{1-s^2}{12}}, \tag{7}$$

where the sum is taken over all integers $s \in [-n-1, n+1]$ which satisfy

$$s \equiv n+1 \pmod 2, \quad s \equiv (-1)^n \pmod 3.$$

Then the first 26 polynomials $C_n(q)$ will coincide with $A_n(q)$ and $B_n(q)$.

The definition (7) is very convenient for practical computations. It allows to find dozens of $C_n(q)$ even without computer. The most elementary expressions we obtain by joining (6) and (7) and considering separately cases of even and odd n. They look as follows:

$$C_{2n}(q) = \sum_{j=[-\frac{n+1}{3}]}^{[\frac{n}{3}]} \left[\binom{2n}{n-3j} - \binom{2n}{n-1-3j}\right] \cdot q^{n^2-3j^2-j},$$

$$C_{2n+1}(q) = \sum_{j=[-\frac{n+2}{3}]}^{[\frac{n}{3}]} \left[\binom{2n+1}{n-3j} - \binom{2n+1}{n-3j-1}\right] \cdot q^{n^2+n-3j^2-2j}.$$

For large n we have the asymptotic expressions

$$C_{2n}(q) \sim c_n \cdot q^{n^2} \cdot \sum_{j\geq 0} (1+6j) q^{-3j^2-j},$$

$$C_{2n+1}(q) \sim c_{n+1} \cdot q^{n^2+n} \cdot \sum_{j\geq 0} (1+3j) q^{-3j^2-2j},$$

where $\sim$ means that the ratio goes to 1 when n goes to infinity.

4. Now we consider the most interesting and sophisticated definition of our polynomials. For any compact group G we denote by $\zeta_G(s)$ the sum

$$\zeta_G(s) := \sum_{\lambda \in \widehat{G}} d(\lambda)^{-s}. \tag{8}$$

Here $\widehat{G}$ denotes the set of (equivalence classes of) unitary irreducible representations of G and $d(\lambda)$ is the dimension of any representation which belongs to the class λ. In particular, for $G = SU(2)$ we obtain the classical Riemann ζ-function.

One can show that the series (8) converges for any compact semisimple Lie group provided that the real part of s is big enough.

For a finite group G we have

$$\zeta_G(-2) = \#G, \quad \zeta_G(0) = \#\widehat{G}.$$

Let now $G_n(\mathbb{F}_q)$ denote the group of all $n \times n$ upper-triangular matrices with elements from the finite field $\mathbb{F}_q$ and with 1's on the main diagonal. This is a finite nilpotent group of order $q^{\frac{n(n-1)}{2}}$. We define the fourth sequence of polynomials in q by

$$D_n(q) := \zeta_{G_n(\mathbb{F}_q)}(-1) = \sum_{\lambda \in \widehat{G}_n(\mathbb{F}_q)} d(\lambda). \tag{9}$$

In fact, it is not clear a priori that $D_n(q)$ are polynomials in q. The most natural proof of it (which is not yet accomplished) would be the following. The representation theoretic meaning of $D_n(q)$ is the dimension of the so called **model space** for the group $G = G_n(\mathbb{F}_q)$: a G-module which contains all irreducible representations with multiplicity one. If we could find a good geometric construction of this module – e.g. as the space of functions or sections of a line bundle over some G-manifold X over $\mathbb{F}_q$ – then $D_n(q)$ would be the number of $\mathbb{F}_q$-points of X. And for nice manifolds the latter quantity is a polynomial in q.

Another interpretation of $D_n(q)$ – the dimension of a maximal commutative C^*-subalgebra in the group algebra of $G_n(\mathbb{F}_q)$. Here again, the explicit construction of such a subalgebra would be of much help for understanding the nature of the quantity $D_n(q)$.

Just now we can only say that for $n \leq 6$ (i.e. for the cases where the classification of unirreps for $G_n(\mathbb{F}_q)$ is known) we have the equality $D_n(q) = A_n(q)$.

5. We finally consider polynomials defined by coadjoint orbits. We can consider our group $G_n(\mathbb{F}_q)$ as the group of $\mathbb{F}_q$-points of an algebraic group over $\mathbb{Z}$. As such it has a Lie algebra, adjoint and coadjoint representations.

The information about coadjoint orbits can be encoded into polynomials

$$O_n^*(q,t)=\sum_m O_{n,m}^*(q)t^m$$

where $O_{n,m}^*(q)$ denotes the number of coadjoint orbits of dimension $2m$ in the dual space $\mathfrak{g}_n^*(\mathbb{F}_q)$ of the Lie algebra $\mathfrak{g}_n(\mathbb{F}_q)$. This dual space can be identified with the space of $n\times n$ strictly lower-triangular matrices over the field $\mathbb{F}_q$.

For the computation of $O_n^*(q,t)$ we use the stratification suggested in [2, §1.6]. The k-th stratum $X_{k,n-k}\subset\mathfrak{g}_n^*(\mathbb{F}_q)$ is defined by the following conditions on the entries $\{f_{ij}\}$ of $F\in\mathfrak{g}_n^*(\mathbb{F}_q)$:

$$f_{n1}=\cdots=f_{n,k-1}=0,\quad f_{nk}\neq 0.$$

Let $x_{k,n-k}^m(q)$ denote the number of $2m$ dimensional orbits in $X_{k,n-k}$ and put

$$x_{k,n-k}=x_{k,n-k}(q,t)=\sum_m x_{k,n-k}^m(q)t^m;\qquad x_{0,n}=0.$$

Now we consider the special case $t=q$. We "restrict" the triangle exactly as we have restricted generalized Euler-Bernoulli triangle in section 2. The new triangle has elements $y_{k,l}=\frac{x_{k+1,l+1}(q,q)}{q-1},\quad k\geq 0,\ l\geq 0$. In particular, $y_{0,0}=1$.

No general formula in spirit of (4) is known for the computation of $y_{k,l}$ or $x_{k,l}$. The complexity of computations of $x_{k,l}$ growths rapidly with n. It is fairly easy to compute the polynomials $x_{k,l}$ manually for $k+l\leq 6$ and it is impossible to compute them without computer for $k+l\geq 8$. However it is easy to show that

$$y_{0,n}=q^n\cdot y_{n-1,0}\quad\text{and}\quad O_n^*(q,q)=y_{n+1,0}.$$

We put $Y_n(q):=y_{n+1,0}$.

The second author succeeded to compute Y_n for $n\leq 11$. They coincide with A_n giving a hope that they coincide for all n.

At the end of this section let us mention some experimental facts concerning $x_{k,l}$ and generalized Euler-Bernoulli triangle. One has $x_{k,l}=e_{k,l}$ for $k+l\leq 5$. However $x_{4,2}\neq e_{4,2}$ and for all k,l such that $k+l\geq 8$ one has $x_{k,l}\neq e_{k,l}$. Unlike this $b_{k,l}=y_{k,l}$ for all k,l that we could check, i.e. such that $k+l<9$.

6. In this section we discuss properties of the quantities we introduced above and give some arguments in favor of the

***Main Conjecture* —** *For all $n\in\mathbb{N}$ we have*

$$A_n(q)=B_n(q)=C_n(q)=D_n(q)=Y_n(q).\tag{10}$$

First of all we recall a result from the representation theory of finite groups which is not so widely known as Burnside theorem. Let $\mathrm{Inv}(G)$ denote the set of involutions (=elements of order ≤ 2) in G. We also recall the notion of the index for $\lambda \in \widehat{G}$:

$$\mathrm{ind}(\lambda) = \begin{cases} 1, & \text{if } \pi_\lambda \text{ is of real type,} \\ 0, & \text{if } \pi_\lambda \text{ is of complex type,} \\ -1, & \text{if } \pi_\lambda \text{ is of quaternionic type.} \end{cases}$$

Here, as usual, π_λ is a representative of the class $\lambda \in \widehat{G}$.

It is known that the index can be expressed through the corresponding character:

$$\mathrm{ind}(\lambda) = \frac{1}{\#G} \sum_{g \in G} \chi_\lambda(g^2).$$

The fact we needed is the following

Proposition — *For any finite group G*

$$\sum_{\lambda \in \widehat{G}} \mathit{ind}(\lambda) \cdot d(\lambda) = \#\mathit{Inv}(G).$$

Corollary — *For any finite group G we have*

$$\zeta_G(-1) \geq \#\mathit{Inv}(G),$$

where the equality holds iff all representations of G are real.

We refer to [2] for the detailed discussion of these results.

Now, assume that $q = 2^l$. Then, writing $g \in G_n(\mathbb{F}_q)$ in the form $1 + X,\ X \in \mathfrak{g}_n(\mathbb{F}_q)$, we get

$$g \in \mathrm{Inv}(G) \iff X^2 = 0.$$

So, for $q = 2^l$, we have from the Corollary above:

$$D_n(q) \geq A_n(q) \tag{11}$$

with equality only when all representations of $G_n(\mathbb{F}_q)$ are real.

Thus, the Main Conjecture implies, in particular, that $G(\mathbb{F}_{2^l})$ has only real representations, hence real characters, hence any element g of this group is conjugate to its inverse g^{-1}.

This very transparent property holds for all examples we could check, but we still have no proof of it in the general case.[2]

[2]Martin Isaacs announced a counterexample to the conjecture $g \sim g^{-1}$ for $G_{13}(\mathbb{F}_2)$.

Conversely, if we could prove that all unirreps of $G_n(\mathbb{F}_q)$ for even q are real, it would imply the equality in (11) for $q = 2^l$, hence for all q, provided we know that $D_n(q)$ are polynomials.

We would like to mention here the conjectural formula for the irreducible representation of $G_n(\mathbb{F}_q)$ corresponding to the coadjoint orbit $\Omega \subset \mathfrak{g}_n^*(\mathbb{F}_q)$:

$$\chi(1 + X) = q^{-\frac{1}{2}\dim\Omega} \cdot \sum_{F\in\Omega} \theta(< F, X >) \tag{12}$$

where θ is a fixed non-trivial additive character of the field $\mathbb{F}_q$.

Putting $X = 0$ in this formula we get $D_n = Y_n$. This formula also implies that for $q = 2^l$ all characters are real.

As a final remark, we want to say that the proof of equalities $A_n = B_n = C_n$ seems to be a (rather non-trivial) exercise[3] while the remaining statements of the Main Conjecture, if they are true, are very deep. In a sense, they are equivalent to the non-formal statement that the ideology of the orbit method works for triangular matrices over finite fields.

References

[1] A.A.Kirillov, *On the number of solutions to the equation $X^2 = 0$ in triangular matrices over a finite field*, 1995, 29, 1, Funct. Anal. and Appl.

[1] ————, *Variations on the triangular theme*, 1995, *in* E.B. Dynkin, *Seminar on Lie Groups*, E.B. Vinberg and S.G. Gindikin, Amer. Math. Soc. Transl. (2) 169, 43–73

[3]The equality $A_n = C_n$ was recently proved by S.B. Ekhad and D. Zeilberger, The Electronic J. Combinatorics 3 (1996), #R2.