Number of matrices of certain rank k over $\mathbb{F}_q$

It has long been known [1] that the number of matrices $X \in \mathbb{F}_q^{m\times n}$ of a certain rank k is given by the formula:

$$W_{n,m}(k) := \prod_{i=1}^{k} \frac{(q^m - q^{i-1})(q^n - q^{i-1})}{(q^k - q^{i-1})} \tag{1}$$

Here q is a prime power and we may assume $n \leq m$. As there are q^{mn} matrices of size $m \times n$ over $\mathbb{F}_q$, and each one of those has rank $0 \leq k \leq n$, we get a surprising equality.

Theorem 1. *Let q be a prime power and $n, m \in \mathbb{N}$. Then*

$$\sum_{k=0}^{n} W_{n,m}(k) = q^{nm}.$$

There are a number of proofs for Theorem 1 (by proving equation 1) stemming from linear algebra. We give one here, with credits to Bas Westerbaan:

Proof. Any rank k matrix $X \in \mathbb{F}_q^{m\times n}$ can be seen as a map from $\mathbb{F}_q^n \to \mathbb{F}_q^m$ that factors through $\mathbb{F}_q^k$,

$$\mathbb{F}_q^n \to \mathbb{F}_q^k \to \mathbb{F}_q^m$$

and is uniquely so up to $\mathbb{F}_q^k$ isomorphism. A map $\mathbb{F}_q^k \to \mathbb{F}_q^m$ is defined by picking k independent vectors in $\mathbb{F}_q^m$, which we can count by

$$\Gamma(m,k) := \prod_{i=1}^{k} (q^m - q^{i-1}) \tag{2}$$

As a map $\mathbb{F}_q^n \to \mathbb{F}_q^k$ is defined by its transpose $\mathbb{F}_q^k \to \mathbb{F}_q^n$, we get $\Gamma(n,k)$ maps there. Lastly, an $\mathbb{F}_q^k$ isomorphism is a full rank map $\mathbb{F}_q^k \to \mathbb{F}_q^k$ so the same argument applies which gives us $\Gamma(k,k)$ such maps. Combined, this gives us

$$W_{n,m}(k) = \frac{\Gamma(m,k)\Gamma(n,k)}{\Gamma(k,k)}$$

□

One could now wonder if we can prove theorem 1 without using any argument other than counting and combinatorics. This is indeed the case, and is the goal of this short piece. It is not particularly elegant, and the author hopes that this paper resolves anyone else from going through the same work. The proof goes in three steps:

1. Show that the following q-analogue of Pascal's rule holds:

$$\frac{\Gamma(n+1,k)}{\Gamma(k,k)} = q^k \cdot \frac{\Gamma(n,k)}{\Gamma(k,k)} + \frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)}$$

2. Expand Pascal's rule to $W_{n,m}(k)$ by showing that for any rank k:

$$W_{n+1,m}(k) = q^k \cdot W_{n,m}(k) + (q^m - q^{k-1}) \cdot W_{n,m}(k-1)$$

3. Use Pascal's rule on $W_{n,m}(k)$ in an induction step to show equation 2.

Step 1: The q-analogue of Pascal's rule

In this section we prove the following lemma, which is a q-analogue of Pascal's rule (Pasqal's rule) for binomial coefficients:

Lemma 1 (Pasqal's rule)**.** *For any prime power q and $k, n \in \mathbb{N}$ with $k \leq n$*

$$\frac{\Gamma(n+1,k)}{\Gamma(k,k)} = q^k \cdot \frac{\Gamma(n,k)}{\Gamma(k,k)} + \frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)}.$$

Proof. This basically entails a number of manipulations to the RHS:

$$\begin{aligned}
& q^k \cdot \frac{\Gamma(n,k)}{\Gamma(k,k)} + \frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)} \\
=& \\
& q^k \cdot \frac{(q^n-1)\dots(q^n-q^{k-1})}{(q^k-1)\dots(q^k-q^{k-1})} + \frac{(q^n-1)\dots(q^n-q^{k-2})}{(q^{k-1}-1)\dots(q^{k-1}-q^{k-2})} \\
=& \\
& \frac{q^k\cdot(q^n-1)\dots(q^n-q^{k-1})}{(q^k-1)\dots(q^k-q^{k-1})} + \frac{q^{k-1}\cdot(q^n-1)\dots(q^n-q^{k-2})}{q^{k-1}\cdot(q^{k-1}-1)\dots(q^{k-1}-q^{k-2})} \\
=& \\
& \frac{(q^{n+1}-q)\dots(q^{n+1}-q^k)}{(q^k-1)\dots(q^k-q^{k-1})} + \frac{q^{k-1}\cdot(q^n-1)\dots(q^n-q^{k-2})}{(q^k-q)\dots(q^k-q^{k-1})} \\
=& \\
& \frac{(q^{n+1}-q)\dots(q^{n+1}-q^k)}{(q^k-1)\dots(q^k-q^{k-1})} + \frac{(q^k-1)\cdot q^{k-1}\cdot(q^n-1)\dots(q^n-q^{k-2})}{(q^k-1)\dots(q^k-q^{k-1})} \\
=& \\
& \frac{(q^{n+1}-q)\dots(q^{n+1}-q^k)}{\Gamma(k,k)} + \frac{(q^k-1)\cdot(q^{n+1}-q)\dots(q^{n+1}-q^{k-1})}{\Gamma(k,k)} \\
=& \\
& (q^{n+1}-q^k)\cdot\frac{(q^{n+1}-q)\dots(q^{n+1}-q^{k-1})}{\Gamma(k,k)} + (q^k-1)\cdot\frac{(q^{n+1}-q)\dots(q^{n+1}-q^{k-1})}{\Gamma(k,k)} \\
=& \\
& (q^{n+1}-q^k-q^k+1)\cdot\frac{(q^{n+1}-q)\dots(q^{n+1}-q^{k-1})}{\Gamma(k,k)} \\
=& \frac{\Gamma(n+1,k)}{\Gamma(k,k)}
\end{aligned}$$

□

Step 2: Extending Pasqal's rule to $W_{n,m}(k)$

In this section we show that Pasqal's rule (Lemma 1), can be extended to $W_{n,m}(k)$ to create Pasqal's W-Rule

Lemma 2 (Pasqal's W-Rule)**.** *For any $0 \leq k \leq n$ and any prime power q, we have*

$$W_{n+1,m}(k) = q^k \cdot W_{n,m}(k) + (q^m - q^{k-1}) \cdot W_{n,m}(k-1).$$

Before we prove this using Pasqal's rule, note that there is a two line proof from [1] using linear algebra: remove the last column of any rank k matrix of size $(n+1) \times m$ will give you an $n \times m$ matrix of rank k or rank $k-1$. The rank stays k if the last column was in the span of the k independent columns (q^k options) and drops if it was independent from all other columns ($q^m - q^{k-1}$ options).

Proof. Multiply both sides of Pasqal's rule with $\Gamma(m,k)$ gives us

$$\Gamma(m,k) \cdot \frac{\Gamma(n+1,k)}{\Gamma(k,k)} = q^k \cdot \Gamma(m,k)\frac{\Gamma(n,k)}{\Gamma(k,k)} + \Gamma(m,k)\frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)}$$

This gives us already

$$W_{n+1.m}(k) = q^k \cdot W_{n,m}(k) + \Gamma(m,k)\frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)}$$

Now per definition $\Gamma(m,k) = (q^m - q^{k-1}) \cdot \Gamma(m,k-1)$ which gives

$$\Gamma(m,k)\frac{\Gamma(n,k-1)}{\Gamma(k-1,k-1)} = (q^m - q^{k-1}) \cdot W_{n,m}(k-1)$$

□

Step 3: Use Pasqal's W-Rule to show the main theorem

We are close to our end goal, showing that only by counting, Theorem 1 holds:

$$\sum_{k=0}^{n} W_{n,m}(k) = q^{nm}.$$

We will now use Pasqal's W-Rule (lemma 2) to show this holds by induction on n.

Proof. For $n = 1$:

$$\sum_{k=0}^{n} W_{n,m}(k) = W_{n,m}(0) + W_{n,m}(1) = 1 + (q^m - 1) = q^m$$

Assume theorem 1 holds for n, then we get for $n+1$ using Paswal's W-Rule in the first step

$$\begin{aligned}
\sum_{k=0}^{n+1} W_{n+1,m}(k) &= \sum_{k=0}^{n+1} q^k \cdot W_{n,m}(k) + (q^m - q^{k-1}) \cdot W_{n,m}(k-1) \\
&= \sum_{k=0}^{n} q^k \cdot W_{n,m}(k) - \sum_{k=1}^{n+1} q^{k-1} \cdot W_{n,m}(k-1) + \sum_{k=1}^{n+1} q^m \cdot W_{n,m}(k-1) \\
&= q^m \cdot \sum_{k=0}^{n} W_{n,m}(k) \\
&= q^m \cdot q^{nm} \\
&= q^{(n+1)m}
\end{aligned}$$

By induction it therefore holds for all n. □

References

[1] G. Landsberg. *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. Reine Angew. Math. 111 (1893) 87–88.