Counting matrices over finite fields

Steven Sam

Massachusetts Institute of Technology

September 30, 2011

Invertible matrices

- $\mathbf{F}_q$ is a finite field with $q = p^r$ elements.
- $[n] = \frac{1-q^n}{1-q} = q^{n-1} + q^{n-2} + \cdots + q + 1$
- $[n]! = [n][n-1]\cdots[2][1]$.
- $\mathbf{GL}_n(\mathbf{F}_q) = \{n \times n$ invertible matrices with entries in $\mathbf{F}_q\}$.

$$\begin{aligned}\#\mathbf{GL}_n(\mathbf{F}_q) &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) \\ &= q^{\binom{n}{2}}(q-1)^n[n]!\end{aligned}$$

The first equality just says to choose the columns of the matrix one at a time in such a way that they are not in the linear span of the previous columns. Note:

$$\lim_{q\to 1} \frac{\#\mathbf{GL}_n(\mathbf{F}_q)}{(q-1)^n} = \#S_n$$

Another interpretation for $\#\mathbf{GL}_n(\mathbf{F}_q) = q^{\binom{n}{2}}(q-1)^n[n]!$:

The first two terms give the size of the Borel subgroup B of upper triangular matrices. So the last term is the size of the flag variety

$$\mathcal{B} = \mathbf{GL}_n(\mathbf{F}_q)/B = \{V_1 \subset V_2 \subset \cdots \subset V_n = \mathbf{F}_q^n \mid \dim V_i = i\}.$$

Bruhat decomposition: for each $w \in S_n$ (permutation matrices), define $U_w = BwB \subset \mathcal{B}$. Then $\mathcal{B} = \coprod_{w \in S_n} U_w$ and $\#U_w = q^{\ell(w)}$, and then use the identity

$$\sum_{w \in S_n} q^{\ell(w)} = [n]!.$$

Bruhat decomposition also says $\mathbf{GL}_n(\mathbf{F}_q) = \coprod_{w \in S_n} BwB$.
Completely general when $\mathbf{GL}_n(\mathbf{F}_q)$ is replaced by a finite group of Lie type

Restricted positions

Choose a subset S of positions in the $n \times n$ grid.

- How many invertible matrices are there such that the entries in S must be 0?
- Is the function a polynomial in q?
- Are there $\lim_{q \to 1}$ interpretations?
- How about other rank conditions? Non-square matrices?

Aside: Given S and a rank condition, the set of matrices above is naturally an algebraic variety. The geometric properties were studied by Giusti–Merle and the homological properties studied by Boocher.

Work with $m \times n$ grid, and subset S.

Let $t_{q,r}$ be the number of $m \times n$ matrices over $\mathbf{F}_q$ with rank r and that are 0 in S.

Let $t_{1,r}$ be the number of ways to mark r squares outside of S in the $m \times n$ grid such that each row and each column has at most 1 marked box (i.e., rook placements)

Theorem (LLMPSZ)

$t_{q,r} = (q-1)^r t_{1,r} \pmod{(q-1)^{r+1}}$.

In other words,

$$\lim_{q \to 1} \frac{t_{q,r}}{(q-1)^r} \text{“}=\text{''}\, t_{1,r}.$$

Take $m = n$ and S to be the set of diagonal entries. Then

$$t_{1,n} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)!$$

counts derangements (permutations without fixed points).

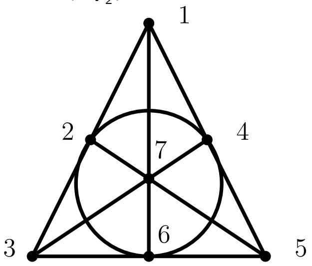
Theorem (LLMPSZ)

$t_{q,n} = q^{\binom{n-1}{2}-1}(q-1)^n \sum_{i=0}^{n} (-1)^i \binom{n}{i} [n-i]!$. *More generally,*

$$t_{q,r} = q^{\binom{r-1}{2}-1}(q-1)^r \sum_{i=0}^{r} (-1)^i \binom{r}{i} \frac{[n-i]!}{[n-r]!}$$

Bruhat decomposition: the number of points in cells indexed by non-derangements is divisible by $(q-1)^{n+1}$

Let $S(\mathbf{P}^2_{\mathbf{F}_2}) \subset 7 \times 7$ be complement of support of the Fano plane:



$$A = \begin{array}{|c|c|c|c|c|c|c|} \hline a_{11} & a_{12} & 0 & 0 & 0 & 0 & a_{17} \\ \hline a_{21} & 0 & a_{23} & 0 & 0 & a_{26} & 0 \\ \hline a_{31} & 0 & 0 & a_{34} & a_{35} & 0 & 0 \\ \hline 0 & a_{42} & a_{43} & 0 & a_{45} & 0 & 0 \\ \hline 0 & a_{52} & 0 & a_{54} & 0 & a_{56} & 0 \\ \hline 0 & 0 & a_{63} & a_{64} & 0 & 0 & a_{67} \\ \hline 0 & 0 & 0 & 0 & a_{75} & a_{76} & a_{77} \\ \hline \end{array}$$

Theorem (Stembridge 1998)

$\#$ of invertible matrices A is a quasi-polynomial:

$$\begin{cases} (q-1)^7(q^{14} + \cdots -97q^9 + \cdots + q^3) & \textit{if } q \textit{ even}, \\ (q-1)^7(q^{14} + \cdots -98q^9 + \cdots -6q^5) & \textit{if } q \textit{ odd}. \end{cases}$$

$S(\mathbf{P}^2_{\mathbf{F}_2})$ is smallest example with respect to n and $\#S$.

Let G be a connected graph with edge set E. Define

$$P_G(x) = \sum_T \prod_{e \notin T} x_e$$

where the sum is over all spanning trees T of G.

Kontsevich: Is $\#\{x \in \mathbf{F}_q^E \mid P_G(x) = 0\}$ a polynomial in q?

Stanley: This question is equivalent to polynomiality of counting invertible *symmetric* matrices with restricted positions.

Belkale–Brosnan: These functions are **very** complicated, and the answer to the question is no: if we treat the functions $q^n - q$ for $n > 1$ as units, then the ring of counting functions for restricted symmetric matrices is the same as the ring of counting functions for *arbitrary* varieties

So when is it a polynomial?

A natural question to ask now is what properties of S would impose polynomiality of the counting function.
Given a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$, we get the Young diagram S_λ.

Theorem (Haglund)

For $S = S_\lambda$ and any r, the counting function is a polynomial $P_\lambda(q)$, and $P_\lambda(q)/(q-1)^r$ has **positive** *coefficients.*

For two partitions $\mu \subset \lambda$, also have skew diagram $S_{\lambda/\mu}$.

Theorem (Klein–Morales)

When S is the complement of $S_{\lambda/\mu}$ and for any r, the counting function is a polynomial $P_{\lambda/\mu}(q)$ and $P_{\lambda/\mu}(q)/(q-1)^r$ has **positive** *coefficients.*

Positivity comes from an interpretation in terms of “inversion” statistics.

Given a permutation $w \in S_n$, its Rothe diagram is

$$D(w) = \{(i, w(j)) \mid i < j, w(i) > w(j)\}.$$

(They generalize Young diagrams)

Conjecture: When S is the complement of $D(w)$ and for any r, the counting function is a polynomial $P_w(q)$ and $P_w(q)/(q-1)^r$ has **positive** coefficients.

Known cases: if $D(w)$ can be transformed into $S_{\lambda/\mu}$ via row and column swaps, then the above is true. We say w is **skew-transformable**.

Theorem (Klein–Lewis)

w is skew-transformable if and only if it avoids the following patterns:

$$52143, 25143, 42153, 24153, 32514, 32541, 31524, 31542, 214365$$

Theorem (Klein–Lewis)

For any S and $r = 1$, the counting function is a polynomial $P_S(q)$.

Theorem (Lewis)

If S has at most 2 zeroes in each row and column, then for any r, the counting function is a polynomial.

How about symmetric and skew-symmetric matrices? We consider q odd for simplicity. We have the "curious relations":

Theorem (LLMPSZ)

Fix n even. The following three sets have the same size:

- *Symmetric invertible matrices of size n with 0 on the diagonal*
- *Symmetric invertible matrices of size $n-1$*
- *Skew-symmetric invertible matrices of size n*

The equivalence of the last two was shown independently by Oliver Jones via the Weil conjecture philosophy by calculating the Betti numbers of the corresponding complex varieties

Note: No explicit bijections (without considering several cases) known for these sets!

The equality between $\#\{$ symmetric invertible $(n-1) \times (n-1)$ matrices$\}$ and $\#\{$ skew-symmetric invertible $n \times n$ matrices $\}$ can be reinterpreted in terms of Schubert varieties.

Let V be a $2n$-dimensional vector space with a symplectic form ω. The Lagrangian Grassmannian is the set of isotropic n-dimensional subspaces $U \subset V$, i.e., $\omega(u, u') = 0$ for all $u, u' \in U$.

Let W be a $2n$-dimensional vector space with a (split) orthogonal form β. The spinor variety is a connected component of the set of isotropic n-dimensional subspaces $U \subset W$, i.e., $\beta(u, u') = 0$ for all $u, u' \in U$.

They are homogeneous spaces for the symplectic and special orthogonal groups, respectively. The Schubert cells X_v are the B-orbits (B is upper triangular matrices under a suitable choice of basis). For opposite Schubert cells X_v^-, same but use B^- (lower triangular).

Parabolic R-polynomials

The Schubert cells X_v form a poset via $w \leq v$ if and only if $\overline{X_w} \subseteq \overline{X_v}$. Furthermore, we have $X_v \cap X_w^- \neq \varnothing$ if and only if $v \geq w$.

Given $w \leq v$ in this poset, Deodhar defined an associated polynomial $R_{w,v}(x)$ which generalizes the R-polynomials of Kazhdan–Lusztig. They have the property that $R_{w,v}(q) = \#(X_v \cap X_w^-)$

The (skew-)symmetric matrices can be identified with the biggest opposite Schubert cell in the spinor variety, and Lagrangian Grassmannian, respectively (the notion of skew switches). Furthermore, rank conditions on the matrices are given by intersecting with certain Schubert varieties.

The intersection posets for the Lagrangian Grassmannian and spinor variety are isomorphic as abstract posets. So we are done if we know that the R-polynomials only depend on the poset structure. Brenti showed this to be true in the *cominuscule* case, which covers our situation.

Let K be an algebraically closed field. Given an embedded projective variety $X \subset \mathbf{P}^N$, the **projective dual** $X^\vee$ of X is the closure of the set of hyperplanes that are tangent to some smooth point of X. It is a subvariety of the dual projective space $(\mathbf{P}^N)^\vee$, and $(X^\vee)^\vee = X$.

In the case that $X^\vee$ is a hypersurface, it is the solution set of a single polynomial, the X-**discriminant**.

Example

$\mathbf{P}^d$ is the space of degree d binary forms $\sum_{i=0}^d a_i x^{d-i} y^i$ (let $b_0, \dots, b_d$ be the dual coordinates to $a_0, \dots, a_d$), X is the Veronese variety: $X = \{(ax + by)^d \mid a, b \in K\}$. The dual is a hypersurface and its equation is the usual discriminant, i.e., it is 0 if and only if $\sum_{i=0}^d b_i x^{d-i} y^i$ has a multiple root.

Example

$\mathbf{P}^{n^2-1}$ is the space of $n \times n$ matrices, X is the Segre variety: $X = \{A \mid \mathrm{rank}(A) = 1\}$. Then the projective dual can be identified with matrices of rank at most $n-1$, so the discriminant is the usual determinant.

Generalization: instead of $n \times n$ matrices, we consider tensors of format $n_1 \times \cdots \times n_k$ (assume $n_1 \geq \cdots \geq n_k$). The Segre variety $X \subset \mathbf{P}^{n_1 \cdots n_k - 1}$ consists of all pure tensors of the form $v_1 \otimes \cdots \otimes v_k$.

Theorem (Gelfand–Kapranov–Zelevinsky)

$X^\vee$ is a hypersurface if and only if $n_1 \leq n_2 + \cdots + n_k - k + 2$.

Question: How many tensors have nonzero hyperdeterminant over $\mathbf{F}_q$?

Unravelling the definition of hyperdeterminant

Hyperdeterminants are basically impossible to write down (even on a computer!) outside of very small cases, but we can work with the definition directly.

Having zero hyperdeterminant can be rephrased as follows. For each j and $1 \leq N \leq n_j$, consider the equation

$$\sum_{(i_1,\ldots,i_k)} a_{i_1\cdots i_k} x^{(1)}_{i_1} \cdots \hat{x}^{(j)}_{i_j} \cdots x^{(k)}_{i_k} = 0$$

where the sum is over all $(i_1, \ldots, i_k)$ with $i_j = N$ and $1 \leq i_d \leq n_d$. Then the tensor $(a_{i_1,\ldots,i_k})$ has zero hyperdeterminant if and only if these equations have a solution $(x^{(d)}_{i_d})$ where each vector $x^{(d)}$ is nonzero. (When $k = 2$, these equations are linear.)

Warning: Even if we only care about tensors with coefficients in $\mathbf{F}_q$, we have to check for the solutions to the above equation in an algebraic closure of $\mathbf{F}_q$.

Theorem (Musiker–Yu)

For $2 \times 2 \times 2$, the number of nondegenerate tensors is $(q^4 - 1)(q^4 - q^3)$.

(Compare this to $(q^2 - 1)(q^2 - q)$ for 2×2)

Theorem (Lewis–Sam)

For $2 \times 2 \times 3$, the number is $q^4(q-1)^4[2]^2[3]$.
For $2 \times 3 \times 3$, the number is $q^{10}(q-1)^3[2]^2[3]$.
For $2 \times 2 \times 4$, the number is $q^4(q-1)^2[3][4](q^3 + q^2 - 1)$

Caveat: these need to be double-checked...

$2 \times 2 \times 4$ doesn't give a hypersurface, but there is still a $\mathbf{GL}_2 \times \mathbf{GL}_2 \times \mathbf{GL}_4$-invariant hypersurface (this representation is exceptional in this sense)

Question: What are these q-analogues of?

- $m \times n$ matrices of rank k (determinantal varieties) are a q-analogue of partially defined functions:

$$q^{\binom{k}{2}}(q-1)^k[k]!\frac{[m]!}{[k]![m-k]!}\frac{[n]!}{[k]![n-k]!}$$

  How about matrix Schubert varieties? Ladder determinantal varieties? (put different rank conditions on certain submatrices)
- Representations of equioriented A_n quiver should be a q-analogue of lacing diagrams. Other types of quivers?
- What about when q is a root of unity? Cyclic sieving interpretations?
- Could also ask for quasi-polynomiality of counting functions: when does it hold for graph polynomials? Matroid polynomials?
- Singular loci of graph/matroid polynomials? Do they have interesting interpretations?