I. Lower and Upper bounds on the Number of Matrices of a Given Rank

A. Number of $n \times m$ Matrices of Rank t

In the proof of [1, Lemma 3.13], the following formula for the number of $n \times m$ matrices of rank t over $\mathbb{F}_q$ is given:

$$\mathrm{NM}_{t,n,m} = \prod_{i=0}^{t-1} \frac{(q^m - q^i)(q^n - q^i)}{q^t - q^i}. \tag{1}$$

B. Approximation

For $t \ll n, m$, we have $q^m - q^i \approx q^m$ and $q^n - q^i \approx q^n$ for $i \leq t$, so we get

$$\mathrm{NM}_{t,n,m} \approx q^{t(n+m)-t^2} \underbrace{\prod_{i=0}^{t-1} \frac{1}{1-q^{i-t}}}_{\approx 0.288^{-1}}. \tag{2}$$

C. An Upper Bound

The approximation in the previous subsection gives an upper bound as follows.

$$\begin{aligned}
\mathrm{NM}_{t,n,m} &= \prod_{i=0}^{t-1} \frac{(q^m - q^i)(q^n - q^i)}{q^t - q^i} \\
&\leq \prod_{i=0}^{t-1} \frac{q^{n+m}}{q^t - q^i} \\
&\leq q^{t(n+m)-t^2} \underbrace{\prod_{i=0}^{t-1} \frac{q^t}{q^t - q^i}}_{=:\,\gamma} \\
&= q^{t(n+m)-t^2} \gamma,
\end{aligned}$$

where, by the argument in the proof of [1, Lemma 3.13], we have $\gamma \leq 0.288^{-1} \leq 3.48$. Hence, we obtain.

$$\log_q(\mathrm{NM}_{t,n,m}) \leq t(n+m-t) + \log_q(3.48) \tag{3}$$

D. A Lower Bound

In [2, Section IV.B], a constructive way of obtaining rank-t matrices is given. More precisely, an injective mapping

$$\varphi \,:\, {\mathbb{F}_q}^{t(n+m-t-1)} \to \{\boldsymbol{A} \in {\mathbb{F}_q}^{n \times m} \,:\, \mathrm{rank}\, \boldsymbol{A} = t\}$$

is given. Hence, we have

$$\mathrm{NM}_{t,n,m} \geq |{\mathbb{F}_q}^{t(n+m-t-1)}|,$$

so

$$\log_q(\mathrm{NM}_{t,n,m}) \geq t(n+m-t-1). \tag{4}$$

E. Summary

In total, we have

$$t(n+m-t-1) \leq \log_q(\mathrm{NM}_{t,n,m}) \leq t(n+m-t) + \log_q(3.48), \tag{5}$$

where for $t \ll n, m$, the value is approximately the upper bound.

References

[1] R. Overbeck, "Public key cryptography based on coding theory," Ph.D. dissertation, TU Darmstadt, Darmstadt, Germany, 2007.

[2] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.