$q$-analogues,
cyclic sieving phenomena
and invariant theory

OUTLINE:

- What is a $q$-analogue?
- What is a cyclic sieving phenomenon (CSP)?
- "BAD" proof technique
- GOOD proof technique
- $\text{GL}_n(\mathbb{F}_q)$-analogue
What is a $q$-analogue?

Say we have a finite set $X$ with cardinality $|X|$

**DEFINITION**: A $q$-analogue for $|X|$ (my own, not standard) is an element $X(q) \in \mathbb{Z}[q]$ (and even sometimes $X(q) \in \mathbb{Q}(q)$)

that, at a minimum, has $\left[ X(q) \right]_{q=1} = |X|

and hopefully also has at least one of these other pleasant properties ....
Pleasant properties for $q$-analogues $X(q)$:

- $X(q) = \sum_{x \in X} q^{s(x)}$ for some interesting statistic $s : X \to \{0, 1, 2, \ldots\}$

- $X(q)$ has a simple product formula

- $[X(q)]_{q=p^d}$ for $p=p^d$ a prime power counts the points of a variety $X(\mathbb{F}_q)$ defined over $\mathbb{F}_q$

- $X(q) = \sum_{i \geq 0} \dim_k (R_i) \cdot q^i =: \text{Hilb}(R, q)$ is the Hilbert series for some interesting graded $k$-algebra $R = \bigoplus_{i \geq 0} R_i$

- $X(q^2) = \sum_{i \geq 0} \beta_i q^i =: \text{Poin}(X(\mathbb{C}), q)$ is the Poincaré polynomial for some interesting complex variety $X(\mathbb{C})$ (with only even-dimensional cohomology)

- $X(q^2)$ is, up to some factor of $q^N$, the formal character $\sum \dim_{\mathbb{C}}(V_i) q^i$ of an $\text{SL}_2(\mathbb{C})$-representation $V$ where $V_i$ is the weight space where $[\frac{g \cdot q}{q}]$ acts as $q^i$. 
The PROTO-Example

\[ X := k\text{-element subsets of } \{1,2,...,n\} \]

\[ X(q) := \binom{n}{k}_q = \text{the } q\text{-binomial coefficient} \]

\[ := \frac{[n]_q!}{[k]_q! \cdot [n-k]_q!} \quad \text{where} \quad [m]_q := [m]_q [m-1]_q \cdots [2]_q [1]_q \]

\[ q=1 \sum_{m=0}^{\theta} \binom{n}{k} = |X| \quad \checkmark \]

\[ = \frac{1-\theta^n}{1-\theta} \]

\[ q=1 \sum_{m=0}^{\theta} m \]

It actually has all of the pleasant properties:

\[ \binom{n}{k}_q = \sum_{\text{k-subsets } S \text{ of } \{1,\ldots,n\}} \text{sum}(S) - \binom{|S|}{k} \]

= \# points of the finite Grassmannian \( \text{Gr}(k, \mathbb{F}_q^n) \) = \( k \)-planes in \( \mathbb{F}_q^n \)

\[ \binom{n}{k}_q = \text{Poin}\left( \text{Gr}(k, \mathbb{C}^n), q \right) \]

= formal character of \( \text{SL}(n, \mathbb{C}) \cdot \Lambda^k(\mathbb{C}^n) \)

(up to a shift by \( q^{-k(n-k)} \))

\[ \binom{n}{k}_q = \text{Hilb}\left( \frac{\mathbb{C}[x_1,\ldots,x_n]}{(\mathbb{C}[x_1,\ldots,x_n]_+)^{\otimes k}} , q \right) \]

an interesting graded \( \mathbb{C} \)-algebra!
What is a cyclic sieving phenomenon (CSP)?

Sometimes our finite set $X$ naturally carries some cyclic group action, that is,

$X$ is a $C$-set for some group $C = \langle c \rangle \cong \mathbb{Z}/n\mathbb{Z}$

$= \{e, c, c^2, \ldots, c^{n-1}\}$

with interesting orbit structure.

**DEFINITION:** Given a finite set $X$,

a $q$-analogue $X(q)$,

and a cyclic group $C \subseteq X$ with $|C| = n$,

say that the triple $(X, X(q), C)$ exhibits a CSP if for every integer $d$,

$$\# \{ x \in X : c^d(x) = x \} = \left[ X(q) \right]_q^{f^d}$$

where $f$ is any primitive $n^{th}$ root of unity (e.g., $f = e^{2\pi i/n}$).
**The PROTO-Example CSP**

**Theorem (Stanton-White-R. 2004)**

The triples \((X, X(g), C)\) where

\[ X = \text{\(k\)-subsets of} \ \{1, 2, \ldots, n\} \]

\[ X(g) = \left[ \begin{array}{c} n \\ k \end{array} \right]_g \]

\[ C = \begin{cases} \mathbb{Z}/n\mathbb{Z} \text{ generated by an } n\text{-cycle} \\ \text{or} \\ \mathbb{Z}/(n-1)\mathbb{Z} \text{ generated by an } (n-1)\text{-cycle} \end{cases} \]

both exhibit a CSP.
**Example:**

\[ n = 4 \]
\[ k = 2 \]

\[ X = \text{2-subsets of } \{1,2,3,4\} \]

\[ X(q) = \binom{4}{2}_q = \frac{\left\lfloor \frac{4}{2} \right\rfloor_3}{\left\lfloor \frac{2}{2} \right\rfloor_3} = \frac{(1+q+q^2)(1+q+q^2)}{(1+q)(1+q)} \]

\[ = (1+q)(1+q+q^2) \]
\[ = 1+q+2q^2+q^3 \]

\[ C = \langle \begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array} \rangle \cong \mathbb{Z}/4\mathbb{Z} \]

has orbits

\[ \xi = e^{\frac{2\pi i}{5}} = i \]

\[ C = \langle \begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array} \rangle \cong \mathbb{Z}/3\mathbb{Z} \]

has orbits

\[ \xi = e^{\frac{2\pi i}{3}} \]

\[ q_1 = \frac{5}{2} \quad 1+1+2+1+1=4=|X| \]

\[ q_2 = \frac{5}{4} \quad 1+1+2+1+1=4=|X| \]

\[ q_3 = \frac{5}{8} \quad 1-1+2-1+1=2=|X| \]

\[ q_4 = \frac{5}{16} \quad 1+i-2-i+1=0=|X| \]

\[ X(q) = 1+q+2q^2+q^3+q^4 \]

\[ q = \frac{5}{2} \quad 1+1+2+1+1=4=|X| \]

\[ q = \frac{5}{4} \quad 1+1+2+1+1=4=|X| \]

\[ q = \frac{5}{8} \quad 1-1+2-1+1=2=|X| \]

\[ q = \frac{5}{16} \quad 1+i-2-i+1=0=|X| \]
So when \((X, X(q), C)\) exhibits a CSP,

the polynomial \(X(q)\) is hiding the \(C\)-permutation representation character values as its evaluations at \(\{1, s, s^2, \ldots, s^{n-1}\}\).

What about \(C\)-orbit structure? An equivalent phrasing...

**Definition**: \((X, X(q), C)\) exhibits a CSP if the unique expansion

\[
X(q) = a_0 + a_1 q + a_2 q^2 + \ldots + a_{n-1} q^{n-1} \mod q - 1
\]

has this interpretation:

\[
a_i = \# \text{ \(C\)-orbits on } X \text{ where the stabilizer/isotropy subgroup has size dividing } i
\]

In particular,

\[
a_0 = \text{ total } \# \text{ of } C\text{-orbits}
\]

\[
a_1 = \# \text{ of free } C\text{-orbits}
\]

i.e. orbits of size \(|C|\)
**Example:** \( (X, X(q), C) \)

\[
\begin{align*}
2\text{-subsets of } \{2,3,4\} & \quad \left\{ \begin{array}{c}
\{1,2,3\} \\
\{1,4\} \\
\{2,3\} \\
\{3,4\}
\end{array} \right\} \\
\mathbb{Z}/4\mathbb{Z} \text{ or } \mathbb{Z}/3\mathbb{Z}
\end{align*}
\]

\[
X(q)
\]

\[
1 + q + 2q^2 + q^3 + q^4
\]

\[
\begin{align*}
\frac{2 + 1 + 2q + 2q^2 + 1 - q^3}{a_0, a_1} \mod q^4 - 1
\end{align*}
\]

\[
\begin{align*}
a_1 = 1 \text{ free orbit}
\end{align*}
\]

\[
\begin{align*}
a_0 = 2 \text{ orbits total,}
\end{align*}
\]

and \(a_2 = 2\) since both orbits have stabilizer subgroup size dividing 2.
A frustrating, but important, example...

**Theorem** (Stanton-White-R. 2004)

\[ X := \text{triangulations of an } (n+2)\text{-gon} \]

\[ X(q) := \frac{1}{[n+1]_q} \left[ \binom{2n}{n} \right]_q =: \text{the } q\text{-Catalan number} \]

\[ C = \mathbb{Z}/(n+2)\mathbb{Z} \text{ generated by } \frac{2\pi}{n+2} \text{-rotations} \]

gives a triple \((X, X(q), C)\) exhibiting a CSP.

e.g. \(n=6\)

\[ f := e^{\frac{2\pi i}{6}} \]

\[ X(q) = \frac{1}{[5]_q} \left[ \frac{8}{4} \right]_q = \frac{[8][7][6][5][3][2]}{[4][3][1]_q} \]

\[ = 1 + \frac{q^2 + q^3 + 2q^4 + q^5 + q^6 + 2q^7 + q^8 + q^9 + q^{10}}{1 + q + q^2 + q^3 + q^4 + q^5 + q^6} \]

\[ \equiv 4 + 1 \cdot q + 3q^2 + 2q^3 + 3q^4 + 1q^5 \mod q^6 - 1 \]

\[ q = 5 \]

\[ |H| = |X_q^6| = 6 = |X_q^3| = 2 = |X_q^2| = 0 = |X_q^1| \]
A yet more frustrating example...

**THEOREM** (Stanton 2007)

\[ X := \text{n x n alternating sign matrices} \]

= matrices in \{0, 1, -1\}^{n x n} with
row and column sums +1, and nonzero entries
alternate in sign along any row or column

\[ X(g) := \prod_{k=0}^{n-1} \frac{(3k+1)! g}{(n+k)! g} \]

\[ C = \mathbb{Z}/4\mathbb{Z} \text{ rotating by } \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \]

e.g.

\[
\begin{bmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

\[ \left\{ \frac{\pi}{4} \right\} \mathbb{Z} = i \]

\[ X(g) = \frac{[2]_g [4]_g [6]_g}{[3]_g [4]_g [5]_g} = \frac{[7]_q [6]_q}{[6]_q [2]_q} \]

\[ = 1 + q + q^2 + q^3 + q^4 + q^5 + q^6 + q^7 \]

\[ \equiv 3 + 1 \cdot q^4 + 2q^2 + 1 \cdot q^3 \mod q^4 - 1 \]

\[ q = \left\{ \begin{array}{c}
\frac{\sqrt{5} - 1}{2} \\
\frac{\sqrt{5} + 1}{2} \\
\end{array} \right. \]

\[ \frac{2}{q} = \frac{2}{\sqrt{5} - 1} = -1 \]

\[ q^2 = \frac{3}{2} \]

\[ q^3 = \frac{5}{4} \]

\[ q^4 = \frac{7}{8} \]

\[ 0 = \frac{0}{16} = 1 \]

\[ 1 = |X^{q^4}| \]

\[ 3 = |X^{q^2}| \]

\[ 7 = |X^{q^3}| \]

\[ 3 = |X^q| \]
Each of the previous $3$ CSP's can be proven by a "BAD" (but effective) proof technique:

To show $(X, X(q), C)$ has

$$|X^{cd}| = [X(q)]_{q=q_0}$$

when one has a product formula of the form

$$X(q) = \frac{[N_1]_q \cdots [N_k]_q \cdots [N_{l}]_q}{[M_1]_q \cdots [M_{k}]_q \cdots [M_{l}]_q}$$

e.g.

$$X(q) = [\mathbb{N}]_q = \frac{[n]_q \cdots [n-(k-1)]_q}{[k]_q \cdots [k-1]_q \cdots [1]_q}$$

$$X(q) = \frac{1}{[m]_q} [2n]_q = \frac{[2n]_q \cdots [2n-k+1]_q}{[n]_q \cdots [n-k+1]_q}$$

$$X(q) = \prod_{k=0}^{n-1} \frac{[3k+1]_q}{[2k+1]_q} \approx \frac{n(3n-1)}{2} \text{ factors}$$

- Evaluate $[X(q)]_{q=q_0}$ via L'Hôpital's Rule
- Count $|X^{cd}|$ directly, or find it in the literature

(And then hope for an insightful proof later!)
EXAMPLE

\[ X = \{ k \text{-subsets of } \{1,2,\ldots,n\} \} \]

\[ X(q) = \left[ \begin{array}{c} n \\ k \end{array} \right]_q \]

\[ C = \mathbb{Z}/n\mathbb{Z} \]

(L'Hôpital)

**EXERCISE:** If \( q^d \) is a primitive \( D \text{-th} \) root-of-unity then whenever \( N \equiv M \mod D \), one has

\[
\lim_{q \to q^d} \frac{[N]_q}{[M]_q} = \begin{cases} \frac{N}{M} & \text{if } N \equiv M \equiv 0 \mod D \\ 1 & \text{if } N \equiv M \not\equiv 0 \mod D \end{cases}
\]

This can be used to check that...

**EXERCISE:** If \( n = n_1.D + n_2 \) with \( 0 \leq n_2 \leq D-1 \)

\[ k = k_1.D + k_2 \quad 0 \leq k_2 \leq D-1 \]

then

\[
\left[ \begin{array}{c} n \\ k \end{array} \right]_{q^d} = \left( \begin{array}{c} n_1 \\ k_1 \end{array} \right) \cdot \left[ \begin{array}{c} n_2 \\ k_2 \end{array} \right]_{q^d}
\]

(with convention that \( [M]_q = 0 \) if \( M > N \))

In particular, \( X(q) \) \( [X(q)]_{q^d} = \left[ \begin{array}{c} n \\ k \end{array} \right]_{q^d} = \begin{cases} \frac{n}{D} & \text{if } D \text{ divides } k \\ 0 & \text{otherwise} \end{cases} \)

(since \( q^d = 1 \implies D \text{ divides } N \))

But \( k \)-subsets of \( \{1,2,\ldots,n\} \) fixed by \( q^d \)

biject with \( k.D \)-subsets of \( n.D \):

\[
\left[ \begin{array}{c} 15 \\ 10 \end{array} \right]_{q^6} = \left( \begin{array}{c} 3 \\ 2 \end{array} \right) \]

e.g. \( n=15 \quad d=6 \quad D=5 \)

\( k=10 \)

\[ \text{c}^6 \]

\[ \text{c}^6 \]

\[ \text{c}^6 \]

\[ \text{c}^6 \]

\[ \text{c}^6 \]
The **GOOD** proof technique is a linear-algebraic paradigm, generalizing one of J. Stembridge (1994) for his "$q=-1$ phenomenon".

To show $\# \{ x \in X : d^1(x) = x \} = \left[ X(q) \right]_{q=\frac{1}{d}}$

by finding a $C$ vector space $V$ having ...

- a basis $\{ e_x : x \in X \}$ permuted by $c$ as in the $C$-action on $X$, that is, $c(e_x) = e_{cx}$

- a grading $V = \bigoplus_{i \geq 0} V_i$ in which $c$ acts on $V_i$ as $S^i$ (so $d^1$ acts on $V_i$ as $(S^i)^d$) and $\text{Hilb}(V, q) = \sum_{i \geq 0} \dim V_i \cdot q^i = X(q)$

Then computing in two ways

$$\text{Trace}(d^1 : V \rightarrow V)$$

$$= \# \{ e_x : d^1(e_x) = e_x \} = \sum_{i \geq 0} \text{Trace}(d^1 : V_i \rightarrow V_i)$$

$$= \sum \dim V_i \cdot (S^i)^d \quad \text{(same as } \left[ X(q) \right]_{q=\frac{1}{d}} \text{)}$$
Several examples of the GOOD technique have been found using invariant theory and representation theory more generally, e.g.

- Springer's Theorem on regular elements in reflection groups
  (and its positive characteristic generalizations — to appear later...)

- Kazhdan-Lusztig bases
  (Dual) Canonical bases
  Web bases
  for invariant tensors in group representations

(Rhoades, Fontaine-Kamnitzer, Westbury, Rubey-Westbury)

**Problem:** Find proofs via GOOD technique for

the CSP's

- $X = \text{triangulations of (n+2)-gon}$
  \[ X(q) = \frac{1}{[n+1]_q} \prod_{k=0}^{[2n]} \]
  \[ C = \mathbb{Z}/(n+2)\mathbb{Z} \]

- $X = n \times n$ alternating sign matrices
  \[ X(q) = \prod_{k=0}^{n-1} \frac{[3k+1]_q!}{[n+k]_q!} \]
  \[ C = \mathbb{Z}/4\mathbb{Z} \]
GLn(F_q) - Proto - Example

Recall one of our Proto - examples of a CSP:

\[ X = \{ k\text{-subsets of } [n, n+1, \ldots, n+k] \} \]

\[ X(g) = \binom{n}{k}_q = \frac{(q^n - q^k)(q^{n-k} - q^k) \cdots (q^{n-k^{k-1}})}{(q^k - q^k)(q^{k-1} - q^k) \cdots (q^{k-k^{k-1}})} = q\text{-binomial} \]

\[ C = \langle c \rangle \quad c = n\text{-cycle} \quad \text{inside } G_n \]

\[ \cong \mathbb{Z}/n\mathbb{Z} \]

\[ \cong \text{ for a fixed prime power } q = p^m \]

\[ X := \text{finite Grassmannian } Gr(k, F_q^n) \]

\[ = k\text{-dimensional } F_q\text{-subspaces inside } F_q^n \quad (\cong F_q^k) \]

\[ X(t) := \binom{n}{k}_{q,t} = \frac{(1-t^{q^n-q^k})(1-t^{q^{n-k}q^k}) \cdots (1-t^{q^{k^{k-1}}q^k})}{(1-t^{q^k,q^k})(1-t^{q^{k-1}q^k}) \cdots (1-t^{q^{k^{k-1}}q^k})} = (q,t)\text{-binomial} \]

\[ C = \langle c \rangle \quad c \text{ a Singer cycle} \]

\[ = F_q^{Xn} = \{ 1, g, c^2, \ldots, c^{n-1} \} \quad \hookrightarrow GL_{F_q^n}(F_q^n) \cong GLn(F_q^n) \]

\[ \cong \mathbb{Z}/(q^n-1)\mathbb{Z} \]

---


The latter triple \((X, X(g), C)\) exhibits a CSP.
EXAMPLE: \( q=2, n=4, k=2 \)

\[
F_{2^4} = F_{2^4} = F_{16} \cong F_2[\alpha]/(\alpha^4 + \alpha + 1)
\]

\[
C = \{ \begin{array}{c} \alpha^0, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{16} \end{array} \} \cong \mathbb{Z}/(2^4 - 1)\mathbb{Z} = \mathbb{Z}/15\mathbb{Z}
\]

\[
GL_{F_{16}}(\mathbb{F}_2) \cong GL_4(\mathbb{F}_2)
\]

\[
\begin{bmatrix}
0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

a Singer cycle in \( GL_4(\mathbb{F}_2) \)

How many 2-dimensional \( \mathbb{F}_2 \)-subspaces of \( \mathbb{F}_2^4 \) are preserved by \( C^3 \)?

The CSP says:

\[
\# \{ x \in X : C^3(x) = x \} = \binom{4}{2} = 6
\]

\[
\text{where } s = e^{2\pi i/8} = e^{\frac{2\pi i}{15}}
\]

\[
= \frac{(-t^{3/2} + 2)(1-t^{3/2})}{(1-t^{3/2})(1-t^{2/2})} \quad \text{t} = s^3, \text{ a 3rd root of unity}
\]

\[
= \frac{(1-t^3)(1-t^4)}{(1-t^3)(1-t^2)} \quad \text{t} = e^{\frac{2\pi i}{3}}
\]

\[
= \frac{15}{3} = 5
\]
"BAD" proof: Given $c^d \in \mathbb{F}_q^n = \{1, c, c^2, \ldots, c^{n-1}\}$

name the intermediate subfield generated by $c^d$:

$$
\mathbb{F}_q^m
$$

$$
\mathbb{F}_q(c^d) = \mathbb{F}_q^m \quad \text{for some divisor } m \text{ of } n
$$

$$
\mathbb{F}_q
$$

Then check using the L'Hôpital exercise

$$\begin{cases}
\left[\frac{n}{k}\right]_{\mathbb{F}_q^n, t=c^d} & \text{if } m \text{ divides } k, \\
0 & \text{otherwise}.
\end{cases}$$

Meanwhile, an $\mathbb{F}_q^n$-subspace of dimension $k$ inside $\mathbb{F}_q^n$ will be preserved by $c^d$ $\iff$ it is an $\mathbb{F}_q(c^d)$-subspace,

$$
\mathbb{F}_q^m
$$

and the number of such $k/m$-dimensional $\mathbb{F}_q^m$-subspaces of $\mathbb{F}_q^n$

is $$\begin{cases}
\left[\frac{n}{k}\right]_{\mathbb{F}_q^m} & \text{if } m \text{ divides } k, \\
0 & \text{otherwise}.
\end{cases}$$

E.g., $\mathbb{F}_2^4, [4]_{\mathbb{F}_2} = [\frac{4}{2}]_{\mathbb{F}_2} = \left[\frac{2}{2}\right]_{\mathbb{F}_2} = [2]_{\mathbb{F}_2} = (1+q^2)_{\mathbb{F}_2} = 5$
Sketch of "BAD" proof: Given \( c^d \in \mathbb{F}_{q^n}^x = \{ 1, c, c^2, \ldots, c^{n-1} \} \), name the intermediate subfield generated by \( c^d \):

\[
\mathbb{F}_{q^n} \quad \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n
\]

\( \mathbb{F}_q \)

Then check using the L'Hôpital exercise

\[
\begin{bmatrix} \eta \\ k \end{bmatrix}_{q, t = c^d} = \begin{cases} \begin{bmatrix} \eta/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise}. \end{cases}
\]

Meanwhile, an \( \mathbb{F}_q \)-subspace of dimension \( k \) inside \( \mathbb{F}_{q^n} \) will be preserved by \( c^d \) \( \iff \) it is an \( \mathbb{F}_{q^m} \)-subspace, and the number of such \( k/m \)-dimensional \( \mathbb{F}_{q^m} \)-subspaces of \( \mathbb{F}_{q^n} \) is

\[
\begin{cases} \begin{bmatrix} \eta/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise}. \end{cases}
\]

E.g. \( \mathbb{F}_{q^3} = \mathbb{F}_{q^2} \)

\[
\begin{bmatrix} \frac{4}{2} \\ 2 \end{bmatrix}_{q^3} = \begin{bmatrix} 4/2 \\ 2 \end{bmatrix}_{q^2} = [2]_{q^2} = (1 + q^2)_{q^2} = 5
\]

\( \mathbb{F}_2 \)
Sketch of "BAD" proof: Given \( c^d \in \mathbb{F}_q^n = \{1, c, c^2, \ldots, c^{n-1}\} \)

name the intermediate subfield generated by \( c^d \):

\[
\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n} \quad \text{for some divisor } m \text{ of } n
\]

Then check using the L'Hôpital exercise:

\[
\begin{bmatrix} \eta \cr k \end{bmatrix}_{q^d, t=y^d} = \begin{cases} \begin{bmatrix} \eta m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise}. \end{cases}
\]

Meanwhile, an \( \mathbb{F}_{q^d} \)-subspace of dimension \( k \) inside \( \mathbb{F}_{q^n} \)

will be preserved by \( c^d \) \( \iff \) it is an \( \mathbb{F}_{q^m} \)-subspace,

and the number of such \( k/m \)-dimensional \( \mathbb{F}_{q^m} \)-subspaces of \( \mathbb{F}_{q^n} \)

is

\[
\begin{cases} \begin{bmatrix} \eta m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise}. \end{cases}
\]

e.g. \( \mathbb{F}_2^4 \quad [4]_{2^2} = [2^{\frac{\sqrt{2}}{2}}]_{2^{\sqrt{2}}} = [2]_{q^2} = (1+q^2)_{q^{2g}} = 5 \)
Sketch of "BAD" proof: Given $c^d \in \mathbb{F}_q^n = \{1, c, c^2, ..., c^{n-1}\}$

name the intermediate subfield generated by $c^d$:

$\mathbb{F}_q^n$

$\mathbb{F}_q(c^d) = \mathbb{F}_{q^m}$ for some divisor $m$ of $n$

$\mathbb{F}_q$

Then check using the L'Hôpital exercise

$$\left[ \frac{n}{k} \right]_{q, t=c^d} = \begin{cases} \left[ \frac{nm}{km} \right]_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise}. \end{cases}$$

Meanwhile, an $\mathbb{F}_q$-subspace of dimension $k$ inside $\mathbb{F}_q^n$ will be preserved by $c^d \iff$ it is an $\mathbb{F}_q(c^d)$-subspace, $\mathbb{F}_{q^m}$

and the number of such $k/m$-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_q^n$ is

$$\left\{ \left[ \frac{nm}{km} \right]_{q^m} : \text{if } m \text{ divides } k, \right\}
\quad 0 \quad \text{otherwise}.$$
Sketch of "BAD" proof: Given $c^d \in \mathbb{F}_p^* = \{1, c, c^2, ..., c^m\}$

name the intermediate subfield generated by $c^d$:

$$\mathbb{F}_q(c^d) = \mathbb{F}_m$$ for some divisor $m$ of $n$

$$\mathbb{F}_q$$

Then check using the L'Hôpital exercise

$$[\frac{\eta}{k}]_{q^k, t=c^d} = \begin{cases} \left[\frac{\eta m}{k/m}\right]_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

Meanwhile, an $\mathbb{F}_q$-subspace of dimension $k$ inside $\mathbb{F}_q^n$

will be preserved by $c^d \iff$ it is an $\mathbb{F}_q(c^d)$-subspace,

$$\mathbb{F}_m$$

and the number of such $k/m$-dimensional $\mathbb{F}_m$-subspaces of $\mathbb{F}_q^n$ is

$$\begin{cases} \left[\frac{\eta m}{k/m}\right]_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

E.g. $\mathbb{F}_2(c^3) = \mathbb{F}_2$

$$\left[\begin{array}{c} 4 \\ 2 \end{array}\right] = [\frac{4}{2}]_{q^4} = [\frac{2}{1}]_{q^2} = [2]_{q^2} = (1+q^2)_{q^{2\cdot 4}} = 5$$
Sketch of "BAD" proof: Given \( c^d \in \mathbb{F}_{q^n}^x = \{1, c, c^2, \ldots, c^{d-1}\} \), name the intermediate subfield generated by \( c^d \):

\[
\mathbb{F}_{q^m}^c = \mathbb{F}_{q^m} 
\]

for some divisor \( m \) of \( n \).

Then check using the L'Hôpital exercise:

\[
\begin{align*}
\left[ \begin{array}{c} n \\ k \end{array} \right]_{q^t, t=c^d} &= \begin{cases} 
\left[ \begin{array}{c} \eta m \\ k/m \end{array} \right]_{q^m} & \text{if } m \text{ divides } k, \\
0 & \text{otherwise}.
\end{cases}
\end{align*}
\]

Meanwhile, an \( \mathbb{F}_q \)-subspace of dimension \( k \) inside \( \mathbb{F}_{q^n} \) will be preserved by \( c^d \) \( \iff \) it is an \( \mathbb{F}_{q^m}(c^d) \)-subspace, \( \mathbb{F}_{q^m} \)

and the number of such \( k/m \)-dimensional \( \mathbb{F}_{q^m} \)-subspaces of \( \mathbb{F}_{q^n} \) is

\[
\begin{align*}
\left[ \begin{array}{c} \eta m \\ k/m \end{array} \right]_{q^m} & \text{ if } m \text{ divides } k, \\
0 & \text{otherwise}.
\end{align*}
\]

\[
\begin{align*}
\mathbb{F}_{q^4} = \mathbb{F}_{q^2} & \\
\mathbb{F}^{x}_{2} = \mathbb{F}_{q^2}^c = \mathbb{F}_q & \\
\left[ \begin{array}{c} 2 \\ 2 \end{array} \right]_{q^2} = \left[ \begin{array}{c} \frac{3}{2} \\ \frac{3}{2} \end{array} \right]_{q^2} = \left[ \begin{array}{c} 2 \\ 2 \end{array} \right]_{q^2} = \left( 1 + q^2 \right)_{q^2} = 5
\end{align*}
\]