CountingEquations Solution

Sevenkplus

1 Notes

See a and b and x as matrices. In the analysis, we denote them as A and B and X respectively.

Unless otherwise indicated, we assume that all works are done over $\mathbb{F}_p$.

Warning: In the analysis, many details are omitted. The readers are expected to figure them out.

2 Original problem

First we solve the original problem: given n, m, p, A, B, count the number of X's that satisfy $AX = B$.

It's not hard to see that there are two situations:

(1) There are no solutions;

(2) There are $p^{n-\mathrm{rk}(A)}$ solutions.

For fixed A, there are $p^m - p^{\mathrm{rk}(A)}$ possible B's that satisfy (1) and $p^{\mathrm{rk}(A)}$ possible B's that satisfy (2).

Proof Consider one maximal linear independent set of rows of A. □

3 Our problem

Back to our problem. We have already seen that number of possibilities for S (number of possible X's) is not very large. Note that $\mathrm{rk}(A) \le \min\{n, m\}$ lies in a small range. So we enumerate $\mathrm{rk}(A)$ and transform the problem into counting number of $m \times n$ matrices with rank r and with positions in set w identically zero. Denote the answer as $\mathrm{mat}(m, n, r, w)$.

4 Counting matrices with given rank

First we give a lemma.

Lemma Suppose we have a $m \times n$ matrix $M = (v_1, v_2, \dots, v_n)$. $\mathrm{rk}(M) = r$ and rank of the submatrix $(v_{n-k+1}, \dots, v_n) = r'$.

Consider all $n-k$ tuples $(w_1, w_2, \dots, w_{n-k})$ and the corresponding matrices

$$\begin{bmatrix} v_1 & v_2 & \dots & v_{n-k} & v_{n-k+1} & \dots & v_n \\ w_1 & w_2 & \dots & w_{n-k} & 0 & \dots & 0 \end{bmatrix}.$$

$p^{r-r'}$ of the matrices have rank r and the other $p^{n-k} - p^{r-r'}$ have rank $r+1$. □

Proof The rank-nullity theorem. □

With this lemma we can get some recurrence relations of $\mathrm{mat}(m, n, r, w)$. In general, our method is deleting one row (or one column) and reduce the problem to smaller subproblems. WLOG, assume we are to delete the last row. In all the cases below, we will use the lemma.

(The readers are expected to figure out what w' and w'' are in the following analysis.)

4.1 No positions in the last row are in w

There are two cases:

(1) The first $n-1$ rows span a space of dimension r, and the last row is in the span;

(2) The first $n-1$ rows span a space of dimension $r-1$, and the last row is not in the span.

In the first case we reduce to the problem $\mathrm{mat}(m-1, n, r, w')$. In the second case we reduce to the problem $\mathrm{mat}(m-1, n, r-1, w')$.

4.2 One position in the last row is in w

WLOG, assume the position is in the last column. If the last column is zero, then we delete the last row and the last column and reduce to the problems $\mathrm{mat}(m-1, n-1, r, w')$ and $\mathrm{mat}(m-1, n-1, r-1, w')$.

Otherwise, the last column must span a space of dimension 1. We reduce to the problems $\mathrm{mat}(m-1, n, r, w'')$ and $\mathrm{mat}(m-1, n, r-1, w'')$. (We need to subtract the numbers by appropriate values calculated before to get the desired answer.)

4.3 Two positions in the last row are in w

WLOG, assume the positions are in the last two columns. If at least one of the two columns are zero, we reduce to some smaller subproblems. So we only discuss the case that both columns are nonzero.

Two cases remain:

(1) The two columns are parallel;

(2) The two columns are not parallel.

In the first case, we reduce to a smaller problem $\mathrm{mat}(m-1, n-1, r, w'')$ and in the second case, we reduce to $\mathrm{mat}(m-1, n, r, w')$. (We need to subtract the numbers by appropriate values calculated before to get the desired answers.)

4.4 No positions in the last row are not in w

We simply delete this row and reduce to the problem $\mathrm{mat}(m-1, n, r, w')$.

4.5 One position in the last row is not in w

There are two cases:

(1) The number in this position is 0;

(2) The number in this position is not 0.

In the first case, we simply delete this row and reduce to the problem $\mathrm{mat}(m-1, n, r, w')$. In the second case, we use the last row to eliminate the previous rows. So we delete this row and this column and reduce to the problem $\mathrm{mat}(m-1, n-1, r-1, w'')$.

4.6 Two positions in the last row are not in w

If at least one of the two positions are zero, we reduce to some smaller problems. So we only discuss the case that both positions are nonzero.

We can use one position to eliminate the other position, and then use the last row to eliminate previous rows. In this case, nonzero entries can be thought of as transferred from one column to the other column. So we reduce the problem to $\mathrm{mat}(m-1, n-1, r-1, w')$.

5 What's special about 17?

17 is the largest possible $|w|$ that satisfies that there exists one row or one column that at least one of the above six cases are met.

If we delete the rows and columns in a good order, the total number of states that occur during calculation is not very large. (Note that we can shuffle the rows and columns without changing the answer.)

References

[1] Aaron J. Klein, Joel Brewster Lewis, and Alejandro H. Morales. Counting matrices over finite fields with support on skew Young diagrams and complements of Rothe diagrams. arXiv:1203.5804 [math.CO], 2012.