An Explicit Formula for the Number of Solutions of $X^2 = 0$ in Triangular Matrices Over a Finite Field

Shalosh B. EKHAD\textsuperscript{1} and Doron ZEILBERGER\textsuperscript{1}

Abstract: We prove an explicit formula for the number of $n \times n$ upper triangular matrices, over $GF(q)$, whose square is the zero matrix. This formula was recently conjectured by Sasha Kirillov and Anna Melnikov[KM].

Theorem: The number of $n \times n$ upper-triangular matrices over $GF(q)$ (the finite field with $q$ elements), whose square is the zero matrix, is given by the polynomial $C_n(q)$, where,

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

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

Proof: In [K] it was shown that the quantity of interest is given by the polynomial $A_n(q) = \sum_{r \geq 0} A^r_n(q)$, where the polynomials $A^r_n(q)$ are defined recursively by:

$$A^{r+1}_n(q) = q^{r+1} \cdot A^r_n(q) + (q^{n-r} - q^r) \cdot A^0_n(q) \quad ; \quad A^0_n(q) = 1 . \quad (Sasha)$$

For any Laurent formal power series $P(w)$, let $CT_w P(w)$ denote the coefficient of $w^0$. Recall that the $q$-binomial coefficients are defined by

$$\binom{m}{n}_q := \frac{(1-q^m)(1-q^{m-1}) \cdots (1-q^{m-n+1})}{(1-q)(1-q^2) \cdots (1-q^n)} , \quad (Carl)$$

whenever $0 \leq n \leq m$, and 0 otherwise.

The following lemma gives an explicit expression for $A^r_n(q)$.

Lemma 1:

$$A^r_n(q) = CT_w \left[ \frac{(1-w)(1+w)^n q^r(n-r)}{w^r} \sum_{i=0}^\infty (-1)^i q^{-(i+1)/2-i(n-2r)} \binom{i+n-2r}{i}_q w^i \right] . \quad (Anna)$$

Proof: Call the right side of Eq. (Anna), $S^r_n(q)$. Since $S^0_{n+1}(q) = 1$, the lemma would follow by induction if we could show that

$$S^{r+1}_{n+1}(q) - q^{r+1} \cdot S^r_n(q) - (q^{n-r} - q^r) \cdot S^r_n(q) = 0 . \quad (Sasha')$$


Supported in part by the NSF. Nov. 28, 1995.
Using the linearity of $CT_w$, manipulating the series, using the definition ($Carl$) of the $q$–binomial coefficients, and simplifying, brings the left side of ($Sasha'$) to be $CT_w \Phi^n_r(q,w)$, where $\Phi^n_r$ is zero except when $n$ is odd and $r = (n-1)/2$, in which case it is a monomial in $q$ times $\frac{(1-w^n)(1+w^n)}{w^{n+1}}$, and applying $CT_w$ kills it all the same, thanks to the symmetry of the Chu-Pascal triangle. □

Summing the expression proved for $A^n_r(q)$, yields that

$$A_n(q) = C T_w \left[ (1-w)(1+w)^n \cdot \sum_{r=0}^{\infty} \sum_{i=0}^{r} (-1)^i q^{r(i+1/2)-(i+1)i/2-i(n-2r)} \left( \frac{i + n - 2r}{n - 2r} \right) q^{i/2} \right].$$

Letting $l = r - i$, and changing the order of summation, yields

$$A_n(q) = C T_w \left[ (1-w)(1+w)^n \cdot \sum_{l=0}^{[n/2]} w^{-l} \cdot q^{n-2l} \sum_{i=0}^{[n-2l]/2} (-1)^i q^{i/2} \left( \frac{n-2l-i}{i} \right) q \right].$$

(Lemma 2: $SumAnna$)

$$\sum_{i=0}^{[m/2]} (-1)^i q^{i(i-1)/2} \left( \frac{m-i}{i} \right) q = (-1)^{[m/3]} q^{(m-1)/6} \cdot \chi(m \not\equiv 2 \text{ mod } 3).$$

(Proof: While this is unlikely to be new², it is also irrelevant whether or not it is new, since this is now routine, thanks to the package qEXHAD, accompanying [PWZ]. Let’s call the left side divided by $q^{m(m-1)/6} \cdot Z(m)$. Then we have to prove that $Z_0(m) := Z(3m)$ equals $(-1)^m$, $Z_1(m) := Z(3m+1)$ equals $(-1)^m$, and $Z_2(m) := Z(3m+2)$ equals 0. It is directly verified that these are true for $m = 0, 1$, and the general result follows from the second order recurrences produced by qEXHAD. The input files inZ0, inZ1, inZ2 as well as the corresponding output files, outZ0, outZ1, outZ2 can be obtained by anonymous ftp to ftp.math.temple.edu, directory pub/exhad/sasha. The package qEXHAD can be downloaded from http://www.math.temple.edu/~zeilberg. □

To complete the proof of the theorem, we use lemma 2 to evaluate the inner sum of ($SumAnna$), then to get $A_{2n}(q)$, we replace $n$ by $2n$, and then replace $l$ by $l + n$, and finally use the binomial theorem. Similarly for $A_{2n+1}(q)$. □

References


