COUNTING COLORINGS ON VARIETIES

FERNANDO RODRÍGUEZ-VILLEGAS

Abstract

We present a combinatorial mechanism for counting certain objects associated to a variety over a finite field. The basic example is that of counting conjugacy classes of the general linear group. We discuss how the method applies to counting these and also to counting unipotent matrices and pairs of commuting matrices.

1. Setup

1.1. Introduction. The goal of this note is to present a combinatorial mechanism for counting certain objects associated to a variety $X$ defined over a finite field. The basic example, discussed in Section 2.2, is that of counting conjugacy classes in $\text{GL}_n(F_q)$, where $X = G_m$ (the multiplicative group).

We give four different forms of the main formula (which is somewhat reminiscent of Pólya’s theory of counting). The principle that emerges is that in a given setup the counting generating functions for $X = \bullet$ (a point), $X = G_a$ (the additive group) and $X = G_m$ are related to one another in a simple way. Often one of the cases will be significantly easier to compute than the others yielding a closed formula for all three generating functions. For example, in Section 3 we describe how one can go from counting all matrices in $M_n(F_q)$, corresponding to $X = G_a$, to counting unipotent matrices in $M_n(F_q)$, corresponding to $X = \bullet$.

None of the special cases considered here are really new; the point is, instead, to stress the main combinatorial principle. For more general applications (to quiver and character varieties) we refer the reader to [5] and [4].
1.2. The zeta function of $X$. Let $\mathbb{F}_q$ be a finite field with $q$ elements. Fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. For each $r \in \mathbb{N}$ let $\mathbb{F}_{q^r}$ be the unique subfield of $\overline{\mathbb{F}}_q$ of cardinality $q^r$. Let $\text{Frob}_q \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ be the Frobenius automorphism $x \mapsto x^q$. Then $\mathbb{F}_{q^r}$ is the fixed field of $\text{Frob}_q^r$.

Let $X$ be an algebraic variety defined over $\mathbb{F}_q$. For each $r \in \mathbb{N}$ let $N_r(X) := \#X(\mathbb{F}_{q^r})$. The zeta function of $X$ is defined as

$$Z(X, T) := \exp \left( \sum_{r \geq 1} N_r(X) \frac{T^r}{r} \right).$$

Let $\tilde{N}_d(X)$ be the number of Frobenius orbits in $X(\overline{\mathbb{F}}_q)$ of size $d$. Then

$$N_r(X) = \sum_{d|r} d \tilde{N}_d(X).$$

We can write the zeta function as an Euler product

$$Z(X, T) = \prod_{d \geq 1} (1 - T^d)^{-\tilde{N}_d(X)}.$$

1.3. Colorings on $X$. We consider the following general setup. Let $\mathcal{C}$ be a set, whose members we call colors, and

$$| \cdot | : \mathcal{C} \longrightarrow \mathbb{Z}_{\geq 0}$$

a function called degree such that

1. there are finitely many colors of a given degree;
2. there is a unique color $0 \in \mathcal{C}$ of degree $0$.

A coloring on $X$ is a map

$$\Lambda : X(\overline{\mathbb{F}}_q) \longrightarrow \mathcal{C}.$$

The degree of $\Lambda$ is defined as

$$|\Lambda| := \sum_{x \in X(\overline{\mathbb{F}}_q)} |\Lambda(x)|.$$

We will only consider colorings of finite degree, so that $\Lambda(x) = 0$ for all but finitely many $x$. We let the Frobenius automorphism act on colorings via

$$\Lambda^{\text{Frob}_q}(x) := \Lambda(\text{Frob}_q(x))$$

and say $\Lambda$ is defined over $\mathbb{F}_{q^r}$ if $\Lambda$ is fixed by $\text{Frob}_q^r$. In this case we will write: $\Lambda$ is a coloring of $X/\mathbb{F}_{q^r}$. 

Given a pair \((d, \lambda)\), with \(d \in \mathbb{N}\) and \(\lambda \in C\) a non-zero color, we define its multiplicity \(m_{d,\lambda}\) in a coloring \(\Lambda\) of \(X/F_q\) to be the number of Frobenius orbits \(\{x\}\) in \(X(F_q)\) of degree \(d\) with \(\Lambda(x) = \lambda\). Note that
\[
|\Lambda| = \sum_{d \geq 1, \lambda \neq 0} m_{d,\lambda} d|\lambda|.
\]
We call the combinatorial data \(\{m_{d,\lambda}\}\) of multiplicities the type of \(\Lambda\) and denote it \(\tau(\Lambda)\).

**Example 1.** Let \(C = \mathbb{Z}_{\geq 0}\) with degree function \(|n| = n\). Then a coloring is an effective 0-cycle on \(X\). The actions of Frobenius are compatible hence \(\Lambda\) is defined over \(F_{q^r}\) if and only if the corresponding 0-cycle is.

**Example 2.** If \(X = \mathbb{G}_m\) and \(C = P\) is the set of all partitions of non-negative integers with \(|\lambda| = \lambda_1 + \lambda_2 + \cdots\) if \(\lambda = \lambda_1 \geq \lambda_2 \geq \cdots\) then colorings of degree \(n\) are in one-to-one correspondence with conjugacy classes in \(\text{GL}_n(F_q)\) by the Jordan decomposition theorem. Indeed, to each coloring \(\Lambda\) we may associate the direct sum of Jordan blocks with eigenvalue \(x \in F_q^*\) and size \(\lambda_i\), where \(\Lambda(x) = \lambda_1 \geq \lambda_2 \geq \cdots\). This correspondence preserves the action of Frobenius and therefore colorings defined over \(F_{q^r}\) are in bijection to conjugacy classes of \(\text{GL}_n(F_{q^r})\).

Similar statements hold for \(X = \mathbb{G}_a\) with colorings corresponding to conjugacy classes in \(\text{M}_n(F_q)\) instead.

We need one more ingredient. Let \(R = \mathbb{Z}[t_1, \ldots, t_N][[t_1^{-1}, \ldots, t_N^{-1}]]\) be the ring of Laurent series with integer coefficients in the variables \(t_1, \ldots, t_N\). We let
\[
W(\Lambda) := \prod_{\{x\}} W(\Lambda(x))(t^{d(x)}),
\]
where \(\{x\}\) runs through the Frobenius orbits in \(X(F_q)\), \(d(x) = \#\{x\}\) is the degree of \(x\) (the size of its Frobenius orbit) and \(t^d := t_1^d \cdots t_N^d\). Note that \(W(\Lambda)\) only depends on the type \(\tau(\Lambda)\):
\[
W(\Lambda) = \prod_{d \geq 1, \lambda \neq 0} W(\lambda)(t^d)^{m_{d,\lambda}}.
\]
We say that \(W\) is homogeneous if for each \(\lambda \in C\) we have that \(W(\lambda) \in R\) is homogeneous of degree \(|\lambda|\). In this case \(W(\Lambda)\) is also homogeneous of degree \(|\Lambda|\).
1.4. Coloring zeta function of X. Given the coloring data $C = (\mathcal{C}, |\cdot|, W(\cdot))$ we define the coloring zeta function of $X$ as the formal power series in $R[[T]]$

(12) 
\[ Z_C(X, t, T) := \sum_{\Lambda} W(\Lambda)T^{\left|\Lambda\right|}, \]

where the sum runs over all colorings of $X/F_q$. If $X = \bullet$ (a point) then the coloring zeta function simply reduces to

(13) 
\[ Z_C(\bullet, t, T) := \sum_{\Lambda \in \mathcal{C}} W(\Lambda)T^{\left|\Lambda\right|}. \]

Example 3. In the standard setup $C = (\mathbb{Z}_{\geq 0}, |\cdot|, 1)$, $Z_C(X, T)$ is just the usual zeta function $Z(X, T)$. In particular, if $X = \bullet$ then

\[ Z_C(\bullet, T) = \sum_{n \geq 0} T^n = (1 - T)^{-1}. \]

Example 4. In the partition setup $C = (\mathcal{P}, |\cdot|, 1)$ and if $X = \bullet$ then

\[ Z_C(\bullet, T) = \sum_{\lambda \in \mathcal{P}} T^{\left|\lambda\right|} = \prod_{d \geq 1} (1 - T^d)^{-1}. \]

2. Main formula

2.1. First form. This form of the main formula is similar to the Euler product (3) for the usual zeta function (to which it reduces to in the standard setup).

Theorem 1. The following identity of generating functions holds

(14) 
\[ Z_C(X, t, T) = \prod_{d \geq 1} Z_C(\bullet, t^d, T^d)^{\tilde{N}_d}. \]

Proof: Write $Z_C(\bullet, t, T) = 1 + z(T)$. For $N \in \mathbb{N}$ we have

\[ Z_C(\bullet, t, T)^N = 1 + \sum_{m \geq 1} N(N - 1) \cdots (N - m + 1) \frac{z(T)^m}{m!} \]

by the binomial theorem. On the other hand by the multinomial theorem

\[ \frac{z(T)^m}{m!} = \sum_{m_\lambda \lambda \neq 0} \frac{W(\lambda)^{m_\lambda}}{m_\lambda!} T^{m_\lambda |\lambda|} \]
summed over all sequences of non-negative integers $m_\lambda$ with $\sum_{\lambda \neq 0} m_\lambda = m$. Putting these two identities together we get that the coefficient of $T^n$ on the right hand side of (14) equals

$$\sum_{m_d,\lambda \geq 1, \lambda \neq 0} \tilde{N}_d (\tilde{N}_d - 1) \cdots (\tilde{N}_d - m_d + 1) \frac{W(\lambda)(t^d)^{m_d,\lambda}}{m_d,\lambda!}$$

summed over all $m_d,\lambda$ sequences of non-zero integers satisfying

$$n = \sum_{d \geq 1, \lambda \neq 0} m_{d,\lambda} d|\lambda|,$$

where $m_d := \sum_{\lambda \neq 0} m_{d,\lambda}$.

On the other hand to give a coloring of $X/F_q$ with multiplicities $m_{d,\lambda}$ we need to pick $m_d = \sum_{\lambda \neq 0} m_{d,\lambda}$ Frobenius orbits of size $d$ and color $m_{d,\lambda}$ of them with color $\lambda \neq 0$. There are $\binom{\tilde{N}_d}{m_d}$ ways of picking the orbits and $m_d!/\prod_{\lambda \neq 0} m_{d,\lambda}!$ ways to color them in this way and the weight of $\Lambda$ is $W(\Lambda) = \prod_{d \geq 1, \lambda \neq 0} W(\lambda)(t^d)^{m_{d,\lambda}}$. It follows that the coefficients of $T^n$ on both sides of (14) agree.

\[\square\]

### 2.2. Second form.

**Theorem 2.** The following identity of generating functions holds

\begin{equation}
Z_C(X, t, T) = \prod_{m \in \mathbb{Z}, d \geq 1} Z(X, t^m T^d)^{v_{d,m}}
\end{equation}

where the exponents $v_{d,m}$ are defined by the formal identity

\begin{equation}
Z_C(\bullet, t, T) = \prod_{m \in \mathbb{Z}, d \geq 1} (1 - t^m T^d)^{-v_{d,m}}.
\end{equation}

**Proof:** Taking logarithms of both sides of (14) we get

$$\log Z_C(X, t, T) = \sum_{d \geq 1} \tilde{N}_d \log Z_C(\bullet, t^d, T^d).$$

By Möbius inversion of (2)

$$\tilde{N}_d = \frac{1}{d} \sum_{e|d} \mu(e) N_{d/e}.$$

Taking logarithm of both sides of (16) we get

$$\log Z_C(\bullet, t, T) = - \sum_{m \in \mathbb{Z}, d \geq 1} v_{d,m} \log (1 - t^m T^d).$$
On the other hand,

\[ T = - \sum_{r \geq 1} \mu(r) \log(1 - T^r) \]

and hence

\[
\log Z_C(X, t, T) = - \sum_{r, s \geq 1} \frac{1}{s} \mu(r) N_s \sum_{m \in \mathbb{Z}^N, d \geq 1} v_{d,m} \log(1 - t^{msr} T^{d sr})
\]

\[ = \sum_{s \geq 1} \frac{1}{s} N_s \sum_{m \in \mathbb{Z}^N, d \geq 1} v_{d,m} t^{sm} T^{sd} \]

\[ = \sum_{m \in \mathbb{Z}^N, d \geq 1} v_{d,m} \log Z(X, t^m T^d) \]

proving our claim. \(\square\)

Remark. It is easy to see by induction that the \(v_{d,m}\) in (16) are integers uniquely determined by \(Z_C(\bullet, t, T)\).

Example 5. In the partition setup \(C = (\mathcal{P}, | \cdot |, 1)\) with \(X = \mathbb{G}_m\) we have

\[ Z_C(\mathbb{G}_m, T) = \sum_{n \geq 0} C_n T^n, \]

where \(C_n\) is the number of conjugacy classes in \(\text{GL}_n(\mathbb{F}_q)\) (see Example 2); by (15) this equals

\[ \prod_{n \geq 1} \left( \frac{1 - T^n}{1 - q T^n} \right) \]

as \(Z(\mathbb{G}_m, T) = (1 - T)/(1 - q T)\). See [1], [3], [6].

Similarly, if we take \(X = \mathbb{G}_a\) then we get the expression

\[ \prod_{n \geq 1} (1 - q T^n)^{-1} \]

for the generating function for the conjugacy classes in \(\text{M}_n(\mathbb{F}_q)\) instead.

2.3. Third form. This form of the expression for the coloring zeta function is a simple variant of the second form (15) but it is convenient to state it separately.

Let

\[ Z_C(u, t, T) := \prod_{m \in \mathbb{Z}^N, d \geq 1} (1 - u t^m T^d)^{-v_{d,m}} \]

where \(u\) is another formal variable and \(v_{d,m}\) is as in (16).
Theorem 3. Let
\[(20)\quad Z(X, T) = \prod_i (1 - x_i T)^{-n_i},\]
for some \(x_i \in \mathbb{C}\) and \(n_i \in \mathbb{Z}\). Then with the above notation we have
\[(21)\quad Z_C(X, t, T) = \prod_i Z_C(x_i, t, T)^{n_i}.\]

Example 6. In the standard setup \(Z_C(\bullet, T) = (1 - T)^{-1}\) so that \(Z_C(u, T) = (1 - uT)^{-1}\) and (21) is simply a restatement of (20).

Remark. It is known by the work of Dwork that \(Z(X, T)\) is a rational function of \(T\) of the form (20).

2.4. Fourth form. Recall that \(R = \mathbb{Z}[t_1, \ldots, t_N][t_1^{-1}, \ldots, t_N^{-1}]\) is the ring of Laurent series in variables \(t_1, \ldots, t_N\) with integer coefficients. Given \(Z \in 1 + TR[[T]]\) we define, following Getzler \(2\)
\[(22)\quad \text{Log}(Z) := \sum_{d \geq 1, m \in \mathbb{Z}^N} v_{d,m} t^m T^d \in R[[T]],\]
where
\[Z = \prod_{m \in \mathbb{Z}^N, d \geq 1} (1 - t^m T^d)^{-v_{d,m}},\]
as in (16).

In this section we assume that \(X\) is a polynomial count variety; i.e.
\[N_p(X) = N_X(q^r), \quad r \in \mathbb{N},\]
for some fixed polynomial \(N_X \in \mathbb{Z}[q]\). We also assume that one of the variables in \(R\) is \(q\). To simplify the notation we relabel the variables as \(q, t_1, \ldots, t_N\) and the exponents as \(i \in \mathbb{Z}\) for \(q\) and \(m \in \mathbb{Z}^N\) for \(t_1, \ldots, t_N\). For example, with this relabeling (19) becomes
\[(23)\quad Z_C(u, t, T) = \prod_{i \in \mathbb{Z}, m \in \mathbb{Z}^N, d \geq 1} (1 - u q^i t^m T^d)^{-v_{d,i,m}}.\]

Theorem 4. The following identity holds
\[(24)\quad \text{Log}(Z_C(X, t, T)) = N_X(q) \text{Log}(Z_C(\bullet, t, T)).\]

Proof: The claim is a simple consequence of the third form (21) of our main formula. If \(N_X(q) = \sum_j n_j q^j\) then
\[Z(X, T) = \prod_j (1 - q^j T)^{-n_j}.\]
Hence by (21)

\[ Z_{C}(X, t, T) = \prod_{j \in \mathbb{Z}} Z_{C}(q^j, t, T)^{n_j} \]

\[ = \prod_{i, j, m \in \mathbb{Z}, d \geq 1} (1 - q^{i+j} t^m T^d)^{-n_{j \nu_{d,i,m}}} \]

\[ = \prod_{k \in \mathbb{Z}, m \in \mathbb{Z}, d \geq 1} (1 - q^k t^m T^d)^{-\sum_{i+j=k} n_{j \nu_{d,i,m}}} . \]

Hence

\[ \log(Z_{C}(X, t, T)) = \sum_{k \in \mathbb{Z}, m \in \mathbb{Z}, d \geq 1} \sum_{1+i+j=k} n_{j \nu_{d,i,m}} q^k t^m T^d \]

which equals the right hand side of (24).}

\[ \square \]

3. Applications

3.1. Unipotent matrices. We consider the coloring data \( \mathcal{C} = \mathcal{P} \) with the usual degree function \( |\cdot| \) but with a non-trivial weight function. For all results and concepts related to partitions our reference will be [7], whose notation we will follow.

Let \( X = G_{\alpha} \) and \( \Lambda \) a coloring of \( X/\mathbb{F}_q \) corresponding to a conjugacy class \( c \) in \( M_n(\mathbb{F}_q) \). The centralizer \( z_c \) of \( c \) in \( G_n := GL_n(\mathbb{F}_q) \) has order \[ \prod_{\{x\}} a_{\lambda(x)}(q^{d(x)}), \]

where, as before, \( \{x\} \) runs through the Frobenius orbits, \( d(x) \) is the size of \( \{x\} \) and where for \( \lambda \in \mathcal{P} \)

\[ a_{\lambda}(q) := q^{|\lambda| + 2n(\lambda)} b_{\lambda}(q^{-1}), \]

with

\[ n(\lambda) := \sum_{i \geq 1} (i - 1) \lambda_i \]

\[ b_{\lambda}(q) := \prod_{i \geq 1} \phi_{m_i(\lambda)}(q) \]

\[ \phi_{m}(q) := (1 - q)(1 - q^2) \cdots (1 - q^m) \]

and, finally, \( m_i(\lambda) \) is the multiplicity of \( i \) in \( \lambda \).
It follows that if we define our weight function as
\[ W(\lambda) := a_\lambda(q)^{-1} \in R \]
where \( R = \mathbb{Z}[[q]][q^{-1}] \) then
\[ \sum_{\Lambda / \mathbb{F}_q, |\Lambda| = n} W(\Lambda) = 1 \]
and therefore
\[ Z_C(\mathbb{G}_m, q, T) = \sum_{n \geq 0} T^n = (1 - T)^{-1}. \]

Applying (24) to this situation we find that
\[ Z_C(\bullet, q, T) = \prod_{n \geq 1} (1 - q^n T), \]

since \( N_{\mathbb{G}_m} = q - 1 \) and \((q - 1)^{-1} = -(1 + q + q^2 + \cdots)\); since \( N_{\mathbb{G}_a} = q \) by (24) we also have the identity
\[ Z_C(\mathbb{G}_a, q, T) = \prod_{n \geq 1} (1 - q^n T). \]

On the other hand, for \( X = \mathbb{G}_a \) we have
\[ \sum_{\Lambda / \mathbb{F}_q, |\Lambda| = n} W(\Lambda) = \frac{|M_n(\mathbb{F}_q)|}{|G_n|} = \frac{q^{2n(n+1)}}{(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)} \]
and we have therefore proved the following identity of Euler
\[ \sum_{n \geq 0} q^{2n(n+1)} T^n (q^n - 1)(q^{n-1} - 1) \cdots (q - 1) = \prod_{n \geq 1} (1 - q^n T). \]

If, instead, \( X = \bullet \) we obtain
\[ \sum_{|\Lambda| = n} \frac{1}{a_\lambda(q)} = \frac{u_n}{|G_n|}, \]
where \( u_n \) is the number of unipotent matrices in \( G_n \). Combining (31) with Euler’s identity (33) with \( T \) replaced by \( T/q \) we find
\[ \frac{u_n}{|G_n|} = \frac{q^{2n(n+1)} - n}{(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)} \]
we deduce the known result \( u_n = q^{n^2-n} \) (see [8] for a general result on the number of unipotent elements in linear algebraic groups over finite fields).

### 3.2. Commuting pairs of matrices.

We now consider a weight function arising from the centralizer algebra \( Z_A \) of a matrix \( A \in M_n(F_q) \). It is known that

\[
\dim_{F_q}(Z_A) = \sum_{\{x\}} d(x) \langle \Lambda(x), \Lambda(x) \rangle
\]

where for a partition \( \lambda \) we define \( \langle \lambda, \lambda \rangle := |\lambda| + 2n(\lambda) \).

Since \( |Z_A| \) only depends on the conjugacy class \([A]\) of \( A \), we can count ordered pairs of commuting matrices in \( M_n(F_q) \) as follows

\[
\gamma_n := \# \{ A, B \in M_n(F_q) \mid AB = BA \} = \sum_{[A]} \#[A] |Z_A|,
\]

where \([A]\) runs through the conjugacy classes in \( M_n(F_q) \). Hence if we define

\[
W(\lambda) := \frac{q^{\langle \lambda, \lambda \rangle}}{a_{\lambda}(q)}
\]

then

\[
W(\Lambda) = \frac{\#[A]}{|G_n|} |Z_A|,
\]

where \([A]\) corresponds to the coloring \( \Lambda \) on \( G_n/F_q \), and therefore

\[
\gamma_n = |G_n| \sum_{\Lambda} W(\Lambda).
\]

Consequently,

\begin{equation}
Z_C(G_n, q, T) = \sum_{n \geq 0} \frac{\gamma_n}{|G_n|} T^n.
\end{equation}
On the other hand,
\[
Z_C(\bullet, q, T) = \sum_{\lambda} \frac{q^{\langle \lambda, \lambda \rangle}}{a_\lambda(q)} T^{\langle \lambda \rangle} = \sum_{\lambda} \frac{T^{\langle \lambda \rangle}}{b_\lambda(q^{-1})} = \prod_{i \geq 1} \sum_{m_i \geq 0} T^{m_i} \phi_{m_i}(q^{-1}) = \prod_{i, n \geq 1} (1 - q^n T^i)
\]
using Euler's identity (33). Applying (21) we recover (in an equivalent form) a result of Feit and Fine [1]
\[
\sum_{n \geq 0} \frac{\gamma_n}{|G_n|} T^n = \prod_{i, n \geq 1} (1 - q^{n+1} T^i).
\]
Similarly, we obtain
\[
\sum_{n \geq 0} \frac{\gamma'_n}{|G_n|} T^n = Z_C(G_m, q, T),
\]
where
\[
\gamma'_n := \#\{ A \in \text{GL}_n(F_q), B \in M_n(F_q) | AB = BA \}.
\]
Again by (21) we find
\[
Z_C(G_m, q, T) = \prod_{i, n \geq 1} \left( \frac{1 - q^{n+1} T^i}{1 - q^n T^i} \right) = \prod_{i \geq 1} (1 - q^i T)^{-1}.
\]
We now recognize this generating series as (18) and conclude that \(\gamma'_n/|G_n|\) is the number of conjugacy classes in \(M_n(F_q)\). This, in fact, can be proved directly by a simple application of Burnside's lemma to \(\text{GL}_n(F_q)\) acting on \(M_n(F_q)\) by conjugation. By our main combinatorial principle, this means that we can run the argument backwards and prove (35) starting from (18).

References

[3] J. A. Green, The characters of the finite general linear groups, 

[4] T. Hausel, E. Letellier and F. Rodríguez-Villegas, in 
preparation.

[5] T. Hausel and F. Rodríguez-Villegas, On the E-polynomial of 
certain character varieties, math.AG/0612668.

[6] I. G. Macdonald, Numbers of conjugacy classes in some finite 

Second edition, With contributions by A. Zelevinsky, Oxford Math-

[8] R. Steinberg, “Endomorphisms of linear algebraic groups”, Mem-
oirs of the American Mathematical Society 80, American Mathematic-
sical Society, Providence, R.I., 1968.

Department of Mathematics
University of Texas at Austin
1 University Station, C1200
Austin, Texas 78712-1082
USA
E-mail address: villegas@math.utexas.edu