Elias S. Cleusters
Lars Felix Lerner

Diagonalizable matrices over finite fields

Notation

p	a prime number
n	a natural number
$\mathbb{F}_p$	a field with p elements
$\mathbb{F}_p^{n\times n}$	$n \times n$ matrices over $\mathbb{F}_p$
$\mathrm{GL}_n(p)$	general linear group over $\mathbb{F}_p$
$\mathrm{geom}(D, \lambda)$	geometric multiplicity of λ
$\Xi(n)$	partition function of n
$\mathcal{Z}_k(n)$	some particular partition of n

For example:

$$\Xi(3) = 3$$
$$\mathcal{Z}_1(3) = (1, 1, 1)$$
$$\mathcal{Z}_2(3) = (1, 2)$$
$$\mathcal{Z}_3(3) = (3)$$

diagonalizable matrices

Theorem

The number of diagonalizable $n \times n$ matrices over F_p is:

$$\#\text{diag'ble}\left(\mathbb{F}_p^{n\times n}\right) = \sum_{D\in \mathrm{diag}(\lambda_1,\ldots,\lambda_s)} \frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|G_D|} = \prod_{i=0}^{n-1}(p^n - p^i) \cdot \sum_{\substack{k=1 \\ |\mathcal{Z}_k(n)| \le p}}^{\Xi(n)} \frac{\binom{p}{|\mathcal{Z}_k(n)|}}{\prod_{j\in \mathcal{Z}_k(n)} \prod_{i=0}^{j-1}(p^j - p^i)}$$

Consider the following group action:

$$\psi : \mathrm{GL}_n(p) \times \mathbb{F}_p^{n\times n} \to \mathbb{F}_p^{n\times n}$$
$$(S, A) \mapsto SAS^{-1}$$

Let us look at the diagonal matrices $\mathrm{diag}(\lambda_1, \ldots \lambda_n) \subset \mathbb{F}_p^{n\times n}$ and their stabilizers. Let D be a diagonal matrix.

$$G_D = \{S \in \mathrm{GL}_n(p) \mid SDS^{-1} = D\}$$

Each diagonal matrix can be split up into eigenvalue blocks $\lambda_1, \ldots, \lambda_s$.

$$D = \left(\begin{array}{ccc|ccc} \lambda_1 & & 0 & 0 & \ldots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \lambda_1 & 0 & \ldots & 0 \\ \hline 0 & \ldots & 0 & \lambda_2 & & 0 \\ \vdots & & \vdots & & \ddots & \\ 0 & \ldots & 0 & 0 & & \lambda_s \end{array}\right)$$

Let $B = \bigcup_{i=1}^{s} B_i$ where B_i is a basis of $\mathrm{Eig}(D, \lambda_i)$. We want to find all bases C such that D is stable under a change of basis ${}^{B}\mathrm{id}^{C}$.

Lemma

D is stable under conjugation with ${}^{B}\mathrm{id}^{C}$ iff $(B_i)_C \subset \mathrm{Eig}(D, \lambda_j)$ for all $1 \le i \le s$.

Proof. Let us assume there exists some i with $1 \le i \le s : (B_i)_C \not\subset \mathrm{Eig}(D, \lambda_i)$.
Let $c \in C$ such that $c = c_{ki} + c_m$ where $c_{ki} \in \mathrm{Eig}(D, \lambda_i)$ and $c_m \notin \mathrm{Eig}(D, \lambda_i)$.

$$c = \sum_j \mu_{kji} b_{j,i} + \sum_l \kappa_l b_l$$

Because $b_{j,i}$ and b_l have different eigenvalues:

$${}^{C}\mathrm{id}^{B\,B} f^{B\,B}\mathrm{id}^{C}(c) = {}^{C}\mathrm{id}^{B\,B} f^{B\,B}\mathrm{id}^{C}(c_{ki}) + {}^{C}\mathrm{id}^{B\,B} f^{B\,B}\mathrm{id}^{C}(c_m) \neq (D)_{\bullet,k_i}$$

One can easily show that "$\Leftarrow$" is true. □

To prevent counting the same diagonalizable matrix multiple times let $S, T \in \mathrm{GL}_n(p)$:

$$\begin{aligned} &S^{-1}DS = T^{-1}DT \\ \Leftrightarrow &T \in G_D S \end{aligned}$$

Since $|G_D S| = |G_D|$ it follows that:

$$|\mathrm{GL}_n(p)| = |G_D| \cdot |G.D| \Leftrightarrow |G.D| = \frac{|\mathrm{GL}_n(p)|}{|G_D|}$$

We sum the orbits of all the diagonalmatrices in $\mathbb{F}_p^{n \times n}$.

$$\#\text{diag'ble}\left(\mathbb{F}_p^{n\times n}\right) = \sum_{D \in \mathrm{diag}(\lambda_1,\ldots,\lambda_s)} \frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|G_D|} = \sum_{D \in \mathrm{diag}(\lambda_1,\ldots,\lambda_s)} \frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{\frac{n!}{\prod_{i=1}^{s} \mathrm{geom}(D,\lambda_i)!} \cdot \prod_{i=1}^{s} \#\mathrm{bases}(\mathrm{Eig}(D, \lambda_i))}$$

Because of our Lemma the size of a stabilizer is the number of ordered eigenvector bases. The term

$$\frac{n!}{\prod_{i=1}^{s} \operatorname{geom}(D,\lambda_i)!}$$

arises because we can permute the eigenspaces.
In our formula we do not use the specific eigenvalue. We just care how many eigenspaces there are and what their dimension is. In other words: the dimensions of the eigenspaces partition n. That means for each partition $k \leq \Xi(n)$ we have a partition into $|\mathcal{Z}_k(n)|$ eigenspaces, where the dimension of each eigenspace is given by the elements of $\mathcal{Z}_k(n)$.
We have

$$\frac{n!}{\prod_{i=1}^{s} \operatorname{geom}(D,\lambda_i)!} = \frac{n!}{\prod_{j\in\mathcal{Z}_k(n)} j!}$$

Since we neglected the eigenvalues themselves we need to account for the number of different eigenvalues that are possible. We have:

$$\begin{aligned}
\#\text{diag'ble}\left(\mathbb{F}_p^{n\times n}\right) &= \sum_{\substack{k=1\\ |\mathcal{Z}_k(n)|\leq p}}^{\Xi(n)} \binom{p}{|\mathcal{Z}_k(n)|} \frac{p!\cdot n!}{(p-|\mathcal{Z}_k(n)|)! \prod_{j\in\mathcal{Z}_k(n)} j!} \cdot \frac{|\mathrm{GL}_n(\mathbb{F}_p)|\cdot \prod_{j\in\mathcal{Z}_k(n)} j!}{n! \prod_{j\in\mathcal{Z}_k(n)} \prod_{i=0}^{j-1} p^j - p^i}\\
&= |\mathrm{GL}_n(\mathbb{F}_p)| \cdot \sum_{\substack{k=1\\ |\mathcal{Z}_k(n)|\leq p}}^{\Xi(n)} \frac{\binom{p}{|\mathcal{Z}_k(n)|}}{\prod_{j\in\mathcal{Z}_k(n)} \prod_{i=0}^{j-1}(p^j-p^i)}\\
&= \prod_{i=0}^{n-1}(p^n-p^i) \cdot \sum_{\substack{k=1\\ |\mathcal{Z}_k(n)|\leq p}}^{\Xi(n)} \frac{\binom{p}{|\mathcal{Z}_k(n)|}}{\prod_{j\in\mathcal{Z}_k(n)} \prod_{i=0}^{j-1}(p^j-p^i)}
\end{aligned}$$

If $|\mathcal{Z}_k(n)| > p$ we have an invalid partition since there are not enough numbers in $\mathbb{F}_p$ to partition n.

2×2 matrices

For 2×2 matrices we have $\Xi(2) = 2$ and $\mathscr{Z}_1(2) = (1,1), \mathscr{Z}_2(2) = (2)$.
Plugging this into our formula yields:

$$\begin{aligned}
\#\text{diag'ble}\left(\mathbb{F}_p^{2\times 2}\right) &= (p^2-1)(p^2-p)\cdot\left(\frac{\binom{p}{2}}{(p-1)(p-1)} + \frac{\binom{p}{1}}{(p^2-1)(p^2-p)}\right) \\
&= (p^2-1)(p-1)p\cdot\frac{p(p-1)}{2(p-1)^2} + p = \frac{(p^2-1)\cdot p^2 + 2p}{2} = \frac{p^4-p^2+2p}{2}
\end{aligned}$$