Matrices over $\mathbf{F}_q$ With No Eigenvalues of 0 or 1 *

Kent E. Morrison
Department of Mathematics
California Polytechnic State University
San Luis Obispo, CA 93407

kmorriso@calpoly.edu

19 October 2004

We present a proof of conjecture (68) in Ralf Stephan's article "Prove or Disprove. 100 Conjectures from the OEIS" [5]. The conjecture is that the number of matrices A over the binary field $\mathbf{F}_2$ with the property that both A and $A+I$ are invertible is given by

$$2^{n(n-1)/2}a_n, \quad \text{with } a_0 = 1,\ a_n = (2^n - 1)a_{n-1} + (-1)^n.$$

The sequence begins (starting from $n = 0$) $1, 0, 2, 48, 5824, 2887680, \ldots$. The sequence starting with the $n = 2$ term is A002820 in the Online Encyclopedia of Integer Sequences. In the listing for this sequence there is a reference to a 1971 paper of Duvall and Harley [1]. The sequence $\{a_n\}$ is A005327 in the OEIS and it is the inverse binomial transform of sequence A005321, which counts the number of upper-triangular binary matrices with no row or column that is all zero.

The matrices in question can also be characterized as those A having no eigenvalue equal to 0 or 1. This is equivalent to A defining a projective linear derangement, which means that the map on projective space induced by A has no fixed points. To prove the conjecture we find a generating function for the number of $n \times n$ matrices over $\mathbf{F}_q$ that do not have an eigenvalue of 0 or 1. Let e_n be the number of such matrices and define $e_0 = 1$. We show that the sequence $\{e_n\}$ satisfies the recurrence

$$e_n = e_{n-1}(q^n - 1)q^{n-1} + (-1)^n q^{n(n-1)/2}.$$

(Note that for $q > 2$, projective derangements correspond to matrices with no eigenvalues in the base field $\mathbf{F}_q$. We will point out the generating function for them, but we will not determine the coefficients.)

*www.calpoly.edu/~kmorriso/Research/mnev01.pdf

Define

$$\gamma_n = \prod_{0\le i\le n-1} (q^n - q^i),$$

which is the order of the general linear group of invertible $n\times n$ matrices over $\mathbf{F}_q$. Let e_n be the number of $n\times n$ matrices with entries from $\mathbf{F}_q$ that do not have an eigenvalue of 0 or 1.

Theorem 1

$$1+\sum_{n\ge 1}\frac{e_n}{\gamma_n}u^n = \frac{1}{1-u}\prod_{r\ge 1}\left(1-\frac{u}{q^r}\right).$$

The proof will be given later.

Theorem 2 *Define*

$$a_n = \frac{e_n}{q^{n(n-1)/2}}.$$

Then a_n satisfies the recursion: $a_0 = 1$, $a_n = a_{n-1}(q^n-1)+(-1)^n$.

Proof From Theorem 1 it follows that e_n/γ_n is the sum of the u^i coefficients of $\prod_{r\ge1}(1-u/q^r)$ for $i=0,1,\ldots,n$. Now the u^i coefficient is

$$(-1)^i \sum_{1\le r_1<r_2<\cdots<r_i} \frac{1}{q^{r_1+r_2+\cdots+r_i}}.$$

By induction one can easily show that this coefficient is

$$\frac{(-1)^i}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

Therefore

$$\frac{e_n}{\gamma_n} = 1+\sum_{1\le i\le n}\frac{(-1)^i}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

Next,

$$\frac{e_n}{\gamma_n} = \frac{e_{n-1}}{\gamma_{n-1}} + \frac{(-1)^n}{(q^n-1)\cdots(q-1)}.$$

Making use of the formula for γ_n and γ_{n-1} and canceling where possible we see that

$$e_n = e_{n-1}(q^n-1)q^{n-1} + (-1)^n q^{n(n-1)/2}.$$

Divide both sides by $q^{n(n-1)/2}$ and simplify to see that

$$\frac{e_n}{q^{n(n-1)/2}} = \frac{e_{n-1}}{q^{(n-1)(n-2)/2}}(q^n-1)+(-1)^n.$$

With the definition given for a_n in the statement of the theorem this gives

$$a_n = a_{n-1}(q^n - 1) + (-1)^n.$$

$\square$

Proof of Theorem 1 We use the cycle index for matrices over finite fields introduced by Kung [3] and extended by Stong [6]. See also [2, 4]. The treatment in section 1 of [4] is most convenient for the purpose here. The series of lemmas there give us the following. Let $\mathcal{A}$ be any set of monic irreducible polynomials with coefficients in $\mathbf{F}_q$. Let μ_n be the number of $n \times n$ matrices over $\mathbf{F}_q$ whose characteristic polynomial factors into powers of elements of $\mathcal{A}$. Then

$$1 + \sum_{n \geq 1} \frac{\mu_n}{\gamma_n} u^n = \prod_{\phi \in \mathcal{A}} \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Taking $\mathcal{A}$ to be the full set of monic irreducibles (which we denote $\mathbf{\Phi}$) we have

$$1 + \sum_{n \geq 1} \frac{q^{n^2}}{\gamma_n} u^n = \prod_{\phi \in \mathbf{\Phi}} \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Taking $\mathcal{A}$ to be all monic irreducibles except for $\phi(z) = z$ gives us the invertible matrices with $\mu_n = \gamma_n$ and so

$$1 + \sum_{n \geq 1} u^n = \prod_{\phi \in \mathbf{\Phi} \setminus \{z\}} \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}. \tag{1}$$

Taking $\mathcal{A} = \mathbf{\Phi} \setminus \{z, z-1\}$ gives us the matrices without factors of z or $z - 1$ in their characteristic polynomial, which is exactly the set of matrices without 0 or 1 as eigenvalues. Therefore

$$1 + \sum_{n \geq 1} \frac{e_n}{\gamma_n} u^n = \prod_{\phi \in \mathbf{\Phi} \setminus \{z, z-1\}} \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}. \tag{2}$$

Now multiply the right side of (1) by $\prod_{r \geq 1}(1 - u/q^r)$ to get the right side of (2) by taking out the factor corresponding to the polynomial $z - 1$. Hence, we have the statement of the theorem:

$$\begin{aligned} 1 + \sum_{n \geq 1} \frac{e_n}{\gamma_n} u^n &= \left(1 + \sum_{n \geq 1} u^n\right) \prod_{r \geq 1} \left(1 - \frac{u}{q^r}\right) \\ &= \frac{1}{1-u} \prod_{r \geq 1} \left(1 - \frac{u}{q^r}\right). \end{aligned}$$

$\square$

By omitting all the linear polynomials we can derive the following for the number of projective derangements. Let d_n be the number of $n \times n$ matrices over $\mathbf{F}_q$ with no eigenvalues in $\mathbf{F}_q$. Then

$$1 + \sum_{n \geq 1} \frac{d_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{r \geq 1} \left(1 - \frac{u}{q^r}\right)^{q-1}.$$

Note that we are counting matrices here with no fixed points on projective space. Since matrices which are non-zero scalar mutliples of each other define the same map on projective space, we need to divide d_n by $q-1$ to count distinct maps. Finally, the generating functions presented here will easily give the asymptotic probability that a matrix has no eigenvalues of 0 or 1 or that a matrix has no eigenvalues in the base field. For example, for $q = 2$

$$\lim_{n\to\infty} \frac{e_n}{2^{n^2}} = \prod_{r \geq 1} \left(1 - \frac{1}{2^r}\right)^2 \approx 0.0833986.$$

References

[1] P. F. Duvall, Jr., and P. W. Harley, III, A note on counting matrices, SIAM J. Appl. Math., **20** (1971), 374–377.

[2] J. Fulman, Random matrix theory over finite fields, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 1, 51–85 (electronic); MR 2002i:60012, arXiv:math.GR/0003195

[3] J. P. S. Kung, The cycle structure of a linear transformation over a finite field, Linear Algebra Appl. **36** (1981), 141–155; MR 82d:15012

[4] K. E. Morrison, Eigenvalues of random matrices over finite fields, unpublished (1999), www.calpoly.edu/˜kmorriso/Research/ERMFF.pdf.

[5] R. Stephan, Prove or disprove. 100 Conjectures from the OEIS, unpublished (2004), arXiv:math.CO/0409509.

[6] R. Stong, Some asymptotic results on finite vector spaces, Adv. in Appl. Math. **9** (1988), no. 2, 167–199; MR 89c:05007