ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Образовательная программа «Прикладная математика и информатика»

Отчет об исследовательском проекте на тему:
Тотальный граф кольца матриц: исходящие степени вершин подграфов

Выполнил:
студент группы БПМИ215

Шешеня Данил Сергеевич  25.05.2023
(подпись) (дата)

Принял руководитель проекта:
Промыслов Валентин Валерьевич
Научный сотрудник
Факультета компьютерных наук НИУ ВШЭ


(подпись) 25.05.2023
(дата)

Москва 2023

Содержание

1 Введение

Тотальным графом кольца квадратных матриц над полем называется граф, множеством вершин которого являются сами матрицы, а ребра соединяют в точности те вершины, сумма которых является вырожденной матрицей. До недавнего времени задачи описания автоморфизмов тотального графа была открыта. Одним из подходов к решению этой задачи может состоять в изучении чисел, определённых ниже.

Пусть n – натуральное число и $\mathbb{F}$ – конечное поле (из q элементов) характеристики не 2. Обозначим через $\mathcal{J}_r$ множество $n \times n$ матриц ранга r над полем $\mathbb{F}$. Также для $0 \leqslant i \leqslant n$ и произвольной матрицы $A \in \mathcal{J}_i$ обозначим:

$$d_{ik}(n) = |\{B \in \mathcal{J}_k \mid A + B \text{ – вырождена}\}|$$

Отметим, что числа $d_{ik}(n)$ не зависят от выбора матрицы $A \in \mathcal{J}_i$ (но, конечно, зависят от поля $\mathbb{F}$).

Оказывается, что эти числа тесно связаны задачей описания автоморфизмов тотального графа. Задачей проекта является изучение свойств этих чисел.

1.1 Объект исследования

Числа $d_{ij}(n)$.

1.2 Цель проекта

Изучить свойства чисел $d_{ij}(n)$.

1.3 Задачи проекта

Написать программу и вычислить числа $d_{ij}(n)$ для малых значений параметров.

2 Терминология

Пусть $\mathbb{F}_q$ – конечное поле из q элементов. Далее, мы будем рассматривать матрицы только над полем $\mathbb{F}_q$.
Будем обозачать множество квадратных $n \times n$ матриц M_n.

Определение 1. $\mathcal{J}_r(n) = \{A \in M_n \mid \operatorname{rk} A = r\}$ – множество матриц $n \times n$ ранга r.

Замечание. В тексте иногда будет опускаться зависимость от n, подразумевая, что у нас уже зафиксировано некоторое n.

Замечание. Также иногда будет использоваться $\mathcal{J}_r$ в контексте количества таких матриц, а не их множества, то есть такая запись равносильна $|\mathcal{J}_r|$.

Определение 2. Тотальным графом кольца $n \times n$ матриц над полем $\mathbb{F}_q$ назовем граф $\mathcal{T}_n(\mathbb{F}_q)$, множество вершин которого состоит из всех квадратных $n \times n$ матриц ($V = M_n$), а две матрицы соединены ребром, если и только если их сумма вырождена, при этом петель и кратных ребер в графе нет ($E = \{(A, B) \in M_n \times M_n \mid A \neq B, \det(A + B) = 0\}$).

Определение 3. Рассмотрим $n \times n$ матрицу $A \in \mathcal{J}_i$. Тогда введем

$$d_{ij}(n) = |\{B \in \mathcal{J}_j \mid \det(A + B) = 0\}|$$

Замечание. В терминах тотального графа, это понятие можно проинтерпретировать так. Разобьем множество вершин на $n + 1$ непересекающихся долей – матрицы ранга от 0 до n. Тогда $d_{ij}(n)$ будет степенью вершины, находящейся в доле матриц с рангом i в доле матриц с рангом j. Однако стоит сделать оговорку на на то, что если $i = j < n$, то настоящая степень будет на 1 меньше, чем $d_{ii}(n)$, так как в графе по определению запрещены петли, но A вырождена, значит $A + A$ тоже вырождена и посчитается в $d_{ii}(n)$.

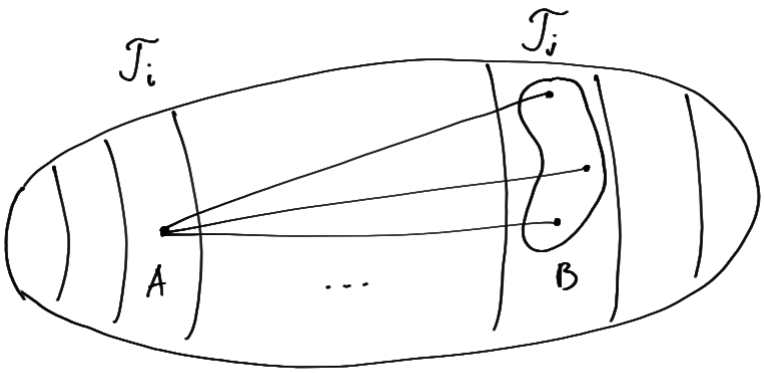

Рис. 1. Иллюстрация $d_{ij}(n)$ в терминах графа

Замечание. Можно заметить, что в обозначении не учавствует матрица A. Оказывается, что $d_{ij}(n)$ не зависит от матрицы A, и это будет доказано далее.

Определение 4. Введем отдельное обозначение для числа невырожденных матриц – γ_n. Также иногда будет использоваться нотация $|GL_n|$

3 Вступление

Для начала, нам необходимо уметь считать количество матриц с некоторыми свойствами над конечным полем, прежде всего – это число невырожденных матриц и матриц фиксированного ранга. Иными словами, знать явную формулу для введеных выше γ_n и $\mathcal{J}_k$. Также, мы установим несколько несложных свойств графа и чисел d_{ij}.

3.1 Найти число невырожденных $n \times n$ матриц над $\mathbb{F}_q$

Утверждение 3.1.

$$\gamma_n = (q^n - 1) \cdot \ldots \cdot (q^n - q^{n-1})$$

Доказательство. Будем действовать таким образом. Выберем первую строку матрицы – она может быть любой, за исключением нулевой, так как тогда матрица уже будет вырожденной. Вторая строка тоже должна быть ненулевой, но еще она должна быть непропорциональна первой, так как тогда тоже определитель сразу будет равен нулю. Так, у нас есть $q^n - 1$ способ для первой строки и $q^n - q$ способов для второй.
Аналогичными рассуждениями, i-тая строка не должна линейно выражаться через предыдующие, поэтому у нас есть $q^n - q^{i-1}$ способов для нее.
Очевидно, что это необходимое условие невырожденности, но можно доказать, что оно достаточно. Предположим, что система строк линейно зависима, тогда рассмотрим линейную комбинацию $(\alpha_1, \ldots, \alpha_n) \neq (0, \ldots, 0)$, зануляющую ее и найдем в ней ненулевой элемент a_j с наибольшим номером. Так как он наибольший, все $\alpha_k = 0$ для $k > j$, но тогда можно выразить $A_{(j)} = -\frac{\alpha_1}{\alpha_j} A_{(1)} - \ldots - \frac{\alpha_{j-1}}{\alpha_j} A_{(j-1)}$ через предыдующие строки, что есть противоречие ■

3.2 Найти число матриц ранга r среди матриц размера $n \times n$ над $\mathbb{F}_q$

Для начала, нам потребуется находить число k-мерных подпространств.

Лемма 3.2. Над n-мерным пространством существует $\dfrac{(q^n - 1)(q^n - q) \ldots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \ldots (q^k - q^{k-1})}$ k-мерных подпространств

Доказательство. Таким же способом, как мы искали число невырожденных матриц, можно найти количество линейно независимых систем из k векторов. Отличие только в том, что мы заканчиваем процесс на k-ом векторе, вместо того, чтобы набирать их n штук. Получаем формулу: $(q^n - 1) \ldots (q^n - q^{k-1})$.
Если мы хотим посчитать число неупорядоченных наборов (или подмножеств) векторов, то необходимо дополнительно поделить на $k!$, так как именно столько перестановок мы можем получить.
Теперь, мы знаем, что каждый такой набор порождает какое-то k-мерное подпространство. Однако реально подпространств меньше, потому что одно подпространство может порождаться несколькими разными наборами. А именно, можно взять любой линейно независимый набор из k векторов в этом k-мерном подпространстве и получить его базис. Так, искомым количеством подпространств будет количество наборов из k векторов в n-мерном пространстве, поделенное на количество наборов из k векторов в k-мерном подпространстве.

$$\frac{\frac{(q^n-1)\ldots(q^n-q^{k-1})}{k!}}{\frac{(q^k-1)\ldots(q^k-q^{k-1})}{k!}} = \frac{(q^n - 1) \ldots (q^n - q^{k-1})}{(q^k - 1) \ldots (q^k - q^{k-1})}$$

■

Утверждение 3.3.

$$\mathcal{J}_r(n) = \frac{(q^n-1)^2 \cdot \ldots \cdot (q^n-q^{r-1})^2}{(q^r-1) \cdot \ldots \cdot (q^r-q^{r-1})}$$

Доказательство. Теперь, если мы зафиксируем n-мерное векторное пространство $V = \mathbb{F}^n$ и какой-нибудь базис в нем, то вместо матриц ранга r можно посчитать число линейных отображений $V \to V$ ранга r. А отображение ранга r мы получим так – возьмем r-мерное подпространство в $\mathbb{F}^n$ и зададим отображение на нем, причем сделаем это сюръективно, а это равносильно тому, что его матрица имеет ранг, равный числу столбцов. Итак, число таких матриц (отображение из $\mathbb{F}^n$ в $\mathbb{F}^r$, поэтому матрица $n \times r$) есть просто количество линейно независимых наборов из r n-мерных векторов, а подобные объекты мы уже неоднократно считали. Их число равно $(q^n-1)\ldots(q^n-q^{r-1})$.
Эту величину нужно умножить на количество всех r-мерных подпространств. Разумеется, если задать отображения на разных подпространствах, то они заведомо не могут совпадать, то есть $\operatorname{Im}\varphi \neq \operatorname{Im}\psi \implies \varphi \neq \psi$. ■

3.3 Доказать, что выбор матрицы A не влияет на $d_{ij}(n)$

Лемма 3.4. Для любых матриц A, A' одного ранга существует представление $A' = UAV$, где U, V – некоторые невырожденные матрицы

Доказательство. Довольно очевидно следует из классических фактов линейной алгебры. Приведение к улучшенному ступенчатому виду элементарными преобразованиями строк выражается умножением слева на некоторую невырожденную матрицу. Однако мы можем получить разные виды, например, единицы могут находиться в разных столбцах. Поэтому, требуется умножение на матрицу справа, соответствующую элементарным преобразованиям столбцов. ■

Обозначим за $f(A)$ множество матриц B ранга j, таких, что $\det(A+B) = 0$, то есть те матрицы, которые мы учли для подсчета $d_{ij}(n)$ с матрицей A.

Утверждение 3.5.

$$\forall A, A' \in \mathcal{J}_i \quad |f(A)| = |f(A')|$$

Выразим A' как UAV и применим такое же отображение к $f(A)$. Если $B \in f(A)$, то $\det(UAV + UBV) = \det U \cdot \det(A+B) \cdot \det V = 0$, значит $UBV \in f(A')$. Но $\det U, \det V \neq 0$, поэтому $UBV \in f(A') \iff B \in f(A)$. Наконец, раз U, V – невырожденные, то отображение $B \mapsto UBV$ биективно и $\operatorname{rk} B = \operatorname{rk}(UBV)$ – это известный факт. Это означает, что $\{UBV \mid B \in \mathcal{J}_j\} = \mathcal{J}_j$, а из этого следует, что $|f(A)| = |f(A')|$. ■
В терминах графа это означает, что у всех вершин из одной доли одинаковая степень в какой-нибудь другой доле. Этот факт очень полезен, потому что теперь мы вправе выбирать удобные нам матрицы A для подсчета $d_{ij}(n)$.

3.4 Найти степень вершины графа

Утверждение 3.6.

$$\sum_{j=0}^{n} d_{ij}(n) = \gamma_n$$

Доказательство. Пусть зафиксирована матрица A – вершина, степень которой мы ищем. Нам требуется найти количество матриц B, таких, что $A + B$ вырождена. Переберем все вырожденные матрицы C и рассмотрим $B = C - A$. Это единственный способ получить конкретную матрицу C для текущего A, и каждую матрицу C так можно получить. Поэтому, количество матриц B в точности совпадает с числом матриц C. Матриц C у нас известное количество – γ_n ■

Однако это не совсем честная степень вершины. Если $\operatorname{rk} A < n$, то мы посчитаем таким образом вершину саму с собой, но петли в нашем графе запрещены. Поэтому, в таком случае надо отнять 1.
Получается, что все вершины в графе имеют почти одинаковую степень, только невырожденные вершины имеют степень на 1 больше чем остальные.

3.5 Переход от $d_{ij}(n)$ к $d_{ji}(n)$

Утверждение 3.7.

$$i \neq j \implies d_{ij}(n) \cdot |\mathcal{J}_i| = d_{ji}(n) \cdot |\mathcal{J}_j|$$

Доказательство. Рассмотрим подграф в тотальном графе, где из вершин мы оставим доли $\mathcal{J}_i$ и $\mathcal{J}_j$, а из ребер оставим только ребра, у которых один конец лежит в одной доле, а второй в другой. Получим двудольный граф. Мы уже установили, что у всех вершин в левой доле в этом графе одинаковая степень (в 3.3), так же как и у вершин правой доли. Тогда можно посчитать число ребер как число вершин слева, умноженное на степень вершины. Или можно сделать то же с другой стороны – число вершин справа, умноженное на степень вершины справа. Из этого и следует формула: $|\mathcal{J}_i|$ – это число вершин слева, $d_{ij}(n)$ – степень одной вершины. ■

3.6 Linear derangements

В статье [2] есть упоминание об интересном объекте – классе матриц, который в оригинале называется linear derangements, что на русский язык можно перевести как “линейные беспорядки”.

Определение 5. $A \overset{def}{\iff}$ линейный беспорядок, если $\det A \neq 0, \quad Av \neq v \quad \forall v \neq 0$

Можно сформулировать альтернативное определение – у матрицы нет собственных значений 0 (гарантирует невырожденность) и 1 (гарантирует условие $Av \neq v$).
Это понятие тесно связано с $d_{n,n}(n)$. Мы уже доказывали, что можем взять любую матрицу ранга n в качестве A, в частности можем взять $-E$. В таком случае, $d_{n,n}(n)$ равно количеству B таких, что $\det B \neq 0, \det(B - E) = 0$, то есть матриц, у которых 0 – не собственное значение, 1 – собственное значение
Если обозначить число линейных беспорядков $n \times n$ за e_n, то будет справедлива формула $d_{nn}(n) = \gamma_n - e_n$, так как d_{nn} включает собственное значение 1, а e_n наоборот исключает, нам нужно их дополнение в классе невырожденных матриц, число которых мы обозначили за γ_n.
В упомянутой выше статье приводится рекуррентная формула для e_n, которая выглядит так:

$$e_n = e_{n-1} \cdot (q^n - 1)q^{n-1} + (-1)^n q^{n(n-1)/2}, \quad e_0 = 1$$

Наличие такой формулы намекает на существование рекуррентной формулы для $d_{nn}(n)$.

3.7 Значение $d_{ij}(n)$ при $i + j < n$

Утверждение 3.8.

$$i + j < n \implies d_{ij}(n) = \mathcal{J}_j$$

Доказательство. Из курса линейной алгебры известно, что ранг субаддитивен: $\operatorname{rk}(A + B) \leqslant \operatorname{rk} A + \operatorname{rk} B$. В нашем случае $\operatorname{rk} A = i, \operatorname{rk} B = j$, поэтому $\operatorname{rk}(A + B) \leqslant i + j < n \iff \det(A + B) = 0$. Поэтому нам подойдет любая матрица B, коих $\mathcal{J}_j$ штук. ■

Так, если рассматривать $d_{ij}(n)$ как таблицу или матрицу с индексами i, j, то мы уже заполнили все ячейки ниже диагонали. Одной из наших следующих целей будет вывод формулы для ячеек на диагонали, то есть при $i + j = n$, а также для $(1, n)$, что выше диагонали.

4 Формула для $d_{1n}(n)$

Нашей первой целью будет выведение явной формулы для $d_{1n}(n)$.

Теорема 4.1.

$$d_{1n}(n) = q^{n-1}(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1})$$
$$d_{n1}(n) = \frac{q^{2n-1} - q^{n-1}}{q-1}$$

Доказательство. Будем считать $d_{n1}(n)$, а $d_{1n}(n)$ потом выразим по формуле $d_{ij}(n)\mathcal{J}_i = d_{ji}(n)\mathcal{J}_j$
В качестве матрицы A возьмем единичную, B – это все матрицы ранга 1. Матрицы ранга 1 представляются как столбец умноженный на строку, скажем, $B = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1 & \dots & b_n \end{pmatrix}$.

Лемма 4.2. $\det(B+E) = 1 + \sum_{i=1}^{n} a_i b_i$

Доказательство. Докажем по индукции.
База – $n = 1 \implies |a_1 b_1 + 1| = a_1 b_1 + 1$
Переход: рассмотрим два случая: когда первая строка матрицы $B+E$ имеет вид $\begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$, и когда имеет другой вид

1. В таком случае, можем разложить определитель по первой строке

$$\det(B+E) = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ a_2b_1 & a_2b_2+1 & a_2b_3 & \dots & a_2b_n \\ a_3b_1 & a_3b_2 & a_3b_3+1 & \dots & a_3b_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & a_nb_3 & \dots & a_nb_n+1 \end{vmatrix} = \begin{vmatrix} a_2b_2+1 & a_2b_3 & \dots & a_2b_n \\ a_3b_2 & a_3b_3+1 & \dots & a_3b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nb_2 & a_nb_3 & \dots & a_nb_n+1 \end{vmatrix}$$

   У получившейся матрицы определитель равен $a_2b_2 + \dots + a_nb_n + 1$ по предположению индукции. Из этого следует утверждение, так как $a_1b_1 = 0$

2. Разобьем определитель по первой строке в сумму двух

$$\det(B+E) = \begin{vmatrix} a_1b_1+1 & a_1b_2 & a_1b_3 & \dots & a_1b_n \\ a_2b_1 & a_2b_2+1 & a_2b_3 & \dots & a_2b_n \\ a_3b_1 & a_3b_2 & a_3b_3+1 & \dots & a_3b_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & a_nb_3 & \dots & a_nb_n+1 \end{vmatrix} =$$

$$= \begin{vmatrix} a_1b_1 & a_1b_2 & a_1b_3 & \dots & a_1b_n \\ a_2b_1 & a_2b_2+1 & a_2b_3 & \dots & a_2b_n \\ a_3b_1 & a_3b_2 & a_3b_3+1 & \dots & a_3b_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & a_nb_3 & \dots & a_nb_n+1 \end{vmatrix} + \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ a_2b_1 & a_2b_2+1 & a_2b_3 & \dots & a_2b_n \\ a_3b_1 & a_3b_2 & a_3b_3+1 & \dots & a_3b_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & a_nb_3 & \dots & a_nb_n+1 \end{vmatrix}$$

У первой матрицы первая строка ненулевая (нулевые разобраны в пункте 1), значит можно прибавить ее ко всем остальным строкам с коэффициентом $-\frac{a_i}{a_1}$, отчего определитель не изменится. $a_1 \neq 0$, так как иначе первая строка была бы нулевой. После такого преобразования матрица следующий вид:

$$\begin{vmatrix} a_1b_1 & a_1b_2 & a_1b_3 & \dots & a_1b_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix}$$

Матрица верхнетрегольная, и ее определитель равен a_1b_1.

Вторая матрица нам уже встречалась в предыдущем пункте, ее определитель равен $a_2b_2 + \ldots + a_nb_n + 1$. Получаем верное равенство

■

Далее нам потребуется уметь находить количество следующих объектов:

Определение 6. $S(n,k)$ – количество упорядоченных последовательностей $(a_1, \ldots, a_n)$, где $a_1 + \ldots + a_n = k,\ a_i \in \mathbb{F}_q \setminus \{0\},\ k \in \mathbb{F}_q$

Заметим, что на $S(n,k)$ верна следующая рекуррентная формула:

$$S(n,k) = \sum_{a \in \mathbb{F}_q \setminus \{0\}} S(n-1, k-a)$$

То есть, мы можем взять первым элементом произвольное ненулевое число a, тогда хвост должен иметь $n-1$ число и сумму $k-a$.
Также заметим, что если $k=0$, то множество $\{k-a\}$ не содержит нуля, а если $k \neq 0$, то содержит ровно один ноль.
Используя этот факт можно доказать, что если $k \neq 0$, то все $S(n,k)$ равны для фиксированного n. Утверждение верно при $n=1$, тогда множество искомых наборов – это просто $\{(k)\}$. Далее по индукции: в сумме присутствует $S(n-1,0)$, а остальные члены – это некоторые

$S(n-1,i)$, где $i \neq 0$, а они все равны по предположению. Значит, при $k \neq 0$ $S(n,k)$ просто состоят из одинаковых слагаемых
Далее, мы будем использовать только обозначения $S(n,0), S(n,1)$, где $S(n,1) := S(n,k),\ k \neq 0$
Из написанного выше следуют следующие формулы:

$$S(n,0) = (q-1)S(n-1,1)$$
$$S(n,1) = S(n-1,0) + (q-2)S(n-1,1)$$

Если сложить $S(n,k)$ по всем k от 0 до $q-1$, то получатся все последовательности из n ненулевых элементов, коих $(q-1)^n$ штук. Можно решить уравнение и выразить $S(n,0)$

$$S(n,0) + (q-1)S(n,1) = (q-1)^n$$
$$S(n,0) = (q-1)^n - (q-1)S(n,1)$$

Подставим это $S(n,0)$ в формулу для $S(n,1)$ и получим:

$$S(n,1) = (q-1)^{n-1} - (q-1)S(n-1,1) + (q-2)S(n-1,1) = (q-1)^{n-1} - S(n-1,1)$$

Лемма 4.3. $S(n,1) = \dfrac{(q-1)^n - (-1)^n}{q}$

Доказательство. База – $n = 1$ верна
Переход:

$$S(n,1) = (q-1)^{n-1} - S(n-1,1) =$$
$$(q-1)^{n-1} - \left(\frac{(q-1)^{n-1} - (-1)^{n-1}}{q}\right) =$$
$$(q-1)^{n-1} - \frac{(q-1)^{n-1}}{q} - \frac{(-1)^n}{q} =$$
$$\frac{(q-1)^n - (-1)^n}{q}$$

■

Определение 7. $F_z(n,k)$ – число последовательностей $(a_1, \ldots, a_n)$, таких что $a_1 + \ldots + a_n = k,\ a_i \in \mathbb{F}_q$, а также среди a_i-тых ровно z нулей

Лемма 4.4. $F_z(n,k) = \binom{n}{z} S(n-z,1)$ при $k \neq 0$

Доказательство. Выберем позиции для z нулей $\binom{n}{z}$ способами. На остальные позиции расставим $n-z$ ненулевых чисел. Их сумма должна быть равна k, так как у нулевых чисел сумма ноль, а так как $k \neq 0$, их число равно $S(n-z,1)$ ■

Теперь, пусть у нас есть последовательность $c_1, \ldots, c_n$ с суммой -1 (в поле $\mathbb{F}_q$). Найдем число способов выбрать a_i, b_i так, что $c_i = a_i b_i$
Если $c_i = 0$, то у нас есть $2q-1$ способ выбрать a_i, b_i, так как подходят пары вида $x \cdot 0, 0 \cdot y$. x и y может быть любым, однако пара $(0,0)$ лежит и там, и там, поэтому ее надо вычесть

Если $c_i \neq 0$, то подходят пары вида $x \cdot (x^{-1} \cdot c_i)$, где x – любое, однако x не может быть нулем, так как он необратим. Поэтому получаем $q-1$ вариант
Из столбца и строки можно выносить ненулевые скаляры, поэтому каждая матрица ранга 1 представляется $q-1$ способами. Надо дополнительно поделить на $q-1$.
Наконец, можем воедино собрать формулу

$$d_{n1}(n) = \frac{1}{q-1}\sum_{z=0}^{n}\binom{n}{z}\frac{(q-1)^{n-z}-(-1)^{n-z}}{q}(2q-1)^z(q-1)^{n-z}$$

Перебирается число нулей, выбирается последовательность из z нулей, и далее есть $2q-1$ вариантов для нулевых и $q-1$ для ненулевых элементов.
Остается последний нюанс – матрицы ранга ноль. К счастью, формула их и так не учитывает, потому что нулевая матрица может посчитаться только в слагаемом $z=n$, однако $F_n(n,-1)=0$ и все слагаемое при $z=n$ будет равно нулю
Но это еще не все – сумму можно упростить

$$\sum_{z=0}^{n}\binom{n}{z}((q-1)^{n-z}-(-1)^{n-z})(2q-1)^z(q-1)^{n-z} =$$
$$\sum_{z=0}^{n}\binom{n}{z}(2q-1)^z((q-1)^{n-z})^2 - \sum_{z=0}^{n}(-1)^{n-z}\binom{n}{z}(2q-1)^z(q-1)^{n-z} =$$
$$\sum_{z=0}^{n}\binom{n}{z}(2q-1)^z(q^2-2q+1)^{n-z} - \sum_{z=0}^{n}\binom{n}{z}(2q-1)^z(1-q)^{n-z} =$$
$$(2q-1+q^2-2q+1)^n - (2q-1+1-q)^n = q^{2n}-q^n$$

Получается следующая формула

$$d_{n1}(n) = \frac{q^{2n}-q^n}{q^2-q} = \frac{q^{2n-1}-q^{n-1}}{q-1}$$

Непосредственна та формула, которую мы искали –

$$d_{1n}(n) = d_{n1}(n)\frac{\mathcal{J}_n}{\mathcal{J}_1} = \frac{(q^{2n}-q^n)(q^n-1)(q^n-q)\dots(q^n-q^{n-1})}{(q^2-q)^{\frac{(q^n-1)^2}{q-1}}} =$$
$$\frac{(q^{2n}-q^n)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})}{q(q^n-1)} =$$
$$\frac{q^n(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})}{q} = q^{n-1}(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})$$

■

Замечание. Формула проверена на $(n,q) \in \{(2,2),(2,3),(2,4),(2,5),(3,2),(3,3),(3,4),(4,2)\}$ путем полного перебора $n \times n$ матриц над $\mathbb{F}_q$

Замечание. Значения формулы на некоторых n и q

n q	2	3	4	5
2	4	18	48	100
3	96	3888	46060	300000
4	10752			

5 Альтернативное доказательство формулы $d_{1n}(n)$

Несколько месяцев спустя после вывода предыдущей формулы я придумал более простое и короткое доказательство. Считаю необходимым поделиться.

Итак, нам надо найти количество невырожденных матриц, таких, что при суммировании с матрицей A ранга 1 получится вырожденная. Возьмем в качестве A матрицу с единственной единицей в левом верхнем углу. Тогда

$$\det(A+B) = \begin{vmatrix} b_{11}+1 & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} = \begin{vmatrix} 1 & 0 & \dots \\ b_{11} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} + \det B$$

Первое слагаемое, после того, как мы разложим определитель по строке, будет является тем, что, называется *дополнительный минор* к элементу $(1,1)$. Будем использовать обозначение $\overline{M}_{i,j}$.

Вспомним классический факт – явная формула для обратной матрицы. Нас будет интересовать ее элемент на позиции $(1,1)$.

$$B^{-1}_{1,1} = \frac{1}{\det B}(-1)^{1+1}\overline{M}_{1,1} \implies \overline{M}_{1,1} = B^{-1}_{1,1} \cdot \det B$$

Подставляем это выражение в исходную формулу

$$\det(A+B) = \det B + B^{-1}_{1,1} \det B = \det B \cdot (B^{-1}_{1,1} + 1)$$

Нас интересуют матрицы B, при которых это выражение равно нулю. $\det B \neq 0$, значит должно быть верно $B^{-1}_{1,1} = -1$. Как найти количество таких матриц?

Заметим, что отображение $B \mapsto B^{-1}$ биективно для невырожденных матриц, а значит можно искать не среди обратных матриц, а среди обычных невырожденных матриц. Другими словами, можно найти просто матрицы, у которых на позиции $(1,1)$ стоит -1 и сказать, что матрицы, для которых наши матрицы являются обратными подходят под условие, и подходят только они.

Но такие матрицы посчитать легко. Поставим на $(1,1)$ число -1, после этого всю первую строку заполним любыми числами. Мы уже не получим никак нулевую строку, разумеется, так как на первой позиции стоит -1. Далее, действуем как в доказательстве формулы для числа невырожденных матриц. Для i-той строки нужно, чтобы она не выражалась через предыдущие $i-1$, поэтому есть $q^n - q^{i-1}$ способов для нее.

Получаем формулу – $q^{n-1}(q^n-q)\dots(q^n-q^{n-1})$. Она в точности совпадает с той, которую мы получили ранее.

6 Формула для $d_{n-r,r}(n)$

Нашей следующей целью будет вывод формулы на случай $i + j = n$

Теорема 6.1.

$$d_{n-r,r}(n) = \frac{(q^n-1)^2 \dots (q^n - q^{r-1})^2 - (q^n - q^{n-r})^2 \dots (q^n - q^{n-1})^2}{(q^r - 1) \dots (q^r - q^{r-1})}$$

Доказательство. Нам будет удобно считать, что B имеет ранг r, а не $n-r$, поэтому посчитаем $d_{n-r,r}$. $d_{r,n-r}$ при необходимости можно получить, воспользовавшись формулой $d_{ij}(n) = \dfrac{d_{ji}(n)\mathcal{J}_j(n)}{\mathcal{J}_i(n)}$ либо сделав замену r на $n-r$.
Итак, B имеет ранг r, A возьмем как диагональную матрицу с $n-r$ единицами в начале.

Лемма 6.2. $\det(A+B)$ равен нижнему правому угловому $r \times r$ минору матрицы B

Доказательство. Докажем по индукции по n. Факт верен для $n = r$, так как тогда матрица A просто является нулевой, а минор матрицы B есть весь определитель. Переход:

$$\begin{vmatrix} b_{11}+1 & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22}+1 & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \dots & b_{n,n} \end{vmatrix} = \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22}+1 & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \dots & b_{n,n} \end{vmatrix} + \begin{vmatrix} 1 & 0 & \dots & 0 \\ b_{21} & b_{22}+1 & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \dots & b_{n,n} \end{vmatrix}$$

У первой матрицы есть $r+1$ строка из исходной матрицы B, которая имеет ранг r, значит эти $r+1$ строки линейно зависимы, $\implies$ определитель первой матрицы равен нулю.
Вторую матрицу раскладываем по первой строке и получаем матрицу $(n-1) \times (n-1)$, для которой можно применить предположение индукции. ■

Теперь нам достаточно посчитать число матриц B, таких что $\operatorname{rk} B = r$ и ее соответствующий минор равен нулю.
Для этого воспользуемся ранговым или скелетным разложением (rank factorization) для B

Определение 8. Для матрицы B ранга r и размера $n \times n$ назовем ранговым разложением представление в виде $B = PQ$, где P – матрица $n \times r$ полного ранга, Q – матрица $r \times n$ полного ранга

Замечание. Если некоторые матрицы P и Q имеют такие размеры и полный ранг, их произведение имеет такой же ранг, то есть $\operatorname{rk} PQ = r \ \forall P, Q$

Лемма 6.3. Для матрицы B существует $|GL_r|$ различных ранговых разложений

Доказательство. Для начала заметим, что если $B = PQ$, то можно получить новое ранговое разложение, если сделать $B = P(RR^{-1})Q = (PR)(R^{-1}Q)$, так как умножение на невырожденную матрицу слева и справа не влияет на ранг. Так можно сделать для любой невырожденной матрицы, поэтому разложений $\geqslant \gamma_r$.
С другой стороны, от любого разложения $B = PQ$ можно перейти к $B = P'Q'$ таким образом. Докажем это.
Мы знаем, что $PQ = P'Q'$. Я хотел бы убрать некоторые столбцы в Q, так чтобы осталось r и они были линейно независимы. Это возможно сделать, так как $\operatorname{rk} Q = r$. Те же столбцы

надо убрать в матрице Q'. Если записать матрицы блочно, то становится очевидно, что так мы просто теряем некоторые равенства в системе уравенений.

$$\begin{bmatrix} p_1^T \\ \vdots \\ p_n^T \end{bmatrix} \begin{bmatrix} q_1 & \dots & q_n \end{bmatrix} = \begin{bmatrix} (p'_1)^T \\ \vdots \\ (p'_n)^T \end{bmatrix} \begin{bmatrix} q'_1 & \dots & q'_n \end{bmatrix} \longmapsto \begin{bmatrix} p_1^T \\ \vdots \\ p_n^T \end{bmatrix} \begin{bmatrix} \tilde{q}_1 & \dots & \tilde{q}_r \end{bmatrix} = \begin{bmatrix} (p'_1)^T \\ \vdots \\ (p'_n)^T \end{bmatrix} \begin{bmatrix} \tilde{q}'_1 & \dots & \tilde{q}'_r \end{bmatrix}$$

Теперь $\tilde{Q}$ – это квадратная матрица, и она невырождена, поэтому можно домножить на ее обратную.

$$P\tilde{Q} = P'\tilde{Q}' \implies P = P'\left(\tilde{Q}'\left(\tilde{Q}\right)^{-1}\right)$$

Получили представление в виде $P = P'R$. Теперь сделаем то же с матрицей P – выкинем строки так, чтобы их осталось r и они были линейно независимы и домножим с обеих сторон на обратную.

$$(P'R)Q = P'Q' \implies P'(RQ) = P'Q' \implies RQ = Q' \implies Q = R^{-1}Q'$$

Из этого факта следует, что с помощью "вставки" невырожденной матрицы и ее обратной в центр может быть получено любое разложение, а значит в неравенстве выше достигается равенство. ■

Этот факт позволяет нам посчитанное число разложений поделить на $|GL_r|$ и получить искомое число матриц.

Представим матрицы P и Q блочно: $P = \begin{pmatrix} U \\ V \end{pmatrix}, Q = \begin{pmatrix} X & Y \end{pmatrix}$, где V, Y имеют размер $r \times r$; U, X имеют размер $n - r \times r$. Их произведение равно $PQ = \begin{pmatrix} UX & UY \\ VX & VY \end{pmatrix}$. Нам нужно, чтобы $\det(VY)$ был равен нулю, что равносильно $\det V = 0$ или $\det Y = 0$

Посчитаем количество следующих вспомогательных объектов:

1. Матрицы, у которых $\det V \neq 0$ и $\operatorname{rk} P = r$.

   Формула для числа невырожденных матриц нам уже известна, выберем блок V через нее. Остальные числа можно выбрать совершенно любыми, так как у нас уже есть r независимых строк, значит ранг $\geqslant r$, но строго больше он, разумеется, быть не может, так как у нас всего r столбцов. Получаем

   $$f(n, r) := (q^r - 1) \cdot \ldots \cdot (q^r - q^{r-1}) \cdot q^{r(n-r)}$$

2. Матрицы, у которых $\det V = 0$ и $\operatorname{rk} P = r$.

   Их можно получить, вычев из общего числа матриц ранга r выражение из пункта (1).

   $$g(n, r) := \mathcal{J}_r(n) - f(n, r) = (q^n - 1) \cdot \ldots \cdot (q^n - q^{r-1}) - (q^r - 1) \cdot \ldots \cdot (q^r - q^{r-1}) \cdot q^{r(n-r)}$$

Формулы верны в том числе для $Q = \begin{pmatrix} X & Y \end{pmatrix}$, так как Q имеет тот же вид с точностью до транспонирования.

Наконец, мы готовы посчитать число разложений. Сначала учтем разложения, где $\det V = 0$ и $\det Y \neq 0$. Их число равно $g(n,r) \cdot f(n,r)$. Аналогично считаются разложения, где $\det V \neq 0, \det Y = 0$, поэтому это выражение можно удвоить. Остаются разложения, где $\det V = \det Y = 0$, их число – это $g(n,r)^2$. Складываем их все, делим на $|GL_r|$ и получаем ответ

$$d_{n-r,r}(n) = \frac{2 \cdot f(n,r) \cdot (\mathcal{J}_r(n) - f(n,r)) + (\mathcal{J}_r(n) - f(n,r))^2}{\gamma_r} =$$
$$\frac{2 \cdot f(n,r) \cdot \mathcal{J}_r(n) - 2 \cdot f(n,r)^2 + \mathcal{J}_r(n)^2 - 2 \cdot \mathcal{J}_r(n) \cdot f(n,r) + f(n,r)^2}{\gamma_r} =$$
$$\frac{\mathcal{J}_r(n)^2 - f(n,r)^2}{\gamma_r} = \frac{(q^n-1)^2 \cdot \ldots \cdot (q^n - q^{r-1})^2 - q^{2r(n-r)} \cdot (q^r-1)^2 \cdot \ldots \cdot (q^r - q^{r-1})^2}{(q^r-1) \cdot \ldots \cdot (q^r - q^{r-1})} =$$
$$\frac{(q^n-1)^2 \cdot \ldots \cdot (q^n - q^{r-1})^2 - (q^n - q^{n-r})^2 \cdot \ldots \cdot (q^n - q^{n-1})^2}{(q^r-1) \cdot \ldots \cdot (q^r - q^{r-1})}$$

■

Замечание. Для $(n,q,i,j) \in \{(3,3,1,2),(3,3,2,1),(4,2,1,3),(4,2,2,2),(4,2,3,1)\}$ формула экспериментально проверена

7 Канонический вид матрицы над $\mathbb{F}_q$ и связь с d_{in}

В этой секции будет описываться новая техника, которая позволит подсчитывать d_{in} для $i > 1$

Обратимся к пункту 3.6. Там мы обсуждали связь матриц с собственным значением 1 и d_{nn}. Это рассуждение можно обобщить – рассмотреть класс матриц ранга i с собственным значением 1. Мощность этого множества есть d_{ni}

Как мы помним, и собственные значения, и ранг совпадают у матриц, связанных отношением подобия, то есть $A = CBC^{-1}$ для невырожденной C. Отсюда возникает идея – взять из каждого класса подобия по одной матрице (каноническому представителю), решить, подходит ли она нам, и если подходит, то взять весь класс целиком.

Вопрос выбора канонического представителя сводится к приведению матрицы к наиболее простому виду сменой базиса. Над полем комплексных чисел этот вопрос решен и ответ на него широко известен – жорданова нормальная форма.

Но, оказывается, и над конечными полями этот вопрос разрешим.

Определение 9. (Сопровождающая матрица)
Пусть $f(t) = t^n - a_{n-1}t^{n-1} - \ldots - a_1 t - a_0$. Тогда сопровождающей матрицей многочлена f называется

$$C_f = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}$$

Теорема 7.1. *(Фробениусова нормальная форма)*
Пусть $A \in M_n(\mathbb{F})$ – произвольная матрица. Тогда A может быть приведена к блочно-диагональному виду с блоками вида

$$\begin{pmatrix} C_f & E & 0 & \ldots & 0 & 0 \\ 0 & C_f & E & \ldots & 0 & 0 \\ 0 & 0 & C_f & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & C_f & E \\ 0 & 0 & 0 & \ldots & 0 & C_f \end{pmatrix}_{rd \times rd}$$

где f – неприводимый фактор характеристического многочлена матрицы, $d \geqslant 1$ – его степень, r – некоторое положительное число, C_f – сопровождающая матрица f. Форма уникальна с точностью до перестановки блоков.

Замечание. Можно видеть полную аналогию с жордановой нормальной формой. В частности, если характеристический многочлен раскладывается на линейные множители, то мы получим ЖНФ.

Определение 10. Запишем для неприводимого фактора f числа r, которые соответствуют его блокам: $\lambda = (\lambda_1, \ldots, \lambda_k), \lambda_1 \geqslant \ldots \geqslant \lambda_k$. Будем называть это разбиением многочлена. Обозначение – λ_f. Сама форма однозначно задается множеством $\{(f, \lambda_f) \mid f \in \mathrm{Irr}(f), f \mid \chi(A)\}$

Замечание. По аналогии с жордановой нормальной формой верно, что $\sum \deg f \cdot |\lambda_f| = n$, где сумма ведется по всем неприводимым факторам.

8 Формула для d_{2n}

Теорема 8.1.

$$d_{2n}(n) = q^{n-1}(q^n + q^{n-1} - q^{n-2} - q - 1)(q^n - q^2)\dots(q^n - q^{n-1})$$

Доказательство. Так, нам нужно описать матрицы ранга 2, имеющие собственное значение 1 в терминах характеристического многочлена. Условие на наличие собственного значения 1 довольно просто реализуется – потребуем, чтобы характеристический многочлен матрицы делился на $(t-1)$.
Также нетрудно заметить, что у матрицы ранга 2 характеристический многочлен должен делиться на t^{n-2}. Можно сказать, что $\dim \operatorname{Im} A = 2 \implies \dim \operatorname{Ker} A = n-2$, а алгебраическая кратность собственного значения $\geqslant$ геометрической
Остается $\chi_A(t) = t^{n-2}(t-1)(t-a)$, где a – это какое-то число, в том числе, возможно, 0 или 1. В нашем случае многочлен разложился на линейные множители, значит мы можем пользоваться Жордановой нормальной формой. Необходимо только аккуратно разобрать случаи a и выяснить, в каких будет ранг 2.
Наличие собственного значения 1 гарантирует ранг хотя бы 1. В случае с собственным значением 0, каждый соответствующий ему блок размера k будет увеличивать ранг на $k-1$.

1. $a = 0$

   Чтобы получить ранг 2, нам придется взять один блок размера 2 с собственным значением 0. Получится вид $\{(0,(2,1,1,\dots)),(1,(1))\}$

   $$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

2. $a \neq 0, a \neq 1$

   В таком случае, мы обязаны взять только вид $\{(0,(1,\dots,1)),(1,(1)),(a,(1))\}$, так как собственные значения $1, a$ уже дают ранг 2

   $$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & a \notin \{0,1\} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

3. $a = 1$

   Здесь, мы можем взять разбиение для единицы $(1,1)$, а можем (2) – они будут оба давать ранг 2, но для нуля мы все так же должны брать $(1,\dots,1)$

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Пронумеруем эти виды в таком же порядке – $(1), (2), (3), (4)$

Теперь, когда у нас есть классы матриц, нам остается только найти число матриц в каждом классе, и у нас будет готова формула для d_{2n}. Для этого нам потребуются некоторые знания алгебры

Рассмотрим действие группы GL_n на множестве матриц ранга 2 сопряжениями: $(g, h) \mapsto ghg^{-1}$. Нам надо найти размеры нескольких орбит такого действия. Для этого воспользуемся формулой $|Gx| = |G|/|St(x)|$. Размер группы GL_n мы знаем. Остается уметь находить количество g таких, что $ghg^{-1} = h \iff gh = hg$, то есть сколько невырожденных матриц коммутируют с данной. Делать мы это будем "в лоб", то есть запишем произведение произвольной матрицы на данную в одном порядке и в другом, и посмотрим, какие ограничения на матрицу это равенство задает

(1)

$$(1) \cdot X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots \\ x_{31} & x_{32} & x_{33} & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x_{11} & 0 & x_{12} & 0 & \dots \\ x_{21} & 0 & x_{22} & 0 & \dots \\ x_{31} & 0 & x_{32} & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = X \cdot (1)$$

Из клетки $(2, 3)$ видно, что $x_{22} = x_{33}$. Из $(1, 2)$ видно, что $x_{12} = 0$, а из $(1, 3)$ видно, что $x_{12} = x_{13}$, то есть $x_{13} = 0$. Из клеток $(1, 4), (1, 5), \dots$ видно, что $x_{14} = x_{15} = \dots = 0$. Симметрично дела обстоят с $(2, 1)$ и $(3, 1)$ – отсюда видно, что $x_{21} = x_{31} = 0$, и аналогично со всем первым столбцом – он нулевой, начиная со второго элемента. Из третьего столбца, начиная с третьего элемента, видно, что $x_{i2} = 0 \ \forall i \geqslant 3$. То же самое со второй строкой – из нее $x_{3i} = 0 \ \forall i \geqslant 4$. Что насчет остальных элементов, то они либо не учавствуют в произведении, либо не дают никакой информации, как $x_{11} = x_{11}$ в $(1, 1)$. Получаем такой вид матрицы

$$\begin{pmatrix} \lambda & 0 & 0 & 0 & 0 & \dots \\ 0 & \mu & * & * & * & \dots \\ 0 & 0 & \mu & 0 & 0 & \dots \\ 0 & 0 & * & & & \\ 0 & 0 & * & & A & \\ \vdots & \vdots & \vdots & & & \end{pmatrix}$$

где звездочки – любые числа. Однако у нас есть еще условие на невырожденность. Очевидно, что $\lambda \neq 0, \mu \neq 0$, потому что тогда у нас будут нулевые столбцы. Теперь определитель можно разложить по первому и второму столбцам и третьей строке, откуда получается, что звездочки не влияют на определитель и остается только потребовать,

чтобы подматрица A была невырожденной. Отсюда можно собрать формулу для числа матриц X, которые нам подходят

$$GL_{n-3} \cdot (q-1)^2 \cdot q^{2n-5}$$

(2)

$$(2) \cdot X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots \\ ax_{21} & ax_{22} & ax_{23} & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x_{11} & ax_{12} & 0 & \dots \\ x_{21} & ax_{22} & 0 & \dots \\ x_{31} & ax_{32} & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = X \cdot (2)$$

В $(1,2)$ видно, что $x_{12} = ax_{12}$. Так как a по условию $\neq 1$, $x_{12} = 0$. Далее, из первой строки видно, что далее $x_{1i} = 0$. Аналогично в первом столбце – $x_{21} = x_{31} = \ldots = 0$. Из второй строки и второго столбца видно, что $x_{23} = x_{24} = \ldots = 0, x_{32} = x_{33} = \ldots = 0$. Про остальные элементы ничего не известно. Получаем вид:

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 0 & \mu & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & A & \\ 0 & 0 & & & \end{pmatrix}$$

Аналогично, $\lambda \neq 0, \mu \neq 0, \det A \neq 0$, и получаем формулу:

$$GL_{n-2} \cdot (q-1)^2 \cdot (q-2)$$

(3)

$$(3) \cdot X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots \\ x_{21} & x_{22} & x_{23} & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & 0 & \dots \\ x_{21} & x_{22} & 0 & \dots \\ x_{31} & x_{32} & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = X \cdot (3)$$

Легко увидеть, что элементы в 2×2 ведущей подматрице могут быть любыми, так же как и в следующей за ней $(n-2) \times (n-2)$ подматрице, а все оставшиеся – то есть элементы из первой и второй строк и первого и второго столбца, кроме $x_{11}, x_{12}, x_{21}, x_{22}$ должны быть равны нулю

$$\begin{pmatrix} * & * & 0 & \dots & 0 \\ * & * & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & A & \\ 0 & 0 & & & \end{pmatrix}$$

Чтобы матрица была невырождена, нужно чтобы определитель каждого из блоков не был равен нулю, поэтому получаем такую формулу

$$GL_2 \cdot GL_{n-2}$$

(4)

$$(4)\cdot X = \begin{pmatrix} x_{11}+x_{21} & x_{12}+x_{22} & x_{13}+x_{23} & \dots \\ x_{21} & x_{22} & x_{23} & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x_{11} & x_{11}+x_{12} & 0 & \dots \\ x_{21} & x_{21}+x_{22} & 0 & \dots \\ x_{31} & x_{31}+x_{32} & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = X\cdot(4)$$

Из равенства $x_{12}+x_{22}=x_{11}+x_{12}$ в клетке $(1,2)$ следует, что $x_{11}=x_{22}$. Из равенства в $(1,1)$ или $(2,2)$ можно заключить, что $x_{21}=0$. Из первого столбца видно, что $x_{31}=x_{41}=\ldots=0$. Со знанием этого можно получить, что $x_{32}=x_{42}=\ldots=0$ из второго столбца, так как слагаемые из первого столбца, которые там записаны, равны нулю. Таким же способом доказывается, что первая и вторая строки матрицы равны нулю, начиная с третьего номера. Остается клетка $(1,2)$, про которую ничего не известно, и как обычно, $(n-2)\times(n-2)$ подматрица

$$\begin{pmatrix} \lambda & * & 0 & \dots & 0 \\ 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & A & \\ 0 & 0 & & & \end{pmatrix}$$

Из второй строки этой матрицы видно, что $\lambda\neq 0$ для невырожденности всей матрицы. Если по ней разложить определитель, то звездочка уйдет, $\Longrightarrow$ она может быть любой. И, $\det A\neq 0$, конечно

$$GL_{n-2}\cdot(q-1)\cdot q$$

Наконец, пользуясь формулами для размера орбиты и перехода от d_{ij} к d_{ji}, выводим формулу для $d_{2n}(n)$. Также, для упрощения выкладок, нам потребуется простой факт

Лемма 8.2. $q^n(q^{n+1}-1)GL_n = GL_{n+1}$

Доказательство.

$$GL_n=(q^n-1)\dots(q^n-q^{n-1}) \Longrightarrow q^nGL_n=(q^{n+1}-q)\dots(q^{n+1}-q^n) \Longrightarrow$$
$$\Longrightarrow q^n(q^{n+1}-1)=(q^{n+1}-1)\dots(q^{n+1}-q^n)=GL_{n+1}$$

■

$$d_{n2}(n) = \frac{GL_n}{GL_{n-3}(q-1)^2q^{2n-5}} + \frac{GL_n}{GL_{n-2}(q-1)^2}(q-2) + \frac{GL_n}{GL_{n-2}GL_2} + \frac{GL_n}{GL_{n-2}(q-1)q} =$$
$$\frac{GL_n}{GL_{n-2}}\left(\frac{q^{n-2}-1}{(q-1)^2q^{n-2}} + \frac{q-2}{(q-1)^2} + \frac{1}{(q^2-1)(q^2-q)} + \frac{1}{(q-1)q}\right) =$$
$$\frac{GL_n}{GL_{n-2}}\left(-\frac{1}{(q-1)^2q^{n-2}} + \frac{q-1}{(q-1)^2} + \frac{1}{q(q+1)(q-1)^2} + \frac{1}{(q-1)q}\right) =$$
$$\frac{GL_n}{GL_{n-2}}\frac{-q-1+q^{n-2}(q-1)(q+1)+q^{n-3}+(q-1)(q+1)q^{n-3}}{q^{n-2}(q-1)^2(q+1)} =$$
$$\frac{GL_n}{GL_{n-2}}\frac{-q-1+q^{n-2}(q^2-1)+q^{n-3}+q^{n-3}(q^2-1)}{q^{n-2}(q-1)^2(q+1)} =$$
$$\frac{GL_n}{GL_{n-2}}\frac{q^n+q^{n-1}-q^{n-2}-q-1}{q^{n-2}(q-1)^2(q+1)}$$

$$d_{2n}(n) = d_{n2}(n)\frac{\mathcal{J}_n(n)}{\mathcal{J}_2(n)} = d_{n2}(n)\frac{GL_n}{\frac{(q^n-1)^2(q^n-q)^2}{(q^2-1)(q^2-q)}} =$$
$$d_{n2}(n)\frac{(q^n-q^2)\dots(q^n-q^{n-1})\cdot(q^2-1)(q^2-q)}{(q^n-1)(q^n-q)} =$$
$$\frac{GL_n}{GL_{n-2}}\frac{q^n+q^{n-1}-q^{n-2}-q-1}{q^{n-3}}\frac{(q^n-q^2)\dots(q^n-q^{n-1})}{(q^n-1)(q^n-q)} =$$
$$\frac{(q^n+q^{n-1}-q^{n-2}-q-1)(q^n-q^2)^2\dots(q^n-q^{n-1})^2}{q^{n-3}(q^{n-2}-1)\dots(q^{n-2}-q^{n-3})} =$$
$$\frac{(q^n+q^{n-1}-q^{n-2}-q-1)q^{2n-4}(q^{n-2}-1)\dots(q^{n-2}-q^{n-3})\cdot(q^n-q^2)\dots(q^n-q^{n-1})}{q^{n-3}(q^{n-2}-1)\dots(q^{n-2}-q^{n-3})} =$$
$$q^{n-1}(q^n+q^{n-1}-q^{n-2}-q-1)(q^n-q^2)\dots(q^n-q^{n-1})$$

■

Замечание. При $n = 3, q = 2, 3, 4$ формула экспериментально проверена.

Замечание. Подобным образом можно, судя по всему, вывести явную формулу для любого d_{in}, где i – фиксированное число, но, разумеется, придется разбирать намного больше случаев и совершать больше вычислительной работы.

Следствие. $d_{2n}(n) \geqslant d_{1n}(n)$, причем $d_{2n}(n) = d_{1n}(n) \iff n = 2, q = 2$

Доказательство.

Лемма 8.3. $q^{n-1} - q^{n-2} - 1 \geqslant 0$ при $n, q \geqslant 2, n, q \in \mathbb{N}$. Равенство достигается только при $n = 2, q = 2$

Доказательство. $q^{n-1} - q^{n-2} - 1 = q^{n-2}(q-1) - 1 \geqslant 0$, так как $q^{n-2} \geqslant 1, (q-1) \geqslant 1$.
Если $q > 2$, то $q - 1 > 1$ и неравенство будет строгим. Если $q = 2$, то $2^{n-2} = 1$ только при $n = 2$. То, что при $n = 2, q = 2$ равенство выполнено, проверяется простой подстановкой. ■

$$d_{2n}(n) = q^{n-1}(q^n + q^{n-1} - q^{n-2} - q - 1)(q^n - q^2)\dots(q^n - q^{n-1}) \geqslant$$
$$q^{n-1}(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}) = d_{1n}(n)$$

Замечание. В системе компьютерной алгебры `sage`, которая позволяет по типу Фробениусовой нормальной формы находить число соответствующих матриц и решать прочие вычислительные задачи, мною была написана программа вычисляющая $d_{2n}(n)$ в виде многочлена при заданном n. Полученные формулы совпали с полученными теоретически на небольших значениях n.

■

9 Ссылки

Ссылка на github-репозиторий

10 Список используемой литературы

[1] Macdonald, I.G.: Symmetric Functions and Hall Polynomials, 2nd edn. Clarendon, Oxford (1995)

[2] Morrison, K.: Integer sequences and matrices over finite fields. J. Integer Seq. **9**, 06.2.1 (2006). 28 pp.

[3] Prasad, A.: Representations of $GL_2(F_q)$ and $SL_2(F_q)$, and some remarks about $GL_n(F_q)$