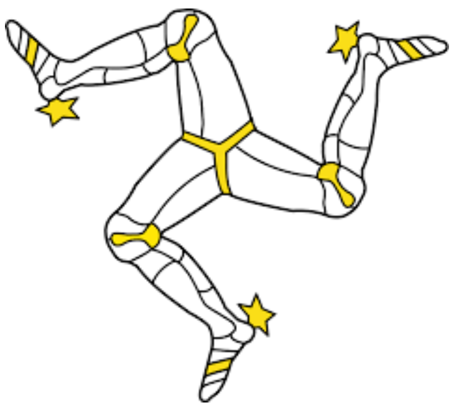
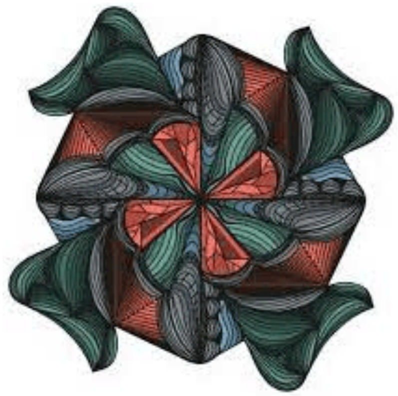
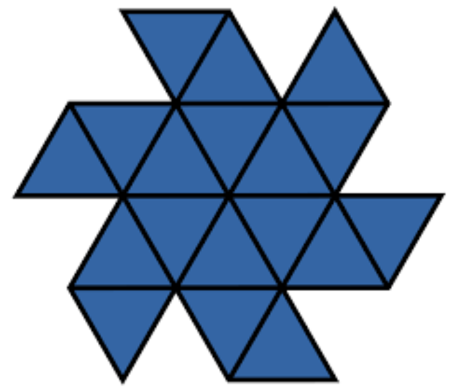
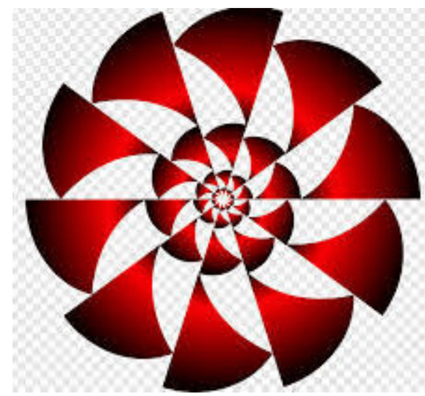
Counting and cyclic symmetry

Vic Reiner
Univ. of Minnesota

Sue Geller Lecture

Texas A&M University

April 10, 2025

1. Counting formulas

2. Some old and beloved ones

3. They're hiding some new tricks, about counting with cyclic symmetry!

4. Brute force versus linear algebra explanations

1. Counting formulas

Enumerative combinatorics often seeks

exact formulas $a_n = |X_n|$

counting families of combinatorial sets X_n

indexed by $n = 1, 2, 3, \ldots$

We like them best when

a_n has a product formula,

with no summations involved.

EXAMPLE X_n = permutations of $\{1, 2, \dots, n\}$

$= \text{bijective maps } \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$

$$a_n = |X_n| = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 = n! \quad \text{factorial}$$

$n=3$

$$\left.\begin{array}{ccc} 1 \to 1 & & 1 \to 2 \\ 2 \to 2 & & 2 \to 1 \\ 3 \to 3 & & 3 \to 3 \end{array}\right\} 2!$$

$$\left.\begin{array}{ccc} 1 \to 1 & & 1 \to 3 \\ 2 \to 3 & & 2 \to 1 \\ 3 \to 2 & & 3 \to 2 \end{array}\right\} 2!$$

$$\left.\begin{array}{ccc} 1 \to 2 & & 1 \to 3 \\ 2 \to 3 & & 2 \to 2 \\ 3 \to 1 & & 3 \to 1 \end{array}\right\} 2!$$

$$a_3 = 3!$$

$$= 3 \cdot 2!$$

$$= 3 \cdot 2 \cdot 1$$

Why prefer product formulas?

- easier asymptotic growth analysis

EXAMPLE: $a_n = n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ Stirling's approximation 1730

... useful in algorithmic complexity, probability estimation

- easier for checking divisibilities, vanishing modulo primes p

EXAMPLE: $a_n = n! = n(n-1)\cdots 3\cdot 2\cdot 1$ $\equiv 0 \bmod p$ if $p \leq n$
$\not\equiv 0 \bmod p$ if $p > n$

2. Some old and beloved counting formulas

EXAMPLE $X_{n,k} = \{k\text{-element subsets of } \{1,2,\dots,n\}\}$

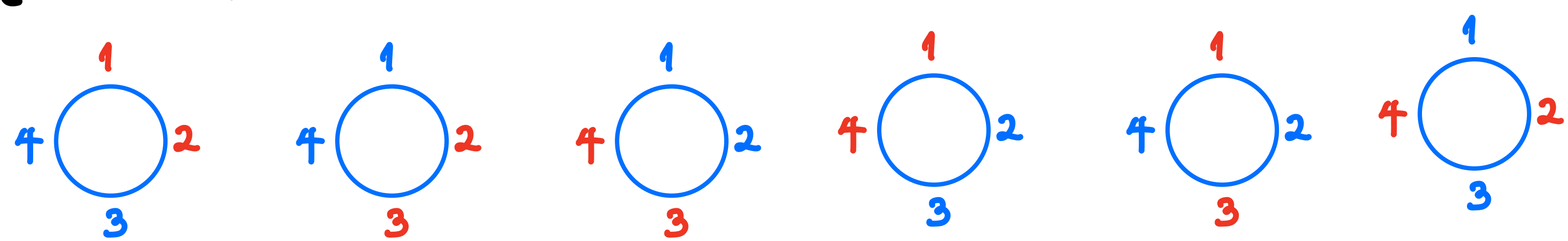
$$|X_{n,k}| = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

binomial coefficient

$n=4$
$k=2$

$X_{4,2} = \{2\text{-element subsets of } \{1,2,3,4\}\}$

$= \{ \{1,2\}, \{2,3\}, \{3,4\}, \{1,4\}, \{1,3\}, \{2,4\} \}$



$$|X_{4,2}| = \binom{4}{2} = \frac{4!}{2!\,2!} = \frac{4\cdot 3\cdot \cancel{2}\cdot \cancel{1}}{2\cdot \cancel{1}\cdot \cancel{2}\cdot \cancel{1}} = \frac{4\cdot 3}{2} = 6$$

Slightly miraculous that $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ lies in $\mathbb{Z}$!

Less miraculous if you know Pascal's recurrence

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{for } k, n \geq 1$$

$$\binom{n}{0} = \binom{n}{n} = 1$$

$k = 0$, 1, 2, 3, 4, 5

$n = 0$ 1

1 .... 1 1

2 .... 1 2 1

3 .... 1 3 3 1

4 .... 1 4 6 4 1

5 .... 1 5 10 10 5 1

$\vdots$

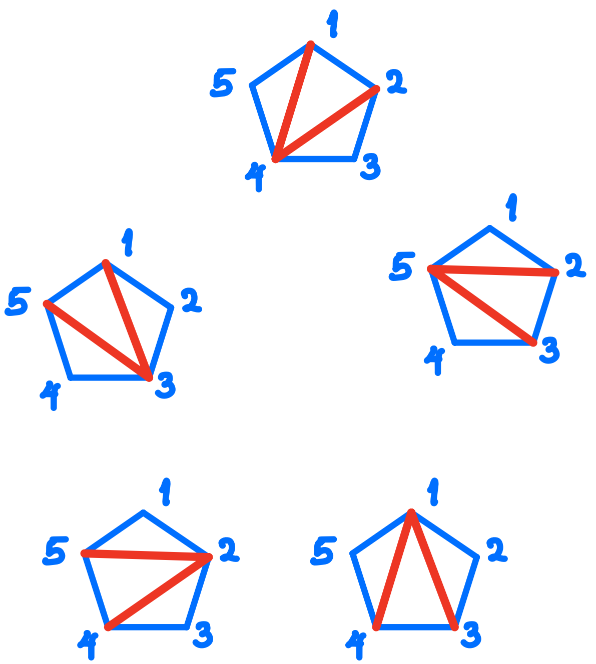
$\binom{3}{1} + \binom{3}{2} = \binom{4}{2}$

EXAMPLE

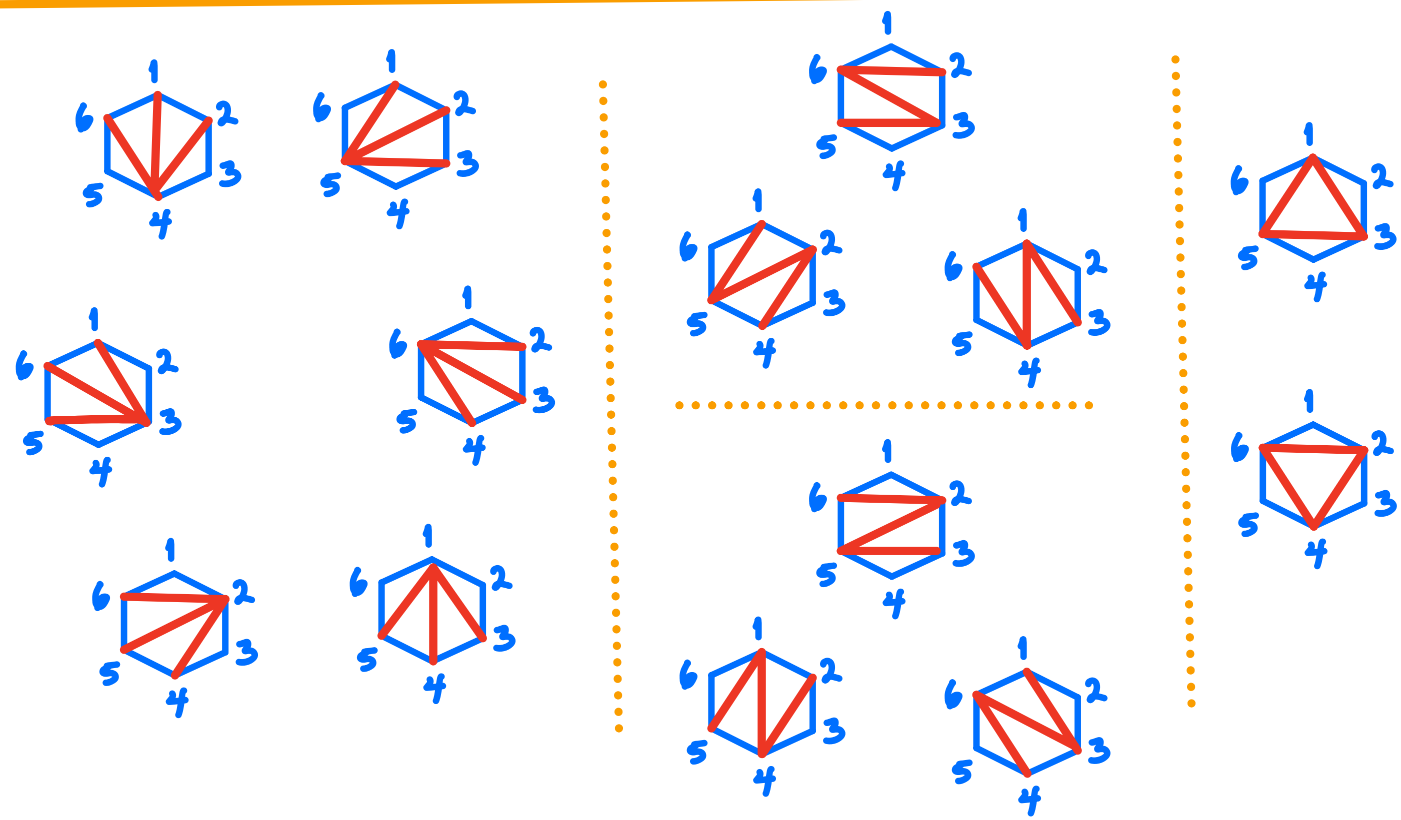
X_n = triangulations of an $(n+2)$-sided polygon

have $|X_n| = \frac{1}{n+1}\binom{2n}{n} = \frac{(n+2)(n+3)\cdots(2n-1)(2n)}{2\cdot 3\cdot \cdots (n-1)\cdot n}$

Catalan number
(Euler, Segner, Goldbach 1750's)



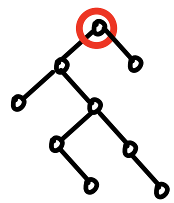
$$|X_3| = \frac{1}{4}\binom{6}{3} = \frac{5\cdot\cancel{6}}{\cancel{2}\cdot\cancel{3}} = 5$$



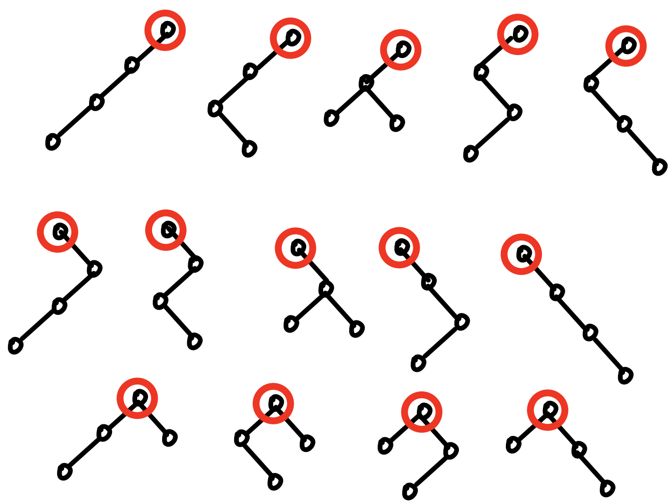
$$|X_4| = \frac{1}{5}\binom{8}{4} = \frac{\cancel{6}\cdot 7\cdot 8}{\cancel{2}\cdot\cancel{3}\cdot 4} = 14$$

Actually, the Catalan number $\frac{1}{n+1}\binom{2n}{n}$ counts many things, some with apparent cyclic symmetry, some not ...

X_n = rooted plane binary trees with n nodes



X_4

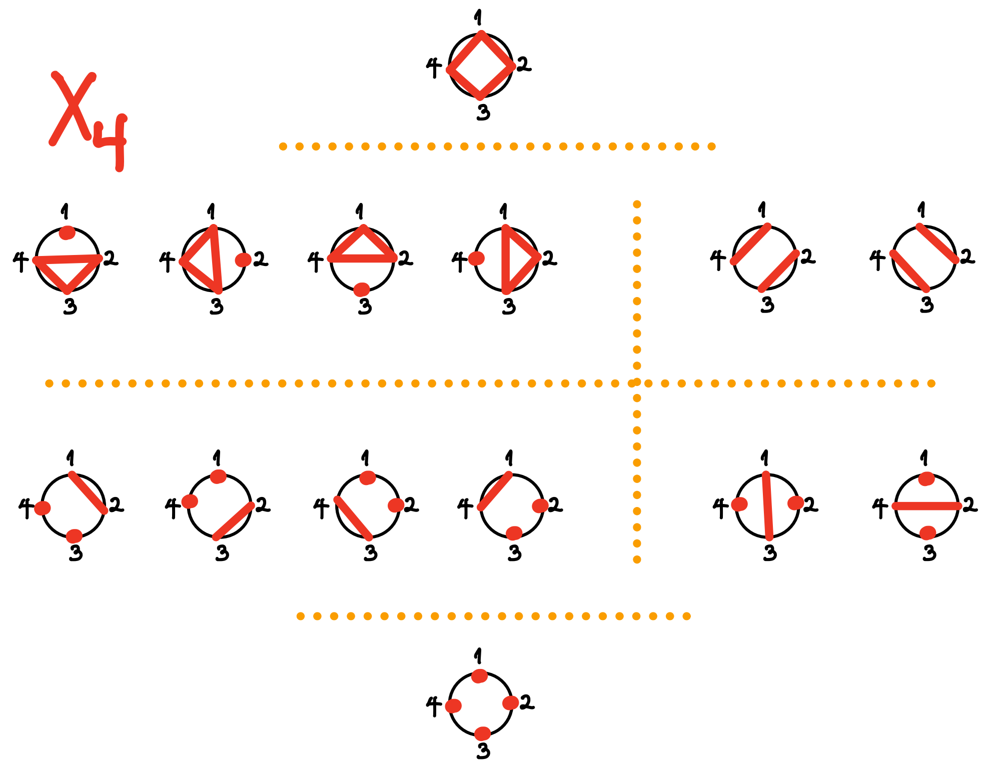


$$|X_4| = \frac{1}{5}\binom{8}{4} = 14$$

NO SYMMETRY?

X_n = set partitions of $\{1,2,\ldots,n\}$ around a circle whose blocks are noncrossing

X_4



4-FOLD SYMMETRY

$$|X_4| = \frac{1}{5}\binom{8}{4} = 14$$

EXAMPLE

$X_n =$ $n \times n$ alternating sign matrices

$= n \times n$ matrices of $0, +1, -1$ entries,

alternating $+1, -1, +1, -1, \ldots, +1, -1, +1$ in each row, column

if one ignores the 0 entries

$$\begin{bmatrix} 0 & +1 & 0 & 0 & 0 \\ +1 & -1 & 0 & +1 & 0 \\ 0 & +1 & 0 & -1 & +1 \\ 0 & 0 & 0 & +1 & 0 \\ 0 & 0 & +1 & 0 & 0 \end{bmatrix}$$

has $$|X_n| = \frac{1! \cdot 4! \cdot 7! \cdots (3n-2)!}{n!\,(n+1)!\,(n+2)! \cdots (2n-1)!} = \prod_{i=0}^{n-1} \frac{(3i+1)!}{(n+i)!}$$

CONJECTURED by Mills, Robbins, Rumsey 1982

PROVEN by Zeilberger 1992, Kuperberg 1995

$n=3$

$$|X_3| = \frac{1!\,4!\,7!}{3!\,4!\,5!} = 7$$

$$\begin{bmatrix} +1 & 0 & 0 \\ 0 & 0 & +1 \\ 0 & +1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & +1 & 0 \\ 0 & 0 & +1 \\ +1 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & +1 \\ +1 & 0 & 0 \\ 0 & +1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & +1 & 0 \\ +1 & 0 & 0 \\ 0 & 0 & +1 \end{bmatrix}$$

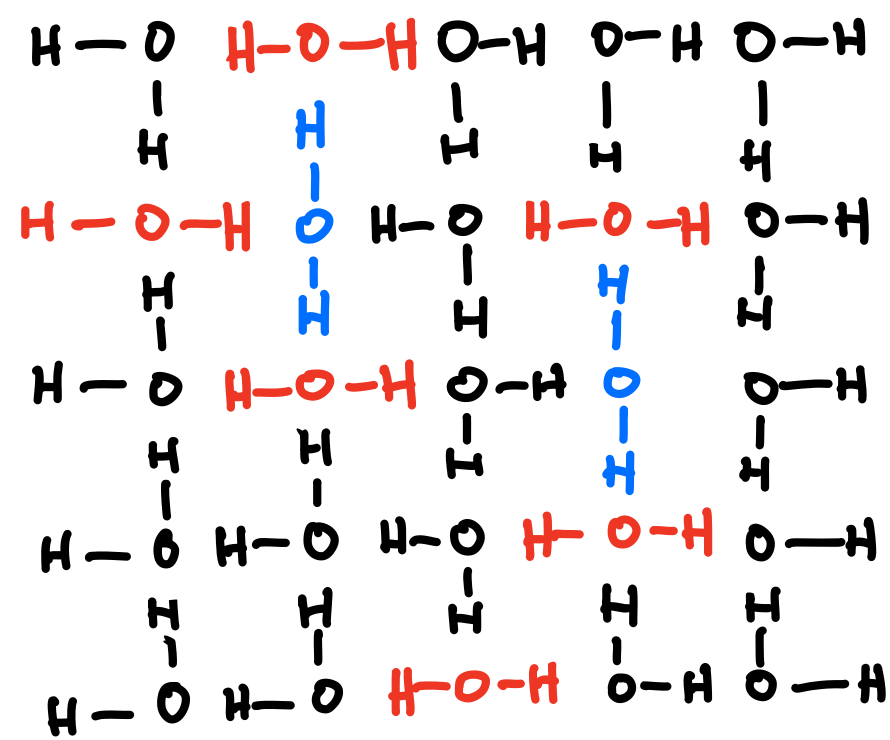
4-FOLD SYMMETRY

$$\begin{bmatrix} +1 & 0 & 0 \\ 0 & +1 & 0 \\ 0 & 0 & +1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & +1 \\ 0 & +1 & 0 \\ +1 & 0 & 0 \end{bmatrix}$$

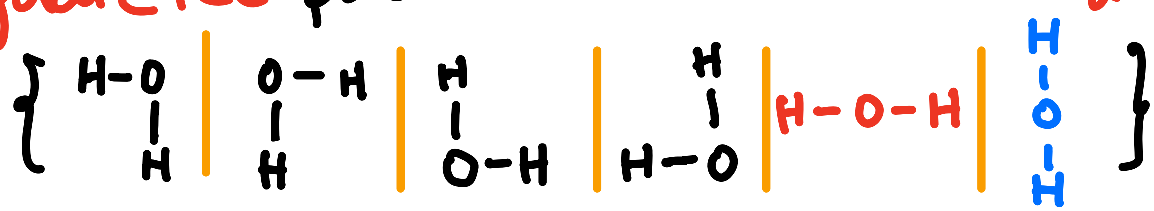
$$\begin{bmatrix} 0 & +1 & 0 \\ +1 & -1 & +1 \\ 0 & +1 & 0 \end{bmatrix}$$

Kuperberg's proof used statistical physics results where alternating sign matrices were counted in the guise of square-ice configurations :

$$\begin{bmatrix} 0 & +1 & 0 & 0 & 0 \\ +1 & -1 & 0 & +1 & 0 \\ 0 & +1 & 0 & -1 & +1 \\ 0 & 0 & 0 & +1 & 0 \\ 0 & 0 & +1 & 0 & 0 \end{bmatrix} \xleftrightarrow{\text{bijection}}$$



square ice packs 6 orientations of H_2O



3. Hiding counts with cyclic symmetry

Sometimes the set X has a natural cyclic symmetry operation c of order m acting on it,

that is
$$\begin{aligned} X &\xrightarrow{\ c\ } X \\ x &\longmapsto c(x) \end{aligned} \qquad \text{with } c^m = \text{identity on } X$$

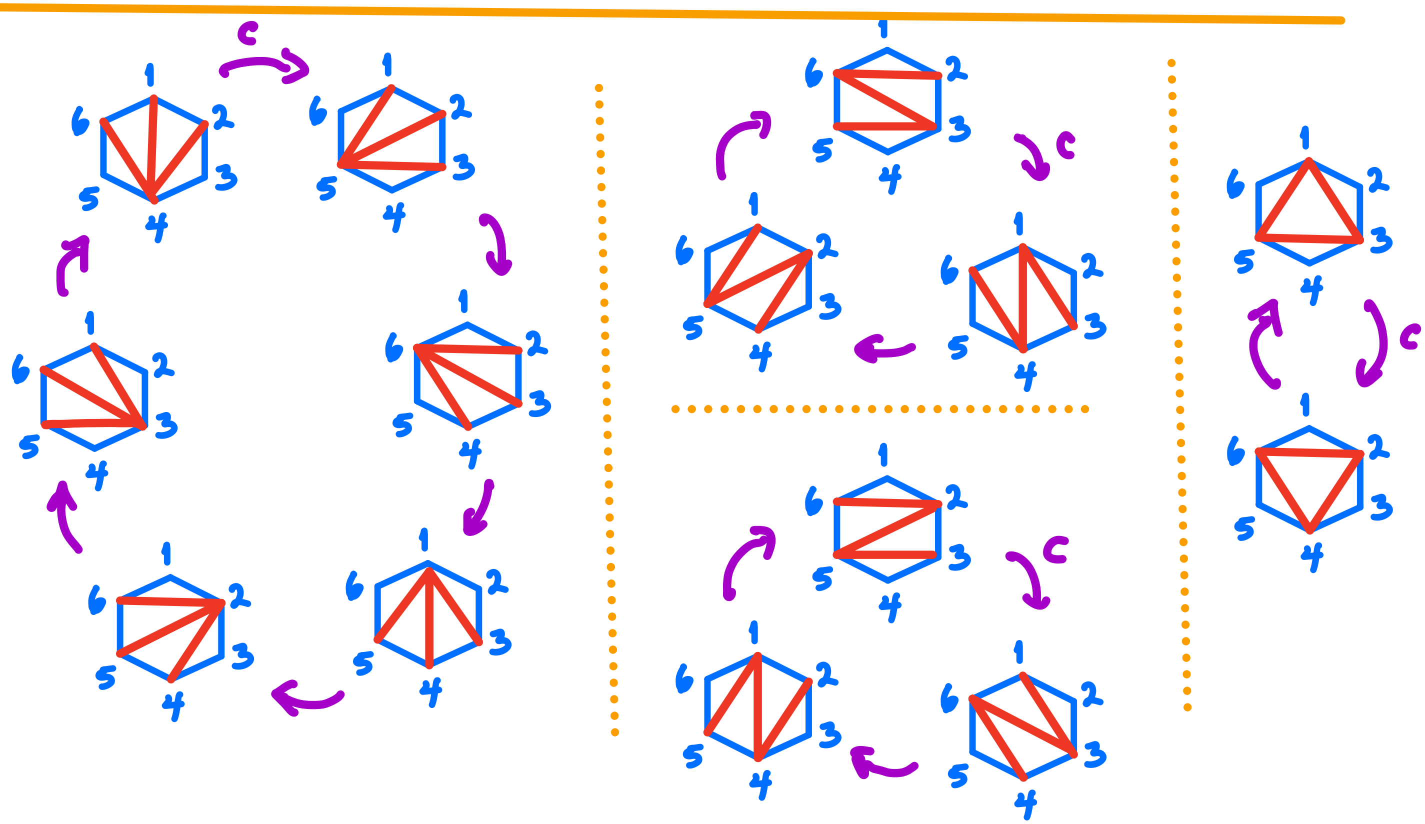
EXAMPLE

X = triangulations of 6-gon

$X \xrightarrow{c} X$

rotation through $2\pi/6$

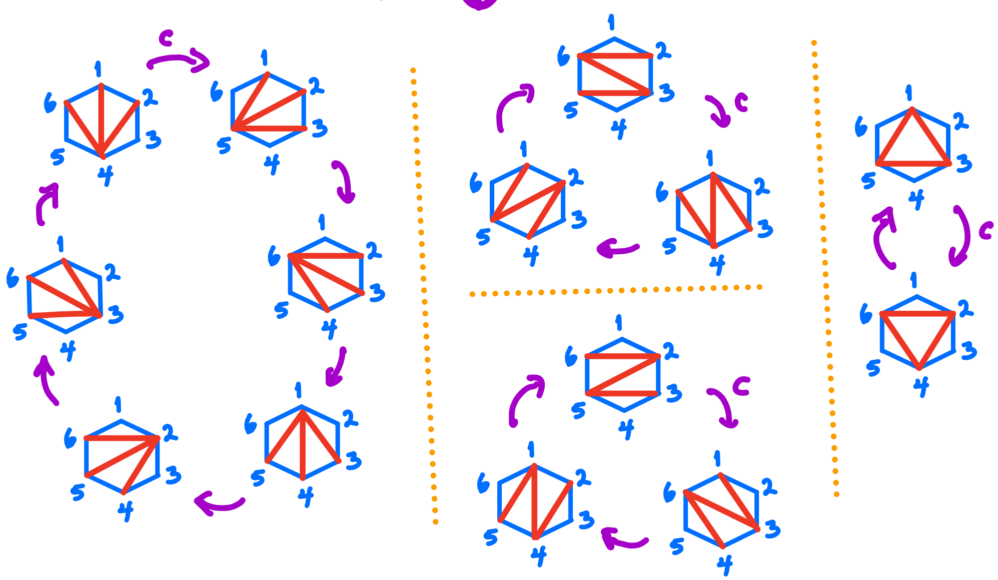
$m=6$



NATURAL QUESTION: What is the c-orbit structure, that is...

- Number $o(d)$ of orbits of size d for each d dividing m?
- Cardinalities $|X^{c^d}|$ of $X^{c^d} := \{x \in X : c^d(x) = x\}$
  $= c^d$-fixed set for each d dividing m?

EXAMPLE $m=6$



d	$o(d)$	$\lvert X^{c^d} \rvert$
6	1	14
3	2	6
2	1	2
1	0	0

Actually, $\begin{cases} \{\theta(d)\}_{d \text{ dividing } m} \\ \{|X^{c^d}|\}_{d \text{ dividing } m} \end{cases}$ are equivalent data:

2-PART EXERCISE:

(a) $$|X^{c^d}| = \sum_{e \text{ dividing } d} e \cdot \theta(e)$$

(b) $$d \cdot \theta(d) = \sum_{e \text{ dividing } d} \mu\left(\tfrac{d}{e}\right) \cdot |X^{c^e}|$$

Möbius function

Our old friends are hiding the $\{|X^{c^d}|\}_{d \text{ dividing } m}$ data in their q-analogues ...

These q-analogues of $|X|$ are polynomials $X(q)$ in a variable q, all with $|X| = X(1)$:

$$|X| \xleftarrow{q=1} X(q)$$

n $\qquad [n]_q \overset{\text{DEF}}{:=} 1+q+q^2+q^3+\cdots+q^{n-1} = \frac{1-q^n}{1-q}$ $\leftarrow$ q-number

$n!$ $\qquad [n]!_q \overset{\text{DEF}}{:=} [1]_q[2]_q[3]_q\cdots[n]_q$ $\leftarrow$ q-factorial

$\binom{n}{k}$ $\qquad \begin{bmatrix} n \\ k \end{bmatrix}_q \overset{\text{DEF}}{:=} \frac{[n]!_q}{[k]!_q\,[n-k]!_q}$ $\leftarrow$ q-binomial (Euler, Gauss)

$\frac{1}{n+1}\binom{2n}{n}$ $\qquad \frac{1}{[n+1]_q}\begin{bmatrix} 2n \\ n \end{bmatrix}_q$ $\leftarrow$ q-Catalan (MacMahon) 1915

$\prod_{i=0}^{n-1} \frac{(3i+1)!}{(n+i)!}$ $\qquad \prod_{i=0}^{n-1} \frac{[3i+1]!_q}{[n+i]!_q}$

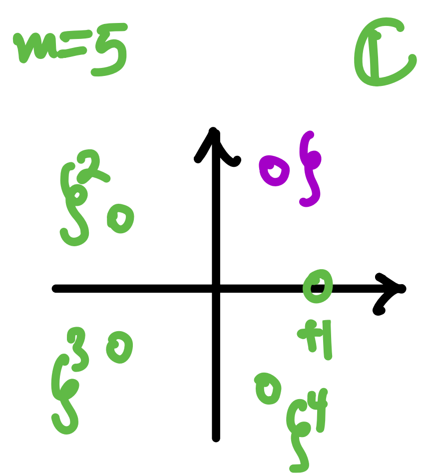
How do these $X(q)$ hide the $\{|X^{c^d}|\}$ data?

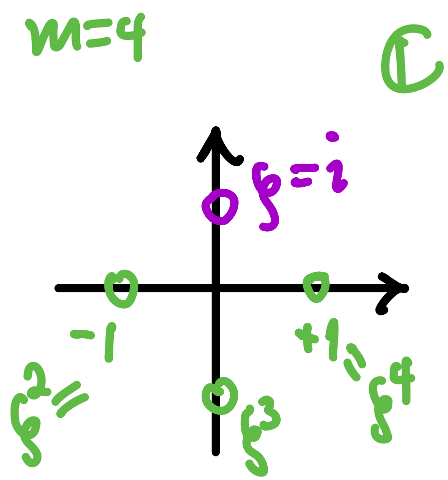
DEFINITION: (Stanton-White 2004 -R.)

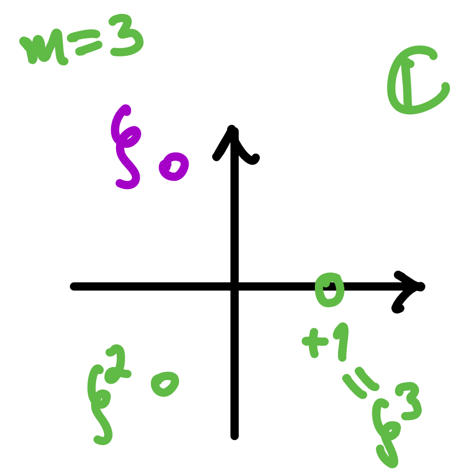
Say a polynomial $X(q)$ in q and a symmetry $X \xrightarrow{c} X$ of order m exhibit a cyclic sieving phenomenon (CSP)

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

where $\zeta = e^{\frac{2\pi i}{m}}$ a complex (primitive) m^{th} root-of-unity







THEOREM: (RSW 2004)

$$X_{n,k} = k\text{-element subsets of } \{1,2,\dots,n\}$$

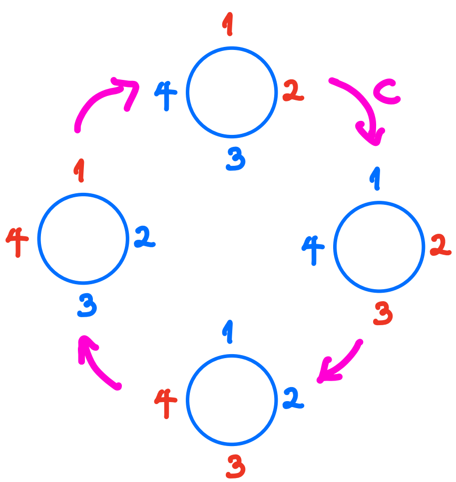
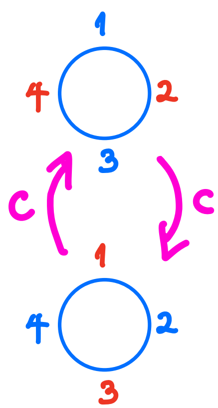
$$\Big\downarrow\ c = \text{rotating } i \mapsto i+1 \text{ modulo } n$$

$$X_{n,k}$$

and $X_{n,k}(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q$ exhibits a CSP.

EXAMPLE:

$X_{4,2}$

$$X_{4,2}(q) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4]!_q}{[2]!_q\,[2]!_q}$$

$$= \frac{[4]_q\,[3]_q\,\cancel{[2]_q}\,\cancel{[1]_q}}{[2]_q\,\cancel{[1]_q}\cdot\cancel{[2]_q}\,\cancel{[1]_q}}$$

$$= \frac{(1+q+q^2+q^3)(1+q+q^2)}{1+q}$$

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

$q = \zeta^0 = \zeta^4 = 1$: $1+1+2+1+1 = 6 = |X^{c^0}| = |X|$

$q = \zeta^2 = -1$: $1-1+2-1+1 = 2 = |X^{c^2}|$

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

$m=4$, $\zeta = i$

REMARK: $\begin{bmatrix} n \\ k \end{bmatrix}_q$ also has meaning when $q = p^\ell$ for a prime p, so $q = |\mathbb{F}_q|$ for a finite field $\mathbb{F}_q$:

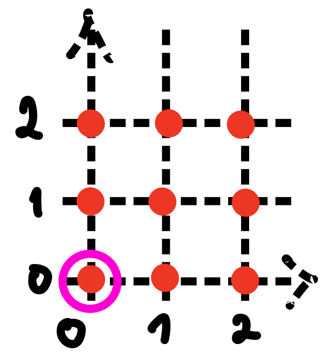
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \left| \, k\text{-dimensional } \mathbb{F}_q\text{-linear subspaces of } (\mathbb{F}_q)^n \, \right|$$

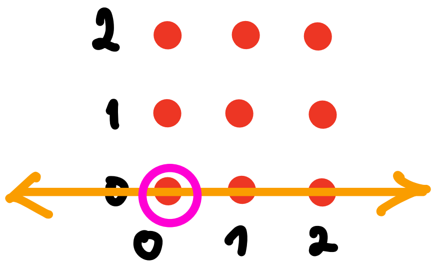
EXAMPLE

$q=3$

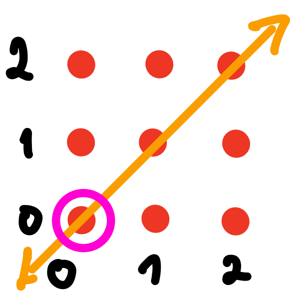
$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = \frac{[2]!_q}{[1]!_q \, [1]!_q} = [2]_q = q+1 \overset{q=3}{=} 3+1 = 4$$

counts lines in $(\mathbb{F}_3)^2$ through $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$

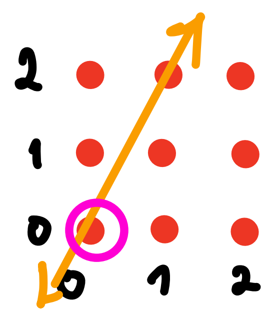




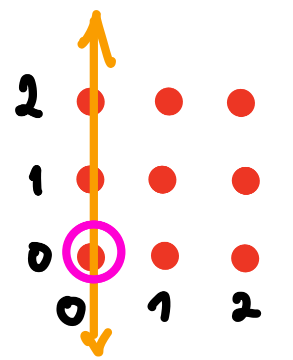
slope 0



slope 1



slope 2



slope ∞

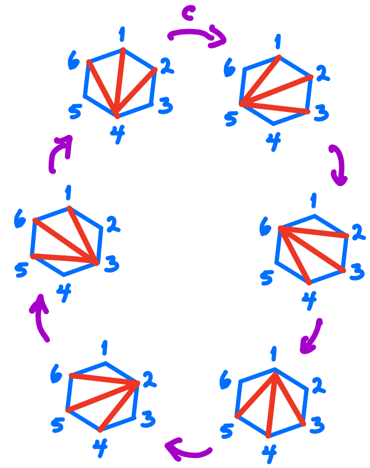
q-Catalan polynomials $\frac{1}{[n+1]_q}\begin{bmatrix} 2n \\ n \end{bmatrix}_q$ perform double duty:

THEOREM: Using the polynomial $X_n(q) := \frac{1}{[n+1]_q}\begin{bmatrix} 2n \\ n \end{bmatrix}_q$,
(RSW 2004) one obtains a CSP for both

- $X_n = \{$ triangulations of $(n+2)$-sided polygon $\}$

$$X_n \xrightarrow{c \,=\, \text{rotating by } \frac{2\pi}{n+2} \text{ of order } m=n+2} X_n$$

$n=4$
$m=6$

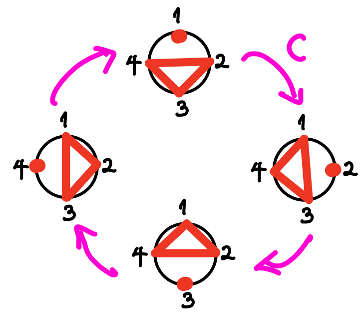


AND

- $X_n = \{$ set partitions of $\{1,2,\ldots,n\}$ whose blocks are circularly noncrossing $\}$

$$X_n \xrightarrow{c \,=\, \text{rotating by } \frac{2\pi}{n} \text{ of order } m=n} X_n$$

$n=4$
$m=4$



EXAMPLE $n=4$

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

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

$q=\zeta^0=\zeta^6=1$ $\rightsquigarrow$ $14=|X|$

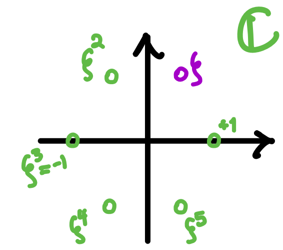
$q=\zeta^3=-1$ $\rightsquigarrow$ $6=|X^{c^3}|$

$q=\zeta^2$ $\rightsquigarrow$ $2=|X^{c^2}|$

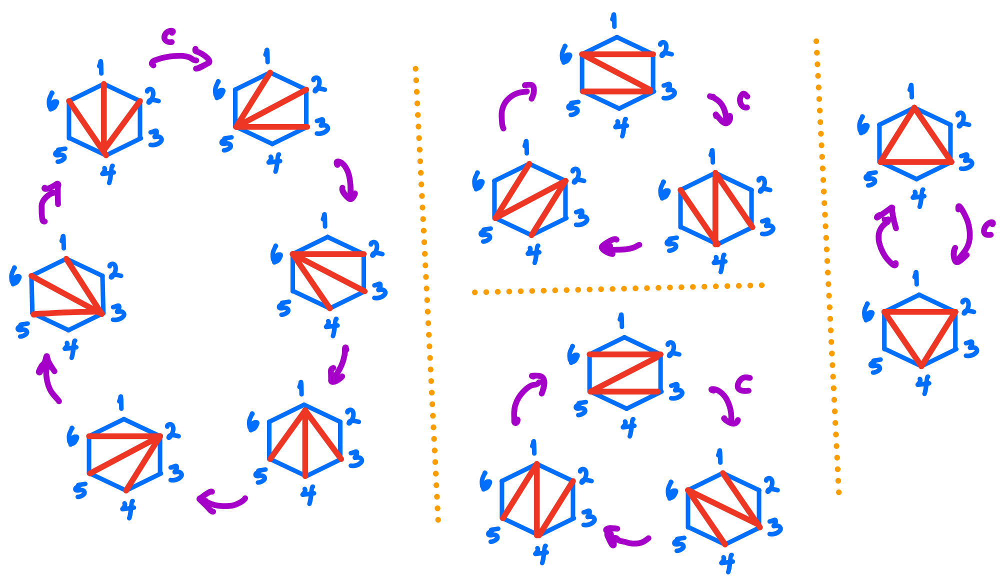
$q=\zeta^1$ $\rightsquigarrow$ $0=|X^{c^1}|$

$m=6$

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



X_4 = triangulations of hexagon



d	$\lvert X^{c^d}\rvert$
6	14
3	6
2	2
1	0

EXAMPLE $n=4$

$$X_n(q) = \frac{1}{[4+1]_q}\begin{bmatrix}8\\4\end{bmatrix}_q = \frac{[6]_q\,[7]_q\,[8]_q}{[2]_q\,[3]_q\,[4]_q} \quad \text{(same!)}$$

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

$q=\zeta^0=\zeta^4=1$ $\rightsquigarrow$ $14=|X|$

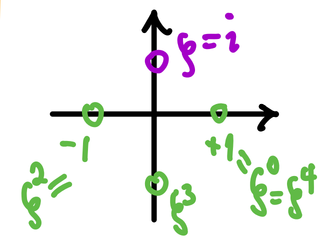
$q=\zeta^2=-1$ $\rightsquigarrow$ $6=|X^{c^2}|$

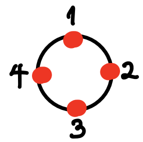
$q=\zeta^1=i$ $\rightsquigarrow$ $2=|X^{c^1}|$

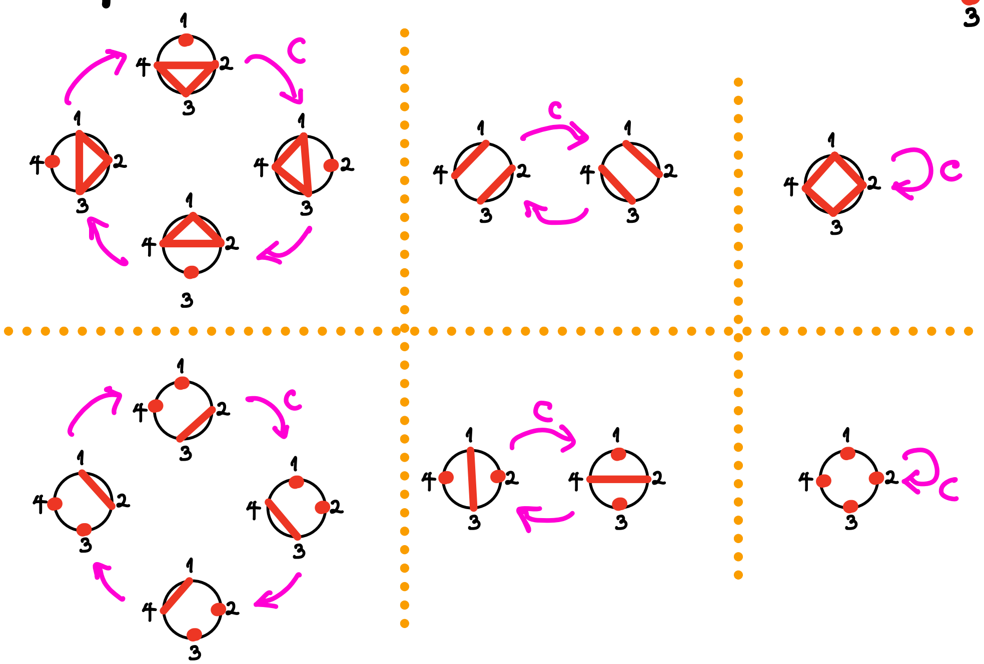
$m=4$

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

$\mathbb{C}$



$X_4 =$ noncrossing partitions of 



d	$\lvert X^{c^d}\rvert$
4	14
2	6
1	2

UMN REU 2007

THEOREM: (Stanton, Cloninger, Stephens-Davidowitz)

X_n = $n \times n$ alternating sign matrices and $X_n(q) = \prod_{i=0}^{n-1} \frac{[3i+1]!_q}{[n+i]!_q}$

$\Big\downarrow c$ = 4-fold rotation

X_n

exhibits a CSP.

$n=3$ $\quad X_3(q) = \frac{[1]!_q [4]!_q [7]!_q}{[3]!_q [4]!_q [5]!_q} = \frac{[6]_q [7]_q}{[2]_q [3]_q} = 1 + q^2 + q^3 + q^4 + q^5 + q^6 + q^8$

$q = \zeta^0 = \zeta^4 = 1$ $\quad q = \zeta^2 = -1$ $\quad q = \zeta^1 = i$

$7 = |X|$ $\quad 3 = |X^{c^2}|$ $\quad 1 = |X^{c^1}|$

d	$\lvert X^{c^d} \rvert$
4	7
2	3
1	1

$$\begin{bmatrix} +1 & 0 & 0 \\ 0 & 0 & +1 \\ 0 & +1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & +1 \\ +1 & 0 & 0 \\ 0 & +1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & +1 & 0 \\ +1 & 0 & 0 \\ 0 & 0 & +1 \end{bmatrix} \quad \begin{bmatrix} 0 & +1 & 0 \\ 0 & 0 & +1 \\ +1 & 0 & 0 \end{bmatrix}$$

c

$$\begin{bmatrix} +1 & 0 & 0 \\ 0 & +1 & 0 \\ 0 & 0 & +1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & +1 \\ 0 & +1 & 0 \\ +1 & 0 & 0 \end{bmatrix}$$

c

$$\begin{bmatrix} 0 & +1 & 0 \\ +1 & -1 & +1 \\ 0 & +1 & 0 \end{bmatrix}$$

c

4. Brute force versus conceptual explanations

Every example shown above was provable by ...

METHOD 1: BRUTE FORCE!

- Compute a formula for $|X^{C^d}|$ somehow.

- Use the formula for $X_n(q)$ to evaluate

  $$\left[X_n(q) \right]_{q=\zeta^d} \quad \text{where } \zeta = e^{2\pi i/m}$$

  easier for products, e.g. $\lim_{q\to\zeta} \frac{[A]_q}{[B]_q} = \begin{cases} \frac{A}{B} & \text{if } A \equiv B \equiv 0 \bmod m \\ 1 & \text{if } A \equiv B \not\equiv 0 \bmod m \end{cases}$

- Compare the answers!

We would much prefer proving all CSP's with...

METHOD 2: LINEAR ALGEBRA PARADIGM

Find

a vector space $V = \mathbb{C}^N$ where $N = |X|$

AND

a linear map $V \xrightarrow{\gamma} V$

AND

two bases $\{v_x\}_{x \in X}$ and $\{w_{x \in X}\}$ for V

AND

a statistic $X \xrightarrow{stat} \{0,1,2,\ldots\}$

$x \longmapsto stat(x)$

having the following magical properties...

1st $V \xrightarrow{\gamma} V$ permutes the basis $\{v_x\}_{x \in X}$

by $X \xrightarrow{c} X$ permuting the subscripts:

$$\gamma(v_x) = v_{c(x)}$$

This implies $\gamma^d(v_x) = v_{c^d(x)} \quad \forall d$

and hence γ^d acts in the $\{v_x\}$ basis

by a permutation matrix P with

$$\begin{array}{c|c} & \begin{array}{cccccccc} x_1 & x_2 & x_3 & \cdots & & & & x_N \end{array} \\ \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ \\ \vdots \\ \\ \\ x_N \end{array} & \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

$$\mathrm{Trace}(P) = \text{sum of diagonal entries}$$

$$= |\{x \in X : c^d(x) = x\}|$$

$$= |X^{c^d}|$$

2nd

$$X(q) = \sum_{x \in X} q^{\mathrm{stat}(x)} \qquad \text{AND}$$

$\{w_x\}_{x \in X}$ is a γ-eigenvector basis for V

with eigenvalues $\xi^{\mathrm{stat}(x)}$: $\gamma(w_x) = \xi^{\mathrm{stat}(x)} \cdot w_x$

This implies $\gamma^d(w_x) = (\xi^d)^{\mathrm{stat}(x)}$ and

hence γ^d acts by a diagonal matrix D in the $\{w_x\}$ basis, with

$$\mathrm{Trace}(D) = \text{sum of diagonal entries}$$

$$= \sum_{x \in X} (\xi^d)^{\mathrm{stat}(x)}$$

$$= \left[X(q) \right]_{q = \xi^d}$$

$$\begin{array}{c} \\ x_1 \\ \vdots \\ x_N \end{array}
\begin{array}{c} x_1 \quad \cdots \quad x_N \\ \left[\begin{array}{ccc} (\xi^d)^{\mathrm{stat}(x_1)} & & 0 \\ & \ddots & \\ 0 & & (\xi^d)^{\mathrm{stat}(x_N)} \end{array} \right] \end{array}$$

CONCLUSION: Since D and P are both matrices for the same $V \xrightarrow{\gamma} V$ expressed in different bases for V,

one has $D = B^{-1} P B$ for some change-of-basis matrix B

$$\mathrm{Trace}(D) = \mathrm{Trace}(B^{-1} P B) = \mathrm{Tr}(B \cdot B^{-1} P) = \mathrm{Tr}(P)$$

$\mathrm{Trace}(AB) = \mathrm{Trace}(BA)$

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

We have LINEAR ALGEBRA proofs only for some of our examples:

YES!

- $\begin{bmatrix} n \\ k \end{bmatrix}_q$ and k-subsets of $\{1, 2, \ldots, n\}$
- $\dfrac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q$ and noncrossing set partitions

NO!

- $\dfrac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q$ and triangulations
- $\displaystyle\prod_{i=0}^{n-1} \frac{[3i+1]!_q}{[n+i]!_q}$ and alternating sign matrices

I hope maybe someday you will remedy this sad state of affairs.

Meanwhile,

thanks for your attention,

and THANK YOU, A & M !