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
- $GL_n(\mathbb{F}_q)$-analogue

②

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

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

- $X(q) = \sum'_{i \geq 0} \dim_k(R_i) \cdot q^i =: \mathrm{Hilb}(R, q)$

  is the Hilbert series for some interesting graded k-algebra $R = \bigoplus_{i \geq 0} R_i$

- $X(q^2) = \sum_{i \geq 0} \beta_i q^i =: \mathrm{Poin}(X(\mathbb{C}), q)$

  is the Poincaré polynomial for some interesting complex variety $X(\mathbb{C})$ (with only even-dimensional (co)homology)

- $X(q^2)$ is, up to some factor of q^N, the formal character $\sum_i \dim_{\mathbb{C}}(V_i)\, q^i$ of an $SL_2(\mathbb{C})$-representation V where V_i is the weight space where $\begin{bmatrix} q & 0 \\ 0 & q^{-1} \end{bmatrix}$ acts as q^i.

The PROTO-Example

$X :=$ k-element subsets of $\{1, 2, \ldots, n\}$

$X(q) := \begin{bmatrix} n \\ k \end{bmatrix}_q$ = the q-binomial coefficient

$:= \dfrac{[n]!_q}{[k]!_q \, [n-k]!_q}$ where $[m]!_q := [m]_q [m-1]_q \cdots [2]_q [1]_q$

$[m]_q := 1 + q + q^2 + \cdots + q^{m-1}$

$= \dfrac{1 - q^m}{1 - q}$

$\overset{q=1}{\rightsquigarrow} m$

$\overset{q=1}{\rightsquigarrow} \binom{n}{k} = |X|$ ✓

It actually has all of the pleasant properties:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\substack{k\text{-subsets } S \\ \text{of } \{1, \ldots, n\}}} q^{\mathrm{sum}(S) - \binom{k+1}{2}}$$

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

$= k$-planes in $\mathbb{F}_q^n$

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q^2} = \mathrm{Poin}\left(Gr(k, \mathbb{C}^n), q \right)$$

$=$ formal character of $SL_2(\mathbb{C}) \curvearrowright \Lambda^k(\mathbb{C}^n)$

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

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \mathrm{Hilb}\Bigg(\underbrace{\mathbb{C}[x_1, \ldots, x_n]^{\mathfrak{S}_k \times \mathfrak{S}_{n-k}} \Big/ \left(\mathbb{C}[x_1, \ldots, x_n]^{\mathfrak{S}_n}_+ \right)}_{\text{an interesting graded } \mathbb{C}\text{-algebra!}}, q \Bigg)$$

5

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 $C \circlearrowright X$ with $|C| = n$,

say that the triple $(X, X(q), C)$ exhibits a CSP

if for every integer d,

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

$\# X^{c^d}$

where ζ is any primitive n^{th} root-of-unity
(e.g. $\zeta = e^{\frac{2\pi i}{n}}$)

The PROTO-Example CSP

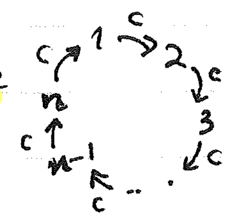
THEOREM (Stanton-White-R. 2004)

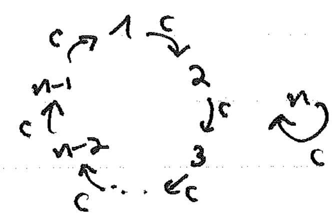
The triples $(X, X(q), C)$ where

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

$$X(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

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





both exhibit a CSP.

EXAMPLE: $n=4$, $k=2$

$X =$ 2-subsets of $\{1,2,3,4\}$

$$X(q) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4]_q [3]_q}{[2]_q [1]_q} = \frac{(1+q+q^2+q^3)(1+q+q^2)}{(1+q)\quad(1)}$$

$$= (1+q^2)(1+q+q^2)$$

$$= 1+q+2q^2+q^3+q^4$$

$$C = \left\langle \begin{tikzcd} & 1 \arrow[dr] & \\ 4 \arrow[ur] & & 2 \arrow[dl] \\ & 3 \arrow[ul] & \end{tikzcd} \right\rangle \cong \mathbb{Z}/4\mathbb{Z}$$

has orbits $\qquad \zeta := e^{\frac{2\pi i}{4}} = i$

$$\begin{tikzcd} & \{1,2\} \arrow[dr, "c"] & \\ \{1,4\} \arrow[ur, "c"] & & \{2,3\} \arrow[dl, "c"] \\ & \{3,4\} \arrow[ul, "c"] & \end{tikzcd} \qquad \begin{tikzcd} \{1,3\} \arrow[d, bend left, "c"] \\ \{2,4\} \arrow[u, bend left, "c"] \end{tikzcd}$$

$$X(q) = 1+q+2q^2+q^3+q^4 \quad \underset{q=\zeta^0=1}{\rightsquigarrow} \quad 1+1+2+1+1 = \cancel{4}\,6 = |X|$$

$$\underset{q=\zeta^2=-1}{\rightsquigarrow} \quad 1-1+2-1+1 = 2 = |X^{c^2}|$$

$$q=\zeta^1=i \rightsquigarrow 1+i-2-i+1 = 0 = |X^{c^1}|$$

$$C = \left\langle \begin{tikzcd} & 1 \arrow[dr, "c"] & \\ 3 \arrow[ur, "c"] & & 2 \arrow[ll, "c"] \end{tikzcd} \quad \begin{tikzcd} 4 \arrow[loop below, "c"] \end{tikzcd} \right\rangle \cong \mathbb{Z}/3\mathbb{Z}$$

has orbits $\qquad \zeta := e^{\frac{2\pi i}{3}}$

$$\begin{tikzcd} & \{1,2\} \arrow[dr, "c"] & \\ \{1,3\} \arrow[ur, "c"] & & \{2,3\} \arrow[ll, "c"] \end{tikzcd} \qquad \begin{tikzcd} & \{1,4\} \arrow[dr, "c"] & \\ \{3,4\} \arrow[ur, "c"] & & \{2,4\} \arrow[ll, "c"] \end{tikzcd}$$

$$X(q) = 1+q+2q^2+q^3+q^4 \quad \underset{q=\zeta^0=1}{\rightsquigarrow} \quad 1+1+2+1+1 = 4 = |X|$$

$$q=\zeta^1 \rightsquigarrow 1+\zeta+2\zeta^2+\zeta^3+\zeta^4 = 0 = |X^{c^1}|$$

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 $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$.

What about C-orbit structure? An equivalent phrasing...

DEFINITION: $(X, X(q), C)$ exhibits a CSP

if the unique expansion $\boxed{X(q) \equiv a_0 + a_1 q + a_2 q^2 + \ldots + a_{n-1} q^{n-1} \mod q^n - 1}$

has this interpretation:

$$\boxed{a_i = \#\ C\text{-orbits on } X \text{ where the stabilizer/isotropy subgroup has size dividing } i}$$

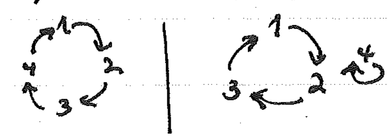
In particular, $a_0 =$ total # of C-orbits

$a_1 =$ # of free C-orbits

i.e. orbits of size $|C|$

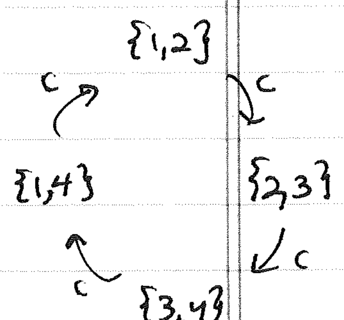
EXAMPLE: $(X, X(q), C)$

$$X = \text{2-subsets of } \{1,2,3,4\}, \qquad X(q) = \begin{bmatrix}4\\2\end{bmatrix}_q, \qquad C \cong \mathbb{Z}/4\mathbb{Z} \text{ or } \mathbb{Z}/3\mathbb{Z}$$

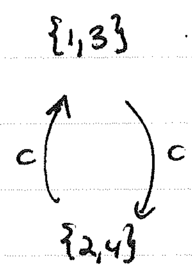


$$X(q) = 1 + q + 2q^2 + q^3 + q^4$$

$$\underbrace{2}_{a_0} + \underbrace{1}_{a_1}\cdot q^1 + \underbrace{2}_{a_2} q^2 + 1\cdot q^3 \mod q^4 - 1$$



$\boxed{a_1 = 1}$ free orbit

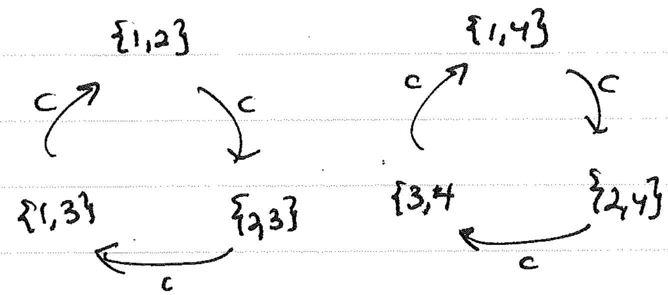


stabilizer subgroup of size 2

$\boxed{a_0 = 2}$ orbits total,

and $\boxed{a_2 = 2}$ since both orbits have stabilizer subgroup size dividing 2

$$\underbrace{2}_{a_0} + \underbrace{2}_{a_1}\cdot q^1 + 2q^2 \mod q^3 - 1$$



$\boxed{a_0 = a_1 = 2}$ orbits total, both free

A frustrating, but important, example ...

THEOREM (Stanton-White-R. 2004)

$X :=$ triangulations of an $(n+2)$-gon

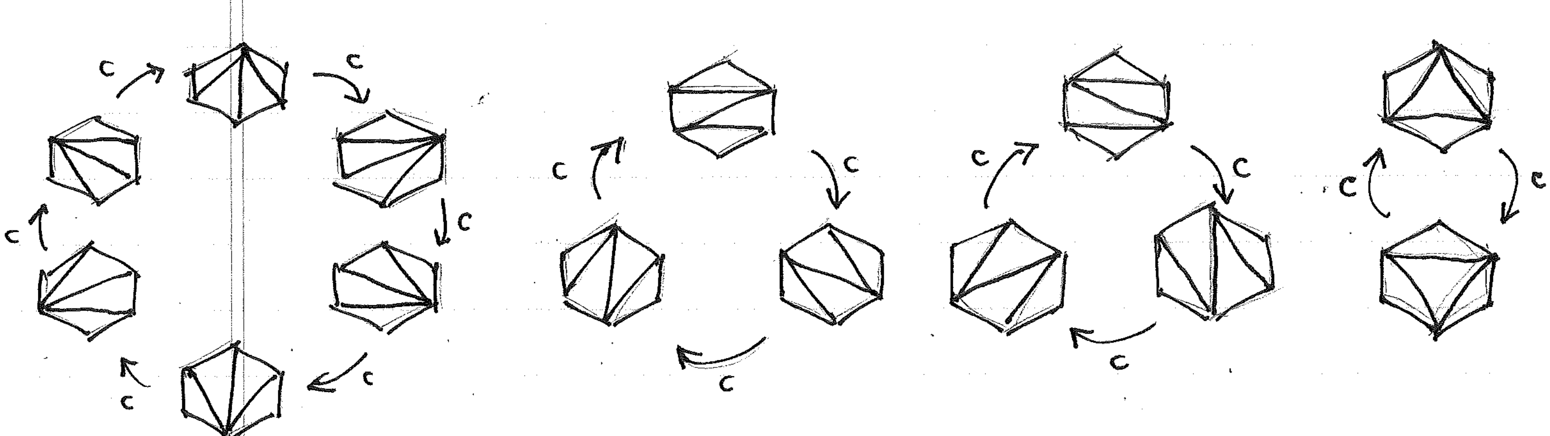
$$X(q) := \frac{1}{[n+1]_q}\begin{bmatrix} 2n \\ n \end{bmatrix}_q =: \text{the } q\text{-Catalan number}$$

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

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

---

e.g. $n=6$



$$X(q) = \frac{1}{[5]_q}\begin{bmatrix} 8 \\ 4 \end{bmatrix}_q = \frac{[8]_q[7]_q[6]_q}{[4]_q[3]_q[2]_q}$$

$\zeta := e^{\frac{2\pi i}{6}}$

$$= 1 + q^2 + q^3 + 2q^4 + q^5 + 2q^6 + q^7 + 2q^8 + q^9 + q^{10} + q^{12}$$

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

$q = \zeta^0 = 1$ | $q = \zeta^3 = -1$ | $q = \zeta^2$ | $q = \zeta^1$

$14 = |X^{c^0}| = |X|$ $\quad$ $6 = |X^{c^3}|$ $\quad$ $2 = |X^{c^2}|$ $\quad$ $0 = |X^{c^1}|$

A yet more frustrating example...

<u>THEOREM</u> (Stanton 2007)

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

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

$C = \mathbb{Z}/4\mathbb{Z}$ rotating by $\{0, \pi/2, \pi, 3\pi/2\}$

---

e.g. $n=3$

$$\begin{tikzcd}
\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix} \arrow[r, "c"] & \begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix} \arrow[d, "c"] & \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} \arrow[d, bend left, "c"] & \begin{bmatrix}0&1&0\\1&-1&1\\0&1&0\end{bmatrix} \arrow[loop right, "c"] \\
\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix} \arrow[u, "c"] & \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix} \arrow[l, "c"] & \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix} \arrow[u, bend left, "c"] &
\end{tikzcd}$$

$\zeta = e^{\frac{2\pi i}{4}} = i$

$$X(q) = \frac{[1]!_q\,[4]!_q\,[7]!_q}{[3]!_q\,[4]!_q\,[5]!_q} = \frac{[7]_q[6]_q}{[3]_q[2]_q}$$
$$= 1+q^2+q^3+q^4+q^5+q^6+q^8$$
$$\equiv 3+1\cdot q^1+2q^2+1\cdot q^3 \mod q^4-1$$

$q=\zeta^0=1$ ⟶ $7 = |X^{c^0}| = |X|$

$q=\zeta^2=-1$ ⟶ $3 = |X^{c^2}|$

$q=\zeta^1=i$ ⟶ $1 = |X^{c^1}|$

Each of the previous 3 CSP's can be proven by a "BAD" (but effective) proof technique:

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

$$|X^{c^d}| = [X(q)]_{q=\zeta^d}$$

when one has a product formula of the form

$$X(q) = \frac{[N_1]_q [N_2]_q \cdots [N_\ell]_q}{[M_1]_q [M_2]_q \cdots [M_\ell]_q}$$

e.g. $X(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q = \dfrac{[n]_q [n-1]_q \cdots [n-(k-1)]_q}{[k]_q [k-1]_q \cdots [1]_q}$

$X(q) = \dfrac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q = \dfrac{[2n]_q [2n-1]_q \cdots [n+2]_q}{[n]_q [n-1]_q \cdots [2]_q}$

$X(q) = \displaystyle\prod_{k=0}^{n-1} \frac{[3k+1]!_q}{[n+k]!_q}$ $\frac{n(3n-1)}{2}$ factors in numerator and denominator

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

(And then hope for an insightful proof later!)

EXAMPLE

$X =$ k-subsets of $\{1,2,\ldots,n\}$

$X(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q$

$C = \mathbb{Z}/n\mathbb{Z}$

(L'Hôpital)
EXERCISE: If ζ^d is a primitive D^{th} root-of-unity then whenever $N \equiv M \bmod D$, one has

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

This can be used to check that...

EXERCISE: If $n = n_1 \cdot D + n_2$ with $0 \leq n_2 \leq D-1$
$k = k_1 \cdot D + k_2$ $\quad 0 \leq k_2 \leq D-1$

then $$\begin{bmatrix} n \\ k \end{bmatrix}_{q=\zeta^d} = \binom{n_1}{k_1} \cdot \begin{bmatrix} n_2 \\ k_2 \end{bmatrix}_{q=\zeta^d}$$

(with convention that $\binom{N}{M} = \begin{bmatrix} N \\ M \end{bmatrix}_q = 0$ if $M > N$)

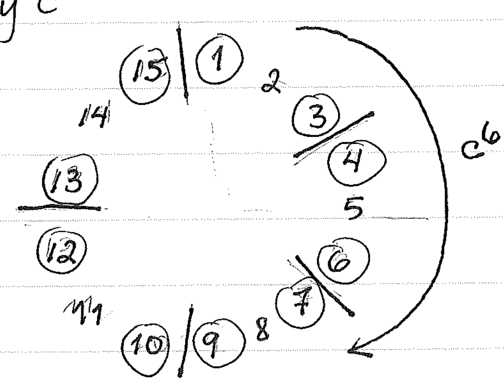
In particular, $$[X(q)]_{q=\zeta^d} = \begin{bmatrix} n \\ k \end{bmatrix}_{q=\zeta^d} = \begin{cases} \binom{n/D}{k/D} & \text{if } D \text{ divides } k \\ 0 & \text{otherwise.} \end{cases}$$

(since $\zeta^n = 1$ implies D divides N)

But k-subsets of $\{1,2,\ldots,n\}$ fixed by c^d biject with k/D-subsets of n/D:

e.g. $n=15$ $\quad d=6$
$k=10$ $\quad D=5$

$$\begin{bmatrix} 15 \\ 10 \end{bmatrix}_{q=\zeta^6} = \binom{3}{2}$$



The GOOD proof technique

is a linear-algebraic paradigm, generalizing one of J. Stembridge (1994) for his "$q=-1$ phenomenon":

To show $\quad \#\{x \in X : c^d(x) = x\} = [X(q)]_{q=\zeta^d}$

try to find a $\mathbb{C}$-vector space V having ...

- a basis $\{e_x : x \in X\}$ permuted by c as in the C-action on X, that is,
$$c(e_x) = e_{c(x)}$$
- a grading $V = \bigoplus_{i \geq 0} V_i$ in which c acts on V_i as ζ^i (so c^d acts on V_i as $(\zeta^i)^d$)

and $\mathrm{Hilb}(V,q) := \sum_{i \geq 0} \dim_{\mathbb{C}} V_i \cdot q^i = X(q)$

Then computing in two ways

$$\mathrm{Trace}(c^d : V \to V)$$

$$
\begin{array}{l|l}
= \#\{e_x : c^d(e_x) = e_x\} & = \sum_{i \geq 0} \mathrm{Trace}(c^d : V_i \to V_i) \\
= \#\{x \in X : c^d(x) = x\} & = \sum_{i \geq 0} \dim_{\mathbb{C}} V_i \cdot (\zeta^i)^d \\
= |X^{c^d}| & = [X(q)]_{q=\zeta^d}
\end{array}
$$

same as $(\zeta^d)^i$

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 = triangulations of $(n+2)$-gon
  $X(q) = \frac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q$
  $C = \mathbb{Z}/(n+2)\mathbb{Z}$

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

$GL_n(\mathbb{F}_q)$ - PROTO - Example

Recall one of our PROTO-Examples of a CSP:

X = k-subsets of $\{1,2,\dots,n\}$

$$X(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-q^0)(q^n-q^1)\cdots(q^n-q^{k-1})}{(q^k-q^0)(q^k-q^1)\cdots(q^k-q^{k-1})} = q\text{-binomial}$$

$C = \langle c \rangle \cong \mathbb{Z}/n\mathbb{Z}$, c = n-cycle  inside $\mathfrak{S}_n$

for a fixed prime power $q = p^m$

$X :=$ finite Grassmannian $Gr(k, \mathbb{F}_q^n)$
$=$ k-dimensional $\mathbb{F}_q$-subspaces inside $\mathbb{F}_q^n$ $(\cong \mathbb{F}_{q^n})$

$$X(t) := \begin{bmatrix} n \\ k \end{bmatrix}_{q,t} := \frac{(1-t^{q^n-q^0})(1-t^{q^n-q^1})\cdots(1-t^{q^n-q^{k-1}})}{(1-t^{q^k-q^0})(1-t^{q^k-q})\cdots(1-t^{q^k-q^{k-1}})} = (q,t)\text{-binomial}$$

$C = \langle c \rangle$, c a Singer cycle

$= \mathbb{F}_{q^n}^\times = \{1, c, c^2, \dots, c^{q^n-2}\} \longleftrightarrow GL_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong GL_n(\mathbb{F}_q)$

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

THEOREM (Stanton-White-R. 2004; cf. K. Drudge 2002)
The latter triple $(X, X(q), C)$ exhibits a CSP

EXAMPLE: $q=2,\ n=4,\ k=2$

$$\mathbb{F}_{q^n} = \mathbb{F}_{2^4} = \mathbb{F}_{16} \cong \mathbb{F}_2[\alpha]/(\alpha^4+\alpha+1)$$

$$C = \mathbb{F}_{q^n}^\times = \mathbb{F}_{2^4}^\times = \{1, \overset{c}{\overset{\shortparallel}{\alpha}}, \alpha^2, \alpha^3, \ldots, \alpha^{14}\} \cong \mathbb{Z}/(2^4-1)\mathbb{Z} = \mathbb{Z}/15\mathbb{Z}$$

$$\begin{array}{ccc} \downarrow & & \overset{c}{\downarrow} \\ GL_{\mathbb{F}_2}(\mathbb{F}_{16}) \cong GL_4(\mathbb{F}_2) & & \begin{bmatrix} 0&0&0&1\\ 1&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \end{bmatrix} \end{array}$$

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

$$\#\{x \in \underset{Gr(2,\mathbb{F}_2^4)}{\overset{\shortparallel}{X}} : c^3(x) = x\} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{\underset{2}{q}, \underset{\zeta^3}{t}}$$

where $\zeta = e^{2\pi i/q^n-1} = e^{\frac{2\pi i}{15}}$

$$= \left[\frac{(1-t^{2^4-2^0})(1-t^{2^4-2^1})}{(1-t^{2^2-2^0})(1-t^{2^2-2^1})}\right]_{t=\zeta^3}$$

a 5^{th} root-of-unity

$$= \left[\frac{(1-t^{15})(1-t^{14})}{(1-t^3)(1-t^2)}\right]_{t=e^{\frac{2\pi i}{5}}}$$

$$= \frac{15}{3} \cdot 1 = 5$$

<u>Sketch of "BAD" proof:</u> Given $c^d \in \mathbb{F}_{q^n}^\times = \{1, c, c^2, \ldots, c^{q^n-2}\}$

name the intermediate subfield generated by c^d:

$$\begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q(c^d) = \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n \\ | \\ \mathbb{F}_q \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q, t=\zeta^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

will be <u>preserved by c^d</u> $\iff$ it is an $\underset{\mathbb{F}_{q^m}}{\underset{\parallel}{\mathbb{F}_q(c^d)}}$-subspace,

and the number of such k/m-dimensional $\mathbb{F}_{q^m}$-subspaces of $\underset{\mathbb{F}_{(q^m)^{n/m}}}{\underset{\parallel\!\mathrm{S}}{\mathbb{F}_{q^n}}}$

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(c^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\quad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q, t=\zeta^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$

Sketch of
"BAD" proof: Given $c^d \in \mathbb{F}_{q^n}^\times = \{1, \varsigma, \varsigma^2, \ldots, \varsigma^{q^n-2}\}$

name the intermediate subfield generated by c^d:

$$\begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q(c^d) = \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n \\ | \\ \mathbb{F}_q \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q, t=\varsigma^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

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

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

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(c^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\quad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q, t=\varsigma^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$

Sketch of
<u>"BAD" proof:</u> Given $\zeta^d \in \mathbb{F}_{q^n}^\times = \{1, \zeta, \zeta^2, \ldots, \zeta^{q^n-2}\}$

name the intermediate subfield generated by ζ^d:

$$\begin{array}{cl} \mathbb{F}_{q^n} & \\ | & \\ \mathbb{F}_q(\zeta^d) = \mathbb{F}_{q^m} & \text{for some divisor } m \text{ of } n \\ | & \\ \mathbb{F}_q & \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q,\, t=\zeta^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

will be <u>preserved by ζ^d</u> $\iff$ it is an $\underset{\mathbb{F}_{q^m}}{\underset{\parallel}{\mathbb{F}_q(\zeta^d)}}$-subspace,

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

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(\zeta^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\qquad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q,\, t=\zeta^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$

Sketch of
"BAD" proof: Given $c^d \in \mathbb{F}_{q^n}^\times = \{1, \varsigma, \varsigma^2, \ldots, \varsigma^{q^n-2}\}$

name the intermediate subfield generated by c^d:

$$\begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q(\varsigma^d) = \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n \\ | \\ \mathbb{F}_q \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q, t=\varsigma^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

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

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

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(\varsigma^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\quad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q, t=\varsigma^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$

Sketch of
<u>"BAD" proof</u>: Given $c^d \in \mathbb{F}_{q^n}^\times = \{1, c, c^2, \ldots, c^{q^n-2}\}$

name the intermediate subfield generated by c^d:

$$\begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q(c^d) = \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n \\ | \\ \mathbb{F}_q \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q, t=\zeta^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

will be <u>preserved by c^d</u> $\iff$ it is an $\underset{\mathbb{F}_{q^m}}{\underset{\|}{\mathbb{F}_q(c^d)}}$-subspace,

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

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(c^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\quad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q, t=\zeta^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$

Sketch of
<u>"BAD" proof:</u> Given $c^d \in \mathbb{F}_{q^n}^\times = \{1, c, c^2, \ldots, c^{q^n-2}\}$

name the intermediate subfield generated by c^d:

$$\begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q(c^d) = \mathbb{F}_{q^m} \quad \text{for some divisor } m \text{ of } n \\ | \\ \mathbb{F}_q \end{array}$$

Then check using the L'Hôpital exercise

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q, t=\zeta^d} = \begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$$

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

will be <u>preserved by c^d</u> $\iff$ it is an $\underset{\mathbb{F}_{q^m}}{\underset{\parallel}{\mathbb{F}_q(c^d)}}$-subspace,

and the number of such k/m-dimensional $\mathbb{F}_{q^m}$-subspaces of $\underset{\mathbb{F}_{(q^m)^{n/m}}}{\underset{\parallel\!\mathrm{S}}{\mathbb{F}_{q^n}}}$

is $\begin{cases} \begin{bmatrix} n/m \\ k/m \end{bmatrix}_{q^m} & \text{if } m \text{ divides } k, \\ 0 & \text{otherwise.} \end{cases}$ ∎

e.g. $\begin{array}{c} \mathbb{F}_{2^4} \\ | \\ \mathbb{F}_2(c^3) = \mathbb{F}_{2^2} \\ | \\ \mathbb{F}_2 \end{array}$ $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_{2=q, t=\zeta^3} = \begin{bmatrix} 4/2 \\ 2/1 \end{bmatrix}_{q^2=4} = [2]_{q^2=4} = (1+q^2)_{q^2=4} = 5$